Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes

Amir Abiri Jahromi, *Member, IEEE*, Anthony Kemmeugne, Deepa Kundur, *Fellow, IEEE*, and Aboutaleb Haddadi, *Member, IEEE*

***Abstract*—The dependence of modern societies on electric energy is ever increasing by the emergence of smart cities and electric vehicles. This is while unprecedented number of cyber-physical hazards are threatening the integrity and availability of the power grid on a daily basis. On one hand, physical integrity of power systems is under threat by more frequent natural disasters and intentional attacks. On the other hand, the cyber vulnerability of power grids is on the rise by the emergence of smart grid technologies. This underlines an imminent need for the modeling and examination of power grid vulnerabilities to cyber-physical attacks. This paper examines the vulnerability of the communication-assisted protection schemes like permissive overreaching transfer trip to cyberattacks using a co-simulation platform. The simulation results show that the transient angle stability of power systems can be jeopardized by cyberattacks on the communication-assisted protection schemes. To address this vulnerability, two physical solutions including the deployment of communication channel redundancy, and a more advanced communicated-assisted protection scheme, i.e., directional comparison unblocking scheme (DCUB), are considered and tested. The proposed solutions address the vulnerability of the communication-assisted protection schemes to distributed denial of service attack to some extent. Yet, the simulation results show the vulnerability of the proposed solutions to sophisticated cyberattacks like false data injection attacks. This highlights the need for the development of cyber-based solutions for communication channel monitoring.**

***Index Terms*—Cyber-physical systems, power system resilience, co-simulation platforms, communicated-assisted protection schemes, transient angle stability.**

I. Introduction

THE modern society and its vital infrastructures such as water supply, communication system, health system and public security depend on electricity. This dependence is ever increasing as the transportation system also becomes dependent on reliable power supply by the emergence of electric vehicles. Accordingly, the large area, long duration electricity outages can disrupt the functioning of critical infrastructure services and throw society into chaos and distress. This may result in billions of dollars of societal and economical costs and damages as well as the possibility of loss of lives [1], [2].

In this environment, the increased energy demands, aging legacy transmission and distribution assets, and increasing rate of natural disasters such as hurricanes, ice storms and floods are threatening the reliability and resiliency of the electricity grid. The many high-profile electric-service interruptions that have occurred due to natural disasters such as Super-storm Sandy, and hurricane Katrina are testaments to ever increasing vulnerabilities of electricity grid [3], [4]. At the same time, there is a soaring risk of intentional physical attacks on electricity infrastructures. This is while, the proliferation of smart grid related technologies is also expected to expand cyber vulnerabilities of power grids through increased connectivity and remote access points [5]–[7]. The physical attacks on substation transformers in California [8] and cyber-attacks on the Ukrainian power grid [9], [10] are prime examples of cyber-physical attacks on power grids in recent years. In addition, the possibility of a joint cyber-physical attack is a growing concern in modern societies, where an attacker may seek to identify and exploit power grid vulnerabilities to obtain self benefits or boost political interests [11]. The concerns about the vulnerability of power systems to cyber-physical threats have been reflected in several publications by governmental and non-govermental organizations [12]–[14]. For instance, the need for the protection of critical cyber assets in power systems have been recongnized by North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) through standard 002-009 [15].

To address these ever-increasing vulnerabilities, utility managers, investors and other stakeholders are developing strategies to reduce the costly large area, long duration electricity interruptions. These strategies include programs to address potential cyber vulnerabilities, fortify and expand existing cyber-physical infrastructure, improve asset management and introduce automation strategies [16]–[18]. For instance, several North American utilities have initiated investment programs to bring together academia, private technology companies, and government defense agencies and motivate research and development in cyber-physical security area [19]. Nevertheless, such tasks can be daunting considering the size and complexity of the electricity grid and limited resources available for research and

Manuscript received November 30, 2018; revised April 4, 2019; accepted June 9, 2019. Date of publication June 24, 2019; date of current version January 7, 2020. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants Program and NSERC Strategic Partnerships for Projects Programs and in part by the Fonds de Recherche du Québec – Nature et Technologies (FRQNT) postdoctoral fellowship. Paper no. TPWRS-01809-2018. *(Corresponding author: Amir Abiri-Jahromi.)*

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

A. Haddadi is with the Electrical Engineering Department, Montréal Polytechnique, Montréal, QC H3T 1J4, Canada (e-mail: aboutaleb.haddadi@polymtl.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2019.2924441

development programs. Another challenge is the diversity of power system vulnerabilities and the wide-variety of potential failures that can happen due to these vulnerabilities. The difficulty in quantifying the consequences of potential failures in terms of magnitude and duration of electricity interruptions as well as the number and type of affected customers and businesses is another restraining factor. Therefore, there is a pressing need for co-simulation platforms and testbeds with the ability to model and simulate various cyber-physical vulnerabilities of power systems. The co-simulation platforms and testbeds will facilitate the identification and protection of power system critical functions and assets whose failure may result in catastrophic consequences [20].

The cyber-physical vulnerabilities of power systems have been the subject of extensive research in recent years [21]. The cyberattacks on power system state estimation have been examined in [22]–[24], and potential solutions provided. In [25]–[27] various attacks targeting the stability of power systems have been studied. The role of protection schemes in cyber security risk analysis has been studied in [28] from power system operations point of view. The development of a cyber-resilient line current differential relay has been presented in [29].

Several co-simulation platforms have also been developed over the past decade to bridge the gap between power system and communication simulation tools and study cyber-physical aspects of power systems [20]. A co-simulation platform based on PSCAD/EMTDC electromagnetic transient simulator, the PSLF electromechanical transient simulator, and the communication Network Simulator 2 (NS2) has been presented in [30]. A co-simulation platform based on RINSE and PowerWorld has been employed in [31] to study the vulnerability of the network client to a distributed denial of service attack. In [32], an integrated platform for power and communication systems co-simulation is described and implemented. The virtual control system environment (VCSE) is proposed in [20], [33] for studying cyber threats on system infrastructures. A testbed based on Riverbed Modeler and PowerWorld has been employed in [34] for analyzing security of SCADA control systems. A testbed consisting of control center EMS, substations and external link has been presented in [35] for intrusion detection and defense against cyberattacks. A testbed for SCADA vulnerability assessment has been developed in [36]. In [37], a real-time co-simulation platform using OPAL-RT and OPNET has been presented for analyzing smart grid performance. The available co-simulation platforms reviewed in [38] and a PowerCyber testbed has been presented for evaluating the impact of cyberattacks on voltage and rotor angle stability. This is while to the best of our knowledge, no prior work has investigated the vulnerability of communication-assisted protection schemes to cyber-physical attacks. The cyber-physical attacks targeting communication-assisted protection schemes are of high importance since they target power systems in the most vulnerable state.

This paper investigates the vulnerability of the communication-assisted protection schemes like permissible overreaching transfer trip (POTT) to cyberattacks using a cosimulation platform based on OPAL-RT real-time simulator and Riverbed Modeler. Two potential physical solutions including communication channel redundancy and a more advanced protection scheme, *i.e.* directional comparison unblocking scheme (DCUB), are considered and tested to address the vulnerability of the POTT protection scheme to cyberattacks. Although the proposed physical solutions are resilient to distributed denial of service (DDoS) attack to some extent, they are vulnerable to false data injection (FDI) attack. This vulnerability highlights the need for developing cyber-based solutions for communication channel monitoring.

The main contributions of this paper are as follows.

- The notion of cyber-physical attacks on communication-assisted protection schemes is demonstrated using a co-simulation platform based on OPAL-RT real-time simulator and Riverbed Modeler.
- The potential physical solutions for addressing the cyber-physical attacks targeting POTT protection scheme is presented and their vulnerability to false data injection attacks is revealed.
- The importance of co-simulation platforms in developing cyber-based solutions for communication channels monitoring is revealed and highlighted.

The reader should note that despite the distinct features of the co-simulation platform presented in this paper, we do not claim the development of the co-simulation platform using OPAL-RT real-time simulator and Riverbed Modeler as a contribution.

The remainder of this paper is organized as follows. Section II provides the necessary background about power system transient angle stability and communication-assisted protection schemes. The cyber-phyiscal attacks targeting communication-assisted protection schemes and the potential physical solutions for addressing these attacks are further discussed. The co-simulation platform based on OPAL-RT real-time simulator and Riverbed Modeler is presented in Section III. The vulnerability of the power system stability to cyber-physical attacks targeting POTT protection schemes is uncovered in Section IV using the co-simulation platform. Moreover, the ability of the physical solutions for addressing the vulnerability of the POTT protection scheme to DDoS attacks is demonstrated. Yet, it is shown that the proposed physical solutions are vulnerable to FDI attacks. Finally, the conclusions of the paper are drawn in Section V.

II. Background

A power system fault should be cleared quickly enough such that the fault-on transient remains inside the stability boundary and power system maintains stability. Power systems with small transient stability margins may benefit from communication networks to reduce the fault clearing time and prevent transient instability. This is because the speed of information transfer using communication networks is much faster than power system instability propagation. Communication-assisted protection scheme is a particular type of the power system protection that relies on communication networks to reduce fault clearing time and prevent instability.

Power system stability margins have been declining over the past decade due to power system restructuring, and the integration of renewable energy resources. The limited investments in transmission lines caused by more strict environmental constraints have further exacerbated the existing stability problems. In this environment, protection schemes have been under constant pressure to operate more quickly and reliably to counteract transient stability dynamics and avoid wide area blackouts. For instance, failure to isolate a faulted line near generating units in a timely fashion can cause prolonged unbalance between mechanical and electrical output of generators and lead to transient angle instability. Additionally, clearing faults as quickly as possible is always favorable since it reduces potential damages to critical assets like transformers.

The need for high speed and reliable protection devices has promoted communication-assisted protection schemes as a prominent solution for addressing transient angle stability problems. The deployment of communication-assisted protection schemes can result in significant reductions in the clearing time of faults and disturbances compared to other protection schemes. Nevertheless, the complete reliance on communication-assisted protection schemes increases the possibility and consequences of cyber-physical attacks on these protection schemes.

A. Transient Angle Stability

Transient angle stability is concerned with the ability of a power system to settle down to a stable steady state operating point after it is subjected to a fault for a certain duration of time [39], [40]. The transient angle stability analysis is commonly performed by means of numerical integration of a set of differential and algebraic equations (DAEs) describing power system dynamics. An alternative approach to numerical transient angle stability analysis is direct methods. Direct methods refer to the analytical approaches used to calculate power system stability margin and the associated fault clearing time [40].

The maximum duration that a fault can remain on a power system without causing instability is called critical clearing time. If the critical clearing time is exceeded, the generators will lose synchronism. In this situation, protection system will remove the generator from the system to avoid damage to the rotor shaft. Therefore, an attacker can cause a severe disturbance or even a blackout in power systems by creating a fault on a transmission line close to a power plant and prolonging the fault clearing time beyond the critical clearing time. The same scenario happens when a cyber intruder disables the communication channel of the communication-assisted protection schemes when a fault has occurred due to natural disasters such as hurricanes or thunder storms. This is a legitimate concern in particular at locations where communication-assisted protection schemes are indispensable for reducing the fault clearing time and preventing instability.

An attacker can use both numerical and analytical methods to calculate the stability margin and critical clearing time of a power system and target protection schemes whose misoperation results in instability. This is an interesting and relevant topic which is out of the scope of this paper. This topic will be pursued as an important next step by the authors.

B. Communication-Assisted Protection Schemes

The objective of communication-assisted protection is to provide high-speed tripping from both ends of a protected line for faults along the entire line segment [41]–[43]. Multizone distance protection (commonly referred to as step-distance protection) does not provide such a high-speed tripping for line-end faults since relays on the protected line are time coordinated with relays on remote lines [42], [43]. High-speed clearing is desirable and may even be required for the following reasons: i) to reduce the duration of a fault on a power system and thereby reduce the likelihood of power system instability; ii) to enable protection coordination in step-distance applications involving two adjacent lines with significantly different lengths; and iii) for power quality purposes to reduce the duration of voltage sag caused by a fault.

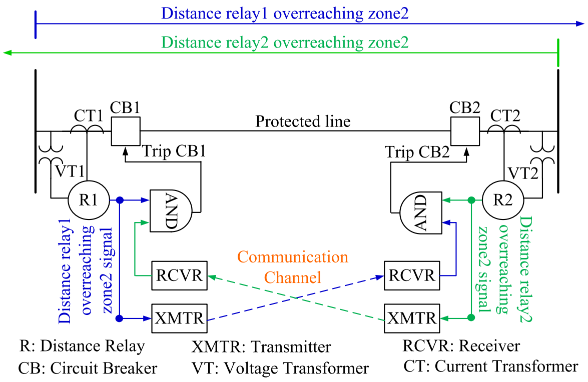

Fig. 1. The POTT protection scheme.

Communication-assisted protection achieves high-speed fault clearing through communication between line terminals. Each line terminal communicates its status as a bit of data to the remote end(s) over a communication channel. In some schemes, this bit represents a signal which tells the other side that it has permission to trip (permissive). In other schemes, the bit prevents the other end from tripping (block). There are many variations of communication-assisted protection; the most prevalent schemes include: 1) permissive overreaching transfer trip (POTT), 2) permissive underreaching transfer trip (PUTT), 3) direct transfer trip (DTT), direct underreaching transfer trip (DUTT), directional comparison blocking (DCB), and directional comparison unblocking (DCUB) [41]–[43]. This paper focuses on the POTT scheme. Yet, the proposed co-simulation platform can be extended to study other communication-assisted protection schemes without the loss of generality. Moreover, the cyber-physical vulnerabilities demonstrated in this paper for POTT scheme exist in other communication assisted protection schemes as well.

Fig. 1 illustrates the basic logic of the POTT protection scheme based on distance relay zone 2 elements. The POTT protection scheme trips the circuit breaker at each end of a protected line immediately after receiving the overreaching zone 2 signals from both terminals of a line. In other words, the POTT logic allows the local overreaching zone 2 signal to trip the circuit breaker of the protected line instantaneously upon the receipt of the permissive trip signal, *i.e.*, overreaching zone 2 signal, from the remote end of the line. The permissive trip signal from the remote end of the protected line is communicated through a communication channel. By contrast, under steps-distance protection the overreaching zone 2 has to wait typically 15 to 30 cycles after picking up a fault before tripping the breaker

[42], [43]; this time delay may be large enough to cause system instability.

C. Cyber-Physical Attacks Targeting Communication-Assisted Protection Schemes

The power grid is a cyber-physical system consisting of information and communication technologies (cyber assets) and power delivery components such as generators, transmission lines and loads (physical assets). Here, the physical-to-cyber bridge is at sensors that convert physical signals to data (information) and the cyber-to-physical bridge is at actuation whereby information is used to make changes to the power system operations; common forms of actuation include control and protection.

Cyberattacks are unwanted actions applied to target cyber assets that exploit a vulnerability; their impacts are measured in terms of their effects on information. In contrast, cyber-physical attacks typically aim to exploit vulnerabilities in cyber assets (in the form of a cyberattack) to cause disruption in target physical assets such as generators and transmission lines. They also can involve coordinating cyberattacks with physical disruptions such as faults to maximize negative impacts on power systems. Cyber-physical attacks are often measured in terms of their physical impacts; hence co-simulation represents an ideal framework in which to model the application of cyberattacks and describe its physical impacts.

Cyberattacks target information confidentiality, integrity or availability (C-I-A). The C-I-A paradigm is a rich framework employed for general cybersecurity studies whereby availability and integrity represent the most important cyber security services for power grid operations because information must be both accessible in a timely manner and accurate for critical use in operational settings. Cyberattacks on availability and integrity are known as distributed denial of service (DDoS) and false data injection (FDI), respectively.

Communication-assisted protection schemes represent cyber-physical assets in which communications facilitates more responsive breaker action. Hence, attacking the associated communication channel when breaker action is very much needed can cause significant power grid disruption. Cyber-physical attacks of communication-assisted protection may be applied, say, after a physical fault (caused naturally or otherwise) has occurred. The cyber-physical attack could, for example, apply either a DDoS or FDI to prolong the fault clearing time at critical transmission lines by either disabling the communication channel between distance relays through say packet flooding (for DDoS) or by providing incorrect permissive trip signals (FDI). Possible physical impacts include instability and blackout.

Execution of DDoS or FDI requires that a device with access to the relay communication channels be corrupt. This could occur through malware that has propagated into a component of the transceiver or by physically introducing a new communication device that can access the channel. For DDoS the corrupt entity could flood the network with packets making permissive trip communications impossible. For FDI, the corrupt entity can insert fabricated permissive trip signals that can confuse normal operation of communication-assisted protection scheme.

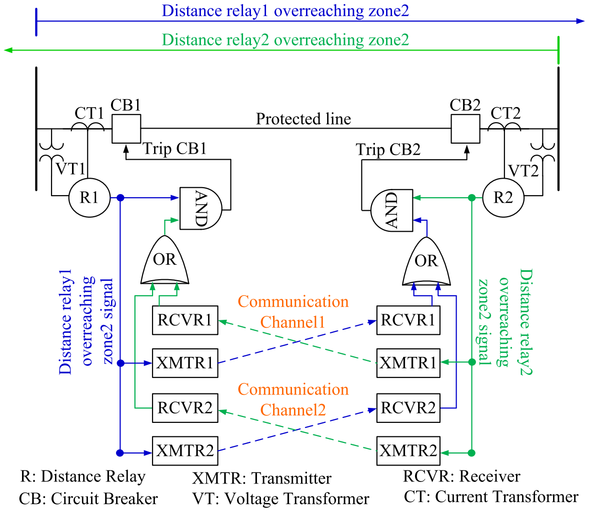

Fig. 2. The POTT protection scheme with communication channel redundancy.

D. Physical Solutions to Cyber Attacks Targeting Communication-Assisted Protection Schemes

Solutions to address cyber-physical attacks can take both cyber and physical forms. Cyber solutions, as typically defined, involve employing existing cyber assets for mitigation of the impacts of cyberattacks. Cyber solutions can include the modification of communication protocols, transceiver operation or the application of cryptographic primitives on data. Whereas physical solutions entail actions on the part of physical assets for mitigation. Physical solutions can also include the addition of redundant physical infrastructure (including communication channels).

Cyber solutions are most appropriately applied when there are sophisticated information and communication systems in place to enable complex information processing or communication network reconfiguration. For the application focus of this paper, communication-assisted protection, such cyber solutions are not feasible. Hence, we focus on physical solutions.

Two physical solutions are considered in this paper for addressing the cyber-attacks targeting communication-assisted protection schemes like POTT. The first physical solution is based on communication channel redundancy. The POTT protection scheme with communication channel redundancy is illustrated in Fig 2. Channel redundancy is an effective way to provide resilience to system operation and its advantages in communication-assisted protection schemes is studied in this paper. Communication redundancy increases an attackers level of required effort often beyond available resources.

The second physical solution is based on considering a more complex protection scheme, *i.e.*, directional comparison unblocking (DCUB) scheme. Accounting for possible loss of a communication channel is imperative for overall POTT operation. The DCUB protection scheme is similar to the POTT protection scheme in that they both share information about overreaching zone 2 pickup signal through a communication channel. The difference is that DCUB scheme permits fast tripping when the communication channel is lost. In DCUB scheme

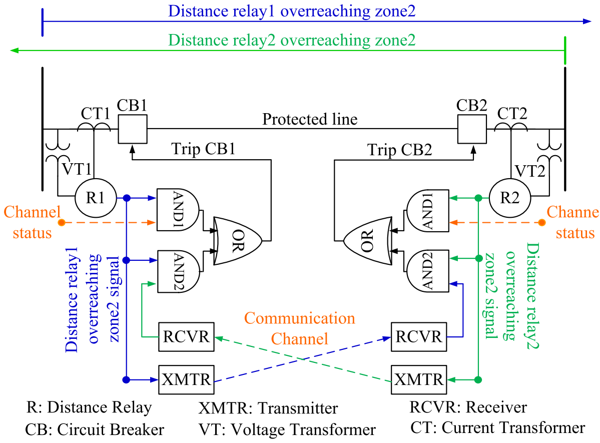

Fig. 3. The DCUB protection scheme.

distance relays initiate a timer in case the communication channel is lost and permit the distance relays to trip the breaker faster provided their overreaching zone 2 elements still see the fault. After certain time elapses, distance relay tripping with overreaching zone 2 pickup signal is blocked to prepare for the next fault incident.

Fig. 3 illustrates the basic logic of the DCUB protection scheme. As illustrated in Fig. 3, the DCUB protection scheme consists of two AND gates and one OR gate. The AND1 gate operates when the communication channel is lost and the local overreaching zone 2 signal is present. It is noteworthy that the communication channel status is 0 when the channel is operational and becomes 1 when the channel is lost. The AND2 gate implements a logic similar to the POTT protection scheme where the permissive trip signal *i.e.* the overreaching zone 2 signal from the remote end of the protected line is communicated through a communication channel. Thus, the DCUB protection scheme allows fast circuit breaker tripping in two cases; 1) The communication channel has been lost and the local overreaching zone 2 pickup signal is present *i.e.* the AND1 gate in Fig. 3, 2) The communication channel is operational and the POTT logic of the DCUB protection operates *i.e.* the AND2 gate in Fig. 3.

III. Co-Simulation Platform

The main objective of the real-time co-simulation platform presented here is to provide the ability to simulate both cyber and physical parts of a communication-assisted protection scheme like POTT for a benchmark test system. The co-simulation platform is of immense importance since cyber-physical attacks on communication-assisted protection schemes involve both electrical and communication parts of an electric system. The OPAL-RT real-time simulator and Riverbed Modeler are integrated together to create such a co-simulation platform. Riverbed Modeler is a flexible communication networking simulator that models a variety of protocols, technologies and network types and provides a sophisticated development environment to develop proprietary protocols, evaluated enhancements to standards-based protocols and technologies, and demonstrate design in a realistic environment.

The OPAL-RT real-time simulator provides the interface with a communication simulator such as Riverbed Modeler through its input/output (I/O) modules and Ethernet ports. Moreover, OPAL-RT real-time simulator supports the IEC 61850 protocols such as generic object oriented substation event (GOOSE) and sampled value (SV) [44]. The IEC 61850 GOOSE protocol is used for fast event driven messaging while IEC 61850 SV protocol is used for the transmission of analog values such as current and voltage. In this paper, the IEC 61850 GOOSE protocol is employed to communicate information between OPAL-RT real-time simulator and Riverbed Modeler. The IEC 61850 GOOSE packets generated by the OPAL-RT real-time simulator is embedded in Ethernet frames with source and destination address fields containing the medium access control (MAC) addresses of the communicating nodes. The network interface cards enable the GOOSE traffic exchange between OPAL-RT real-time simulator and Riverbed Modeler. The publisher and subscriber traffic between the two simulators is separated using two Ethernet switches and cables as illustrated in Fig. 4. The system-in-the-loop (SITL) feature of the Riverbed Modeler permits the real-time simulation. The SITL publisher and subscriber ports provide the interface between Riverbed Modeler and hardware/software applications such as OPAL-RT real-time simulator.

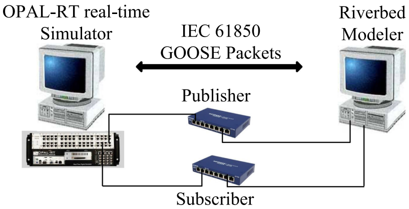

Fig. 4. Schematic representation of the co-simulation platform.

A benchmark test system involving distance relays and POTT protection scheme is implemented in the OPAL-RT real-time simulator. The distance relays issue permissive trip signals, *i.e.*, overreaching zone 2 pickup signals, whenever a fault occurs in the zone 2 of the distance relays. The OPAL-RT real-time simulator generates IEC 61850 GOOSE packets containing the permissive trip signals through its I/O module and sends them toward Riverbed Modeler using the interface network cards. The SITL publisher ports in the Riverbed Modeler receive the real GOOSE packets from the network interface card of the Riverbed Modeler machine. SITL publisher ports then convert the real GOOSE packets to simulated GOOSE packets and send them to the communication network model implemented in the Riverbed Modeler using SITL links. The communication network model implemented in Riverbed Modeler consists of two router switches and a SITL link which connects the router switches. Each of the router switches represents the substation gateway at one end of the protected line and the SITL link between the router switches represents the communication channel. The IEC 61850 GOOSE packets enter the SITL subscriber ports through a SITL link after passing through the network model. The SITL subscriber ports convert the simulated GOOSE packets to real GOOSE packets and deliver them to the network interface card of the Riverbed Modeler machine. The OPAL-RT real-time simulator receives the IEC 61850 GOOSE packets from the network interface cards and delivers them to the POTT

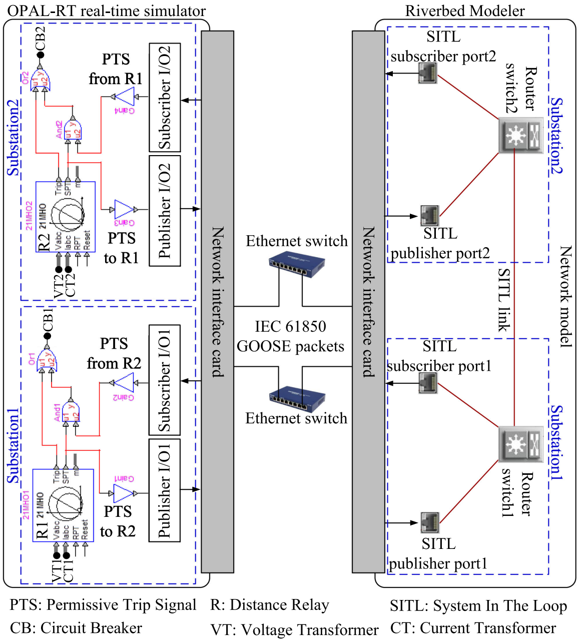

Fig. 5. Schematic representation of the implementation of the benchmark test system in the cosimulator.

protection scheme. The implementation of the benchmark test system in the cosimulator is schematically shown in Fig. 5.

In Fig. 5, the SITL publisher port1 in Riverbed Modeler receives the IEC 61850 GOOSE packets generated by the publisher I/O1 in OPAL-RT real-time simulator and delivers it to the SITL subscriber port2 through the router switches and the SITL link. The SITL subscriber port2 in Riverbed Modeler then sends the IEC 61850 GOOSE packets toward the subscriber I/O2 in OPAL-RT real-time simulator. Similarly, the SITL publisher port2 in Riverbed Modeler receives the IEC 61850 GOOSE packets generated by the publisher I/O2 in OPAL-RT real-time simulator and delivers it to the SITL subscriber port1 through the router switches and SITL link. The SITL subscriber port1 in Riverbed Modeler then sends the IEC 61850 GOOSE packets toward the subscriber I/O1 in OPAL-RT real-time simulator.

It is noteworthy that the physical attack *i.e.*, fault caused by intentional or unintentional factors on the electric grid is simulated in the OPAL-RT real-time simulator and the cyberattacks *i.e.*, DDoS and FDI attacks are simulated in the Riverbed Modeler.

IV. Simulation Results

Fig. 6 illustrates the IEEE power system relaying committee (PSRC) D6 benchmark test system [45], [46]. The benchmark test system consists of a 500 kV transmission system connecting four identical 400 MVA synchronous generators to the rest of the grid. The rest of the grid is modeled by a 230 kV ideal voltage source. All the circuit breakers in the benchmark test system except the circuit breaker CB10 are initially closed as illustrated in Fig. 6. The power flows from G1-G4 to S1 through the transmission lines L1-L4.

Five case studies are considered here. The objective of the case studies I and II is to demonstrate the need for the communication-assisted protection scheme to maintain the transient rotor angle stability of the generators G1-G4 when a fault occurs. The transmission lines L1-L4 of the benchmark test system are protected by step-distance protection in case study I and by POTT protection in case study II. Case study III demonstrates the vulnerability of the POTT protection scheme to DDoS attack. Case study IV investigates the DDoS attack on the POTT protection with communication channel redundancy. Case study V examines both DDoS and FDI attacks on DCUB protection and underlines the need for the development of cyber-based solutions for communication channel monitoring.

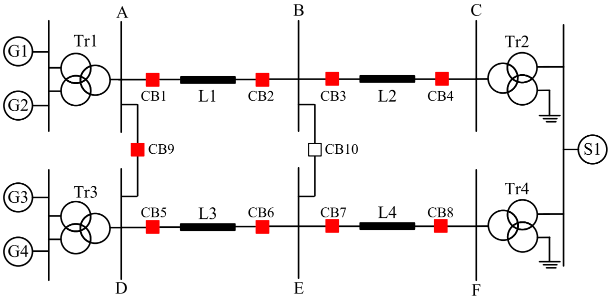

Fig. 6. The IEEE PSRC D6 benchmark test system.

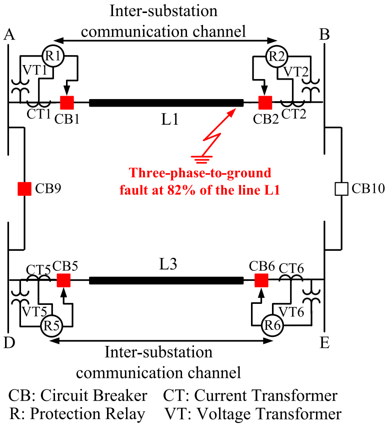

Fig. 7. Part of the IEEE PSRC D6 benchmark test system illustrating a permanent three-phase-to-ground fault on line L1.

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. 7. The location of the fault is at 82% of the transmission line from bus A which is within zone 2 of the protection relay 1 (R1) and zone 1 of the protection relay 2 (R2). The reach of zone 1 and 2 of the distance relays are respectively set at 80% and 120% of the transmission lines. The zones 1 and 2 of the distance relays are forward zones. Zone 1 is instantaneous, while backup zone 2 has a time delay of 30 cycles *i.e.* 0.5 s.

A. Case Study I: Simulating the IEEE PSRC D6 Test System Under Step-Distance Protection

In this case study, transmission lines L1-L4 are protected by step-distance relays. As illustrated in Fig. 8(b), the step-distance relay 2 (R2) sees the fault in zone 1 and 2 (21G_Z1 PKP, and 21G_Z2 PKP) and instantaneously issues 21G_Z1 trip signal to the circuit breaker CB2. The opening of the circuit breaker CB2 disconnects the transmission line L1 from bus B. However,

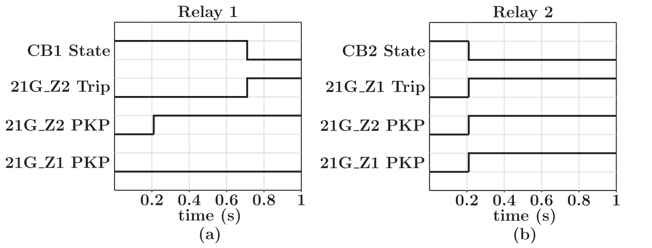

Fig. 8. Step-distance relay signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

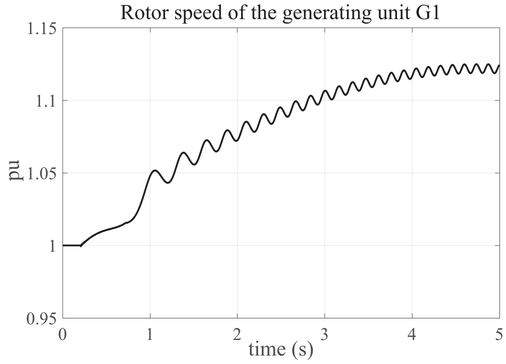

Fig. 9. The rotor speed of the generating unit G1 when the permanent three-phase-to-ground fault at 82% of the line L1 is cleared after 30 cycles.

the fault does not get isolated instantaneously because the step-distance relay 1 (R1) sees the fault in zone 2 (21G_Z2 PKP) which has the time delay of 30 cycles before issuing the 21G_Z2 Trip to the circuit breaker CB1 as illustrated in Fig. 8(a). Within this time delay, the transmission line L1 remains connected to the bus A, and the generators G1-G4 continue to feed the fault. As illustrated in Fig. 9 for the generating unit G1, the rotor speed of the generating units continues to increase and the generators eventually lose synchronism. This is because the fault clearing time is longer than the critical clearing time of the generators. This instability problem can be resolved by clearing the fault from both ends of the transmission line L1 more quickly through a communication-assisted protection such as POTT. In practice, the over speed protection of the generator trips the unit when the rotor speed exceeds a certain limit typically 1.1 per unit. Nevertheless, this protection has not been modeled in this paper.

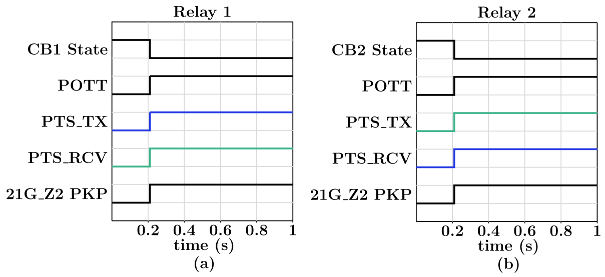

Fig. 10. POTT protection signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2.

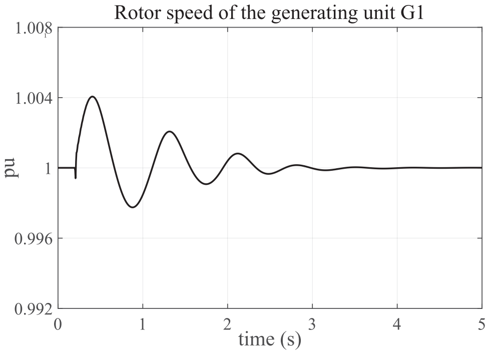

Fig. 11. The rotor speed of the generating unit G1 when the permanent three-phase-to-ground fault at 82% of the line L1 is cleared instantaneously.

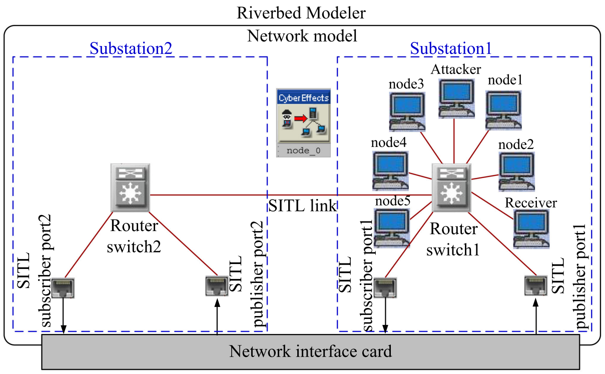

Fig. 12. The DDoS attack implemented in Riverbed Modeler on the communication channel between distance relays.

B. Case Study II: Simulating the IEEE PSRC D6 Test System Under POTT Protection

In this case study, transmission lines L1-L4 are protected by POTT protection scheme. The successful operation of the POTT protection scheme requires the receipt of the permissive trip signal (PTS), *i.e.* overreaching zone 2 signal, from the remote relay and the presence of the overreaching zone 2 signal (21G_Z2 PKP) at the local relay. As illustrated in Fig. 10(a), relay 1 sees the fault in zone 2 and sends the permissive trip signal (PTS_TX in blue) to relay 2. Similarly, relay 2 sees the fault in zone 2 and sends the permissive trip signal (PTS_TX in green) to relay 1 as illustrated in Fig. 10(b). The POTT protection scheme receives the permissive trip signals (PTS_RCV) from the remote relay and instantaneously issues permissive overreaching transfer trip signals (POTT) to the circuit breakers CB1 and CB2. The opening of the circuit breakers CB1 and CB2 disconnects the transmission line L1 from the buses A and B and instantaneously clears the faults. As illustrated in Fig. 11 for the generating unit G1, the generators' rotor speed remains stable in this case.

C. Case Study III: Simulating DDoS Attack on POTT Protection

In this case study, transmission lines L1-L4 are protected by POTT protection scheme. The DDoS attack is implemented in Riverbed Modeler as illustrated in Fig. 12 to disable the communication channel between distance relays R1 and R2. The CyberEffects tool in Riverbed Modeler is used to implement the DDoS attack. The DDoS attack execution involves two phases; 1) infection, and 2) flooding. In order to implement the infection and flooding phases, two workstation nodes *i.e.* attacker

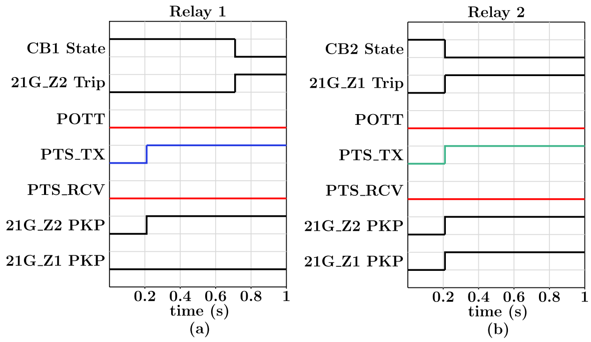

Fig. 13. POTT protection signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2 considering the DDoS attack.

and receiver are required as illustrated in Fig. 12. The attacker workstation is required to infect the workstation nodes in the network *i.e.* nodes 1–5 and execute the flooding phase of the DDoS attack. The IP address of the receiver node is required by the CyberEffects tool to define the destination node of the packets generated by the DDoS attack. The traffic generated by the DDoS attack towards the receiver workstation node overflows the router switch1 in Fig. 12 and causes the denial of service.

As illustrated in Fig. 13(a), relay 1 sees the fault in zone 2 (21G_Z2 PKP) and sends the permissive trip signal (PTS_TX in blue) 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 in green) to the relay 1 as illustrated in Fig. 13(b). Nevertheless, the permissive trip signals get blocked by the DDoS attack and do not reach the respective remote relay. The relay 2 (R2) instantaneously issues 21G_Z1 trip signal to the circuit breaker CB2 as illustrated in Fig. 13(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. 13(a). This is because relay 1 does not receive the permissive trip signal (PTS_RCV) from the relay 2. Thus, the generators lose synchronism in this case similar to Case Study I.

D. Case Study IV: Simulating DDoS Attack on POTT Protection With Communication Channel Redundancy

In this case study, transmission lines L1-L4 are protected by POTT protection scheme with communication channel redundancy (see the logic of the POTT protection with communication channel redundancy in Fig. 2). Fig. 14 illustrates the implementation of the communication channel redundancy in the Riverbed Modeler. As shown in Fig. 14, two sets of SITL subscriber and publisher ports are implemented for each substation. The SITL publisher/subscriber ports in Riverbed Modeler communicate with the publisher/subscriber ports of their respective relays in OPAL-RT real-time simulator shown in Fig. 15.

Two scenarios are considered here. In the first scenario, the DDoS attack is implemented to disable the communication channel1 between the relays R1 and R2. As illustrated in Fig. 16(a) and (b), both relays see the fault in zone 2 (21G_Z2 PKP) and send the permissive trip signals (PTS_TX1 and PTS_TX2) through the communication channels to the remote relay. The

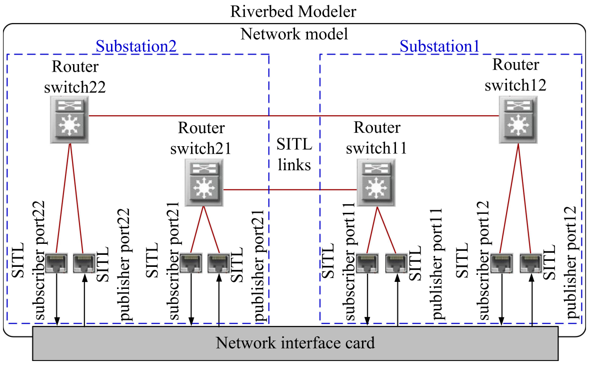

Fig. 14. The implementation of the communication channel redundancy between the relays in Riverbed Modeler.

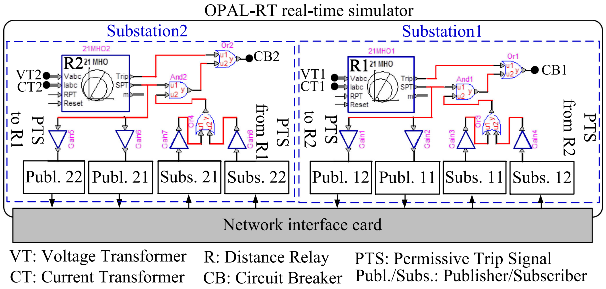

Fig. 15. Schematic representation of the implementation of the POTT protection with communication redundancy in OPAL-RT real-time simulator.

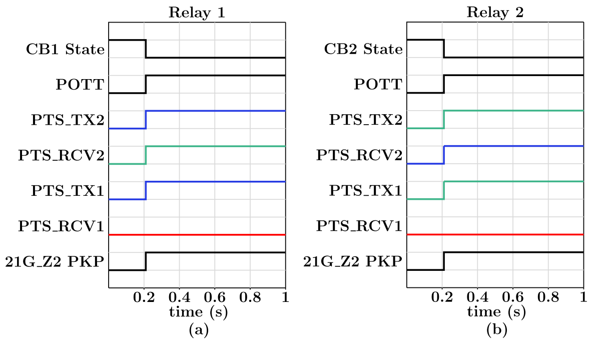

Fig. 16. POTT protection with communication channel redundancy signals and circuit breakers state considering the DDoS attack on the communication channel1 (a) Relay 1 and CB1, (b) Relay 2 and CB2.

POTT protection does not receive the permissive trip signals (PTS_RCV1) through the communication channel1. However, the POTT protection receives the permissive trip signals (PTS_RCV2) through the communication channel2 and instantaneously issues permissive overreaching transfer trip signals (POTT) to the circuit breakers CB1 and CB2. The opening of the circuit breakers CB1 and CB2 isolates the transmission line L1 and instantaneously clears the fault. Therefore, the generators remain stable in this case similar to Case Study II.

In the second scenario, both communication channels are disabled by the DDoS attack. As illustrated in Fig. 17(a) and (b) both relays see the fault in zone 2 (21G_Z2 PKP) and send the permissive trip signals (PTS_TX1 and PTS_TX2) to the remote relay. However, the POTT protection does not receive the permissive trip signals (PTS_RCV1 and PTS_RCV2) due to the DDoS attack on both communication channels and fails to

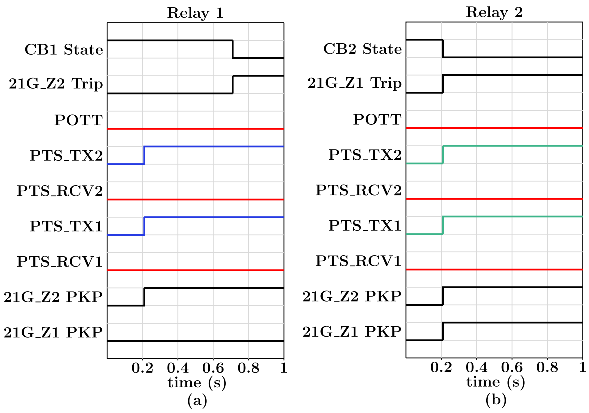

Fig. 17. POTT protection with communication channel redundancy signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2 considering the DDoS attack on both communication channels.

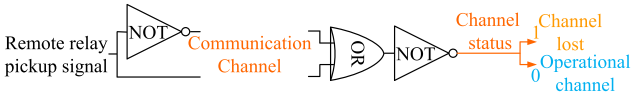

Fig. 18. The logic employed to identify communication channel loss.

open the circuit breaker CB1. The relay 2 (R2) instantaneously trips the circuit breaker CB2 because it sees the fault in zone 1 (21G_Z1 PKP) as illustrated in Fig. 17(b). This is while the relay 1 waits for 30 cycles before tripping the circuit breaker CB1 as illustrated in Fig. 17(a). This is because relay 1 sees the fault in zone 2 (21G_Z2 PKP) and does not receive the permissive trip signal from relay 2 (PTS_TX1 and PTS_TX2). Thus, the generators lose synchronism in this case similar to Case Study I.

It is noteworthy that cyberattackers require more resources to attack two communication channels in the case of communication channel redundancy compared to the case with a single communication channel. Thus, communication channel redundancy reduces the risk of successful cyberattacks against the communication-assisted protection schemes because the required resources in this case are often beyond available resources of cyberattackers.

E. Case Study V: Simulating DDoS and FDI Attacks on DCUB Protection

This case study investigates the performance of DCUB protection under cyberattack. In order to identify communication channel status the logic shown in Fig. 18 is implemented in the co-simulation platform. As illustrated in Fig. 18, the original signal and its inverted value are sent over the communication channel. When the communication channel is operational, the output of the OR gate is always one and the output of the NOT gate on the right hand side of Fig. 18 is zero. This is because one of the signals entering the OR gate is always one. In contrast, when the communication channel is lost, the output of the OR gate becomes zero and the output of the NOT gate becomes one. This is because both signals entering the OR gate become zero when the communication channel is lost. Thus, it is possible to identify the status of the communication channel using the logic shown in Fig. 18.

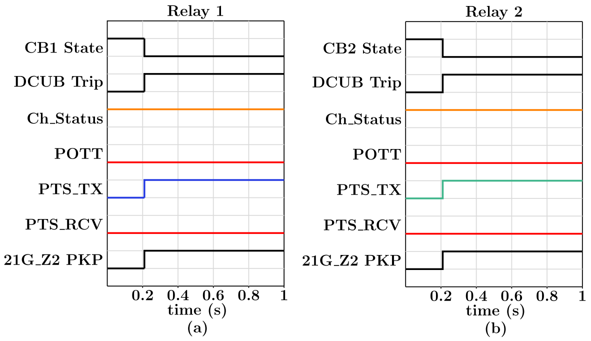

Fig. 19. DCUB protection signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2 considering the DDoS attack on the communication channel.

Two scenarios are considered here. In the first scenario, the DDoS attack is implemented in Riverbed Modeler as illustrated in Fig. 12 to disable the communication channel between the relays R1 and R2. The study starts from a condition where the DDoS attack on the communication channel has been in progress. As illustrated in Fig. 19(a) and (b), both relays see the fault in zone 2 (21G_Z2 PKP) and send the permissive trip signals (PTS_TX) through the communication channel to the remote relay. As illustrated in Fig. 19, the DCUB protection does not receive the permissive trip signals (PTS_RCV) because of the DDoS attack. Nevertheless, the DCUB protection identifies the communication channel loss (Ch_Status). The DCUB protection issues the DCUB trip signals (DCUB Trip) to the circuit breakers CB1 and CB2 because the local overreaching zone 2 signal (21G_Z2 PKP) is present and communication channel is lost (see DCUB protection logic in Fig. 3). The opening of the circuit breakers CB1 and CB2 isolates the transmission line L1 and clears the fault. Therefore, the generators remain stable in this case similar to case study II.

In the second scenario, the FDI attack is implemented on the communication channel between the relays 1 and 2. In order to implement the FDI attack in the co-simulation environment, the Wireshark tool is employed. Wireshark tool is an open source software which is able to monitor, and save communication packets. First, the OPAL-RT real-time simulator is employed to generate GOOSE packets containing false GOOSE packets indicating that the overreaching zone 2 signal is not present. The Wireshark tool is then employed to save the false GOOSE packets. Afterwards, the benchmark test system is simulated and the false GOOSE packets are injected into the communication channel between the relays 1 and 2 using the Wireshark tool as illustrated in Fig. 20.

As illustrated in Fig. 21(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 with false GOOSE packets indicating no permissive trip signals (PTS_RCV). Moreover, the communication channel status (Ch_Status) is operational in this case. Therefore, DCUB protection does not issue DCUB trip signals (DCUB Trip). 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. 21(b). This is while the distance relay 1

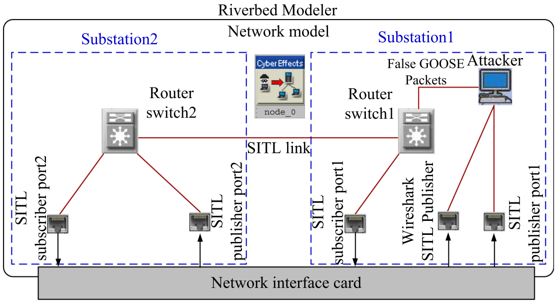

Fig. 20. The FDI attack implemented using Wireshark tool and Riverbed Modeler.

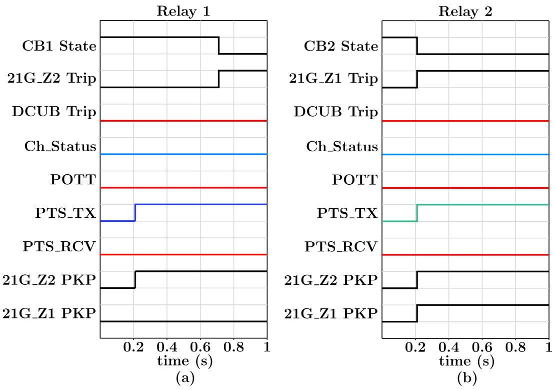

Fig. 21. DCUB protection signals and circuit breakers state of (a) Relay 1 and CB1 and (b) Relay 2 and CB2 considering the FDI attack on the communication channel.

(R1) waits for 30 cycles before issuing the 21G_Z2 trip signal to the circuit breaker CB1 as illustrated in Fig. 21(a). Thus, the generators lose synchronism in this case similar to Case Study I. This case study highlights the vulnerability of the DCUB protection scheme to FDI attacks and the need for the development of cyber-based solutions for communication channel monitoring in the communication-assisted protection schemes.

V. Conclusion

This paper demonstrated the vulnerability of communication-assisted protection schemes like permissible overreaching transfer trip to cyber-physical attacks. Moreover, it is demonstrated that this vulnerability can be exploited to destabilize the power system and potentially create cascading failures. The simulation studies performed using a co-simulation platform based on OPAL-RT real-time simulator and Riverbed Modeler. A case study is employed to demonstrate that a cyber intruder can disable the communication channel between two distance relays at critical times using the distributed denial of service attack and destabilize the power system. Two physical solutions including communication channel redundancy and a more complicated protection scheme *i.e.*, directional comparison unblocking protection scheme are employed for addressing the vulnerability of the POTT protection scheme to DDoS attacks. Although these physical solutions can be employed to address the DDoS attacks to some extent, they are still vulnerable to false data injection attacks. This highlights the importance of co-simulation platforms in developing cyber-based solutions for communication channels monitoring. This topic will be pursued in our future research.

References

[1] *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC, USA: National Academies Press, 2017.

[2] "Economic benefits of increasing electric grid resilience to weather outages," Executive Office of the President, Washington, DC, USA, Tech. Rep., USA, 2013.

[3] "Comparing the impacts of the 2005 and 2008 hurricanes on U.S. energy infrastructure," U.S. Dept. Energy, 2009. [Online] Available: https://www.oe.netl.doe.gov/docs/HurricaneComp0508r2.pdf. Accessed on: Jun. 2019.

[4] "Macroeconomic and budgetary effects of hurricanes Katrina and Rita," Testimony Before the Committee on Budget, U.S. House of Representatives, Congressional Budget Office, Washington, DC, USA, 2005.

[5] J. Hull, H. Khurana, T. Markham, K. Staggs, "Staying in control: Cyber security and the modern electric grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 41–48, Jan./Feb. 2012.

[6] T. Flick and J. Morehouse, *Security the Smart Grid*. Rockland, MA, USA: Syngress, 2011.

[7] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure*. Rockland, MA, USA: Syngress, 2013.

[8] R. Smith, "Assault on California power station raises alarm on potential for terrorism," *Wall Street J.*, 2014.

[9] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[10] *Cyber-Attack Against Ukrainian Critical Infrastructure*, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Feb. 2016. [Online]. Available: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01. Accessed on: Jun. 2019.

[11] D. Kushner, "The real story of stuxnet," *IEEE Spectr.*, vol. 50, no. 3, pp. 48–53, Feb. 2013.

[12] "Vulnerability analysis of energy delivery control systems," Idaho Nat. Lab., Idaho Falls, ID, USA, Tech. Rep. INL/EXT-10-18381, 2011.

[13] M. Govindarasu, A. Hann, and P. Sauer, "Cyber-physical systems security for smart grid," Future Grid Initiative, Power Syst. Eng. Res. Center, Tempe, AZ, USA, White Paper, Feb. 2012.

[14] "Guidelines for smart grid cyber security," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NISTIR 7628, Revision 1, 2011.

[15] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards. 2017. [Online]. Available: http://www.nerc.com

[16] "Post sandy enhancement plan," Consolidated Edison Company, New York, NY, USA, Jun. 2013.

[17] "Hardening and resiliency: U.S. energy industry response to recent hurricane seasons," U.S. Dept. Energy, Washington, DC, USA, Tech. Rep., Aug. 2010.

[18] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1604–1613, Mar. 2016.

[19] "Cyber threat and vulnerability analysis of the U.S. electric sector," Idaho Nat. Lab., Idaho Falls, ID, USA, Tech. Rep. INL/EXT-16-40692, Jun. 2017.

[20] J. McDonald, N. Conrad, C. Service, and H. Cassidy, "Cyber effects analysis using VCSE: Promoting control system reliability," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2008-5954, 2008.

[21] S. K. Khaitan, J. D. McCalley, and C. C. Liu, *Cyberphysical Systems Appraoch to Smart Electric Power Grid*. Berlin, Germany: Springer-Verlag, 2015.

[22] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13–24, 2011.

[23] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[24] W. L. Chin, C. H. Lee, and T. Jiang, "Blind false data attacks against AC state estimation based on geometric approach in smart grid communications," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6298–6306, Nov. 2018.

[25] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards modeling the impact of cyber attacks on a smart grid," *Int. J. Secur. Netw.*, vol. 6, no. 1, pp. 2–13, 2011

[26] A. Farraj, E. Hammad, and D. Kundur, "A cyber-physical control framework for transient stability in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1205–1215 Mar. 2018.

[27] E. Hammad, A. M. Khalil, A. Farraj, D. Kundur, and R. Iravani, "A class of switching exploits based on inter-area oscillations," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4659–4668, Sep. 2018.

[28] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580 Mar. 2017.

[29] 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.

[30] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *IEEE Trans. Power Syst.*, vol. 21, no. 2, pp. 548–558, May 2006.

[31] C. M. Davis, J. E. Tate, H. Okhravl, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cybersecurity test bed development," in *Proc. 38th North Am. Power Symp.*, Sep. 2006, pp. 483–488.

[32] J. Nutaro, P. T. Kuruganti, L. Miller, S. Mullen, and M. Shankar, "Integrated hybrid-simulation of electric power and communications systems," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, 2007, pp. 1–8.

[33] M. J. McDonald *et al.*, "Modeling and simulation for cyber-physical system security research, development and applications," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2010-0568, Feb. 2010.

[34] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol.*, Jan. 2011, pp. 1–7.

[35] J. Hong *et al.*, "An intrusion and defense testbed in a cyberpower system environment," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, Jul. 2011, pp. 1–5.

[36] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASimA framework for building SCADA simulations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec. 2011.

[37] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, 2015, pp. 1–5.

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

[39] P. Kundur, *Power System Stability and Control* (EPRI Power System Engineering Series). New York, NY, USA: McGraw-Hill, 1994.

[40] H. D. Chiang, *Direct Methods for Stability Analysis of Electric Power Systems: Theoretical Foundation, BCU Methodologies, and Applications*. Hoboken, NJ, USA: Wiley, 2011.

[41] *IEEE Guide for Protective Relay Applications to Transmission Lines*, IEEE Standard C37.113-2015, Dec. 2015.

[42] M. Kezunovic, J. Ren, and S. Lotfifard, *Design, Modeling and Evaluation of Protective Relays for Power Systems*. Berlin, Germany: Springer International Publishing, 2006.

[43] S. V. Achanta, R. Bradetich, and K. Fodero, "Speed and security considerations for protection channels," in *Proc. 42nd Annu. Western Protective Relay Conf.*, College Station, TX, Oct. 2015, pp. 1–9.

[44] *Communication Networks and Systems in Substations—Part 8-1: Specific Communication Service Mapping (SCSM) Mappings to MMS*, IEC Standard 61850-8-1-2011, Feb. 2012.

[45] IEEE Power System Relaying Committee WG D6, "Power swing and out-of-step considerations on transmission lines," Jul. 2005.

[46] H. Gras *et al.*, "A new hierarchical approach for modeling protection systems in EMT-type software," in *Proc. Int. Conf. Power Syst. Transients*, Jun. 2017, Paper 17IPST108.

Amir Abiri Jahromi (S'10–M'16) received the Ph.D. degree in electrical and computer engineering from McGill University, Montréal, QC, Canada, in 2016. He was a Postdoctoral Fellow with the University of Denver in 2017. He is currently a Postdoctoral Fellow with the University of Toronto, Toronto, ON, Canada.

He was a Research and Development Engineer with ITA-UIS Company, Dubai, United Arab Emirates, from 2008 to 2010. His research interests include power system modeling, cyberphysical security, reliability, economics, and optimization of power systems.

Anthony Kemmeugne received the Engineering degree in telecommunication and electronics from Telecom Saint-Etienne, Saint-Étienne, France, in 2018, and the M.Sc. degree in electrical and computer engineering from the Université du Quebec à Chicoutimi, Chicoutimi, QC, Canada, in 2018. He is currently working toward the Ph.D. degree with 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 Québec, Montreal, QC, Canada. His research interests include communication systems, and advanced simulation method including telecommunications, power systems cosimulation, and smart grid cybersecurity.

Deepa Kundur (S'91–M'99–SM'03–F'15) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively.

From January 2003 to December 2012, she was a Faculty Member with the Department of Electrical and Computer Engineering, Texas A&M University. From September 1999 to December 2002, she was a Faculty Member with the Department of Electrical and Computer Engineering, University of Toronto, where she is currently a Professor and the Chair of The Edward S. Rogers Sr. Department of Electrical and Computer Engineering. She is an author of more than 200 journal and conference papers. Her research interests include interface of cybersecurity, signal processing, and complex dynamical networks. She has participated on several Editorial Boards and currently serves on the Advisory Board of IEEE Spectrum. She has served as the General Chair for the 2018 Global Conference on Signal and Information Processing (GlobalSIP) Symposium on Information Processing, Learning, and Optimization for Smart Energy Infrastructures, and the Technical Program Committee Co-Chair for the IEEE International Conference on Smart Grid Communications in 2018. She has also served as the Symposium Co-Chair for the Communications for the Smart Grid Track of the International Conference on Communications in 2017, the General Chair for the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems at ACM e-Energy in 2016, the General Chair for the Workshop on Cyber-Physical Smart Grid Security and Resilience at Globecom in 2016, the General Chair for the Symposium on Signal and Information Processing for Smart Grid Infrastructures at GlobalSIP in 2016, the General Chair for the 2015 International Conference on Smart Grids for Smart Cities, the General Chair for the 2015 Smart Grid Resilience (SGR) Workshop at IEEE Global Communications Conference in 2015, and the General Chair for the IEEE GlobalSIP'15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems.

Prof. 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 and Computer Engineering, and the 2011 Cyber Security and Information Intelligence Research Workshop. She is a Fellow of the Canadian Academy of Engineering.

Aboutaleb Haddadi (S'11–M'15) received the Ph.D. degree in electrical and computer engineering from McGill University, Montréal, QC, Canada, in 2015.

From 2015 to 2018, he was a Postdoctoral Fellow with Montréal Polytechnique, Montréal, where he is currently a Research Associate. He is the Lead Author of the CIGRÉ Technical Brochure Power System Test Cases for EMT-Type Simulation Studies. His research interests include power system protection, power system simulation, and renewable resources integration.