Integrated IDS and OT-SDN for Strengthening Cybersecurity Posture of Differential Protection

Behzad A. M. Alizadeh
Toronto Metropolitan University
Toronto, Canada
Behzad.alizadeh@torontomu.ca

Amir Abiri Jahromi
University of Leeds
Leeds, United Kingdom)
A.AbiriJahromi@leeds.ac.uk

Negar Karimipour
Toronto Metropolitan University
Toronto, Canada
nkarimipour@torontomu.ca

Muhammad Jaseemuddin
Toronto Metropolitan University
Toronto, Canada
jaseem@torontomu.ca

Mohammadreza F. M. Arani
Toronto Metropolitan University
Toronto, Canada
marani@torontomu.ca

***Abstract*— Differential protection is increasingly deployed in power systems and microgrids due to its high sensitivity, security, and dependability. Yet, differential protection is vulnerable to false data injection attacks. This paper proposes integrating an intrusion detection system (IDS) with software-defined networking for operational technology (OT-SDN) to strengthen the cybersecurity posture of differential protection. The proposed IDS employs a Discrete Fourier Transform (DFT)–based transient monitor at each terminal of differential protection to evaluate the presence of a fault using the quality of locally measured currents. If differential protection is activated in the absence of fault signatures detected by the transient monitor, or if fault signatures are detected while differential protection remains inactive, the proposed IDS issues an alert to the OT-SDN controller to switch from the compromised communication channel to another channel. The proposed integrated IDS and OT-SDN strategy is validated through a co-simulation environment using Typhoon HIL and OMNeT++. The simulation results demonstrate the effectiveness of the proposed strategy in detecting and mitigating false data injection attacks against differential protection, significantly enhancing its cybersecurity resilience.**

Keywords*— *Cybersecurity, differential protection, intrusion detection systems, transient monitor, software-defined networking for operational technology, resilience.

I. INTRODUCTION (*HEADING 1*)

Substations are moving toward digitization and deployment of the IEC 61850 standard to streamline maintenance, improve reliability, and enhance interoperability between protection and control devices from different vendors. Despite the unquestionable benefits of digitization, the reliance on advanced information and communication technologies in substations introduces new cybersecurity vulnerabilities, which should be addressed properly. Otherwise, the reliability and security of power systems will be jeopardized [1]–[3].

Concerns about the cybersecurity of substations have been on the rise in recent years, in particular, after the cyberattacks on the Ukrainian power grid in 2016 and 2017 [4]. The cybersecurity of protection systems in substations has received a particular attention due to their role as the last line of defence against abnormal conditions in power systems. To address the cybersecurity concerns in power systems, the North American Electric Reliability Corporation (NERC) has mandated critical infrastructure protection (CIP) standards [5].

Differential protection is widely employed in power systems and microgrids. If an attacker manipulates current measurements or communication packets, differential protection may misinterpret the system state, leading to misoperation—either tripping under normal conditions or failing to operate during an actual fault [6], [7]. To address cybersecurity vulnerability of protection, recent studies have explored data-driven anomaly detection and network-based security mechanisms. Machine learning and signal-processing approaches can identify inconsistencies in measurement data [8], but they often require centralized computation or large historical datasets.

In addition, software-defined networking for operational technology (OT-SDN) has emerged as a promising solution for enhancing the cyber resilience of protection relays [9], [10]. By decoupling the control and data planes, SDN enables whitelisting of traffic flows, attack isolation, and real-time reconfiguration of communication paths. However, most SDN-based solutions solely focus on cyber-layer rather than cyber-physical-layer intrusion detection systems.

This paper proposes a detection and mitigation strategy based on integrating an intrusion detection system (IDS) with OT-SDN for enhancing the cybersecurity of differential protection. The proposed IDS employs a local Discrete Fourier Transform (DFT)-based transient monitor to detect false data injection (FDI) attacks from genuine faults. During a fault, transient components in the measured currents exhibit physically consistent spectral characteristics. This is while local measurements lack such transient behavior during FDI attacks. By computing a local signal quality index (SQI) using DFT analysis, the proposed IDS can distinguish genuine faults from FDI attacks.

If the proposed IDS detects an FDI attack, the IED communicates with the OT-SDN controller to switch from the compromised communication channel to another channel. This ensures that the relay remains secure and dependable even under ongoing FDI attacks. The proposed strategy is tested and validated using a co-simulation environment based on Typhoon HIL and OMNeT++. The main contributions of this paper are as follows:

- An intrusion detection system is proposed based on local DFT-based transient monitor at each terminal of differential protection.
- The proposed intrusion detection system is integrated with software-defined networking for operational technology to isolate the cyberattack vector.
- The proposed integrated IDS and OT-SDN is tested and validated using a co-simulation environment based

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE
979-8-3315-8138-1

on Typhoon HIL and OMNeT++. It is demonstrated that the proposed strategy significantly enhances the resilience of differential protection to cyberattacks.

The remainder of this paper is organized as follows. Section II presents a threat model for false data injection attacks against differential protection. The proposed integrated IDS and OT-SDN strategy for detecting and mitigating cyberattacks against differential protection is explained in Section III. The description of the co-simulation environment and the simulation results are provided in Section IV before concluding the paper in Section V.

II. Threat Model for False Data Injection Attack Against Differential Protection

False data injection attack targets the integrity of current measurements transmitted between differential protection relays. In this paper, we assume the attacker compromises the communication channel between differential protection relays and the local measurements are assumed to be secure. The objective is to deceive the differential relay into issuing a false tripping command in the absence of fault or to stay inactive when there is a fault on a feeder.

We assume that a cyberattacker has remote access to the substation communication network through a malicious device which is connected to the inter-substation communication network. The cyberattacker is assumed to recruit a substation employee who has authority to access inter-substation communication network to install a malicious device. The cyberattacker with access to the inter-substation communication network disrupts the flow of SV packets between differential relays and forwards the SV packets with falsified payloads using a combination of MITM and FDI attack (Fig. 1.).

This attack further can be implemented through a malware installed on the inter-substation communication devices to inject a replay attack by replacing SV packets transmitted between differential relays. The malware can be installed on the inter-substation communication devices through a supply chain attack or a threat agent with physical or remote access to the substation automation system. The malware can then eavesdrop and disrupt the information exchange between the differential relays.

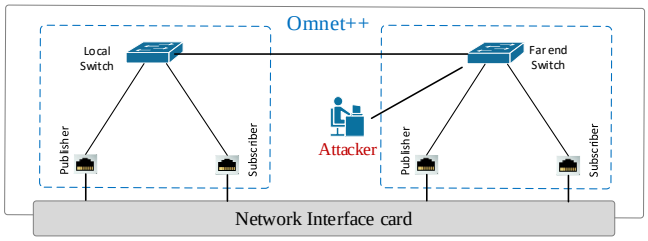

Fig. 1. Evaluation of the transient monitor of the current signal

III. Proposed Integrated IDS and OT-SDN For Differential Protection

A. *Intrusion Detection System Using Local Transient Monitor*

During normal power system operation, the current waveforms after preprocessing are steady state sinusoids that can be accurately represented by a single phasor estimate within each data window. When a fault occurs, however, the waveform contains both pre-fault and post-fault components within the same estimation window. As a result, the phasor estimated by the DFT no longer represents the steady-state value of the signal.

To evaluate the quality of the phasor estimate, the proposed IDS reconstructs a "reproduced" signal from the estimated phasor and compares it to the actual measured waveform. If the reproduced signal closely matches the actual measurement, the phasor quality is high and the system is considered to be in a normal state. Conversely, when a fault occurs, the discrepancy between the actual measurement and the reproduced signal increases sharply [11, 12, 13].

Let $i(t)$ denote the measured current and $\hat{\imath}(t)$ the signal reconstructed from the estimated fundamental phasor. We define $e(t)$ as

$$e(t) = i(t) - \hat{\imath}(t) \quad (1)$$

The magnitude of $e(t)$ over a DFT window serves as a signal quality index (SQI) that indicates the presence of a fault [14]. A low SQI implies high phasor quality and normal state, whereas a high SQI reveals a faulty state. This method avoids the need for conventional superimposed current calculations and directly quantifies the quality of the phasor [15]. It is shown in Figure 2 that immediately after fault occurrence, SQI increases significantly. Before fault and sufficient time after fault its value is zero.

If the locally measured current exhibits high signal quality, the transient monitor in the IDS concludes that no disturbance exists in the system. Therefore, even if the differential relay receives falsified measurements from the remote relay suggesting a fault, the relay does not initiate a trip command. Instead, the local IED communicates with the OT-SDN controller, instructing it to switch from the compromised communication channel to another channel. Conversely, if the transient monitor detects a low signal quality, this indicates that the local current waveform contains transient components associated with a real fault. In such a case, the relay logic proceeds normally, allowing the differential element to operate. This mechanism ensures that protection actions are only based on trustworthy local measurements, thereby maintaining security under FDI attacks and dependability during faults. Similarly, if the locally measured current exhibits low signal quality, the transient monitor in the IDS concludes that a fault exists in the system. In this case if the differential relay is inactive, the IDS detects a false data injection attack and then, the IED communicates with the OT-SDN controller to switch from the compromised communication channel to another channel.

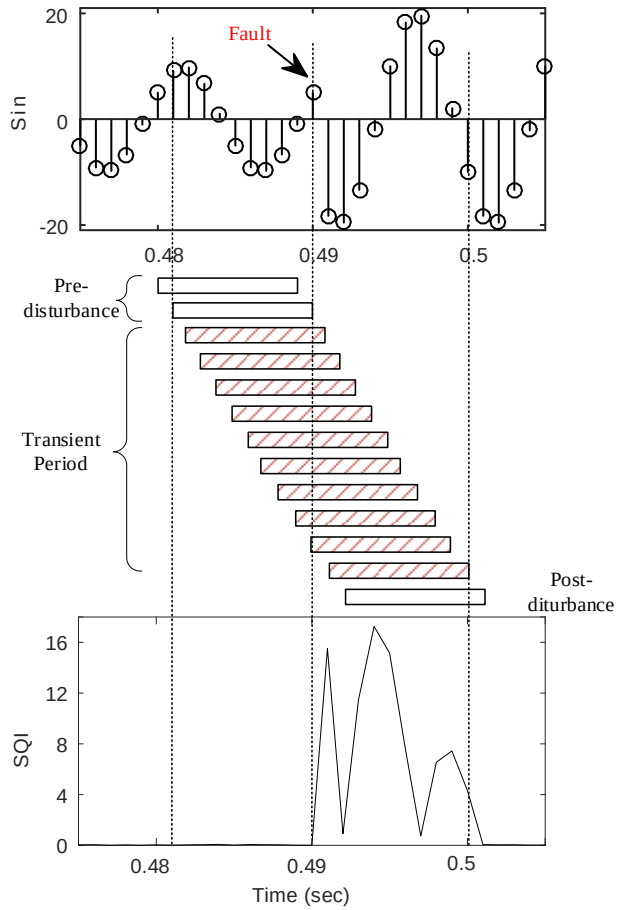

Fig. 2. Evaluation of the transient monitor of the current signal

B. *Integration of IDS with OT-SDN*

The proposed IDS is integrated with software-defined networking for operational technology as illustrated in Fig. 3 to isolate the attack vector and mitigate the false data injection attack. In the proposed strategy as illustrated in Fig. 3, SDN switches supervised by the OT-SDN controller can rapidly reconfigure communication channels when abnormal behavior is detected.

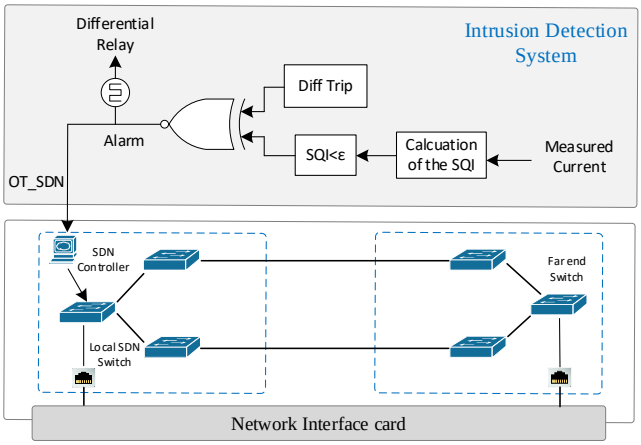

Fig. 3. Integration of the proposed IDS with OT-SDN for resilient differential protection

IV. Simulation Results

To test and verify the effectiveness of the proposed integrated IDS and OT-SDN strategy in detecting and mitigating false data injection attacks against differential protection, a co-simulation environment based on Typhoon HIL 604 and OMNeT++ is developed.

A. *Co-Simulation Environment*

The setup, illustrated in Fig. 4, consists of two Typhoon HIL 604 devices representing the two ends of a protected line section. Each HIL device includes a model of a current differential relay (IED) configured according to the IEC 61850 standard.

- HIL Device 1 (Publisher): Publishes real-time Sampled Value (SV) packets representing local current measurements.
- HIL Device 2 (Subscriber): Receives the SV packets and performs differential current calculation.

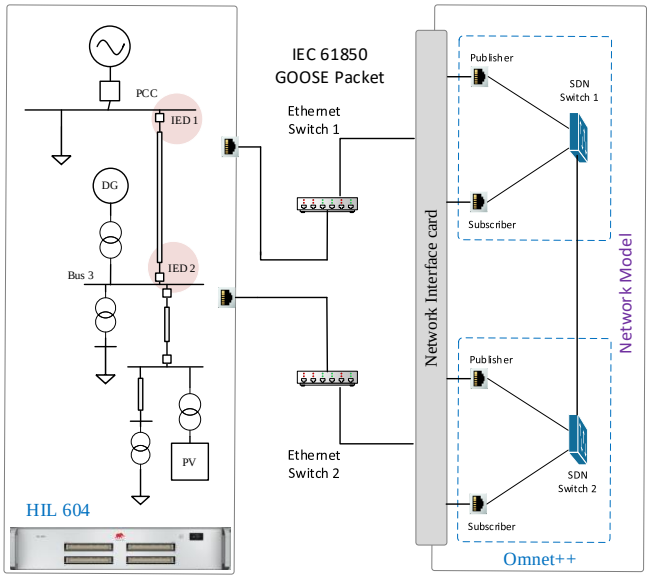

Fig. 4. The provided co-simulation setup for testing the proposed method

B. *Case Studies*

Two case studies are considered here. In the first case study, we investigate a scenario where there is no fault in the system, but the attacker injects falsified measurements to force the differential protection to operate. In the second case study, we consider a scenario, where there is a fault in the differential protection zone, but the attacker injects falsified measurements to prevent the differential protection to operate. In both case studies, we assume that the attacker intercepts the SV packets transmitted from the publisher to the subscriber and manipulates current measurements before forwarding them to the receiving IED.

1) Case Study I

To illustrate the security vulnerability of differential protection to FDI attacks, a baseline simulation was performed without the proposed integrated IDS OT-SDN mitigation strategy. Fig. 5 shows the current measurements and relay response when an FDI attack is introduced at 1.32 s.

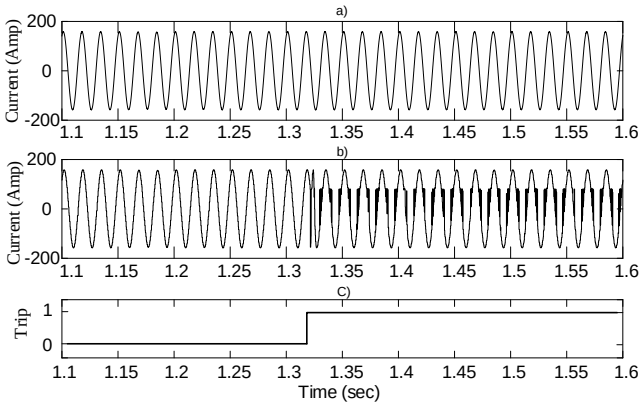

Fig. 5. a) Local current measurement; b) Manipulated current measurements under FDI attack; c) Differential relay trip signal.

In Fig. 5 a), the local current measurement remains intact and consistent with system behavior. However, as shown in Fig. 5 b), the received current measurements from the remote end is manipulated by the attacker to emulate an internal fault condition. As a result, the differential protection interprets this difference between the local and remote measurements as a real fault and initiates a trip command, as illustrated in Fig. 5 c). The simulation results confirm that in the absence of the proposed detection and mitigation strategy, differential protection misoperates.

To demonstrate the effectiveness of the proposed integrated IDS and OT-SDN strategy, the same FDI attack scenario was simulated. The attack again occurs at 1.32 s, during which the attacker manipulates the transmitted SV packets between the two IEDs. The corresponding results are shown in Fig. 6.

In Fig. 6 (a), the local current measurement remains consistent with system conditions. In Fig. 6 (b), the received current measurement from the remote differential relay is again manipulated by false data injection attack. However, in this case, the IDS correctly evaluates the local signal quality as high as illustrated by the SQI in Fig. 6 (d), which remains close to zero throughout the event.

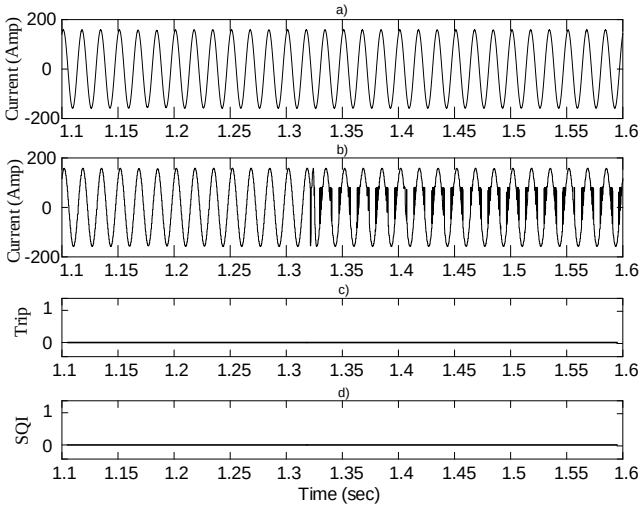

Fig. 6. a) Local current measurement; b) Manipulated current measurements under FDI attack; c) Differential relay trip signal, and d) Signal Quality Index (SQI).

Consequently, the relay blocks its trip command, as seen in Fig. 6 (c), and simultaneously communicates with the OT-SDN controller to switch from the compromised communication channel to another channel. The FDI attack is therefore unsuccessful, and the differential relay remains secure while the system continues normal operation.

2) Case Study II

To illustrate the dependability vulnerability of conventional differential protection to FDI attacks, a baseline simulation was performed without the proposed integrated IDS OT-SDN mitigation strategy. Fig. 7 shows the current measurements and relay response when an FDI attack is introduced at 1.32 s.

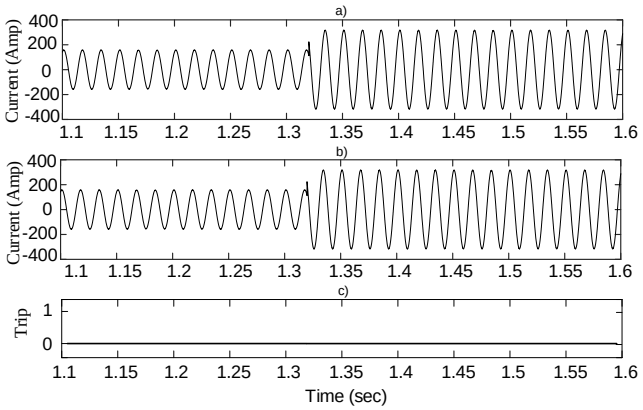

Fig. 7. a) Local current measurement; b) Manipulated current measurements under FDI attack; c) Differential relay trip signal.

In Fig. 7 a), the local current measurement changes abruptly when the fault occurs. However, as shown in Fig. 7 b), the received current measurement from the remote end is manipulated by the attacker to conceal any a fault within differential protection zone. As a result, the differential protection cannot detect the fault and remains inactive, as illustrated in Fig. 7 c). The simulation results confirm that in the absence of the proposed detection and mitigation strategy, differential protection remains inactive and misoperates.

To demonstrate the effectiveness of the proposed integrated IDS and OT-SDN strategy, the same FDI attack scenario was simulated. The attack again occurs at 1.32 s, during which the attacker manipulates the transmitted SV packets between the two IEDs. The corresponding results are shown in Fig. 8.

In Fig. 8, the local current measurement changes consistently with the faulty system condition. In Fig. 8, the received current measurement from the remote differential relay is again manipulated by false data injection attack. However, in this case, the IDS correctly evaluates the local signal quality as low as illustrated by the SQI in Fig. 8 (d), which changes significantly after the fault occurrence.

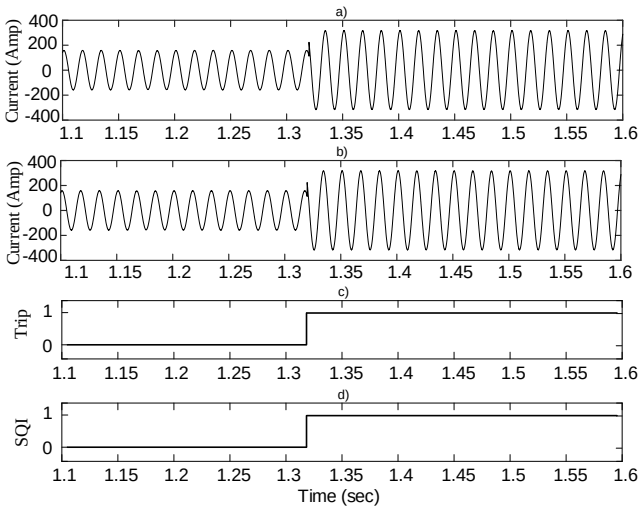

Fig. 8. a) Local current measurement; b) Manipulated current measurements under FDI attack; c) Differential relay trip signal, and d) Signal Quality Index (SQI).

Consequently, the IDS communicates with the OT-SDN controller to switch from the compromised communication channel to another channel. The FDI attack is therefore unsuccessful, and the differential relay operates and clears the fault.

V. CONCLUSION

A detection and mitigation strategy is proposed in this paper based on integrated IDS and OT-SDN to improve the resilience of differential protection to cyberattacks. The IDS employs DFT-based transient monitor for detecting false data injection attacks and communicates with the OT-SDN controller to isolate the attack vector. The simulation results using Typhoon HIL and OMNeT++ demonstrate the capability of the integrated IDS and OT-SDN to effectively detect and isolate attack vectors for two case studies. In the first case study the security vulnerability of differential protection to FDI attacks is demonstrated. Furthermore, the capability of the proposed integrated IDS OT-SDN strategy to detect and mitigate FDI attacks is tested and verified. In the second case study the dependability vulnerability of differential protection to FDI attacks is demonstrated. It is shown that the proposed integrated IDS OT-SDN strategy again successfully detects and mitigates FDI attacks.

REFERENCES

[1] Ashok, Aditya, Manimaran Govindarasu, and Jianhui Wang. "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid." Proceedings of the IEEE 105, no. 7 (2017): 1389-1407.

[2] Ashok, Aditya, Adam Hahn, and Manimaran Govindarasu. "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment." Journal of advanced research 5, no. 4 (2014): 481-489.

[3] Liu, Chensheng, Hao Liang, Tongwen Chen, Jing Wu, and Chengnian Long. "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation." IEEE Transactions on Power Systems 35, no. 2 (2019): 1468-1478.

[4] Liang, Gaoqi, Steven R. Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. "The 2015 Ukraine blackout: Implications for false data injection attacks." IEEE transactions on power systems 32, no. 4 (2016): 3317-3318.

[5] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards. 2025.

[6] Ameli, Amir, Ali Hooshyar, and Ehab F. El-Saadany. "Development of a cyber-resilient line current differential relay." IEEE Transactions on Industrial Informatics 15, no. 1 (2018): 305-318.

[7] Ameli, Amir, Ali Hooshyar, Ehab F. El-Saadany, and Amr M. Youssef. "An intrusion detection method for line current differential relays." IEEE Transactions on Information Forensics and Security 15 (2019): 329-344.

[8] Khaw, Yew Meng, Amir Abiri Jahromi, Mohammadreza FM Arani, Scott Sanner, Deepa Kundur, and Marthe Kassouf. "A deep learning-based cyberattack detection system for transmission protective relays." IEEE Transactions on Smart Grid 12, no. 3 (2020): 2554-2565.

[9] Kemmeugne, Anthony, Amir Abiri Jahromi, and Deepa Kundur. "Resilience enhancement of pilot protection in power systems." IEEE Transactions on Power Delivery 37, no. 6 (2022): 5255-5266.

[10] Ghosh, Uttam, Pushpita Chatterjee, and Sachin Shetty. "A security framework for SDN-enabled smart power grids." In 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 113-118. IEEE, 2017.

[11] Khodaparast, Jalal, and Mojtaba Khederzadeh. "Three-phase fault detection during power swing by transient monitor." IEEE Transactions on Power Systems 30, no. 5 (2014): 2558-2565.

[12] Tekdemir, Ibrahim Gursu, and Bora Alboyaci. "A novel approach for improvement of power swing blocking and deblocking functions in distance relays." IEEE transactions on power delivery 32, no. 4 (2016): 1986-1994.

[13] Khaw, Yew Meng, Amir Abiri Jahromi, Mohammadreza FM Arani, Scott Sanner, Deepa Kundur, and Marthe Kassouf. "A deep learning-based cyberattack detection system for transmission protective relays." IEEE Transactions on Smart Grid 12, no. 3 (2020): 2554-2565.

[14] Sadeghkhani, Iman, Mohamad Esmail Hamedani Golshan, Ali Mehrizi-Sani, Josep M. Guerrero, and Abbas Ketabi. "Transient monitoring function–based fault detection for inverter-interfaced microgrids." IEEE Transactions on Smart Grid 9, no. 3 (2016): 2097-2107.

[15] Phadke, Arun G., and John Samuel Thorp. Synchronized phasor measurements and their applications. Vol. 1, no. 2017. New York: Springer, 2008.