IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society | 978-1-6654-6454-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/IECON55916.2024.10905232

Integration of Software-Defined Networking and Line Outage Distribution Factors for Enhancing the Cyber Resilience of Modern Transmission Systems

Anthony Kemmeugne*, Amr S. Mohamed*, Ahmad Mohammad Saber*, and Deepa Kundur*
*Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 1A1, Canada.

***Abstract*—Different grid codes today require that transmission line relays and circuit breakers be remotely controllable, which potentially exposes them to malicious cyberattacks. This paper presents a cyber resiliency framework based on software-defined networking (SDN) and line outage distribution factors (LODFs) to detect malicious relay control commands at their inception. The framework actively monitors network traffic to power system relays. If a tripping command is expected to adversely affect the power system, as indicated by the LODFs, the framework leverages SDN's network visibility and management capabilities to alert on the traffic, identify the compromised network node, and isolate it to mitigate potential cyberattacks. Conversely, legitimate commands are permitted to proceed. We demonstrate the framework using the IEEE 9-bus benchmark system.**

***Index Terms*—Cyber-physical security, power system security, smart grids, software-defined networking.**

I. Introduction

SOFTWARE-DEFINED NETWORKING (SDN) is poised to play a crucial role in leveraging the convergence of Information Technology (IT) and Operational Technology (OT) in power systems, offering enhanced cybersecurity for these complex environments [1]. SDN is an advanced network architecture that separates the network control plane—responsible for routing decisions—from the data plane, which handles the forwarding of data packets based on those decisions. This separation allows for centralized management and dynamic configuration of network resources [2].

In the context of power systems, applying SDN enables network administrators to control traffic flows and enforce fine-grained security policies across the entire network from a central control point. The programmability of SDN supports real-time automation of security responses, such as rerouting traffic away from compromised nodes, blocking malicious communications, and creating virtual network segments to contain and limit the spread of cyber threats [3].

This paper explores the benefits of using SDN to protect against false tripping commands to transmission lines. Today, transmission lines are remotely monitored and controlled for real-time management and cost efficiency. However, this remote access exposes them to cyberattacks. False tripping of one transmission line can overload other lines beyond their limits, which may also trigger cascading failures, causing widespread power system instability and system collapse. Unplanned overloads may also lead to excessive heating, equipment damage, and increased repair costs.

The literature has proposed various methods to protect against false tripping of transmission lines, including those based on anomaly detection (e.g., [4]) and intrusion detection (e.g., [5]). SDN can offer an additional layer of security when intrusion detection fails to detect cyber breaches or when a false command is inadvertently issued by an insider as investigated in [6]. Additionally, SDN's network management capabilities enable taking mitigation actions, beyond detection, to block false commands and isolate compromised nodes, thereby stopping the spread and impact of the attack. The specific benefits that SDN may bring to power system resilience against accidental commands and cyberattacks remain largely unexplored [7]. In this paper, we provide a new perspective on how SDN can be used to prevent false tripping of transmission lines.

In this paper, we propose a novel cyber resiliency framework that utilizes SDN to detect and block malicious commands to open transmission line circuit breakers before they reach their intended breaker. The framework involves communicating Line Outage Distribution Factors (LODFs) from the power system Energy Management System (EMS) to the SDN controller. This communication alerts the SDN controller to transmission lines whose loss would adversely impact the power system. Utilizing SDN's network visibility, the framework monitors network traffic for any commands, whether issued inadvertently or maliciously, to open these critical transmission lines. When such a command is encountered, the SDN can be programmed to alert the command, identify the source nodes, and even isolate the nodes from the network. This isolation prevents the compromised nodes from continuing to send malicious commands and stops the spread of a malicious cyberattack. Thus, the proposed framework enables SDNs to detect and mitigate cyberattacks against power system transmission lines.

The attack model is discussed in Section II, followed by an outline of LODFs, SDN, and the proposed SDN-based cyber resiliency framework in Section III. Section IV demonstrates the application of this method on a benchmark system. Finally, Section V concludes the paper and discusses future work.

II. Attack Model

In the case of a cyberattack, we consider an adversary who is able to gain unauthorized access to the network in which a relay commanding a transmission line circuit breaker

is embedded. Cyberattackers can gain unauthorized access through stolen credentials obtained via prior social engineering attacks or malware that gives the attacker control over an existing device in the network. If a cyberattacker compromises a legitimate remote host to access the secure wide-area network of the power system, the attacker can bypass existing IT network security measures, spoofing packets to issue commands that appear legitimate. Alternatively, the cyberattacker can exploit insecure remote access points or maintenance backdoors left by third-party vendors, enabling the injection of malicious commands through a remote device [8]. In any case, we assume that the attacker bypasses network defenses and intrusion detection methods.

We limit the scope of this paper by excluding scenarios where the control center (including the EMS and SCADA) or the SDN controller is compromised. Instead, we focus on cases where the cyberattacker can execute man-in-the-middle attacks and inject false data through a compromised device within the secured WAN (Wide Area Network). Such actions could also be executed by disgruntled insiders or inadvertently by operators via a human-machine interface through human error [9].

Given the significant impact of false tripping of circuit breakers, it is crucial to develop an additional layer of security that confirms the legitimacy and verifies the safety of control commands before they are sent to the circuit breakers.

III. Proposed Cyber Resiliency Framework

In this section, we briefly describe LODFs and SDN, before presenting the cyber resiliency framework.

A. Line Outage Distribution Factors

LODFs assess how the flow of electricity on transmission lines changes when specific lines are out-of-service. Consider two lines i and j in a power system with power flows f_i and f_j, respectively. If an outage affects line i, the flow on line i is rerouted to other transmission lines. The $LODF_{i\to j}$ quantifies the fraction of f_i that is rerouted to line j due to this outage. This can be represented as:

$$LODF_{i\to j} = \frac{\Delta f_{i\to j}}{f_i} \tag{1}$$

where $\Delta f_{i\to j}$ is the change in power flow through line j due to the outage of line i.

In power system contingency analysis, LODF helps identify which lines are most likely to experience overloads and hence study stability issues if certain lines or components fail. Consider the maximum rated capacity of line j is C_j. Before the outage on line i, line j is operating at f_j/C_j of its rated capacity. Following the outage on line i, if

$$\frac{f_j}{C_j} + \frac{\Delta f_{i\to j}}{C_j} > 1 \tag{2}$$

then this indicates that line j will be overloaded. The second term in the equation indicates the increase in loading on line j due to the outage on line i.

B. Software-Defined Networking

SDN provides a dynamic network infrastructure that can rapidly respond to changes in network flows, largely due to the OpenFlow protocol. Switches in an SDN network use flow rules to identify packets based on various criteria such as source and destination IP addresses. When a packet is received, the switch matches its header information to predefined flow rules in the flow tables. If there is a match, the associated action is executed and the packet is forwarded accordingly. If the packet does not match any of the switch's flow rules, it is sent to the controller for processing as a packet-in message and an updated rule is created for the packet. The OpenFlow protocol enables this dynamic control of the network, allowing for real-time traffic requirements to be met, unlike conventional network infrastructure.

Besides the programmability of the SDN infrastructure and the standardization of the OpenFlow protocol, SDN devices make the infrastructure highly flexible to network requirement changes thanks to its active monitoring capabilities that can track every packet that has been matched to pre-implemented rules and every new connection to the communication network. Additionally, unlike standard communication network that uses the plug-and-play principle allowing any new connection to participate in the network, SDN implements the deny-by-default principle that only grants access to authorized actors which makes it more resilient to cyberattacks.

C. Preventing False Line Tripping with Software-Defined Networking

We propose a novel cyber resilience framework that capitalizes on IT/OT convergence in power systems to leverage SDNs to detect and mitigate cyberattacks targeting power system relays.

The framework is illustrated in Fig. 1. In the framework, the EMS in the control center computes power flow over the transmission lines and LODFs for the power system and communicates these data to the SDN controller. The SDN controller is a separate entity from the EMS. Relays controlling circuit breakers on transmission lines are (OT) devices communicating over network protocols utilizing IP and MAC addresses.

Once the SDN controller receives the data, it forwards it to the SDN application plane. The application plane hosts the applications that define network behavior and policies, including security and traffic monitoring. The SDN application plane applies Equation 2 to identify critical transmission lines, based on the LODF values, whose opening could result in overloading of adjacent lines. Next, the application plane maps these critical lines to their corresponding protective relays' physical addresses and updates the SDN flow tables, as illustrated in Fig. 2, to further monitor packets to these relays.

The application plane forwards the flow tables to the SDN controller, which translates these high-level policies from the application plane into low-level instructions for the data plane comprising the switches. Subsequently, the SDN controller creates a rule for switches to block all packets destined

for flagged relays on critical lines, even if they originate at legitimate, white-listed hosts, and instructs switches to redirect these packets to the SDN controller for further inspection. This ensures that any attempt to open a critical line will be mitigated.

A case in study: if line $L0$ in Fig. 1, protected by Relay 0, is flagged as critical at the application level, a rule will be sent from the SDN controller to all network switches to drop any packets instructing the relay to open line $L0$'s circuit breaker with the destination address of Relay 0 (00:00:00:00:A1) and forward them to the SDN controller for further inspection.

With the packets redirected to the SDN controller, further policies can be programmed to identify the compromised source nodes, send alerts to security teams, and isolate these nodes from the network to prevent this compromised node from communicating any further with other devices in the network. In the case of a cyberattack, this can limit the spread and impact of the cyberattack. Conversely, safe packets are allowed to flow through the network.

Hence, the proposed framework leverages IT/OT convergence to enable the flow of data between the EMS and SDN controller to enhance the cyber resilience of power systems. The frameworks utilizes OT system data, processed through the EMS to compute LODFs, to give the SDN an understanding of the physical system – which the SDN uses to configure the communication network to prevent false commands that are injected by cyberattackers, who are able to bypass IT security measure, or inadvertently issued by insiders.

IV. Results

To validate the proposed solution, we use the IEEE 9-bus benchmark system, illustrated at the bottom of Fig. 1. This test system comprises 9 buses, 9 lines, 3 generators, and 3 loads. We keep the generation and load parameters as specified in [10], [11], but we reduce the line capacities by 30% to simulate conditions where the transmission lines are operating closer to their rated capacity for demonstration purposes. For load flow computations, one of the generators is designated as the slack bus, and line $L0$ remains closed during the study. The line numbers are indicated in Fig. 1.

A. Impact of Malicious Tripping Commands on the Transmission System

A malicious entity can infiltrate the system, as discussed in Section II, allowing them to send malicious switching commands to line circuit breakers.

To illustrate the impact of false tripping of a transmission line, consider the scenario of a cyberattacker commanding the circuit breaker on line $L7$ to open. The effect of line $L7$'s outage is illustrated in Fig. 3. The available capacities of the transmission lines before line $L7$'s outage for the considered test scenario are shown in the top subfigure of Fig. 3. For example, line $L2$ is operating at 58.1% of its rated capacity before the outage, leaving 41.9% of its capacity available for further loading.

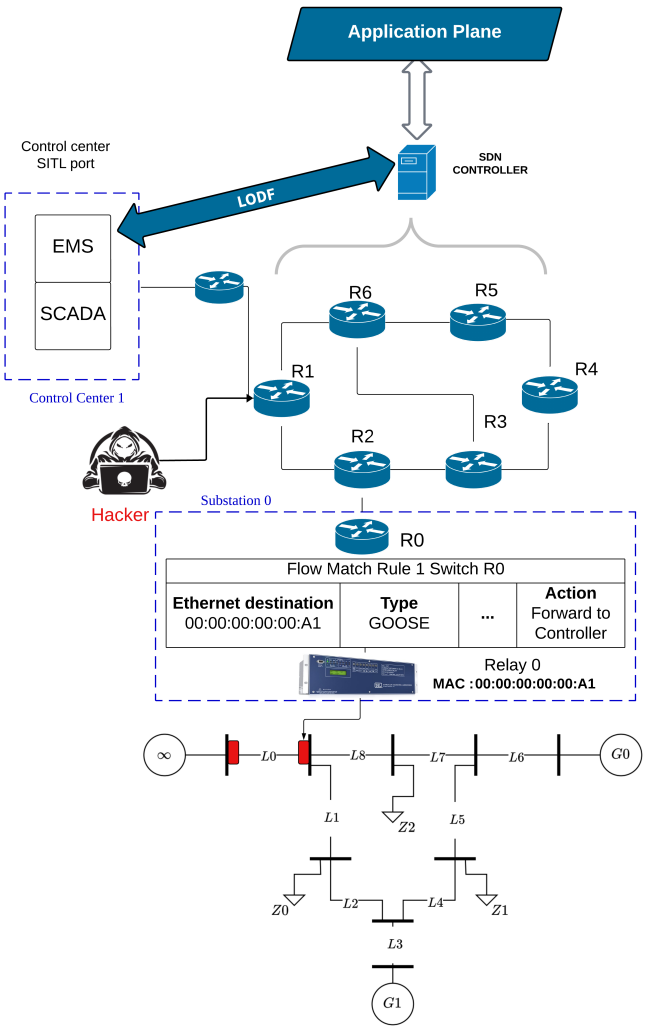

Fig. 1. SDN-LODF Cyber Resiliency Framework

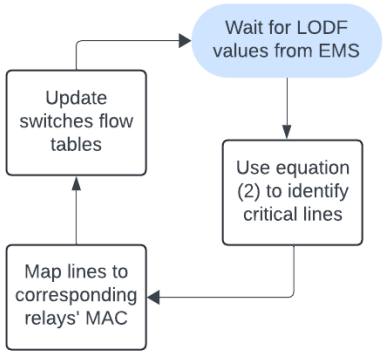

Fig. 2. Application Plane Prevention Algorithm

The bottom subfigure of Fig. 3 displays the lines' loading increase. Each row represents the estimated percentage increase in line loading if the line indicated on the vertical axis is opened. In Fig. 3, the cells are color-coded to indicate how close each line comes to its maximum rated capacity after the outage. Text is highlighted in red when an outage would cause the line's power flow to exceed its maximum rated capacity. Text that is highlighted in red corresponds to cells where the additional loading indicated by the text is higher than the available capacity of this line before the outage.

Line $L7$'s outage increases the power flow on most of the other lines. Particularly, the outage increases the loading of line 2 from 58.1% to 140.9% and increases the current flowing in it by about 2.4 times, potentially triggering the operation of the overcurrent protection on this line, inducing further overloading of other transmission lines and cascading failure in the system.

The decision process in the SDN application plane mirrors the above explanation of the impact of the false tripping of line $L7$. Our proposed framework prevents the cyberattacker from opening this line.

B. Proof-of-Concept Validation of the Proposed Framework

As previously detailed, the EMS computes and communicates the line flows and LODFs to the SDN controller.

Fig. 3 illustrates the decision process in the SDN application plane. Opening all lines except lines $L6$ and $L7$ does not result in any line overloads. However, disconnecting any of these two lines must be avoided, as disconnecting one of them results in an overloading of line $L0$ or $L2$ highly beyond its capacity. Such a condition is unlikely to be a normal operational command for lines $L6$ and $L7$, and could be indicative of a malicious or inadvertent action.

Upon receiving the LODFs from the EMS, the application layer of the SDN identifies lines $L6$ and $L7$ as critical and update flow rules to intercept any packets attempting to open these critical lines.

if an attacker issues a tripping commands to these lines, the packet and its metadata will be redirected to the SDN controller. Using active monitoring and logs, the SDN controller will be able to identify the source of the attack and isolate the threat.

V. Conclusion and Future Work

We have introduced an innovative cyber resiliency framework designed to counter advanced cyberattacks aimed at false tripping of transmission lines in power systems. This new framework leverages OT data, processed into LODFs over transmission lines, and harnesses SDN capabilities to detect, prevent, and isolate cyber threats that could significantly impact power system stability.

Moving forward, we plan to implement this framework on a cyber-physical simulation platform and evaluate its effectiveness across larger systems and under different threat scenarios.

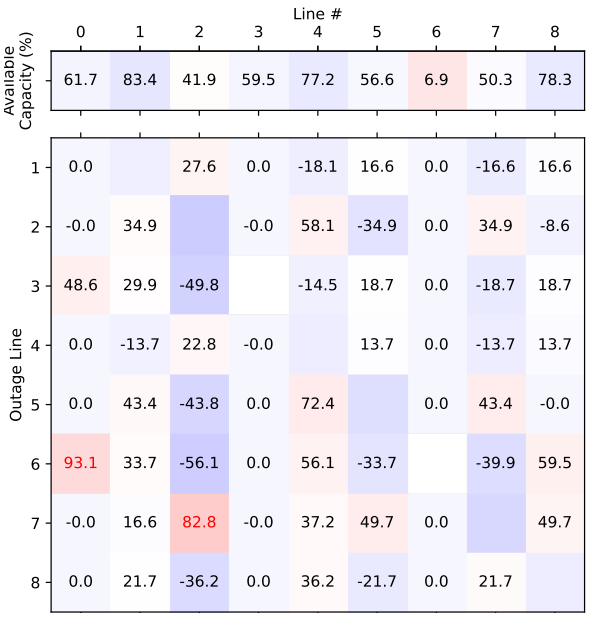

Fig. 3. Top: Available line capacities before any line outage, Bottom: Additional loading to transmission lines following an outage of the line indicated on the vertical axis

References

[1] E. Molina and E. Jacob, "Software-defined networking in cyber-physical systems: A survey," *Computers & electrical engineering*, vol. 66, pp. 407–419, 2018.

[2] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, "Software-defined network (sdn) data plane security: issues, solutions, and future directions," *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pp. 341–387, 2020.

[3] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, "Sdn security review: Threat taxonomy, implications, and open challenges," *IEEE Access*, vol. 10, pp. 45 820–45 854, 2022.

[4] A. M. Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin, and E. F. El-Saadany, "Anomaly-based detection of cyberattacks on line current differential relays," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4787–4800, 2022.

[5] 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.

[6] A. Kemmeugne, A. Jahromi, and D. Kundur, "Resilience enhancement of pilot protection in power systems," *IEEE Transactions on Power Delivery*, vol. 37, no. 6, p. 5255–5266, Dec 2022.

[7] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ser. CPSS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 61–68. [Online]. Available: https://doi.org/10.1145/2732198.2732203

[8] C. Glenn, D. Sterbentz, and A. Wright, "Cyber threat and vulnerability analysis of the us electric sector," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2016.

[9] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Inform.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019.

[10] V. Vittal, J. D. McCalley, P. M. Anderson, and A. Fouad, *Power system control and stability*. John Wiley & Sons, 2019.

[11] Pandapower. Power system testcases: Case 9. [Online]. Available: https://pandapower.readthedocs.io/en/v2.2.2/networks/power_system_test_cases.html#case-9