Analyzing Cyber Vulnerabilities of Protection Systems and Classification of System Anomalies

Ceeman Vellaithurai
School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington 99164
Email: ceeman.vellaithurai@wsu.edu

Meshal Marzooq
School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington 99164
Email: meshal.marzooq@wsu.edu

***Abstract*—The number one reason given by the North American Electric Reliability Corporation (NERC) for cascading power outages is the use of improper relay settings. Power system protection devices can be targets of cyber-attacks that could lead to cascading outages. This work lays out methods to consider for detecting attacks on these devices through the use of continuous and trigger based monitoring schemes through the use of data collected from the field devices. Power system faults have typical signatures associated with them. Through the use of data from surrounding devices, it is possible to verify that the operation or no operation of a device is correct or incorrect by verifying the specific signature. Two major attacks, the man-in-the-middle (MITM) and replay attack on power system protection devices are discussed and highlight the usefulness of the schemes to be proposed are at detecting these attacks are discussed in this paper.**

***Index Terms*—cyber-attack, protection systems, cyber-physical systems, continuous monitoring, trigger-based monitoring, intrusion detection**

I. Introduction

Modern power systems are expected to maintain reliable and secure operation of electric power supply. Power system security has two main aspects, i.e., physical, and cyber. Physical security is linked to the ability of the power system to withstand severe disturbances in the operating condition. Whereas, cyber security is associated with the security of digital devices, related communication devices, and network.

The past few decades have seen continuous advancement in digital devices and information technology. This has led to research in power systems using these technologies and their subsequent implementation in the field. The integration of the physical system with the cyber network is getting deeper by the day. This integration is a double edged sword. On the one hand, it helps increase automation and easy access. On the other hand, it also increases the number of vulnerabilities in the system. Due to the heavy interaction of cyber and physical components in the system, any cyber or physical vulnerability can be used to impact the system. [1], [2].

The power system protection devices are designed to sense faulty conditions and isolate the faulty equipment in quick time in an automated way. These devices can be a target of cyber-attacks. False information about system states can be fed to these devices, which can lead to devise malfunctioning. Malfunction of critical devices in the system may lead to the cascading effect causing partial or full system breakdown.

This paper lays out the different types of cyber-attacks that could be targeted against power system protection devices. The focus is then turned to the description of the simulated system, the power system protection scemes used on the system, and operation. Finally, a look at how the proposed schemes can be used to alarm for potentially attack scenarios are discussed.

II. Cyber Attacks

Apart from the application of incorrect protection settings and potentially faulty sensors, cyber-attacks are discussed as a possible reason for misoperation of protective devices in the power system [3]. Some of the possible well discussed attack scenarios are discussed in this section.

(1) Integrity attack: Integrity attacks attempt to access and modify information without authorization. A well placed integrity attack could cause the protective relay to operate due to activation of logic pre-programmed in the relay. An example of this could be when a direct transfer trip input to the relay is subject to an integrity attack. This would lead to the breaker being open as a result of command issued by the protective device.

(2) Main-in-the-middle attack: In the type of attack, the attacker is a middleman between the source and receiving devices. They attacker can intercept the communication and replace data with data of the attacker's choice. This could lead to misoperation of the protective device.

(3) Replay attack: The attacker gains access to normal operation or fault operation of the system through event logs in the protective devices. The attacker is then able to replay these events which could lead to misoperation of the device.

(4) Unauthorized access: In this case, the attacker gains super access to the device and is able to make modifications to the relay settings. Modifications to the settings could cause the relay to misoperate. Potentially, the protective functions could be turned off causing the relay to do nothing in the event of a fault. This could lead to cascading outages in the system.

(5) Denial-of-service (DoS) attack: The goal of this type of an attack is to overwhelm a device or communication

channel to the extent that it is not able to carry out normal functions. A DoS attack could hamper proper communication between protective devices to carry out a desired functionality. Communication assisted protection schemes can be a target of such attacks.

The attacker can misrepresent the information in two ways: i) by replacing data of stable scenario with a faulty scenario causing the relay to operate although there is no fault, ii) by restricting relay operation by replacing data of actual system fault with data of normal operation. Therefore, the knowledge of data being compromised or not is essential for the cyber-secure operation of the power system.

III. Study System and Protection Scheme

The IEEE 14 bus system is used for this study. An RSCAD model was built for use with the Real Time Digital Simulator (RTDS) to perform simulations. Only the line protection was considered in this project. The line protection considered is shown in Figure 1.

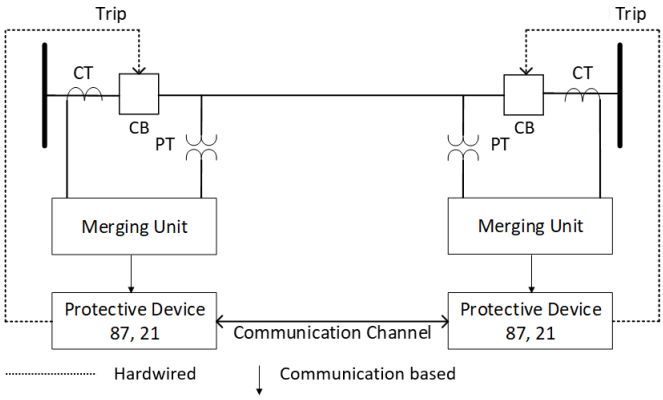

Fig. 1. Line protection scheme

The architecture assumes the use of a merging unit which is responsible for sampling the current and voltage signals from the current transformer and potential transformer respectively. The protective device implements two protection functions: 87, line current differential and 21, distance protection. The distance protection is considered to be implemented as a permissive overreach transfer tripping scheme. The IEC 61850 based merging unit is responsible for providing time stamped data at a fixed number of sample per second.

IV. Basis for Proposed Schemes

The proposed scheme is based on the physical characteristics and traits of the power system.

(1) Kirchoff current law: The kirchoff current law states the the sum of current entering a node is equal to the sume of current leaving the node. Said differently, the sum of all currents measured at a node should always be zero.

(2) Differential scheme: At a basic level, the differential scheme can be explained as operating on the sum of currents entering a device and leaving a device. In ideal conditions, the current entering a device must equal the current leaving a device. Any difference current measured is an indication of a problem. Protective devices are set to operate on this difference current.

(3) Voltage profile during a fault: The sequence components of voltage; positive sequence, negative sequence, and zero sequence voltage can be an useful indicator of the occurrence of faults and in the identification of the faulted phase(s). It is well known that the positive sequence voltage is minimum at the point of fault and recovers back towards the source. In the case of negative sequence and zero sequence voltages, they are maximum at the point of the fault and decay as they go towards the source. Figure 2 shows the typical sequence voltage profile expected during a single-line-to-ground (SLG) fault on a line.

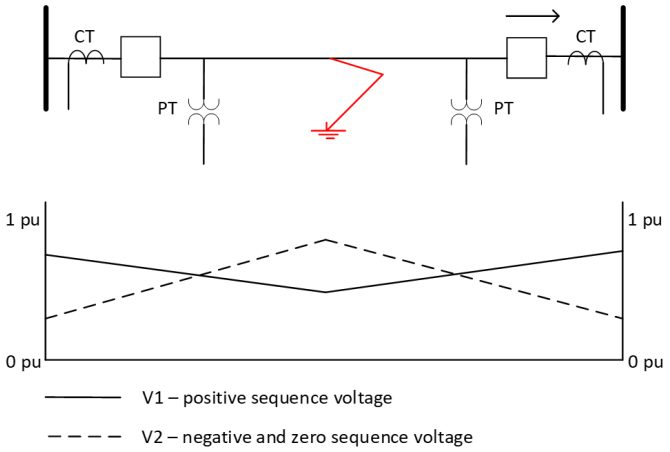

Fig. 2. Sequence Voltage Profile for a SLG fault

(4) Faulted phase identification: In the interest of keeping the proof of concept discussion simple, only single-line-to-ground faults will be detailed here. Figure 3 shows the angle relationship between the zero sequence and negative sequence current for phase AG, BG, and CG faults [4]. The relationships are not absolute degree comparison and there is a plus or minus 30 degree window.

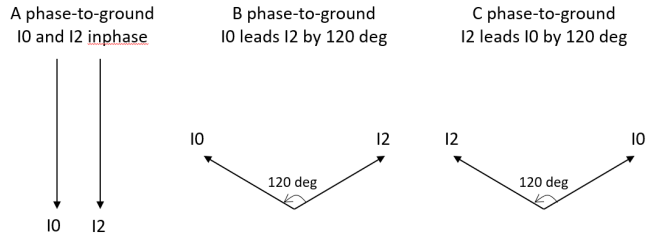

Fig. 3. Angle Relationships for SLG Fault

V. Proposed Schemes

For the identification of false data, a graph-based network model is used. In this model, every substation is considered as a node. The lines interconnecting the substations are considered as edges. A generator or a transformer connected to

the substation is considered as an offshoot node. The offshoot node is connected to the node through an edge with zero weight. A connectivity matrix is constructed. For an edge from node k to node l with breaker placed at node k and not at node l, the connectivity matrix element will be $C_{kl} = 1$ and $C_{lk} = 0$. The connectivity matrix is used to determine the checks to be performed for the two proposed schemes.

Two schemes are formulated to detect an anomaly:

(i) Continuous monitoring scheme – In this method, the power system is continuously monitored to detect an attack.

(ii) Trigger-based scheme – This scheme is initiated following a trip signal from protective relays. Following breaker tripping/opening, data from the last 16 cycles and 16 cycles following the breaker operation are retrieved and analyzed for attack detection.

A. Continuous monitoring scheme

The continuous monitoring scheme can use current or voltage data at system nodes to detect an attack. The current monitoring method is explained in this paper and can be extended for use with voltage as well. The continuous monitoring scheme is based on kirchoff current law and differential scheme as discussed in the previous section. The currents entering and leaving the lines in the system are checked constantly to make sure that they are in agreement. In the event of a disagreement, the scheme looks for indication that the breaker has opened within five cycles of the discrepancy. If no such action has occurred and the disagreement persists, an alarm is raised. If the breaker does indeed open, this scheme does not raise an alarm. Figure 4 shows the scheme logic. In practice, the charging current must be taken into account when setting the threshold for declaring an alarm.

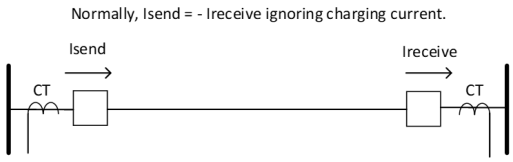

Fig. 4. Differential Principle

The second check in the continuous monitoring scheme is at the substation level. For an ideal network, under normal operation, the sum of currents entering and leaving the node should be zero as discussed before. Figure 5 shows the difference current calculation at Bus 2 in the IEEE 14 bus system.

In a practical system, however, the difference current is non-zero and some finite number. The effects of relay errors, CT and PT errors, and CT saturation must be accounted for. Therefore, when setting the threshold for declaring an alarm, these factors must be accounted for. The magnitude of the difference current at a node is used to detect an attack on the system.

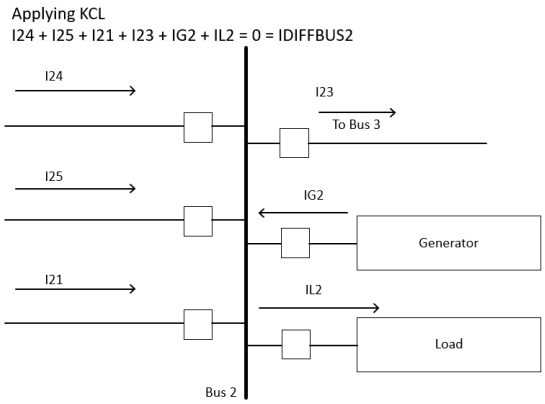

Fig. 5. Difference Current at a Substation

The MITM and replay attacks can be identified using this method. If a MITM attack is in place, and data is compromised, unless the attacker has knowledge of all the network flows, it is not possible to keep the difference current at or near zero. The scheme will flag the discrepancy for further evaluation. In the case of a replay attack, the difference current will spike unnaturally. This again could be an indicator of an attack on the system.

B. Trigger-based scheme

This scheme is initiated after a trip is received from the relay leading to a breaker operation. The data received 16 cycles before and after the fault is analyzed to detect cyber-attacks. This paper explains this scheme from the point of view of detecting replay attacks involving SLG attacks. The zero-sequence and negative-sequence component of the voltage is checked at the neighboring buses. If a step-change is detected at the neighboring buses for these two sequence components, then this portion of the logic does not raise an alarm. However, if only the local station sees a step change in these values exceeding a preset threshold, then an alarm is raised.

In terms of data requirement, using Figure 6 as an example, for a fault on the line protected by the device operating CB5, data from CB1, CB2, CB3, and CB4 are used to crosscheck and verify that the operation reflects a true state.

The second level of check in this scheme is the angle check between zero sequence current and negative sequence current to determine the faulted phase. The level of check is made only if the first level does not raise an alarm. Again, an agreement in these values at the protective devices protecting equipment connected to the substation with the faulted line indicates that it was not an attack. Any discrepancy is used to raise an alarm for the operator.

Additionally, a breaker status integrity check is performed using current as an indicator to firmly declare that a breaker is in the open condition.

VI. Results

The proposed schemes are tested using the IEEE 14-bus system and simulated on RTDS software for real-time analysis

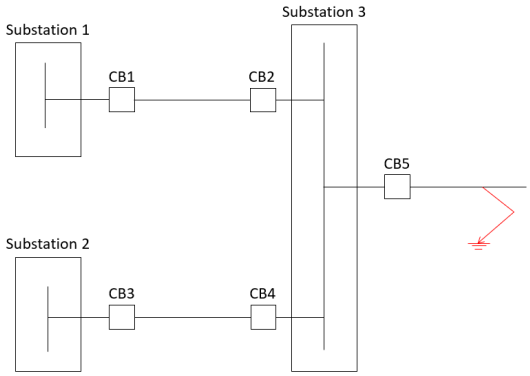

Fig. 6. Trigger Scheme Data Requirements

and validation. A fault is placed at the transmission line between Bus 2 and Bus 3. The normal difference current when there is no attack and the voltage profile at the different buses are as shown in Figure 7 and Figure 8. Figure 9 shows the I0 and I2 angle profile for a SLG fault on A-phase at all the devices looking into bus 2 from the remote substations.

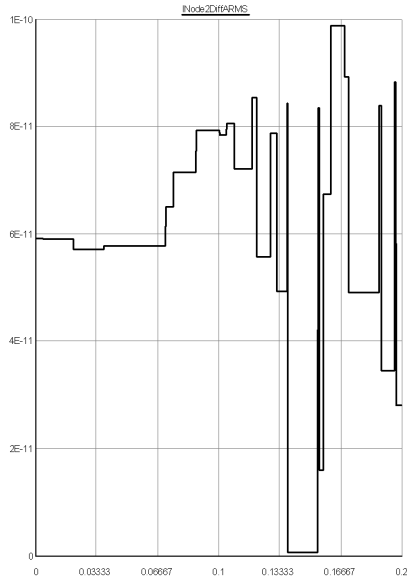

Fig. 7. Difference Current at Bus 2 - No Attack with Fault

A. MITM Attack

For this case, we assume that the attacker has hijacked the connection between the merging unit and the protective device. The attacked has captured a sequence of load data and has replaced this to run in a loop. When a fault occurs or there is a change in load flow, the attack values must be updated. If this is not done, then there will be a difference current measured at the substation. Figure 10 shows the difference current at bus 2 for a fault where the device at bus 2 protecting line 2 to 3 does not react for the fault. The difference current is used to alarm the operator of a potential issue at the substation.

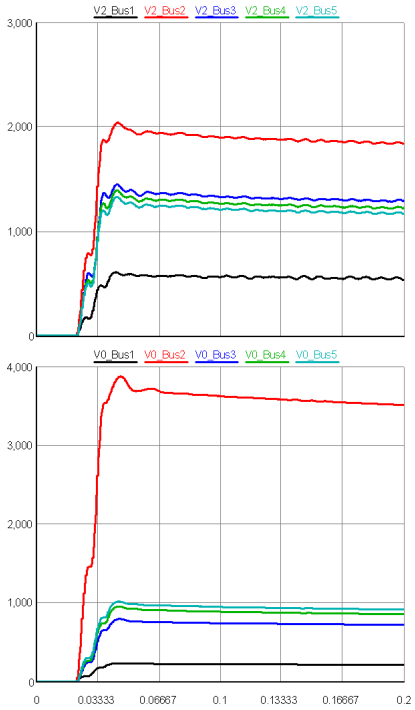

Fig. 8. Voltage Profile at Buses - No Attack with Fault

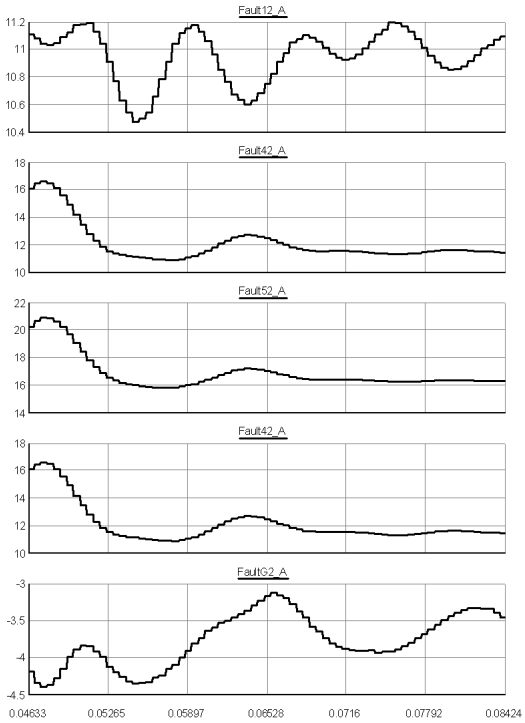

Fig. 9. I0 and I2 Angle Profile - No Attack with Fault

B. Replay Attack

In this case, we consider the same fault but as a replay attack. In this scenario, the current and voltage for the device

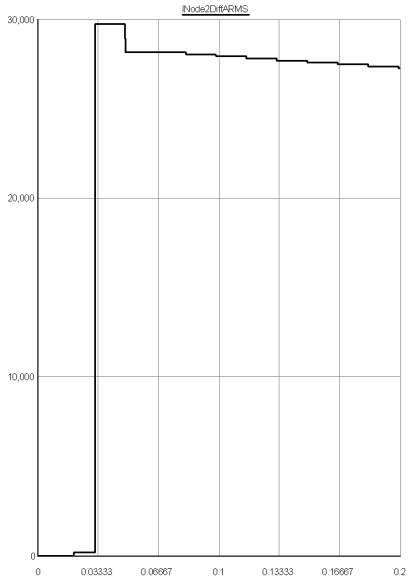

Fig. 10. Difference Current at Bus 2 - Attack with Fault

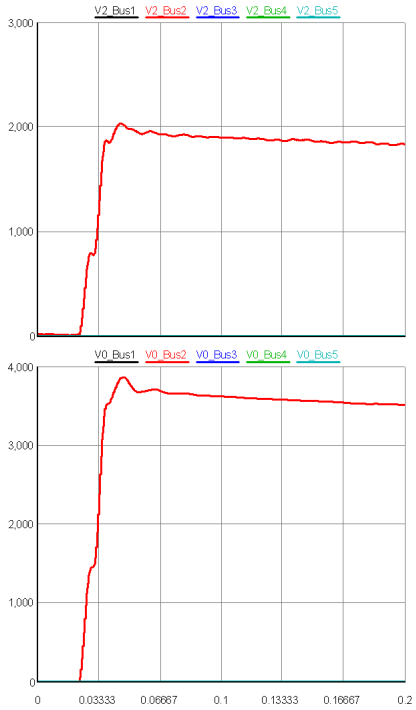

Fig. 11. Voltage Profile at Buses - Attack with Fault

protecting line 2 to 3 is attacked with data from the previous fault. Figure 11 shows the voltage profile during an attack. It can be observed that the zero-sequence and negative-sequence voltage at Bus 2 increases, however, there is no change in the measurements taken at the surrounding substations. This indicates a clear attack.It is observed from the simulation that for an actual fault between Bus 2 and Bus 3, V_0 spikes across all the adjacent buses and has a significant step-change. Whereas, in case of an attack, V_0 spike is only seen on the relay that trips while adjacent relays do not detect any perturbations.

Similarly, the difference current also increases to a high value. Both schemes raise an alarm successfully for this case.

C. Device Settings Integrity Attack

The proposed schemes do not lend themselves well to the detection of a scenario where the attacker has gained super access to the relays and has turned off the protection settings. In this case, both the methods would not raise an alarm as the difference current would be zero and the trigger-based method would never be triggered as the breaker would not open. However, the scheme could be extended to include checks for when a relay at one end trips to make sure that the other end also trips. Additionally, an alarm could be triggered for when the positive sequence voltage is too depressed or negative sequence and or zero sequence voltage is elevated for too long without any action taking place. However, it is likely that backup protection would operate and clear the disturbance before the operator has time to take any action on the alarms.

VII. Conclusion and Future Work

In this project, a continuous monitoring scheme and trigger-based scheme are proposed for the detection of attacks on protection devices. This work documents a proof of concept for the use of physical signature of the power system for a fault. Attacks and potential scenarios were discussed and the operation of the schemes were documented.

The continuous monitoring scheme can be potentially defeated if the attacker has access to all the devices at the local substation and only manipulates a handful of them to make the attack look organic. Further study is required in this context to determine how best the physical signature can be applied to defeat such an attack.

The schemes indicate to the operator that there is something abnormal in the system. It does not make a distinction between whether this is a cyber-attack or a sensor anomaly. This method must be combined with other cyber-attack mechanisms to draw conclusions on how best to classify the event. The operator must investigate whether the cause of malfunctioning is an attack or a genuine error in devices.

The schemes need further adjustment to take in to account topology and devices that could alter the sequence component signature such as series and shunt compensation devices. More detail in the methodology is required to account for these kinds of devices.

Systems with meshed interconnection provide more data that can be used to corroborate events. The application of these schemes on radial systems needs further investigation as the number of additional data sources to corroborate events maybe limited.

These schemes can be further improved by using data mining, machine learning, and deep learning techniques, especially to overcome the non-availability of sensor data. All these are

potential scope for future work based on this proof of concept paper.

REFERENCES

[1] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyberattacks in power systems using heterogeneous time-synchronized data," IEEE Transactions on Industrial Informatics, vol. 11, no. 3, pp. 650–662, 2015. DOI: 10.1109/TII.2015.2420951

[2] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems," IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 436–447, 2017. DOI: 10.1109/TII.2016.2612645.

[3] S. Ntalampiras, "Detection of Integrity Attacks in Cyber-Physical Critical Infrastructures Using Ensemble Modeling," in IEEE Transactions on Industrial Informatics, vol. 11, no. 1, pp. 104-111, Feb. 2015, doi: 10.1109/TII.2014.2367322.

[4] D. Costello, K. Zimmerman,"Determining the Faulted Phase," 63rd Annual Conference for Protective Relay Engineers, March 2010.

[5] 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," in IEEE Transactions on Smart Grid, vol. 8, no. 2, pp. 572-580, March 2017, doi: 10.1109/TSG.2016.2545683.

[6] A. Ashok, M. Govindarasu and J. Wang, "Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid," in Proceedings of the IEEE, vol. 105, no. 7, pp. 1389-1407, July 2017, doi: 10.1109/JPROC.2017.2686394.