Les Cahiers du GERAD ISSN: 0711–2440

Elements of networked protection systems for distribution networks and microgrids: A cyber-security perspective

Y. Seyedi, H. Karimi,
S. Grijalva, B. Sansò

G–2020–10

January 2020

GERAD HEC Montréal
3000, chemin de la Côte-Sainte-Catherine
Montréal (Québec) Canada H3T 2A7

Tél. : 514 340-6053
Téléc. : 514 340-5665
info@gerad.ca
www.gerad.ca

Elements of networked protection systems for distribution networks and microgrids: A cyber-security perspective

Younes Seyedi [a,b]

Houshang Karimi [b]

Santiago Grijalva [c]

Brunilde Sansò [a,b]

[a] *GERAD, Montréal (Québec), Canada, H3T 2A7*

[b] *Department of Electrical Engineering, Polytechnique Montréal (Québec) Canada, H3C 3A7*

[c] *School of Electrical and Comuter Engineering, Georgia Tech, VL E284, Atlanta, USA*

younes.seyedi@polymtl.ca
brunilde.sanso@polymtl.ca

January 2020
Les Cahiers du GERAD
G–2020–10

Abstract: Networked protection systems use information, communication and computation technologies to collect and process sensor data from spatially distributed sensors, and launch protective and control actions by sending commands to local devices. Such protection systems are also capable of supporting specialized tasks including asset control and backup protection in case of traditional relaying failures. This paper explains the structure and the fundamental elements of the networked protection systems in distribution systems and microgrids. The overall system is divided into three subsystems which are interconnected by communication systems. Different types of cyber-attacks on the subsystems and their impacts are discussed from the vantage point of protection. False and delayed tripping, non-detection, cascading failures, and unstable operation of distributed energy resources (DERs) are discussed as the critical issues that can be related to cyber-attacks.

1 Introduction

Smart grids utilize emerging technologies such as advanced metering infrastructure (AMI), synchrophasors, distributed energy resources (DERs), energy storage systems (ESSs), information and communication systems [1]. In smart grids, smart meters and phasor measurement units (PMUs) are specialized sensors that extract useful data from distribution systems and microgrids and transmit them to different applications via communication systems. Specifically, smart meters use two-way communications to exchange power consumption and other quantities between the consumers and the utility management systems [2]. Distribution level PMUs, a.k.a. microPMUs, use communication systems to deliver accurate synchrophasor data including voltage and current phasors, frequency, rate-of-change-of frequency, etc. to distribution substations and to control centers [3].

The distribution substations can host data-driven applications to process the sensor data and derive models, extract dynamical features, take preventive and remedial actions and improve situational awareness. Moreover, the availability of PMU data in distribution networks and microgrids facilitates development of new protection systems that enhance fault detection and isolation with high degree of flexibility and low cost [4]. Moreover, data-centric applications in smart grids are capable of employing artificial intelligence (AI) techniques to detect and classify faults [5], predict outage events [6], and provide insight into the root causes of the events [7]. It should be underscored that the reliability and efficacy of such protection applications rely on the integrity and quality of data as well as on fast and secure communications [8]. Motivated by the above facts, cyber security issues and cyber attack detection in smart grids have been discussed in several papers [9]–[11].

The cyber-security aspects of synchrophasor communications have been investigated in several papers [12]–[14]. The authors in [12] focus on adverse synchrophasor packet dropouts by the attackers who gain control of routers in the communication system. In [13], the software-defined networking technology is employed to restore the synchrophasor datasets when the phasor data concentrator (PDC) is compromised by the attackers. An optimal IP multicast tree construction method is developed in [14] that minimizes the likelihood of cyber attack propagation between PMUs.

It is known that, synchrophasor data that are collected from spatially distributed PMUs can support a wide range of monitoring, control and protection applications simultaneously. In addition, wide area measurement systems (WAMSs) depend on the synchrophasor technology, hence, they become vulnerable to cyber-attacks on the PMUs and the PDCs. Recently, attempts have been made to improve the resiliency of synchrophasor-based monitoring and control applications under cyber-attacks. For instance, power system state estimation and its associate cyber security concerns are well discussed in [15]–[18]. Detection and mitigation of cyber-attacks in WAMSs are investigated in [19]–[21].

Centralized and hierarchical protection schemes are special cases of the networked protection systems and are discussed in [22]–[24]. The main objective of these networked protection systems is to overcome important protection challenges raised by integration of renewable energy sources in microgrids and active distribution networks (ADNs). However, the cyber security of such protection systems is not fully addressed by the existing literature.

The main objective of this paper is to describe the fundamental elements of networked protection systems and their cyber security in smart microgrids and ADNs. The contributions of the paper are as follows: 1) The cyber security aspects of the networked protection systems are discussed. 2) The negative impacts of different cyber-attacks on the system components are explained. The paper is concluded by summarizing the technical challenges that may be addressed by future research.

2 Elements of networked protection systems

The overall structure of networked protection systems can be divided into three interconnected subsystems where each subsystem hosts several key elements. The main components of data-driven and networked protection systems in ADNs and microgrids are shown in Figure 1 and explained in the sequel:

1. **Data acquisition subsystem**: consists of sensors which extract and transmit data (e.g., microPMUs, smart meters, SCADA) and data collectors which gather/align the sensor data (e.g., PDC, meter data concentrators).
2. **Data processing and application subsystem**: consists of data-centric applications that process the collected sensor data and perform decision making to fulfill fault detection, localization, control of protective devices and other auxiliary functions.
3. **Local control and protection subsystem**: consists of smart grid assets such as protective and control devices that can trigger an action upon receiving commands from the applications. These devices can be local controllers/actuators located in DERs or ESSs. Intelligent electronic devices (IEDs) and relays belong to this subsystem as these protective devices can control opening and closing of circuit breakers and switches.

The communication links are essential for transfer of sensor data and control/protective commands between different components of the protection system. The protocol (e.g., UDP/IP, TCP/IP, etc.), technology (e.g., wireless, power line communications, fiber, etc.) and the bandwidth of the communication links should be determined by considering important factors including the type and location of sensors, the data reporting rate, communication latency, security and reliability. Heterogeneous links can be used for communications in networked protection systems. For example, PMUs often use UDP/IP for streaming of synchrophasor packets to the PDC while TCP/IP is preferred for control links that connect the applications to the smart grid assets [25].

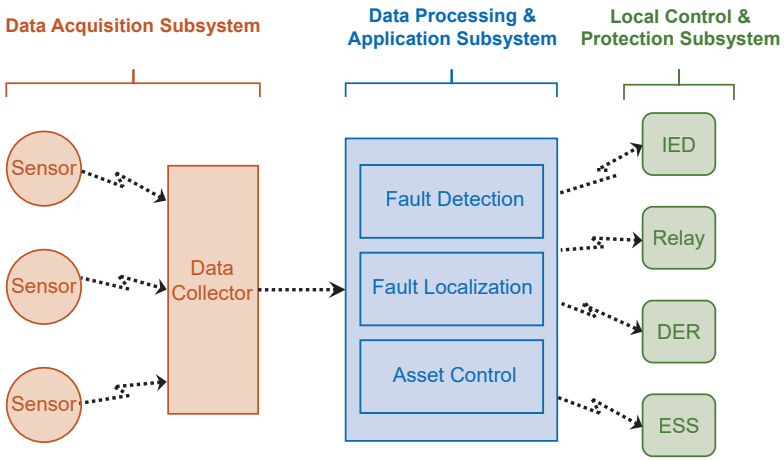

Figure 1: Main components of networked protection systems in smart distribution grids and microgrids. The dotted arrows indicate communication links

3 Cyber attacks on data acquisition subsystem

The sensors and data concentrators are the constituent elements of the data acquisition subsystem and can be adversely affected by different types of cyber-attacks.

Spoofing and tampering attacks on the sensors aim to delete/change the contents of data packets or modify the parameters of the sensors. These attacks directly affect the sources of the data/information in microgrids and ADNs. For example, PMUs and PDCs are vulnerable to GPS spoofing attacks that interfere with the GPS signals. The GPS spoofing attacks affect the time synchronization of the measurements and lead to significant errors in the reported phase angle data. This type of measurement error can be highly detrimental to differential protection schemes.

False data injection (FDI) attacks can maliciously change the values of the measurements in the data packets by gaining access to the communication routers or the hardware of the sensors. For example, the attacker can drastically increase the measured magnitudes of the line currents to create a

false over-current event and trigger unwanted line tripping. Since the PMUs report the instantaneous frequency of the network, an incorrect frequency data injected by the attacker may trigger over/under -frequency protection schemes, lead to disconnection of DERs and ESSs and even unwanted islanding event in microgrids. It should be noted that the FDI attacks on synchrophasor networks can be intelligent such that they are not detectable by advanced PDCs that employ bad data detectors.

In synchrophasor networks, the attacker can change important parameters of the PMUs such as the reporting rate and the transmission protocol. For example, the attacker can hinder the overall system response by reducing the reporting rate of synchrophasors from 120 frames-per-second (fps) to 10 fps for one or more PMUs. The attacks on the reporting rate lead to several data losses and thus frequent not-a-number (NaN) indicators appear at the output datasets of the PDC, as shown in Figure 2(a). It should be noted that such cases of missing data cannot be reliably recovered by data recovery methods that may be employed by advanced PDCs.

Cyber attacks that target the parameters of the data concentrators are the most harmful ones than can take place in the data acquisition subsystem as these devices manage and process the data transmitted from multitude of sensors. For instance, the PDC data aggregation logic (absolute or relative waiting time strategy) and the PDC waiting time can be maliciously changed by the attacker to create significant and prolonged data losses (NaN sequences) in all PMU channels, as illustrated in Figure 2(b). This type of attack can lead to non-detection of faults as the spatio-temporal properties of the synchrophasor datasets are completely compromised and the synchrophasor data become useless for decision making.

Other types of cyber-attacks such as denial of service (DoS) and man-in-the-middle (MITM) can also target the data acquisition subsystem. The DoS attacks may delay or stop the transfer of measurements between the sensors and the data concentrator by limiting the communication resources. Therefore, the primary impact of the DoS attacks on the data acquisition subsystem can be envisaged as significant missing data at the output of the data concentrator. This may result in delayed detection/isolation of faults, cascading contingencies, and failures of smart grid assets. The MITM attacks on the data acquisition subsystem secretly play the role of a data concentrator, receive original measurements from the sensors, and relay datasets to the application subsystem which contain misleading or missing data. Hence, the MITM attacks are capable of triggering a false trip of circuit breakers besides preventing faults from being detected by the applications.

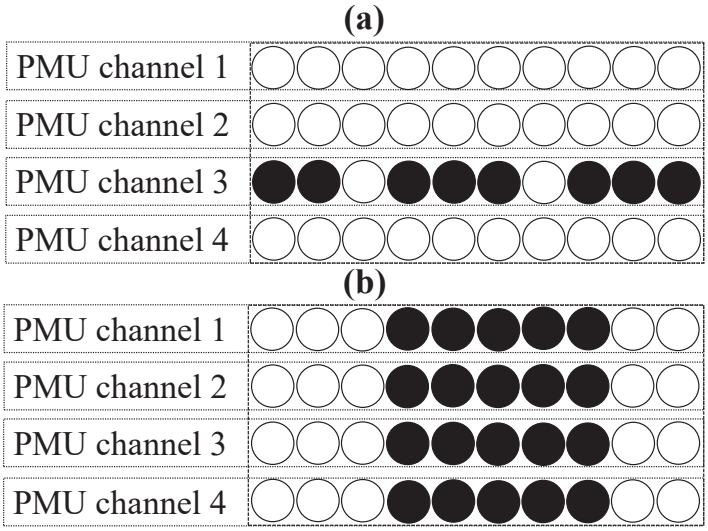

Figure 2: The missing data at the output datasets of the PDC over 10 reporting intervals. NaN indicators are shown as filled circles: (a) The reporting rate of PMU 3 is changed by the attacker (b) The PDC waiting time is decreased by the attacker

4 Cyber attacks on the data processing and application subsystem

The application subsystem consists of several data-driven functionalities that aim to detect, localize, and properly respond to the faults by remote control of the grid assets. Once the faults are detected and localized, the networked protection system should ensure that the faulty part of the grid becomes isolated before the DERs, loads, or ESSs reach their unstable conditions. The fault isolation can be carried out by either local protective devices (e.g., over-current relays) or by the networked protection system. The protection system may send trip commands to relays and IEDs or disconnection commands to the DERs and ESSs before a critical time is elapsed.

The applications can be tampered with cyber-attacks that maliciously modify the parameters of the models, inject false control commands, and deter the asset control. It turns out that, the cyber-attacks that target the application subsystem can lead to a wide range of harmful events in terms of protection and control of microgrids and ADNs. For example, the attacker can disable the fault isolation functionality of the application subsystem by changing the destination IP address of the control packets. Moreover, adversary attacks can bring about physical damage to DERs and ESSs by preventing their disconnection from the network in the presence of persistent faults. It should be noted that, attacks on the application subsystem can potentially cause cascading failures by simultaneously sending false protective commands to assets at different locations. It is worth mentioning that false command injection (FCI) attacks on the application subsystem are analogous to the FDI attack on the data acquisition subsystem.

5 Cyber attacks on local control and protection subsystem

The local control and protection subsystem involves protective and control devices such as local controllers at DERs and ESSs, IEDs, relays, etc. In the framework of networked protection, the controllable devices respond to the faults upon receiving the commands from the application subsystem. The transmission rate and the payload size of the control packets are significantly lower than those of the data packets generated by the data acquisition subsystem. Therefore, it is possible to choose communication links with a lower bandwidth and a higher reliability to connect the application subsystem to the device channels with different priorities.

The local control and protection devices are vulnerable to cyber-attacks since they are connected to the communication systems for exchange of information with the application subsystem for hierarchical control and protection purposes. The assets under cyber-attacks may not operate properly when the grid is subject to a permanent fault. The attacker can modify the device parameters in such a way that the device does not respond to the control/protective commands sent from the application subsystem. In addition to equipment damage, this type of attack can also harm people physically and may lead to unstable operation of DERs.

6 Conclusion and future works

The integration of information and communication technologies with power systems paves the way for development of advanced control and protection applications in ADNs and smart microgrids. Networked protection systems are capable of providing backup and hierarchical protection services that aim to enhance fault detection and isolation under high penetration of renewable energy sources. Such protection systems are essentially data-driven and rely on communication systems for exchange of data and control/protective commands.

In this paper, the main elements of the networked protection systems are classified in three subsystems. The data acquisition subsystem deals with collecting the necessary data that assist fault detection and accommodation. The data processing and application subsystem is concerned with the processing of the acquired data, extracting actionable information and performing decision-making

tasks. In the local control and protection subsystem, different protective and control devices are responsible for executing the received commands.

Inevitably, the networked protection systems may be exposed to cyber-attacks that result in protection issues, power outages, and harmful failures. Therefore, it is of crucial importance to provide strategies for cyber security of the protection systems. Table 1 summarizes the elements of networked protection systems and lists the associate cyber-attacks along with their major consequences for microgrids and ADNs.

Table 1: Different elements of networked protection systems and the associate cyber-attacks

Subsystem	Components	Cyber-attacks	Major consequences
Data Acquisition	PMUs, PDCs, SMs, SCADA, data concentrators, auxiliary sensors	GPS spoofing Device tampering DoS FDI MITM	Sequences of missing data Delayed trips False detection False trips Non-detection
Data Processing and Application	Fault detection, localization, asset control	Application tampering Change of model parameters False command injection	False detection Non-detection False trips Cascading failures Unstable operation of DERs
Local Control and Protection	IEDs, relays, DERs, ESSs, controllable switches and loads	Device tampering	False trips Equipment failures Unstable operation of DERs

Despite the recent advances in smart grid cyber security, detailed investigation of cyber-attacks on the networked protection systems requires further research. Specifically, elaborate methods based on machine learning techniques can be devised for detection of cyber-attacks on different subsystems of the networked protection system. Moreover, new countermeasures against cyber-attacks should be developed to increase reliability and resiliency of protection systems in smart grids.

References

[1] E. Y. Song, G. J. FitzPatrick, and K. B. Lee, Smart sensors and standard-based interoperability in smart grids, IEEE Sensors Journal, 17(23):7723–7730, Dec. 2017.

[2] J. Lloret, et al., An integrated IoT architecture for smart metering, IEEE Communications Magazine, 54(12):50–57, Dec. 2016.

[3] H. Mohsenian-Rad, E. Stewart, and E. Cortez, Distribution synchrophasors: pairing big data with analytics to create actionable information, IEEE Power and Energy Magazine, 16(3):26–34, May–June 2018.

[4] Y. Seyedi, and H. Karimi, Design of networked protection systems for smart distribution grids: A data-driven approach, in Proc. of IEEE Power Energy Society General Meeting, pp. 1–5, Jul. 2017.

[5] T. S. Abdelgayed, W. G. Morsi, and T. S. Sidhu, Fault detection and classification based on co-training of semisupervised machine learning, IEEE Trans. Indust. Electron., 65(2):1595–1605, Feb. 2018.

[6] T. Dokic, et al., Spatially aware ensemble-based learning to predict weather-related outages in transmission, in Proc. of Hawaii International Conference on System Sciences, pp. 3484–3493, Jan. 2019.

[7] E. Hossain, et al., Application of big data and machine learning in smart grid, and associated security concerns: A review, IEEE Access, 7:13960–13988, Jan. 2019.

[8] S. Meliopoulos, et al., Cyber security and operational reliability, in Proc. of Hawaii International Conference on System Sciences, pp. 1–9, Jan. 2015.

[9] C. Beasley, et al., A survey of electric power synchrophasor network cyber security, in Proc. of IEEE PES Innovative Smart Grid Technologies Europe, pp. 1–5, Oct. 2014.

[10] T. H. Morris, S. Pan, and U. Adhikari, Cyber security recommendations for wide area monitoring, protection, and control systems, in Proc. of IEEE Power and Energy Society General Meeting, pp. 1–6, Jul. 2012.

[11] C. Tun, et al.,Cyber-attacks in PMU-based power network and countermeasures, IEEE Access, 6:65594–65603, Oct. 2018.

[12] S. Pal, B. Sikdar, and J. H. Chow, An online mechanism for detection of gray-hole attacks on PMU data, IEEE Trans. Smart Grid, 9(4):2498–2507, Jul. 2018.

[13] H. Lin, et al.,Self-Healing Attack-Resilient PMU Network for Power System Operation, IEEE Trans. Smart Grid, 9(3):1551–1565, May 2018.

[14] R. Kateb, et al.,Optimal tree construction model for cyber-attacks to wide area measurement systems, IEEE Trans. Smart Grid, 9(1):25–34, Jan. 2018.

[15] S. Pal, B. Sikdar, and J. H. Chow, Classification and detection of PMU data manipulation attacks using transmission line parameters, IEEE Trans. Smart Grid, 9(5):5057–5066, Sep. 2018.

[16] H. Lin, et al., Cyber security impacts on all-PMU state estimator —A case study on co-simulation platform GECO, in Proc. of IEEE Third International Conference on Smart Grid Communications, pp. 1–6, Nov. 2012.

[17] Q. Yang, et al.,PMU placement in electric transmission networks for reliable state estimation against false data injection attacks, IEEE Internet of Things Journal, 4(6):1978–1986, Dec. 2017.

[18] A. Mohammadi, and K. N. Plataniotis,Noncircular attacks on phasor measurement units for state estimation in smart grid, IEEE Journal of Selected Topics in Signal Processing, 12(4):777–789, Aug. 2018.

[19] H. M. Khalid, and J. C.-H. Peng, A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks, IEEE Trans. Smart Grid, 7(4):2026–2037, Jul. 2016.

[20] A. S. Musleh, et al., A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications, IEEE Sys. J., 13(1):710–719, Mar. 2019.

[21] J. Wang, et al.,Distributed framework for detecting PMU data manipulation attacks with deep autoencoders, IEEE Trans. Smart Grid, 10(4):4401–4410, Jul. 2019.

[22] M. M. Eissa,Challenges and novel solution for wide-area protection due to renewable sources integration into smart grid: an extensive review, IET Renewable Power Generation, 12(16):1843–1853, Nov. 2018.

[23] M. M. Eissa, A novel centralized wide area protection "CWAP" in phase portrait based on pilot wire including phase comparison, IEEE Trans. Smart Grid, 10(3):2671–2682, May 2019.

[24] Y. Seyedi, and H. Karimi,Coordinated protection and control based on synchrophasor data processing in smart distribution networks, IEEE Trans. Power Syst., 33(1):634–645, Jan. 2018.

[25] Y. Seyedi, H. Karimi, and J. M. Guerrero, "Centralized disturbance detection in smart microgrids with noisy and intermittent synchrophasor data," IEEE Trans. Smart Grid, 8(6):2775–2783, Nov. 2017.