DOI: http://dx.doi.org/10.14236/ewic/ICS2016.9

Data Integrity Attacks in Smart Grid Wide Area Monitoring

Sarita Paudel and Paul Smith
AIT Austrian Institute of Technology
Vienna, Austria
sarita.paudel, paul.smith@ait.ac.at

Tanja Zseby
TU Wien
Vienna, Austria
tanja.zseby@tuwien.ac.at

A smart grid requires the implementation of ICT technologies in order to incorporate new functions into electricity grid monitoring and control. Wide Area Monitoring Systems (WAMSs) are used to measure synchrophasor data at different locations and give operators a near-real-time picture of what is happening in the system. The measurement data is periodically collected via communication channels to monitor, predict and control the power consumption, and detect any problems in the power grid. Attacks on WAMSs can trigger wrong decisions and create dangerous failures in the smart grid system. In this paper, we investigate data integrity attacks at different attack entry points of a WAMS, their impacts on the smart grid system, and existing mitigation strategies. We conclude from our study that the existing techniques, methodologies and mechanisms are not effective enough to detect or mitigate some attacks.

Keywords: Cybersecurity, Data Integrity Attacks, Failure Scenarios, Wide Area Monitoring System

1. INTRODUCTION

Smart grids improve the efficiency of the traditional power grids by adopting modern communication and control technologies. Different devices from various vendors are connected in multiple layers, and establish communication using proprietary or open standard protocols. Though integration of ICT helps power grids to be smarter, it introduces security issues. Attackers can perform malicious cyber attacks using existing vulnerabilities in smart grid devices. Different devices, communication channels between the devices, hardware, software, and many more components in a smart grid might be compromised to perform successful cyber attacks. Attackers also can gather information by sniffing communication networks and use the information for attack preparation. Data integrity attacks on WAMSs can lead to incorrect control decisions and actions.

Situational awareness (Jajodia *et al.* (2010)) relates to the perception of environmental changes with respect to time or space, and projection of the status after changes. Sharing of information is one aspect of situational awareness. Information about threats, vulnerabilities and indicators of compromise is a valuable good for system administrators of complex and interconnected ICT systems. WAMSs improve situational awareness in smart grids and provide information to prevent critical incidents (Zseby and Fabini (2014)). They also support planning and grid operation optimization. WAMSs collect clock-synchronized measurement values from widely distributed Phasor Measurement Units (PMUs), and provides input to various applications in the grid, e.g., as direct input to control functions, feedback in control loops, or stored for future planning and post-incident analysis. The measurement values are processed and decisions regarding appropriate grid control actions are made in the Control Center (CC). As a consequence, utilities are affected by the decisions in the CC.

WAMSs constitute a suite of different solutions consisting of various combinations of components, such as Intelligent Electronic Devices (IEDs), Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs and super PDCs), communication equipment, applications, visualization tools and many more (Kezunovic *et al.*). In Bobba *et al.* (2012) the NASPInet concept of Phasor Gateways (PGWs) is described. PGWs offer a publish-subscribe framework for sharing phasor measurements among different utilities or control centers. Therefore, WAMSs integrate many different components in different topological settings (Searle *et al.* (2016)), and all devices can be entry points for attacks.

In this paper, we investigate the various possibilities of data integrity attacks at different points in a

WAMS. For this we use a generic model of a WAMS that comprises all possible components that could be presented in the system. We consider different attack entry points and elaborate on the consequences for attackers and mitigation strategies.

This paper is structured as follows: in Section 2, we describe the hierarchical structure and communication protocols of WAMSs, Section 3 describes problems and technical deployment issues, Section 4 describes different attack scenarios and our assumptions in this paper, and in Section 5, we classify, categorize and describes existing techniques and describe how they help us to detect attacks that are mentioned in Section 4.

2. WIDE AREA MONITORING STRUCTURE

Most WAMSs have a hierarchical structure and consist of PMUs, PDCs, Super PDCs (Zuo *et al.* (2008)), Phasor Gateways (PGWs), and communication facilities to transfer data between these components and a control center (CC) (Phadke and Thorp (2008)). PMU measurements are time-stamped at the source using the global positioning system (GPS) to ensures clock synchronization.

Regional or organizational PDCs gather data from different PMUs, sort the data according to the timestamps, create a combined record and forwards the combined records up in the hierarchy. Local storage facility, data verification and application functions are usually available in PDCs.

Another possible level of hierarchy is super data concentrators (SDCs), also called super PDCs. Super PDCs have similar functions to regional PDCs but there is a facility for data storage of data aligned with time-tags (at a somewhat increased data latency), as well as a steady stream of near realtime data for applications which require data over the entire system (Phadke and Thorp (2008), Wang *et al.* (2009)).

Furthermore, it is possible to deploy Phasor gateways (PGWs). PGWs are introduced by NASPI as a concept to interconnect multiple organizations. PDCs or PMUs report their data to the PGW. A PGW then communicates the data to other PGWs by a publish-subscribe system. PGWs can support Quality of Service functions and serve as security gateway between organizations. At the top level, a CC is connected via a WAN and controls all activities regarding monitoring, protection, and control. Since PMUs may also directly report to a CC, all hierarchy levels (PDC, Super PDC, PGW) are optional. We call all systems on the way from PMU to CC (PDC, Super PDC, PGW, core and access routers) intermediate systems.

Mostly data flow is upwards in the hierarchy from PMUs to the CC, but commands (e.g., for device configuration), requests (e.g, requesting data formats or device information) or software updates require communication in the reverse direction. PMU messages are transferred using TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) over IP or can also be transmitted directly over Ethernet or other available transport means (Wang *et al.* (2009)). In addition to the measurement data reported from PMUs to PDCs, also configuration files with data interpretation settings can be reported to PDCs. Furthermore, PDCs can send command files to PMUs to request information (Phadke and Thorp (2008)). All these files have a common structure.

2.1. Technical Deployment Issues

For WAMS communication different communication protocols are used from different standards. Figure 1 shows an overview of some standards used for end-to-end communication and the following paragraphs describe them briefly.

Standard IEC 61850 (IEC-61850) is a communication protocol that facilitates utility automation including protection and control (CISCO (2010)). Originally, it was developed for IEDs in substations, but now it covers a variety of communication features (Adamiak *et al.* (2010)). It defines an architecture and data models for communication in electric power systems. Abstract data models defined in this standard can be mapped to a number of protocols, for example, some mappings are to Generic Object Oriented Events (GOOSE), Generic Substation Events (GSE), and Sampled Measured Values (SMV) (IEC Geneva (2007)). It supports sending of real-time data and supervisory control functions using Manufacturing Message Specification (MMS) over TCP/IP and transmission of GOOSE over Ethernet within substation LANs.

IEC 61850-90-1 (IEC-TR-61850-90-1 (2016)) provides guidelines of using IEC 61850 for the communication between substations. Similarly, EN IEC 61850-90-1/5 and IEC 61850-8-1 provide guidelines for communication between PMUs and PDCs inter substations. IEC 61850-90-4 provides guidelines for communication inside a substation. IEC 61850-90-2 (IEC-TR-61850-90-2 (2016)) covers using IEC 61850 standard for the communication between substations and control centers (CENELEC (2012)).

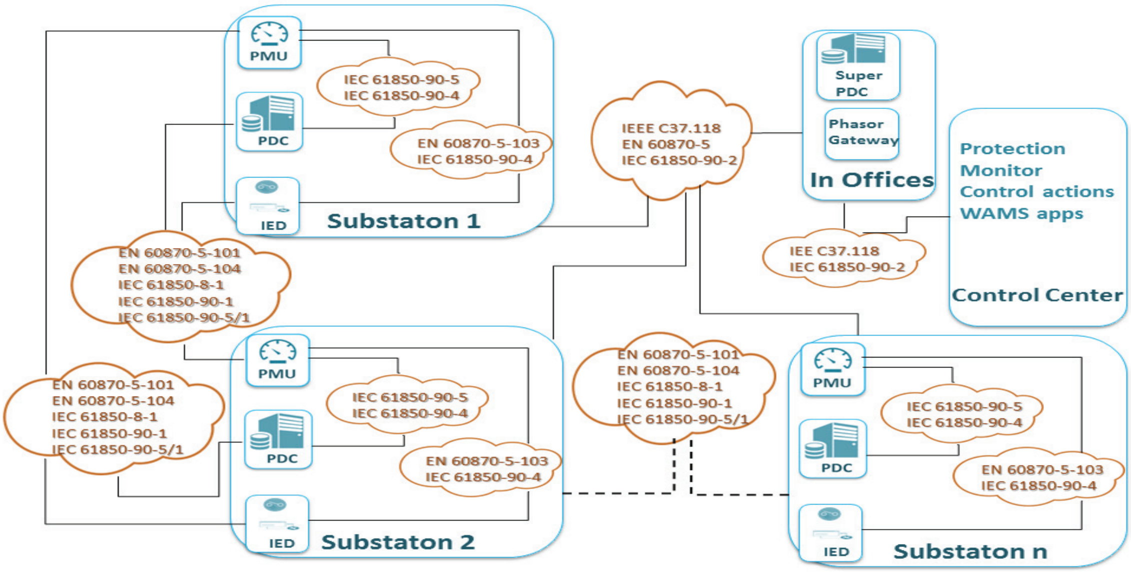

Figure 1: *WAMS Communication Protocols.*

Standard EN 60870-5-103 (IEC-60870-5-103) provides guidelines for connecting PMUs/IEDs inside a substation. EN 60870-5-101 (IEC-60870-5-101) provides transmission procedures between substations. Similarly, EN 60870-5-104 (IEC-60870-5-104) is an extension of standard EN 60870-5-101 and provide guidelines between PMUs and data concentrators between substations (CENELEC (2012)). An overview of the use of these protocols is presented in Figure 1.

Standard IEC 62351 is developed for securing the communication protocols that are defined in IEC 60870-5 and the IEC 61850 series of standards (IEC-62351-1 (2007)). IEC 62351-6 (IEC-62351-6 (2007)) defines the security of IEC 61850 profiles by specifying messages, procedures, and algorithms for securing the operations of all protocols that are derived from the standard IEC 61850. The specification applies at least to the protocols IEC 61850-8-1, IEC 61850-9-2 and IEC 61850-6. It also provides security for profiles not based on TCP/IP, e.g., GOOSE, GSSE (Generic Substation Status Event) and SMV. The IEC 61850 profile using MMS over TCP/IP uses IEC 62351-3 and IEC 62351-4.

PGWs support IEEE C37.118 for phasor data traffic (e.g., traffic to and from PDCs, super PDCs and PGWs), but it is not enough for additional control and administrative traffic beyond the PGW (Chassin *et al.* (2008)). IEEE C37.118.1 (IEEE-C37.118.1 (2011)) specifies measurements of synchrophasor, and EEE C37.118.2 (IEEE-C37.118.2 (2011)) describes a protocol for the real time transfer of phasor data. It defines data messages, configuration messages, header messages and command messages that are required for communication (Zseby *et al.* (2013)).

3. PROBLEM STATEMENT

WAMSs use synchrophasor technology and different devices to generate, receive and utilize synchrophasor data (Searle *et al.* (2016)). Such devices are vulnerable to various security threats. Attackers can compromise devices by leveraging the vulnerabilities in the system. The impact of failures and attack scenarios in a WAMS is dependent on the use of wide area monitoring, protection and control data (NESCOR and TWG1 (2013)). For example, if a wide area monitoring, protection and control application is used to make control decisions, failures in such applications can cause higher impact than a failure in an application used only for monitoring.

PMUs, IEDs, PDCs, super PDCs, PGWs and various network components are connected to support communication between the devices and applications that are used in a WAMS. Attacks on a device, either hardware or software-based, at different points in the WAMS have different levels of impact. A number of attack scenarios are presented in Section 4, which examine these impacts.

In this study, we focus on data integrity attacks that modify measurement data, either the original readings from PMUs or aggregated data (or just events) from PDCs, Super PDCs or PGWs. After processing falsified data, the WAMS may estimates inaccurate states of the power system. The impact can be wrong decisions such as triggering protection elements if not needed or suppress a vital protective action. For example, due to modified measurement data the system may believe that overloaded branches have secure voltage and vice versa (Dehghani *et al.*). It can also cause delay in taking actions, e.g., for load shedding or grid reconfiguration. System delays in other utilities can lead to cascading failures across utilities (NESCOR and TWG1 (2013)) and to equipment damage.

Currently, we have situations where smart attackers can perform successful attacks that are not detected in a WAMS. For example, modified values in one part of the system are not detected in other part of the WAMS. These smart attacks can cause catastrophic failures. We are looking at solutions for such undetected data attacks by smart attackers.

3.1. Assumptions

Our threat model mainly considers the problem of compromised machines in a WAMS: PMUs, PDCs, Super PDCs, PGWs and routers in the path. We consider intrusions that concern both physical power systems, as well as communication networks. For example, intrusions in PMU devices (physical components) and in their embedded software (cyber part). We suppose that software and hardware of WAMS components, as any other systems, are not free from vulnerabilities and assume that an attacker gains access to a WAMS component using any kind of exploit. Furthermore, attackers may have physical access to systems in the field. We concentrate only on data integrity attacks on the measurement data itself. So, we consider only the data flow from the sensors (PMUs) towards the data collection (CC), and do not consider data integrity attacks on the control data that is sent to IEDs.

In general, we assume that if a device is compromised that the attacker has access to all data including cryptographic keys on the system[1]. That means the attacker can generate valid message authentication codes or digital signatures for the measurement data and also can encrypt and decrypt data with the appropriate keys. But this applies only for the end-to-end communication. Devices on the path that are not configured to access or modify the data (e.g., access or core routers) do not have access to appropriate keys. If measurement data is integrity protected and encrypted, attacks on such intermediate devices such as routers are limited to data dropping or duplication attacks. Routers may also delay data in a way that they arrive too late to contribute to control applications. Attacks to routing protocols or those directed to the CC are out of scope of this paper. Also attacks on the clock synchronization system, required in a WAMS, are not considered in this paper.

4. ATTACK SCENARIOS

NESCOR have investigated cybersecurity failure scenarios that result in a failure to maintain the Confidentiality, Integrity and Availability (CIA) of cyber assets, which have a negative impact on generation, transmission, and delivery of power. They provide a set of failure scenarios, prioritize them and develop detailed information for the scenarios with the highest priority (NESCOR and TWG1 (2013)). We study the NESCOR failure scenarios related to wide area monitoring, taking them as basis to derive six failure scenarios that are related to PMUs, PDCs, super PDCs, PGWs, access routers and core routers in a WAMS. We also describe the WAMS's response to the scenarios and their impact on the system. Key components and attack points of a WAMS are shown in Figure 2.

Scenario 1 - PMU compromised: In this scenario an attacker gains access to a PMU and forges PMU frames with wrong data. The frames with wrong information are then sent to a PDC or CC. Such an attack is, for instance, described in (Dehghani *et al.*). If we have PGWs in the network, then frames can also be sent directly to a PGW. We separate this scenario into three cases, based on how a PMU reports falsified data up in the hierarchy.

- *Case 1:* PMUs have a PDC as data aggregation point. A local or regional PDC aggregates the falsified data and sends it up in the hierarchy.
- *Case 2:* PMUs are connected directly to a PGW. Falsified data are sent directly to a PGW, which shares information with other PGWs.
- *Case 3:* PMUs are connected directly to a CC. Falsified data are directly sent to a CC. Due to the lack of an aggregation step, the severity of damage in this case could be higher than in the other cases.

Scenario 2 - PDC compromised: Although access control and connection authentication between a PDC and a PMU are already considered in some protocols (IEC-61850), PDCs may be compromised due to a backdoor or an attack to an authentication database. An attacker can get access to the database in the PDC and modify or steal the information that allows malicious introduction of false measurement data (NESCOR and TWG1 (2013)). A PDC can be connected to other regional PDCs, super PDC, PGW or directly to the CC. We have

[1] In well-secured systems keys may be stored in a separated trusted platform.

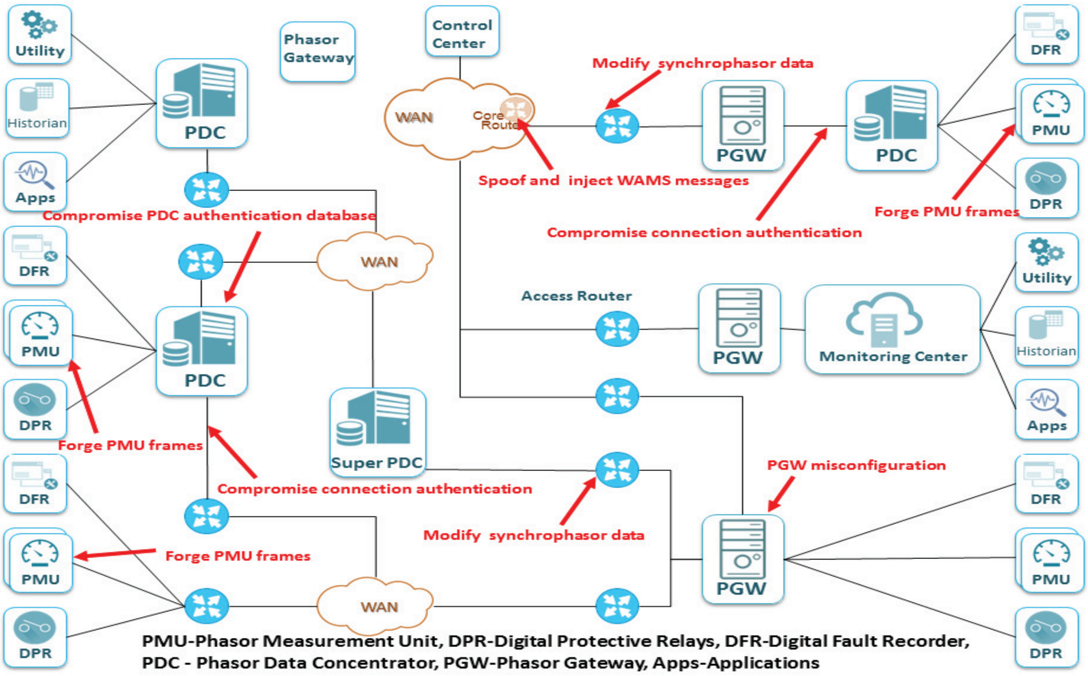
Utility
Historian
Apps
PDC
Phasor Gateway
Control Center
WAN
Core Router
Modify synchrophasor data
PGW
PDC
DFR
PMU
DPR
Spoof and inject WAMS messages
Forge PMU frames
Compromise PDC authentication database
Compromise connection authentication
DFR
WAN
Utility
Access Router
PGW
Monitoring Center
Historian
PMU
PDC
DPR
Apps
Forge PMU frames
Super PDC
PGW misconfiguration
Compromise connection authentication
DFR
DFR
Modify synchrophasor data
PMU
Forge PMU frames
PGW
PMU
WAN
DPR
DPR
PMU-Phasor Measurement Unit, DPR-Digital Protective Relays, DFR-Digital Fault Recorder,
PDC - Phasor Data Concentrator, PGW-Phasor Gateway, Apps-Applications

Figure 2: *WAMS with key components, compromised points and attacks.*

four cases depending on how a PDC sends false measurement data to other components in a WAMS.

- *Case 1:* The PDC sends false measurement to another PDC, which then processes the false measurement values.
- *Case 2:* The PDC sends false measurement to a Super PDC.
- *Case 3:* The PDC sends false measurement values directly to a PGW. The PGW shares the false information to other PGWs.
- *Case 4:* The PDC sends false measurement values directly to a CC. The CC uses the falsified information as inputs in the applications.

Impacts of such attacks can be a failure to take actions when needed, improper synchronous closing, leading to equipment damage, a line trip leading to cascading failures and many more (NESCOR and TWG1 (2013)).

Scenario 3 - super PDC compromised: If a super PDC is compromised, it may send wrong information about all its connected devices (PDCs and PMUs), which are reporting to the Super PDC according to the hierarchical topology. In addition, a super PDC may be misconfigured to not recognize other super PDCs, regional PDCs or PMUs in the network, or just send incomplete measurement data up in the WAMS hierarchy. Super PDCs may report to other super PDCs, PGWs or CC. We have three cases depending on how a super PDC sends false measurements data to other components in a WAMS.

- *Case 1:* The super PDC sends false measurement to another super PDC, which then processes the false measurement values.
- *Case 2:* The super PDC sends false measurement to the next level in hierarchy represented by a PGW. The PGW directly shares information to other PGWs.
- *Case 3:* The super PDC sends false measurement values directly to a CC. The falsified information is used as inputs in the WAMS applications.

Super PDCs are higher in the hierarchy and therefore probably better protected. So we assume that compromising a super PDC is harder than compromising a PDC.

Scenario 4 - PGW compromised: If a PGW is compromised, it can not only falsify the collected data, but may also refuse to share synchrophasor measurement data with other PGWs. An attacker on a PGW may also alter the tagging of PMU IDs associated with the shared data. Since PGWs provide security isolation of trusted internal systems to the external ones, and create a trusted gateway-to-gateway connection (NASPInet (2009)), PGWs should present only a smaller attack surface.

So if all proposed PGW's security measures are implemented, it should be harder to launch attacks against a PGW.

Scenario 5 - access router compromised: An attacker that gains control of access routers on the path from a PMU to a CC can drop or duplicate synchrophasor packets that belong to the PMU communication. If the data is not integrity protected (e.g., by a message authentication code or digital signature), an attacker on a router can act as man in the middle and modify the data or inject their own data packets. Routers may also delay data in a way that they arrive too late to contribute to control applications. If the data is not encrypted, an attacker on a router can read the PMU data, which may include configuration and location information. This does not change the measurement data, but such information may be useful for attack preparation.

Scenario 6 - core router compromised: Attacks on core routers can have the same impact as those on access routers. But core routers handle many more data flows from many different locations, so data from many PMUs, PDCs or PGWs may be affected if an attacker gains control over devices in the core. Nevertheless, core routers are usually better protected than access routers.

For our analysis we assume that (core and access) routers are able to modify data, either because credentials have been compromised from end systems or because data is not end-to-end integrity protected. Furthermore, PDCs mainly aggregate and reorder the records received from multiple PMUs, and do not perform any operation on the sensor data itself. So an attack on PDCs or super PDCs usually does not change the original measurement data (not any derived values or events). As a consequence, mitigation strategies based on sensor data plausibility analysis can also help against attacks in intermediate systems.

We also assume that colluding and coordinated attacks are quite likely. Devices deployed in smart grids are often equal or similar regarding hardware, software and configuration (e.g., multiple PMUs from one vendor). Therefore, it is quite possible that an attacker can gain access to multiple systems at the same time or that attackers collude. Attacks on intermediate systems (PDCs, routers) can enable an attacker to launch a coordinated attack, even if he has only access to one system. For example, if no end-to-end security measures are used and data is neither encrypted nor signed, an attacker on a single router may be able to modify values that originated from many different observation points.

5. MITIGATION STRATEGIES

Various mechanisms have been proposed to detect data injection attacks in smart grid systems. Here we classify the existing approaches and investigate to which extent they can help to detect or mitigate data integrity attacks in the identified scenarios (Section 4). We define three categories depending on the suitability of the methods: Category 1: techniques that directly help to detect attacks at least in some parts of the scenarios. Category 2: techniques that can be modified to be applied to our scenarios. Category 3: techniques that do not help in our scenarios. We map each of the scenarios to the techniques using signs ✓ for category 1, $\sim$ for category 2 and ✗ for category 3 in Table 1.

5.1. State Estimation

State Estimation (SE) is used to deduce the state of the grid based on collected measurements. Static SE (SSE) relies on a single set of measurements all taken at one snapshot in time, whereas Dynamic SE (DSE) covers the evolution of the state over consecutive measurement instants and provides accurate dynamic states of the system. If attackers inject falsified information it could lead to implausible states in the power system and therefore raise suspicion. State estimation methods usually consider the case that wrong measurement data is received directly from PMUs, but the original measurement data can also be modified in PDCs or on routers on the path as described in Section 4. Therefore state estimation methods usually can also help to detect attacks on intermediate systems. We denote this with a $\sim$ to indicate that the solution can be applied even if not originally developed for the specific scenario. Nevertheless, if an attacker compromises a PDC and can modify data from multiple PMUs it is easier to alter data in a way that it still looks consistent for state estimation. This is similar to the situation with a set of colluding attacks from multiple compromised devices.

Dehghani *et al.* discuss attacks by altering PMU data during transmission in PMUs or PDCs. The authors develop an approach based on an SSE algorithm to detect integrity attacks in PMU networks. The PMU network consists of i number of PMUs in the network. The authors calculate a state vector V_i using measurements from all PMUs except data from the i^{th} PMU and then repeat this for all i PMUs. Then they use the average of the state vectors to calculate the Euclidean distance between each state vector and the average vector. They then select the state vector that has the largest distance to the average vector and compare it to a predefined threshold for deviation. If it exceeds the threshold, they assume that the measurement values from that

Table 1: *Mapping of the scenarios to the existing techniques*

Mitigation Strategies	**PMUs** (S1)	**PDCs** (S2)	**super PDCs** (S3)	**PGWs** (S4)	**Access Routers** (S5)	**Core Routers** (S6)
MS1: State estimation	✓(Dehghani *et al.*) ✓(Liu *et al.* (2009)) ✓(Kim and Poor (2011)) ✓(Cui *et al.* (2012)) ∼(Taha *et al.* (2015)) ✓(Pal and Sikdar)	∼(Dehghani *et al.*) ∼(Liu *et al.* (2009)) ∼(Kim and Poor (2011)) ∼(Cui *et al.* (2012)) ✓(Taha *et al.* (2015)) ✓(Pal and Sikdar)	∼(Dehghani *et al.*) ∼(Liu *et al.* (2009)) ∼(Kim and Poor (2011)) ∼(Cui *et al.* (2012)) ✓(Taha *et al.* (2015)) ✓(Pal and Sikdar)	∼(Dehghani *et al.*) ∼(Liu *et al.* (2009)) ∼(Kim and Poor (2011)) ∼(Cui *et al.* (2012)) ∼(Taha *et al.* (2015)) ∼ (Pal and Sikdar)	∼(Dehghani *et al.*) ∼(Liu *et al.* (2009)) ∼(Kim and Poor (2011)) ∼(Cui *et al.* (2012)) ∼(Taha *et al.* (2015)) ✓(Pal and Sikdar)	∼(Dehghani *et al.*) ∼(Liu *et al.* (2009)) ∼(Kim and Poor (2011)) ∼(Cui *et al.* (2012)) ∼(Taha *et al.* (2015)) ✓(Pal and Sikdar)
MS2: Aggregation	✗	∼(Kim *et al.*) ✓(Ni *et al.*)	∼(Kim *et al.*) ✓(Ni *et al.*)	∼(Kim *et al.*)	✗	✗
MS3: Anomaly detection	∼(Sun *et al.*) ✓(Kwon *et al.*)	∼(Sun *et al.*)	∼(Sun *et al.*) ∼(Rahman *et al.* (2013))	∼(Rahman *et al.* (2013))	∼(Pal *et al.*)	∼(Pal *et al.*)

particular PMU have been altered by an attacker. Applying this algorithm in PMU networks, we can detect compromised PMU frames in Scenario 1, but only if the modifications are large enough to cause a large deviation. Also setting appropriate thresholds for such systems is not trivial. The method was developed to detect attacks to PMU measurement values. It may be applied to detect attacks in intermediate systems as explained in Section 4, but with access to multiple PMU values in intermediate systems it can be easier to let values look consistent.

A mitigation scheme using DSE has been developed by Taha *et al.* (2015). A real-time depiction of the nominal system is verified based on the knowledge and parameters of a power system model and real-time PMU measurements. Knowledge and parameters are static, whereas measurements are dynamic as values are updated continuously. This step verifies measurement values with the system model. Then the unknown power system parameters and unknown inputs are estimated using real time PMU data and the system model. As a third step, malfunctions, cyber attacks and disturbances are detected by estimating attack vectors and using an attack detection filter. The filter detects compromised nodes and compromised measurements. Fourth, attack locations and faulty channels are identified. Fifth, the attacked components are diagnosed and reconfigured ensuring observability of the power system. After ensuring the power system, it is brought back to the nominal state and starts operation, otherwise it keeps on diagnosing and reconfiguring the system. The method has been developed for the NESCOR scenario for attacks on PDCs, but can be applied to super PDCs also to detect direct attacks on the PMU data modified at the PMU and also would work if PMU data is changed on PGWs and routers.

Pal and Sikdar assume that nominal transmission line parameters to which the PMUs are connected are known. They then use the measured PMU data to estimate transmission line parameters (bus voltages, current and phase angles). If the deviation between measured and nominal data exceeds a threshold, a data modification alarm is generated. The method is developed for data manipulation attacks on PMU data. The data can be modified in the PMU itself or on the way to the control center in PDCs, super PDCs or routers. The authors do not mention PGWs, but the method can also be applied if an attacker modifies original measurement values in a PGW.

Liu *et al.* (2009) show how malicious attackers can craft a coordinated stealthy attack that bypasses classical bad data detection in state estimation based on a DC power flow model. They show that attack vectors exist, even if attackers have access only to selected measurements and limited resources. In (Kim and Poor (2011)) the use of some highly secured observation points as trusted references is proposed based on the same model. Those trusted anchors make it harder for attackers to find suitable values for stealthy attacks. In (Cui *et al.* (2012)) both approaches are discussed and a distributed algorithm is proposed to detect coordinated data injection attacks. The algorithm is defined for general coordinated attacks in the wide area system.

The methods proposed in Liu *et al.* (2009), Kim and Poor (2011) and Cui *et al.* (2012) are suitable to mitigate data injection attacks on PMUs or intermediate systems. As described in Section 4 we assume that routers are able to modify the data. Therefore the methods are also suitable against attacks on routers.

5.2. Aggregation

For mitigation systems based on aggregation we distinguish between two methods. Data aggregation that deals with aggregating the measured data itself, and event aggregation that aggregates the events that were derived by inspecting measurements from one or multiple observation points.

5.2.1. Data Aggregation

Several components in a WAMS perform data aggregation. Aggregating measurement data at certain points of a system helps to analyze the situation in the system, without the need to store and transmit a vast amount of fine-grain information. Data aggregation can also have a smoothing effect that reduces the impact of wrong data in a larger dataset. Nevertheless, aggregation systems might be compromised.

In Ni *et al.* a data aggregation scheme for smart metering reports is proposed that can cope with malicious aggregating gateways. Their goal is to maintain non-repudiation and integrity under the assumption that the gateways have been compromised. In their scenario, the smart meters and the control center can be trusted and just an intermediate aggregator on the path is compromised. In this scheme the aggregator does not own credentials itself, but rather uses homomorphic authenticators to combine authenticated messages from multiple records into an own authenticated aggregated record, but without knowing the secret. In contrast to other schemes that assume that the gateway just eavesdrop on the data but otherwise follows protocol, the proposed solution does also work if the aggregator does not comply to protocol operations.

The authors also show that their technique has less computational and communication overheads, compared to existing techniques. The scheme can be applied to WAMS scenarios to prevent malicious activities in aggregating devices such as PDCs or super PDCs. But since PDCs mainly combine records, homomorphic operations on the data may not even be necessary.

5.2.2. Event Aggregation

Kim *et al.* present a security event aggregation system to provide situation analysis. This system collects security events from sensors and aggregates the data periodically or on demand. Event aggregation techniques are widely used for identifying correlated activities based on the frequency of information. The assumption is that several suspicious events indicate a problem, whereas a single outlier might be just a false positive.

We can modify and adjust event aggregation systems to aggregate events in PDCs, super PDCs, PGWs and CCs.

5.3. Anomaly Detection

Protecting communication networks against new and unexpected attacks is a challenging task, as new vulnerabilities emerge every day and attacks become more sophisticated (Alcaraz *et al.*, Anwar and Mahmood (2014)). Anomaly detection techniques help to detect such attacks and provide hints to identify the cause and origin of incidents.

Pal *et al.* propose a real-time mechanism for detecting packet drop attacks on sensitive synchrophasor data over the Internet. Packet loss can be due to congestion or due to an attacker. The authors build a classifier to distinguish both cases. In a given time interval, if dropped PMU packets are classified as attack drops and the number exceeds a threshold, then an alarm is generated. This is applicable to attacks on routers.

Sun *et al.* propose a cyber physical monitoring system to detect smart meter bad data injection attacks. The authors use Snort (CISCO (2016)) to analyze the traffic flow, and in addition perform energy measurements in the physical system. Energy measurements are verified against the physical topology and energy conservation laws. Alerts from cyber network and physical systems are fused to detect attacks. This system checks the injection energy by combining the energy consumption, total transmission loss and measurement error. Threshold of total transmission and measurement error is defined as 5% of the injected energy. If the total transmission and measurement error exceeds the threshold then an alarm is triggered and it records IP address, date and time. The method is targeted at smart meters, but by defining threshold values of measurement error, and checking the difference between the generated values from PMUs and received values in a PDC, we can detect compromised PMUs.

Rahman *et al.* (2013) propose a security analysis tool for detecting misconfigurations in Advanced Metering Infrastructures (AMI). They create a formal model representing the global behavior of AMI configuration, compliance with security constraints and verify the potential security threats violating the constraints. The method is targeted at smart meters, but can be modified to be applied to PGWs and super PDCs to detect misconfiguration.

Kwon *et al.* propose a behavior-based Intrusion Detection System (IDS) for the IEC 61850 protocol by using statistical analysis of classical network features and metrics based on the protocol specification. The authors combine static features (e.g., protocol consistency), dynamic features (e.g., frequency and distribution of GOOSE message) and generic features (e.g., bits and packets per seconds) from the communication network. They define three metrics for i) generic network features, ii) GOOSE behavior-based usage pattern and iii) MMS protocol-based commands as input for the anomaly detection. The authors implement the IDS in a substation and demonstrate that the system detects attack scenarios successfully. We can apply a similar combined intrusion detection technique in substation or intra-substation communication, in order to detect anomalous transmission of PMU data using IEC 61850.

6. CONCLUSION

In this paper, we investigate data integrity attacks in WAMSs. We present six attack scenarios based on a hierarchical WAMS structure with the following key components: PMUs, PDCs, super PDCs, PGWs, access and core routers. We analyze their impacts on the system and study different general mitigation strategies and their applicability to the six attack scenarios.

Our study identifies that there are some lacking solutions, e.g., no existing technique directly addresses PGWs misconfiguration. This thin research in PGWs can be addressed by developing techniques for detecting data attacks in PGWs. By learning how to handle similar situations and detecting similar attacks in other components in a WAMS, we can develop attack detection techniques for PGWs. We can also combine various existing techniques and develop a novel approach for detecting cross layer anomalies in the WAMS hierarchy.

ACKNOWLEDGMENT

The research in this paper is supported by the Austrian Research Promotion Agency (FFG) project RASSA (Reference Architecture for Secure Smart Grids in Austria), project number-1.84.00293.0.0, the FFG dissertation project AdA (Adaptive Anomaly Detection in Smart Grids), project number-1.84.00311.0.0, and the EU-funded SPARKS project, Grant Agreement No. 608224.

REFERENCES

Adamiak, M. et al. (2010) IEC 61850 Communication Networks and Systems in Substations.

Alcaraz, C. et al. (2014). Risks and security of Internet and systems. In: *9th International Conference, CRiSIS*.

Anwar, A. and Mahmood, A. N. (2014). Cyber security of smart grid infrastructure.

Bobba, R. B. et al. (2012). Enhancing Grid Measurements: Wide Area Measurement Systems, NASPInet, and Security. *IEEE Power and Energy Magazine*, 10(1), 67–73.

CENELEC. (2012). CEN-CENELEC-ETSI Smart Grid Coordination Group - First Set of Standards.

Chassin, D. et al. (2008). NASPI Phasor Gateways and Their Relationship to Phasor Data Concentrators.

CISCO. (2010). White paper - substation automation for the smart grid.

CISCO. (2016). Snort-intrusion prevention system capable of real-time traffic analysis and packet logging.

Cui, S. et al. (2012). Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. *IEEE Signal Processing Magazine*, 29(5), 106–115.

Dehghani, M. et al. (2015). Integrity attack detection in PMU networks using static state estimation algorithm. In: *PowerTech, 2015 IEEE Eindhoven*, 1–6.

IEC-60870-5-101 *Transmission protocols - Section 101: Companion standard for basic Telecontrol tasks*.

IEC-60870-5-103 *Transmission protocols - Companion standard for the informative interface of protection equipment*.

IEC-60870-5-104 *Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles*.

IEC-61850 *Communication Networks and Systems in Substations*.

IEC-62351-1 (2007) *Part 1: Communication network and system security - introduction to security issues*.

IEC-62351-6 (2007) *Part 6: Security for 61850*.

IEC 62351 (2007) *Part 1: Communication network and system security - Introduction to security issues*. Geneva, Switzerland.

IEC-TR-61850-90-1 (2016) *Use of IEC 61850 for the communication between substations*.

IEC-TR-61850-90-2 (2016) *Using IEC 61850 for communication between substations and control centres*.

IEEE-C37.118.1 (2011) *IEEE Standard for Synchrophasor Measurements for Power Systems*. IEEE-Standard-C37.118.1-2011 (Revision of IEEE Standard C37.118-2005.

IEEE-C37.118.2 (2011) *IEEE Standard for Synchrophasor Data Transfer for Power Systems*. IEEE-Standard-C37.118.2-2011 (Revision of IEEE Standard C37.118-2005).

Jajodia, S. et al., Eds. (2010). *Cyber Situational Awareness - Issues and Research*. Advances in Information Security. Springer, 2010.

Kezunovic, M. et al. (2012). Nescor wide area monitoring, protection, and control systems (WAMPAC) - standards for cyber security requirements.

Kim, T. T. and Poor, H. V. (2011). Strategic Protection Against Data Injection Attacks on Power Grids. *IEEE Transactions on Smart Grid*, 2(2), 326–333.

Kim, J. et al. (2015). Scalable security event aggregation for situation analysis. In: *Big Data Computing Service and Applications (BigDataService), 2015 IEEE First International Conference*, 14–23.

Kwon, Y. et al. (2015). A behavior-based intrusion detection technique for smart grid infrastructure. In: *PowerTech, 2015 IEEE Eindhoven*, 1–6.

Liu, Y. (2009). False Data Injection Attacks Against State Estimation in Electric Power Grids. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 21–32.

NASPInet. (2009). Phasor gateways technical specifications for north American synchro-phasor initiative network.

National Electric Sector Cybersecurity Organization Resources NESCOR and NESCOR Working Technical Group 1 TWG1. (2013). Electric sector failure scenarios and impact analyses.

Ni, J. et al. (2015). Security-enhanced data aggregation against malicious gateways in smart grid. In: *2015 IEEE Global Communications Conference*, 1–6.

Pal, S. and Sikdar, B. A mechanism for detecting data manipulation attacks on PMU data. In: *Communication Systems (ICCS), 2014 IEEE International Conference on*, 253–257.

Pal, S., Sikdar, B., and Chow, J. (2014). Real-time detection of packet drop attacks on synchrophasor data. In: *Smart Grid Communications, 2014 IEEE International Conference on*, 896–901.

Phadke, A. G. and Thorp, J. S. (2008). *Synchronized Phasor Measurements and Their Applications*. Power Electronics and Power Systems. Springer US, 2008.

Rahman, M.A., Al-Shaer, E., and Bera, P. (2013, Mar.) A noninvasive threat analyzer for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, 4(1): 273–87.

Searle, J. et al. (2016). Nescor guide to penetration testing for electric utilities.

Sun, Y., Guan, X., Liu, T. and Liu, Y. (2013). A cyber-physical monitoring system for attack detection in smart grid. In: *Computer Communications Workshops, 2013 IEEE Conference*, 33–34.

Taha, A. F., Qi, J., Wang, J., and Panchal, J. H. (2015). Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. *The Computing Research Repository*.

Wang, Y., Li, W., Lu, J., and Liu, H. (2009). Evaluating multiple reliability indices of regional networks in wide area measurement system. *Electric Power Systems Research*, 79(10), 1353–1359.

Zseby, T. and Fabini, J. (2014). Security challenges for wide area monitoring in smart grids. *Elektrotechnik und Informationstechnik*.

Zseby, T., Fabini, J., and Rani, D. (2013). Synchrophasor communication. *Elektrotechnik und Informationstechnik*.

Zuo, J. et al. Development of tva superpdc: Phasor applications, tools, and event replay. In: *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 1–8.