A behavioral model to detect data manipulation attacks of synchrophasor measurements

Leonidas Stylianou, Lenos Hadjidemetriou, Markos Asprou, Lazaros Zacharia, Maria K. Michael
KIOS Research and Innovation Center of Excellence and Department of Electrical and Computer Engineering
University of Cyprus
Nicosia, Cyprus
{stylianou.leonidas, hadjidemetriou.lenos, asprou.markos, zacharia.lazaros, mmichael}@ucy.ac.cy

***Abstract*—Synchrophasor technology contributes significantly to the power system transformation into smart grid since it enables the wide area monitoring and control concept. At the same time, its integration to the smart grid imposes new cyber security challenges in these cyber-physical systems. The key element of the synchrophasor technology is the Phasor Measurement Unit (PMU) which provides synchronized measurements to the control center with a fast reporting rate. The PMU measurements are kept in a Phasor Data Concentrator (PDC) which collects and time aligns measurements from different PMUs. The communication between PMUs and PDC is defined by the synchrophasor communication standard, C37.118.2-2011, which lacks security mechanisms and hence it is vulnerable to cyber-attacks. Consequently, an intrusion detection system (IDS) that can detect PMU measurement manipulation is necessary to maintain the integrity and reliability of the PMU measurements. In this paper, a Synchrophasor Specific Intrusion Detection System that utilizes a PMU's behavioral model to detect data manipulation attacks against PMU measurements is proposed. The proposed IDS approach is tested and validated using a hardware in the loop setup for power systems considering an actual PMU.**

***Index Terms*—Behavioral modelling, IEEE C37.118, Cyber attacks, Intrusion detection system, Phasor Measurement Units**

I. Introduction

One of the main enablers of the smart grid concept is the synchrophasor technology which enhances considerably the situational awareness of the power system operators. The Phasor Measurement Units (PMUs) are the main devices of a synchrophasor application and they are installed in substations (usually at the transmission system). Among other quantities, a PMU can provide time-stamped measurements for the voltage and current phasors, frequency and rate of change of frequency, all in high reporting rates (i.e., 50 or 100 measurements per second). In addition, the measurements are transmitted to the PDC that is installed in the control center. The communication system in the synchrophasor technology is established by the IEEE C37.118 standard [1]. One of the drawbacks of the C37.118 communication framework is the lack of security mechanisms [1].

The integration of new components to the power grid enabled the appearance of sophisticated malware [2], [3]. Nevertheless, sophisticated malware that targets synchrophasor technology has not been identified yet but authors in [4] have analysed the threats of BlackEnegry malware against synchrophasor technology. As the synchrophasor technology poses a high cyber-attack risk, cyber security analysis has been conducted for the C37.118 communication system in [5]. The authors performed different cyber-attacks (reconnaissance, man in the middle, denial of service and replay) to demonstrate the vulnerabilities of the C37.118 communication system and how the synchrophasor technology is impacted. The authors in [6] demonstrate that an attacker can compromise an IEEE C37.118-2 compatible phasor device in a stealthy manner with ramp and step attacks. The PMU vulnerabilities have been categorized into four different groups in [7]: interruption, intercept, modification and fabrication. The security issues of the synchrophasor architecture due to the C37.118 are highlighted in [8] while the authors in [9] investigate how data integrity attacks can be carried out in the components of a generic synchrophasor architecture.

Motivated by the lack of cyber security features in the synchrophasor communication system, several mitigation techniques have been proposed to detect and prevent cyber-attacks. To identify known and unknown cyber-attacks in synchrophasor systems, Synchrophasor Specific Intrusion Detection System (SS-IDS) have been proposed in [10] and [11]. The authors in [10] have implemented a whitelist categorization with behaviour-based intrusion detection approaches while model-based rules defined for IEEE C37.118 are used in [11] to detect cyber-attacks. An IDS that relies on PMU network logs and phasor measurements as part of a self-healing and attack-resilient PMU network is proposed in [12], while different techniques (monitoring the equivalent impedances of transmission lines, using Thevenin equivalent parameters of the system and deep learning) to detect PMU manipulation attacks are proposed in [13], [14], [15].

Although a wide-range of cyber-attacks in the synchrophasor systems can be detected by the SS-IDSs proposed in the literature, the PMU data manipulation attacks (PDMAs) are only detected if a measurement value is not in the expected range, as defined by the normal operating conditions. In contrast to the above-mentioned state-of-the-art detection systems for PDMAs, this work proposes an approach which alleviates the normal operating condition requirement and it does not trigger any false positive alarm in case of a grid fault. This is because the proposed IDS is based on the behavioral model of a PMU. Furthermore, the proposed approach does not require redundant PMU(s) operating under an attack-free assumption in order to detect an attack. The proposed behavioral model-based approach utilizes analytical redundancy relations, to define new detection rules. The performance of the proposed SS-IDS is validated in an experimental testbed using an actual PMU and manipulation of measurements regarding the voltage phasor, frequency and rate of change of frequency (ROCOF) are detected.

The rest of the paper is organized as follows. In Section II, the synchrophasor system is described and the considered threat model is defined. Section III describes the behavioral model of a PMU used to derive the analytical redundancy relations. These relations are then used to formulate the detection rules and the algorithm for the proposed SS-IDS which is capable to detect PMU data manipulation attacks. The experimental validation along with the results are presented in Section IV, while the main conclusions of this work are reported in Section V.

II. System Description

In this section, the overall system architecture of a synchrophasor system is described (Fig. 1). In this work, we consider that an attacker can compromise the communication link between the PMU and the Local PDC which is installed in the substation. The proposed approach in this work considers that a Local PDC is installed in each substation (Fig. 1). However, an architecture where a single Local PDC exists, to which all PMUs send their measurements can also apply. Functionalities of both a PMU and Local/Regional PDC are briefly presented. Further, a high-level description of how an attacker can intercept the traffic between the PMU and Local PDC and manipulate PMU measurements is also provided in this section.

PMU is an advanced measurement device installed mainly in substations of the transmission system. A PMU receives analog signals from current and voltage transformers (installed in the substation), which are discretized through an analog to digital converter in order to calculate through Fast Fourier Transform algorithms voltage and current phasors. As a PMU is connected with a Global Positioning System (GPS) clock, the PMU can provide synchronized (time stamped) voltage and current phasor measurements, frequency and ROCOF.

The main functionalities of a PDC are the collection, time alignment and forwarding of a set of PMU measurements with the same time stamp to the control center. It usually has large storage facilities to archive PMU data for event analysis and for health monitoring. Some PDCs also have a bad measurement rejection functionality, where if some PMU measurements do not arrive after a certain time (maximum waiting time) the PDC discards the delayed measurements. In a synchrophasor system, there might be more than one Local PDC installed in different substations. A Regional PDC is typically installed in the control center, responsible for the collection of all the PMU measurements from the Local PDCs.

The IEEE C37.118 standard is widely adopted for synchrophasor applications and defines the communication framework between the PMU and the PDC. Four types of messages can be exchanged between PMU and PDC; Data, Configuration, Command and Header messages. These are mapped to either Transmission Communication Protocol (TCP) or User Data Protocol (UDP). All message types have a standard format (Fig. 2) but each type transfers different information. A C37.118 message starts with *SYNC*, which defines the type of message. Next, *FRAMESIZE* defines the total number of bytes in the message and it is followed by *IDCODE* that gives the PMU/PDC ID number. *FRACSEC* is the fraction of the second that the message is transmitted and *SOC* is the message's transmission time stamp. The next fields, *DATA (1,2,..,N)*, hold the message payload, which depends on the message type. Lastly, a 16-bit cyclic redundancy check is used in *CHK* to ensure the integrity of the entire message. In a C37.118 communication system, PMU measurements are transferred to a PDC via a Data frame which contains the PMU measurements in the message payload (DATA) fields. As this work concentrates on PMU data manipulation attacks, we only consider C37.118 Data type messages.

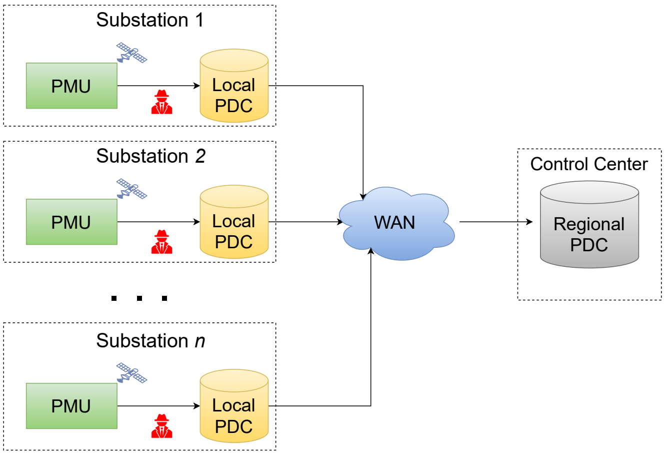

Fig. 1. Architecture of a synchrophasor system

One of the vulnerabilities of the C37.118 standard is the lack of security mechanisms to provide confidentiality. In this work, we focus on PMU data manipulation attacks (PDMAs) in a local substation. We consider that an attacker is able to eavesdrop the Data frames that are transferred from a PMU to a Local PDC, if a Man in The Middle (MiTM) attack is successful on their communication link (as shown in Fig. 1). Moreover, the considered cyclic redundancy check code used to provide data integrity, is not based on a cryptographic function and, thus, it is easily reversible [16]. Consequently, a PDC would not discard the modified data message packet as the attacker is able to re-generate the CHK bits. In this sense, the validity of the PMU measurements can be safeguarded by introducing an IDS system in each substation of the synchrophasor system to alert the operator before the PMU measurements are stored to the Local PDC.

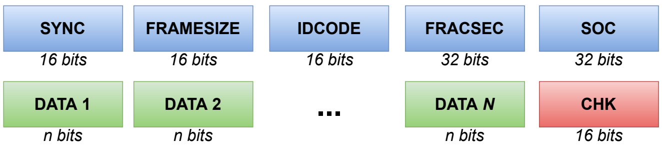

Fig. 2. Message format of a C37.118 frame, where most significant byte (first byte of SYNC) is transmitted first

III. Intrusion Detection System

The IDS proposed in this work is based on the behavioral model of a PMU. Detection rules are specified, based on analytical redundancy relations derived from the behavioral model, to detect data manipulation attacks against PMU measurements. In this section, the behavioral model as well as the detection rules are presented in detail.

A. Behavioral Model

The proposed IDS uses a behavioral model of a PMU to estimate the measurements that the PDC receives. It is assumed that a PMU provides the following measurements: phase voltage phasor, sequence voltage phasor, frequency and ROCOF. Each sample transferred to a PDC contains these measurements. A corresponding behavioral model can be applied for the current phasors as well and is not limited to the voltage phasors considered in this work.

Let us denote a voltage phasor of the k^{th} sample as $\mathbf{v_z}$(k), $z \in S$ and $S = \{0, 1, 2, a, b, c\}$, where $0, 1, 2$ corresponds to zero, positive and negative sequence, respectively, and a, b, c corresponds to each phase of a three-phase system, respectively.

$$\mathbf{v_z}(\mathbf{k}) = \left[V_z(k)\angle\theta_z(k)\right] \tag{1}$$

Let V_z be the amplitude and θ_z be the angle of a phasor z. The frequency and ROCOF measurements of a sample k are denoted as $f(k)$ and as $\frac{df}{dt}(k)$, respectively.

After the IDS receives a sample from a PMU, it uses (2) to calculate a redundant estimation of the phase voltage as a function of the sequence voltage, and (3) the sequence voltage as a function of the phase voltage.

$$\begin{bmatrix}\mathbf{\hat{v}_a(k)}\\ \mathbf{\hat{v}_b(k)}\\ \mathbf{\hat{v}_c(k)}\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 1 & \alpha^2 & \alpha\\ 1 & \alpha & \alpha^2\end{bmatrix}\begin{bmatrix}\mathbf{v_0(k)}\\ \mathbf{v_1(k)}\\ \mathbf{v_2(k)}\end{bmatrix} \tag{2}$$

$$\begin{bmatrix}\mathbf{\hat{v}_0(k)}\\ \mathbf{\hat{v}_1(k)}\\ \mathbf{\hat{v}_2(k)}\end{bmatrix} = \frac{1}{3}\begin{bmatrix}1 & 1 & 1\\ 1 & \alpha & \alpha^2\\ 1 & \alpha^2 & \alpha\end{bmatrix}\begin{bmatrix}\mathbf{v_a(k)}\\ \mathbf{v_b(k)}\\ \mathbf{v_c(k)}\end{bmatrix} \tag{3}$$

where α is a phasor with magnitude equals to 1 and phase angle equals to 120°

$$\boldsymbol{\alpha} = \left[1\angle 120°\right] \tag{4}$$

The equations for estimating current phasor measurements can be derived in a similar manner as above. Without loss of generality, in this work, we concentrate on the voltage phasor measurements. For the proposed IDS, the ROCOF is estimated based on the reporting period (T) which is defined by the reporting rate of the PMU and the current and previous frequency measurement as shown in (5).

$$\frac{\hat{df}}{dt}(k) = \frac{f(k) - f(k-1)}{T} \tag{5}$$

Furthermore, an estimation of the angle of phase voltage is calculated by considering the previous phase angle measurement and the current frequency measurement as given by,

$$\begin{bmatrix}\hat{\phi}_a(k)\\ \hat{\phi}_b(k)\\ \hat{\phi}_c(k)\end{bmatrix} = \begin{bmatrix}\theta_a(k-1)\\ \theta_b(k-1)\\ \theta_c(k-1)\end{bmatrix} + 2\pi f(k)T \tag{6}$$

B. Analytical Redundancy Relations

The behavioral model described in Section III.A is used to formulate Analytical Redundancy Relations (*ARRs*) that can be used by the proposed IDS to detect PDMAs. In general, ARRs have been used in the model-based fault diagnosis field as an indication of a fault or abnormality when the difference between an estimation and a measurement is exceeding some predetermined threshold. In this work, four different categories of *ARRs* are defined and a PMU measurement is considered valid when all relations in each of the four categories are satisfied. If any of the relations considered is not satisfied, a PDMA is detected. The four categories of *ARRs* are given below (7)-(10), where, $y \in R$, $R = \{a, b, c\}$ and $z \in S$, $S = \{0, 1, 2, a, b, c\}$. For each relation category ARR_i, a predefined threshold τ_i, $i = \{1, 2, 3, 4\}$ is used for the purpose of an attack detection.

$$\boldsymbol{ARR1:} \, rV_z = |\hat{V}_z(k) - V_z(k)| < \tau_1 \tag{7}$$

$$\boldsymbol{ARR2:} \, r\theta_y = |\hat{\theta}_z(k) - \theta_z(k)| < \tau_2 \tag{8}$$

$$\boldsymbol{ARR3:} \, r\phi_y = |\hat{\phi}_y(k) - \theta_y(k)| < \tau_3 \tag{9}$$

$$\boldsymbol{ARR4:} \, r\frac{df}{dt} = |\frac{\hat{df}}{dt}(k) - \frac{df}{dt}(k)| < \tau_4 \tag{10}$$

Relation category *ARR1* considers the difference between the reported (by the PMU) and estimated amplitude of sequence or phase voltage phasor while relations of category *ARR2* examine the angle difference between the estimated and the measured angle of sequence or phase voltage phasor. An additional phase angle residual is considered for each phase voltage vector according to the phase angle estimation presented in (6) by the relations in *ARR3*. Finally, the residual between the estimated and the measured ROCOF is considered in *ARR4*.

It should also be noted that the thresholds, τ_i are defined based on the accuracy of the PMU measurements and how the estimated variables are impacted by uncertainties. More details on these are provided in Section IV.A.

C. Detection rules based on ARRs

Given the ARRs defined above, a set of detection rules is derived for detection of PDMAs. As the proposed IDS is specification-based, certain criteria must be met to trigger a rule and thus to detect an attack. Without loss of generality, in this work it is assumed that an attacker is only able to manipulate a single type of measurement in each PMU sample.

The proposed detection rules are tabulated in Table I and they are grouped into five detection categories (C1–C5). The first column is the Detection Category (Det.Category) where C1 and C4 are derived from *ARR1*, C2 and C5 are derived from *ARR2* and C3 is derived from *ARR3* and *ARR4*. The second column defines the Detection Rule (Det.Rule) and the next column describes its condition. Lastly, the last column (Det.PDMA) shows the type of PDMA A_m, $m = \{V_a, V_b, V_c, V_0, V_1, V_2, \theta_a, \theta_b, \theta_c, \theta_0, \theta_1, \theta_2, f, \frac{df}{dt}\}$ that is detected.

The first four rules (R1–R4) belong in category C1 where rV_0, rV_1 and rV_2 are examined. It should be noted that R1 is not used to detect any PDMA but it is supplementary to other rules. If any of R2, R3, R4 is satisfied, the IDS concludes that the amplitude of a sequence voltage phasor is modified as a result of an attack on V_0, or V_1, or V_2. The next category (C2) includes four rules (R5–R8) related to the angle of the sequence voltage phasor and examines $r\theta_0, r\theta_1$ and $r\theta_2$. Thus, a manipulation of the sequence voltage's angle can be detected by rules R6–R8 while R5 is supplementary to other rules.

Rules R9–R12 of detection category C3 examine $r\frac{df}{dt}, \sigma, \phi_a, \phi_b, \phi_c$ to detect attack on frequency or ROCOF. A pre-requisite to R11 and R12 to be satisfied is that R9 is also satisfied. Moreover, σ denotes a flag variable and is initialized to *FALSE*.

Lastly, rules R14–R16 of category C4 are used to identify if any of rV_a, rV_b and rV_c exceed its threshold while R13 is supplementary to other rules. Consequently, an attack on either V_a, or V_b, or V_c, can be detected. The rules of category (C5) are used by the IDS to examine $r\theta_a, r\theta_b$ and $r\theta_c$ to detect an attack on either θ_a, or θ_b, or θ_c.

TABLE I
DETECTION RULES OF THE PROPOSED IDS AND THEIR CONDITIONS OF SATISFACTION

Det. Category	**Det. Rule**	**Rule Condition**	**Det. PDMA**
C1	R1	$\neg((rV_0 \vee rV_1 \vee rV_2) < \tau_1)$	-
	R2	$\neg(rV_0 < \tau_1) \wedge ((rV_1 \wedge rV_2) < \tau_1)$	A_{V_0}
	R3	$\neg(rV_1 < \tau_1) \wedge ((rV_0 \wedge rV_2) < \tau_1)$	A_{V_1}
	R4	$\neg(rV_2 < \tau_1) \wedge ((rV_0 \wedge rV_1) < \tau_1)$	A_{V_2}
C2	R5	$\neg R1 \wedge ((r\theta_1 \wedge r\theta_1 \wedge r\theta_2) < \tau_2)$	-
	R6	$\neg R1 \wedge \neg(r\theta_0 < \tau_2) \wedge ((r\theta_1 \wedge r\theta_2) < \tau_2)$	A_{θ_0}
	R7	$\neg R1 \wedge \neg(r\theta_1 < \tau_2) \wedge ((r\theta_0 \wedge r\theta_2) < \tau_2)$	A_{θ_1}
	R8	$\neg R1 \wedge \neg(r\theta_2 < \tau_2) \wedge ((r\theta_0 \wedge r\theta_1) < \tau_2)$	A_{θ_2}
C3	R9	$R5 \wedge (\neg(r\frac{df}{dt} < \tau_4) \vee \sigma)$	-
	R10	$R9 \wedge \sigma \wedge ((r\phi_a \wedge r\phi_b \wedge r\phi_c) < \tau_3)$	-
	R11	$R9 \wedge \neg\sigma \wedge ((r\phi_a \wedge r\phi_b \wedge r\phi_c) < \tau_3)$	$A_{\frac{df}{dt}}$
	R12	$R9 \wedge \neg((r\phi_a \vee r\phi_b \vee r\phi_c) < \tau_3)$	A_f
C4	R13	$R1 \wedge \neg((rV_a \vee rV_b \vee rV_c) < \tau_1)$	-
	R14	$R1 \wedge \neg(rV_a < \tau_1) \wedge ((rV_b \wedge rV_c) < \tau_1)$	A_{V_a}
	R15	$R1 \wedge \neg(rV_b < \tau_1) \wedge ((rV_a \wedge rV_c) < \tau_1)$	A_{V_b}
	R16	$R1 \wedge \neg(rV_c < \tau_1) \wedge ((rV_a \wedge rV_b) < \tau_1)$	A_{V_c}
C5	R17	$R13 \wedge \neg(r\theta_a < \tau_2) \wedge ((r\theta_b \wedge r\theta_c) < \tau_2)$	A_{θ_a}
	R18	$R13 \wedge \neg(r\theta_b < \tau_2) \wedge ((r\theta_a \wedge r\theta_c) < \tau_2)$	A_{θ_b}
	R19	$R13 \wedge \neg(r\theta_c < \tau_2) \wedge ((r\theta_a \wedge r\theta_b) < \tau_2)$	A_{θ_c}

D. Detection Methodology

Based on the detection categories and rules described in Table I, a new intrusion detection algorithm is proposed which can detect PDMAs for all the PMU measurements. Furthermore, the algorithm can identify the type of measurement which has been manipulated. The flowchart of the proposed algorithm is given in Fig. 3.

Firstly, R2–R4 are used to detect an attack on either V_0, or V_1, or V_2. If none of the rules of the category C1 are satisfied, the detection algorithm proceeds to examine the rules of the category C2. It can determine whether θ_0, or θ_1 or θ_2 has been modified utilizing R6–R8, otherwise, the rules of category C3 are examined.

R11 and R12 are able to identify whether the measurement of ROCOF or frequency is modified respectively. As it is, the flag variable σ is initialized to *FALSE*. Variable σ is set to *TRUE* when R12 is triggered and is set to *FALSE* when R10 is triggered. In addition, rules of the category C4 are examined when R1 is triggered. Attacks on V_a, or V_b, or V_c can be detected when one of R14–R16 is satisfied. Lastly, if R13 is triggered, the rules of category C5 are examined and concludes that θ_a, or θ_b, or θ_c has been modified.

The detection algorithm concludes that a sample of PMU measurements has not been modified when R5 is not satisfied or R10 is satisfied. Otherwise, the detection algorithm alerts about the exact PDMA based on the rule that is satisfied. The proposed detection algorithm is an efficient and quick method to locate the type of the measurement that is manipulated using the *ARRs*.

IV. EXPERIMENTAL VALIDATION

A. Experimental Setup Description

An experimental power system setup using an actual PMU device has been developed to perform the attack and to validate the performance of the proposed IDS, as shown in Fig. 4. The IEEE-9 bus system is simulated using a real-time simulator (OPAL-RT) and voltage measurements are connected to the PMU (1133A Power Sentinel-Arbiter) through the analog output of the simulator. The PMU is configured to send the following measurements to the PDC: phase voltage, sequence voltage, frequency and ROCOF. In addition, the OpenPDC application [17] runs on a server and receives the measurements from the PMU. It is assumed that the attacker has access to the same network that the PMU and Local PDC are connected.

For the attacker we use the python library *scapy* [18] that allows manipulation of network packets. The C37.118 data messages can be modified by the attacker when the Address Resoultion Protocol (*ARP*) table of both PMU and PDC are poisoned. Consequently, an *ARP* poisoning attack is launched and thus, the C37.118 packets with the PMU samples are forwarded to the attacker's machine, manipulated and then forwarded to the Local PDC. In this experimental setup, six different PDMAs are launched on a set of PMU samples. Each of the six PDMAs (A_{V_1}, A_{V_b}, A_{θ_c}, A_{θ_0}, A_f and $A_{\frac{df}{dt}}$) affect two consecutive PMU samples and are performed in a consecutive way.

During the PDMAs for V_1 and V_b, they are increased by 0.5% of their nominal value, respectively. θ_c is increased by $7°$ while θ_0 is increased by $5°$. The measurement of *f* has been

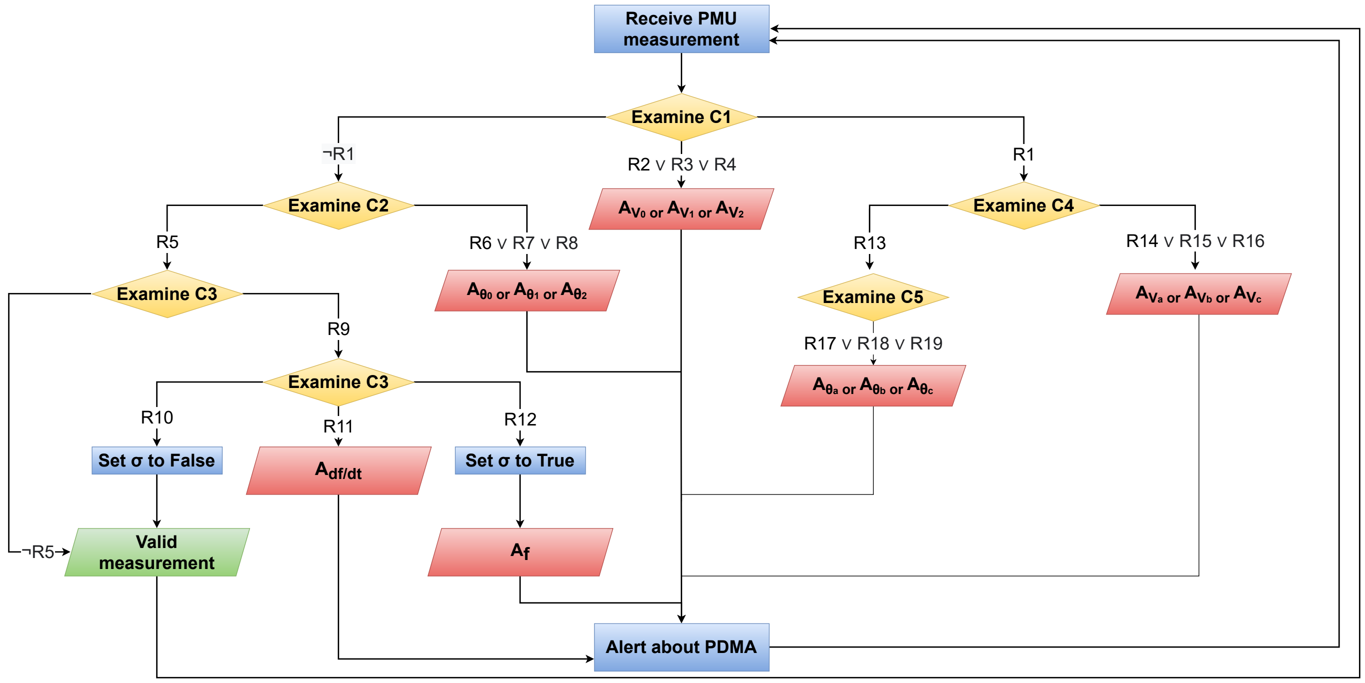

Fig. 3. Flowchart of the proposed rule-based detection algorithm.

increased by 0.2% of its nominal value. Lastly, $\frac{df}{dt}$ is decreased by 0.108 Hz/s in the first sample, followed by an increase of 0.166 Hz/s. The proposed IDS runs on the Local PDC within a substation, and uses *pydivert* [19], a python library to filter and analyse the C37.118 packets received by the PDC.

The thresholds of the behavioral model have been set according to the measurement specifications of the considered 1133A Power Sentinel PMU [20]. Specifically, the threshold of amplitude, τ_1 is set to 15.2 V since the maximum voltage error is given as 0.02% of the reading value (nominal voltage V_n =76.2kV) for this PMU. The thresholds of the phase angles (τ_2 and τ_3) have been set to $0.54°$ in order to satisfy the 1% of Total Vector Error (TVE) according to [1]. The threshold of $r\frac{df}{dt}$, τ_4 is set to 0.005 Hz/s by considering the worst-case measurement error between two frequency measurements, and the time base error according to

$$\tau_4 = \frac{2 \cdot 0.0001\% \cdot frequency}{T} + timebaseerror \qquad (11)$$

where $timebaseerror$ is 1μs, *frequency* is 50 Hz and T is the reporting period that is equal to 0.02s. [1].

B. Results

Eight different plots are presented in Fig. 5 where the first seven show the residual of specific measurements as calculated through the *ARRs*. The last plot shows the type of PDMA detected by the proposed IDS. The x-axis gives the different PMU samples.

The proposed IDS is able to detect the manipulation of V_1 between the samples 1–2. As it can be seen from the first subplot, V_1 is under attack since only rV_1 violates τ_1. Next the value of V_b is manipulated between the samples 6–7. The first and fourth subplots show that rV_0, rV_1, rV_2 and rV_b exceed τ_1 while rV_a and rV_c are below τ_1. Between the samples 11–12, the value of θ_c is manipulated. The first subplot shows that rV_0, rV_1, rV_2 violate τ_1 but rV_a, rV_b, rV_c do not violate τ_1. Therefore, the IDS proceeds to examine $r\theta_a, r\theta_b$ and $r\theta_c$ and concludes that θ_c is under attack since only $r\theta_c$ violates τ_2.

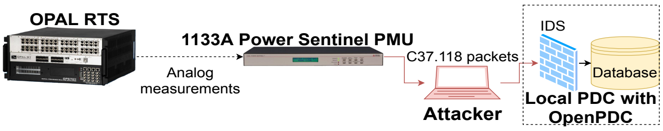

Fig. 4. Illustration of the experimental power system testbed

Phase angle of zero sequence has been modified between the samples 16–17. As rV_0, rV_1, rV_2 do not violate τ_1, $r\theta_0, r\theta_1$ and $r\theta_2$ are examined. The second subplot shows that $r\theta_1$ and $r\theta_2$ do not violate τ_2 but $r\theta_0$ does.

As proceeding to the samples 21–23, rule R5 is triggered. The frequency measurement is modified in the 21^{st} sample as $r\frac{df}{dt}$ exceeds τ_4 while $r\phi_a, r\phi_b$ and $r\phi_c$ are greater than τ_3. Even if the $r\frac{df}{dt}$ is below τ_4 in the 22^{nd} sample, the IDS detects that the frequency measurement is modified. This is because variable $\sigma = True$ (updated in the 21^{st} sample) and $r\phi_a, r\phi_b$ and $r\phi_c$ are greater than τ_3. In addition, as the $r\frac{df}{dt}$ is above τ_4 but both $\sigma = True$ and $r\phi_a, r\phi_b, r\phi_c$ are less than τ_3 (R10 is triggered), the IDS concludes that the 23^{rd} sample contains valid PMU measurements. Lastly, the $r\frac{df}{dt}$ is greater than τ_4 between the samples 26-27 and as σ is set to *FALSE*, the ROCOF measurement has been altered. In terms of scalability, the proposed SS-IDS could run in parallel to

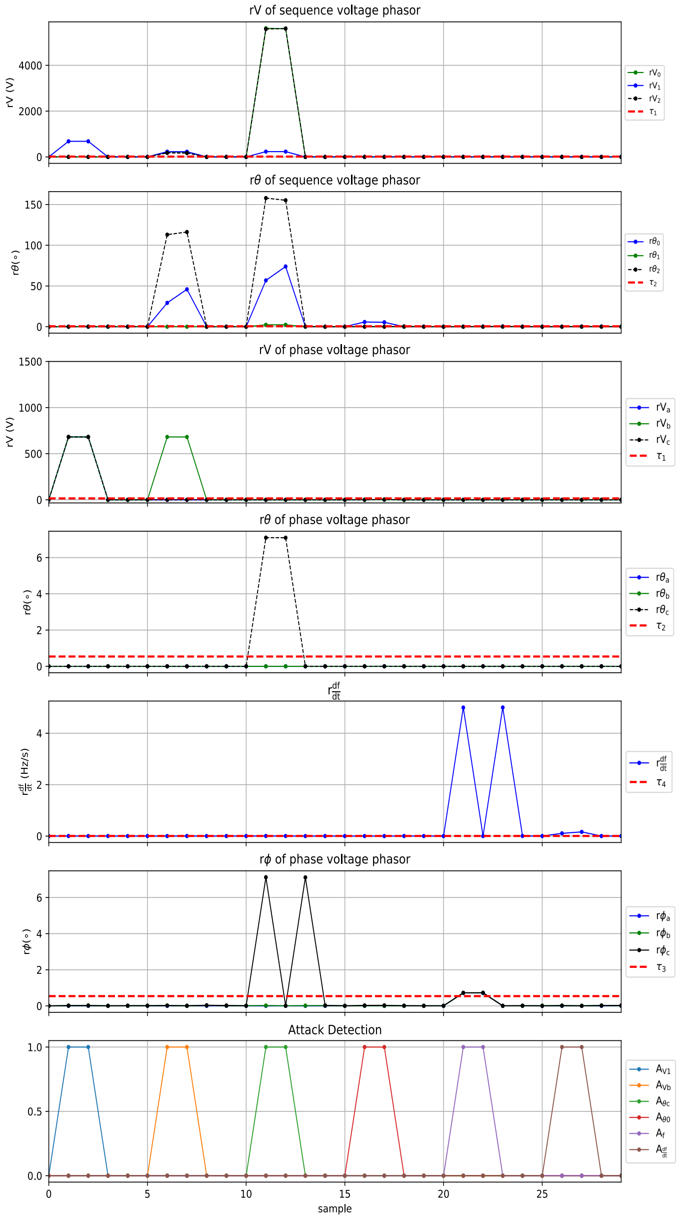

Fig. 5. Experimental results demonstrating the effectiveness of the SS-IDS

detect PDMAs for multiple PMUs.

V. Conclusion

In this paper, we proposed an SS-IDS that uses a behavioral model to detect PDMAs. In order to safeguard wide area monitoring and control applications of smart grids, it is imperative to detect and discard timely and reliably modified PMU data. The experimental validation of the proposed IDS demonstrates that it is capable of detecting attacks even with minor manipulation of the measurements. Since the SS-IDS is based on behavioral model, a false positive alert is not generated in case of grid faults. As future work, we intend to investigate the detection of multiple PMU measurements manipulations in a single sample, as well as extending the overall approach to consider both voltage and current measurements.

Acknowledgment

This work has been supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE), from the Government of the Republic of Cyprus through the Deputy Ministry of Research, Innovation, and Digital Policy and the Erasmus+ Programme of the European Union, Project: 609557-EPP-1-2019-1-LV-EPPKA2-CBHE-JP, "CybPhys".

References

[1] "IEEE Standard for Synchrophasor Data Transfer for Power Systems", IEEE, Piscataway, NJ, USA, 2011.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks,", *IEEE Trans. Power Systems*, vol. 32, no. 4, pp. 3317–3318, Nov. 2017.

[3] Dragos.com. [Online] CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf.

[4] R. Khan, P. Maynard, K. McLaughlin, D. M. Laverty, and S. Sezer, "Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid," in *Proc. ICS-CSR*, Belfast, pp. 53-63, Oct. 2016.

[5] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "IEEE C37.118-2 synchrophasor communication framework - overview, cyber vulnerabilities analysis and performance evaluation," in *Proc. ICISSP*, Rome, pp. 167-178, Feb. 2016.

[6] R. Khan, K. McLaughlin, J. H. D. Laverty, H. David, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *Proc. Annual Conference on PST*, Belfast, pp. 1-10, Aug. 2018.

[7] C. Beasley, X. Zhong, J. Deng, R. Brooks, and G. K. Venayagamoorthy, "A survey of electric power synchrophasor network cyber security," in *Proc. IEEE PES (ISGT-Europe)*, Istanbul, pp. 1-5, Oct. 2014.

[8] S. D'Antonio, L. Coppolino, I. A. Elia, and V. Fromicola, "Security issues of a phasor data concentrator for smart grid infrastructure," in *Proc. EWDC*, Pisa, pp. 3-8, May 2011.

[9] S. Paudel, P. N. Smith, and T. Zseby, "Data integrity attacks in smart grid wide area monitoring," in *Proc. 4th International Symposium ICS-CSR*, Belfast, pp. 74-83, Aug. 2016.

[10] Y. Yang et al., "Intrusion detection system for network security in synchrophasor systems," in *Proc. IET ICT*, Beijing, pp. 246–252, Apr. 2013.

[11] R. Khan, A. Albalushi, K. McLaughlin, D. Laverty, and S. Sezer, "Model based intrusion detection system for synchrophasor applications in smart grid," in *Proc.IEEE PES General Meeting*, Chigaco, pp. 1-5, Jul. 2017.

[12] V. K. Singh, E. Vaughan, and J. Rivera, "SHARP-net: Platform for self-healing and attack resilient PMU networks," in *Proc. IEEE PES ISGT*, Washington, pp. 1-5, Feb. 2020.

[13] S. Pal, B. Sikdar and J. Chow, "Classification and Detection of PMU Data Manipulation Attacks Using Transmission Line Parameters", *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057-5066, Sept. 2018.

[14] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi and J. Yan, "Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids", *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5227-5238, Nov. 2020.

[15] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan, "Distributed framework for detecting PMU data manipulation attacks with deep autoencoders," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4401–4410, Jul. 2019.

[16] Reversing CRC – Theory and Practice. [Online]. Available: https://sar.informatik.hu-berlin.de/research/publications/SAR-PR-2006-05/SAR-PR-2006-05_.pdf

[17] "GridProtectionAlliance/openPDC", GitHub, 2021. [Online]. Available: https://github.com/GridProtectionAlliance/openPDC. [Accessed: 10- Feb- 2021].

[18] "scapy," Pypi.org. [Online]. Available: https://pypi.org/project/scapy/.

[19] "pydivert," Pypi.org. [Online]. Available: https://pypi.org/project/pydivert/.

[20] Arbiter.com, 2021. [Online]. Available: https://www.arbiter.com/files/product-attachments/1133a_manual.pdf.