Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid

Khan, R., Albalushi, A., McLaughlin, K., Laverty, D., & Sezer, S. (2018). Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid. In Proceedings of Power and Energy Society General Meeting (PESGM), 2017 (IEEE Power & Energy Society General Meeting: Proceedings). IEEE .

Published in:
Proceedings of Power and Energy Society General Meeting (PESGM), 2017

Document Version:
Peer reviewed version

Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid

Rafiullah Khan, Abdullah Albalushi, Kieran McLaughlin, David Laverty and Sakir Sezer
Queen's University Belfast, Belfast, United Kingdom
Email: {rafiullah.khan, aalbalushi01, kieran.mclaughlin, david.laverty, s.sezer}@qub.ac.uk

***Abstract*—Synchrophasor technology is used for real-time control and monitoring in modern power systems. IEEE C37.118 communication framework is most widely used by synchrophasor devices such as Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs). The size, format and structure of IEEE C37.118 payloads vary significantly from one PMU/PDC to the other which make traditional signature based IDS tools (i.e., SNORT, Suricata, etc) inefficient for synchrophasor-based systems. Thus, this paper presents the design of a comprehensive model-based Synchrophasor Specific Intrusion Detection System (SS-IDS) and analyzes its features and capabilities. The proposed SS-IDS is implemented as a light-weight efficient multi-threaded tool using optimized PCAP filters. The defined model-based rules enable it to detect known as well as unknown attacks (including unintentional misuse). The functionalities of the proposed SS-IDS are validated in the lab using a testbed consisting of real PMU data and NRL CORE based emulated network.**

I. Introduction

Synchrophasor technology became an integral part of modern power systems with applications ranging from simple grid dynamics monitoring/visualization to emerging real-time protection and control applications. It enables operators to track power system dynamics in real time and take prompt actions whenever necessary. Since the introduction of IEEE C37.118 communication framework in 2005, it has been widely used in most synchrophasor devices such as Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs) [1]. In 2011, IEEE C37.118 split into two parts separating phasor measurement and communication requirements. It consists of 4 types of messages: (i) data (contains actual synchrophasor measurements), (ii) configuration (contains PMU/PDC configurations), (ii) command (contains instructions for data source i.e., PMU) and header (contains human readable information about filters, scaling, algorithms etc). The configuration message has further three types: CFG-1 contains PMU/PDC capabilities, CFG-2 contains information necessary to decode data messages, and CFG-3 contains most of same data as CFG-2 but with added flexibility, signal and PMU location information.

Depending on the PMU type (commanded or spontaneous), IEEE C37.1118 communication semantics could be different. Fig. 1 depicts basic communication scenario for PMU operating in commanded mode. PMU in spontaneous mode cannot receive commands and continuously transmits data to destination without stopping.

A. Related Work

Synchrophasor technology has numerous real-time monitoring, protection and control applications [2]–[4]. Most applications are still in lab testing and validation [5], [6]. At present, IEEE C37.118 is most well-known synchrophasor communication framework. Authors in [7], [8] addressed its evolution and key characteristics.

IEEE C37.118 is highly vulnerable to cyber attacks. Authors in [7], [9]–[11] highlighted vulnerabilities in IEEE C37.118. Authors in [12], [13] investigated how vulnerabilities of IEEE C37.118 can be exploited in the form of different attacks. Several researchers have investigated specific attacks e.g., data integrity attacks [14], packet drop attacks [15], DoS attacks [16], GPS spoofing attacks [17], etc.

Two research articles have addressed Intrusion Detection System (IDS) for synchrophasors [18], [19]. Authors in [18] used single threaded SNORT IDS tool for testing 11 proposed rules. While authors in [19] used ITACA IDS tool for detecting network scanning, PING based Denial of Servie (DoS) and Man In The Middle (MITM) attacks altering line frequency.

B. Paper Motivation and Contributions

Both, SNORT IDS [18] and ITACA IDS [19] lack comprehensive rules sets and have limitations including: (i) the size, format and structure of IEEE C37.118 packets vary from one PMU/PDC to other leaving traditional signature based tools [18], [19] unsuitable for synchrophasor devices under different configurations, (ii) SNORT and ITACA tools require expert technical knowledge of IEEE C37.118 to tailor/use it for a specific PMU/PDC, (iii) certain types of attacks could not be detected (or hard to detect) with signature based tools [18], [19] e.g., packet injection attacks, packet drop attacks, GPS spoofing attacks, detecting delayed, out-dated or replayed packets, unknown attacks etc, (iv) to reduce false positive and false negative detections, multiple IDS instances need to be deployed in network and on synchrophasor devices which communicate with a management server (i.e., correlating between events from multiple IDS instances), and (v) SNORT and ITACA tools are unsuitable and a specifically implemented IDS system for synchrophasors is needed with access to security credentials if packets are encrypted (e.g., IEC recommended GDOI security mechanism for synchrophasors).

These limitations and requirements motivate the need for a new comprehensive Synchrophasor Specific IDS (SS-IDS)

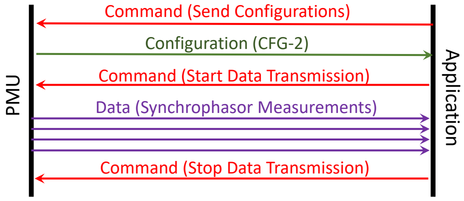
PMU
Application
Command (Send Configurations)
Configuration (CFG-2)
Command (Start Data Transmission)
Data (Synchrophasor Measurements)
Command (Stop Data Transmission)

Figure 1. IEEE C37.118 communication scenario for PMU in command mode.

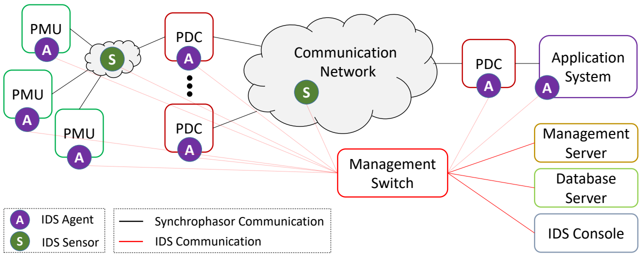

Figure 2. Proposed SS-IDS system for synchrophasor applications.

system. Thus, this paper presents the design of SS-IDS following NIST (National Institute of Standards and Technology) recommended architectural design. The SS-IDS implements a comprehensive set of model-based rules necessary to detect ARP spoofing attacks, port and network scanning attacks, GPS spoofing/blocking attacks, packet injection attacks, packet drop attacks, delayed packets or replay attacks, communication jamming and DoS attacks, data integrity attacks, physical attacks on PMUs/PDCs, command injection and other form of MITM attacks. The SS-IDS is implemented as an efficient, highly flexible and light-weight multi-threaded tool using optimized PCAP filters. It provides user friendly interface for registering rules without requiring technical knowledge about IEEE C37.118 packets. The SS-IDS can work simultaneously for many PMUs/PDCs under different configurations and also keeps their events and state information isolated. The proposed system also uses management server that correlates events from multiple SS-IDS instances to reduce false positives (i.e., benign activity/information detected as malicious) and false negatives (i.e., SS-IDS failed to detect malicious activity/information). This paper also validates functionalities of proposed SS-IDS in lab testbed consisting of real PMU and NRL CORE based emulated network.

II. Proposed SS-IDS: Design and Features

The proposed SS-IDS system is depicted in Fig. 2. All SS-IDS components can be part of organization's network or can be connected through a separate network known as management network (i.e., detection components have two network interfaces). The management network has strict security measures and is normally kept isolated from main organization's network. Management network has additional equipment cost but conceals the SS-IDS from attackers. It ensures adequate bandwidth for SS-IDS to work under adverse conditions (i.e., synchrophasors have usually very high transmission rates).

A. Architectural Components

The proposed SS-IDS system consists of four components:

1) Sensors and Agents: It can be observed in Fig. 2 that proposed SS-IDS performs both network-based detection as well as host-based detection. SS-IDS monitoring and analyzing component is known as sensor for network based detection. While a host-based detection component is known as agent. Sensors are normally deployed on gateway devices and monitor network traffic of entire network (or a segment of network) for suspicious activity. Whereas, agents monitor network traffic of one specific device (e.g., PMU or PDC) and monitor activities occurring within that device. Current SS-IDS implementations provide flexibility to operate it as a sensor or as an agent.

2) Management Server: It is a centralized server that manages received information from sensors and agents and performs correlation. It offers many benefits including detection of activities that an individual agent/sensor cannot detect (e.g., MITM attacker injects a genuine command or attacker modifications seem genuine to agent/sensor). Normally for an IDS, it is impossible to eliminate false positives and false negatives completely. Usually, reducing false positive alarms increases false negatives and vice versa. The choice of many organizations is to reduce false negatives at the cost of increase in false positives. The management server is also beneficial to reduce both, false positives as well as false negatives by performing correlation of information received from multiple agents and sensors.

3) Database Server: It is the repository of events from sensors, agents and management servers.

4) Console: It is the interface for users to access and configure SS-IDS components.

B. Operational Modes

The proposed SS-IDS can operate in two modes:

1) Inline Mode: In this mode, sensors are deployed in network at specific locations where the whole network traffic passes through it. Firewall and gateway devices are the most suitable locations for inline sensor deployment. The benefit of inline mode is to easily stop/drop malicious packets if necessary.

2) Passive Mode: In this mode, no traffic directly passes through sensors. Sensors are usually deployed at more secure locations and monitor the copy of actual network traffic. The network traffic can be accessed using network taps or load balancers which distribute copies of network traffic to multiple sensors.

C. Model-based Rules

The proposed SS-IDS provides model-based rules to characterize acceptable synchrophasor system behavior and detect violations from defined models. Due to limited applications and protocols in power systems, model-based detection is the most favorable choice for synchrophasor based systems in order to detect unknown attacks as well. The SS-IDS raises

Table I
SELECTED SIGNATURE BASED RULES FROM PROPOSED SS-IDS.

Parameter	Msg Type	Field	Significance
Network Settings (MAC, IP, Port)	All	N/A	Detecting ARP spoofing and port scanning attacks.
Protocol Version	All	SYNC	Verifying protocol version (2005 or 2011 version).
Device ID	All	IDCODE	Verifying device identification code.
Clock Failure	All	FRACSEC	PMU clock fault or failure detection (time not reliable).
Data Error	Data	STAT	Detecting if PMU data is erroneous.
Time Sync.	Data	STAT	Detecting if PMU is not sync with UTC time source.
Phasor Values	Data	PHASORS	Detecting dummy value (0x8000) i.e., PMU data absent in PDC packet.
Station Name	CFG 1-3	STN	Verifying station (PMU/PDC) name.
Line Frequency	CFG 1-3	FNOM	Verifying nominal line frequency (50 Hz or 60 Hz).
PMU Latitude	CFG 3	PMU_LAT	Verifying PMU latitude in WGS84 datum.
PMU Longitude	CFG 3	PMU_LON	Verifying PMU longitude in WGS84 datum.
PMU Elevation	CFG 3	PMU_ELEV	Verifying PMU elevation in WGS84 datum.
Command Type	Command	CMD	Detecting malicious command given to the PMU.

Table II
RANGE BASED RULES FROM PROPOSED SS-IDS.

Parameter	Msg Type	Field	Description
Time Quality	All	FRACSEC	Acceptance range of time error from UTC source.
Measurement Time	Data	STAT	Time uncertainty range in PMU measurement.
Unlock Time	Data	STAT	Number of seconds to reacquire time synchronization.
Phasor Values	Data	PHASORS	Acceptable range for phasor values.
Analog Values	Data	ANALOG	Acceptable range for analog values.
Freq. Deviation	Data	FREQ	Acceptable range of frequency deviation from nominal.
ROCOF	Data	DFREQ	Acceptable range for rate of change of frequency.
Time Window	CFG-3	WINDOW	Phasor measurement window length in microsecond.
Group Delay	CFG-3	GRP_DLY	Phasor measurement group delay in microsecond.

Note: Last 6 rules in IDS can also be set as threshold based rules.

Note: Some parameter depend on many fields e.g., calculated Phasor Values also needs PHNMR, PHUNIT, FORMAT etc. For simplicity, most relevant field is shown in table.

Table III
SELECTED STATEFUL BEHAVIOR BASED RULES FROM PROPOSED SS-IDS.

Parameter	Msg Type	Field	Behavior
Protocol Semantics	All	SYNC	Detecting unnecessary messages to/from PMU/PDC.
Time-stamp	All	SOC	Detecting delayed, outdated or replayed packets.
Leap Second Pending Bit	All	FRACSEC	Should be set no more than 60 sec nor less than 1 sec before a leap second occurs.
Leap Second Occurred Bit	All	FRACSEC	Should be set in first message after leap second and remains set for 24 hours.
Leap Second Direction Bit	All	FRACSEC	Should be 0 (add) or 1(delete) same time or before leap second pending bit and stay same for 24 hours.
Message Size	Data	FRAMESIZE	Message sizes matches information received in CFG-2.
Data Error	Data	STAT	Detecting if PMU data error persists for prolonged time.
Time Sync.	Data	STAT	Detecting if out of sync persists for prolonged time.
PMU Trigger	Data	STAT	Should be set for at-least 1 data message and 1 min.
Config. Change	Data	STAT	Should be set for 1 min before configuration change.
Phasor Values	Data	PHASORS	Detecting unexpected variation in phasor values.
Config. Count	CFG 1-3	CFGCNT	Incremented each time configuration changes.
Data Rate	CFG 1-3	DATA_RATE	Detecting packet drop or injecting attacks.
Command	Command	CMD	Detecting unusual/unexpected command given to PMU.

Note: Some parameter depend on many fields e.g., Time-stamp also depends on FRACSEC and TIME_BASE. For simplicity, most relevant field is shown in table.

alerts whenever violations from defined models are detected. The model-based rules are carefully defined for IEEE C37.118 to reduce or eliminate false alarms. In proposed SS-IDS, model-based rules are sub-categorized into four types:

1) Signature-Based Rules (SBRs): A signature is a pattern that SS-IDS looks for in received IEEE C37.118 packets. The SS-IDS raises an alert when a malicious signature is detected or genuine signature is violated. The SBRs cannot track or understand complex states of applications or protocols (e.g., analysis of a packet based on information in previously exchanged packets). The SBRs are very effective to detect known attacks but ineffective to detect unknown attacks or variants of known attacks.

In the proposed SS-IDS, a total of 41 SBRs have been defined for IEEE C37.118. Due to space limitation, Table I lists selected rules of significant importance. The network parameters inside packets (e.g., source and destination MAC and IP addresses and transport port numbers) are very helpful in detecting ARP spoofing (i.e., normally the first step of MITM attacks), network and port scanning attacks. The SBRs are also useful in detecting GPS spoofing/blocking attacks (e.g., clock failure) on PMUs/PDCs, command injection attacks and different form of MITM attacks.

2) Range-Based Rules (RBRs): The RBRs define acceptable upper and lower bounds for different IEEE C37.118 parameters. The SS-IDS raises an alert when a parameter value outside acceptable defined range is detected. The RBRs are effective to detect violations from defined models but ineffective to detect attacks that do not violate range models (e.g., an attacker intelligently fakes a parameter value so that it still lies within acceptable range).

In the proposed SS-IDS, a total of 9 RBRs have been defined for IEEE C37.118 as reported in Table II. The RBRs are suitable to detect GPS spoofing/blocking attacks and different forms of MITM attacks manipulating the parameters values.

3) Threshold-Based Rules (TBRs): The TBRs set limits for normal and abnormal behaviors. The threshold represents maximum acceptable variation as a percentage of a parameter value. The SS-IDS raises an alert when a parameter value exceeds the threshold. Similarly to RBRs, TBRs are effective to detect violations from defined models but ineffective to detect attacks that do not violate threshold.

In the proposed SS-IDS, a total of 6 TBRs have been defined for IEEE C37.118 (last 6 rules in Table II). The TBRs can be applied to same parameters as RBRs. However, current SS-IDS implementations are flexible enough and allow user to decide what type of rules to activate/deactivate based on system requirements. The TBRs are normally suitable to detect different forms of MITM attacks manipulating the parameters values.

4) Stateful Behavior-Based Rules (SBBRs): The SBBRs differentiate benign protocol activity from malicious activity by analyzing acceptable state models for deviations in each received packet. Unlike other rule types, SBBRs understand and keep track of network/protocol behavior by storing necessary state information in previously exchanged packets. SBBRs are useful to detect more advanced attacks especially those which involve a series of packet exchanges. They are particularly useful for IEEE C37.118 to detect unexpected sequences of packets (data, configuration, command etc) from PMU, PDC and/or control center applications. SBBRs can detect if the same command is issued repeatedly, unexpectedly or out of sequence based on IEEE C37.118 semantics (depending on PMU type: commanded or spontaneous). The primary drawback of SBBRs is that they have high computational complexity and resource intensive.

In the proposed SS-IDS, a total of 32 SBBRs have been defined for IEEE C37.118. Due to space limitation, Table III lists selected rules of significant importance. The SBBRs are useful to detect GPS spoofing/blocking attacks, packet injection attacks, packet drop attacks, delayed packets or replay attacks, communication jamming and DoS attacks, data integrity attacks, physical attacks on PMUs/PDCs, command injection and other form of MITM attacks as well as uninten-

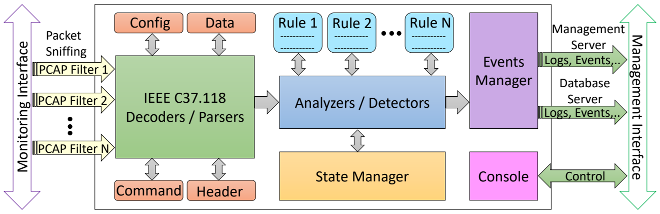

Figure 3. Architectural design of agent/sensor in proposed SS-IDS.

tional misuse.

III. Implementations

The implementation of the proposed SS-IDS encompasses three software entities: (i) sensor/agent, (ii) management server and (iii) database server. The functionalities of the management server (i.e., events management and correlation) and database server (storing events information with time-stamp) are comparatively straight forward. Due to space limitation, this paper addresses implementations of only the sensor/agent.

The agent/sensor software is implemented in Linux OS using standard C/C++ programming language (along with Boost and PCAP libraries). It is implemented as a single software that acts as either agent or sensor in passive or inline mode based on user specified settings in a configuration database. Further configurations can be specified for monitoring and management interfaces (also works if no separate management network is used). The software enables a user to add more than one PMU or PDC, and works simultaneously for all of them while keeping their events and state information isolated.

The basic agent/sensor software architecture is depicted in Fig. 3. It includes PCAP filters, IEEE C37.118 decoder, analyzer/detector, set of rules, state manager, events manager and console. A number of BPF driver optimized PCAP filters are activated in promiscuous mode based on registered active rules by user. Each rule can be in active or inactive state and corresponds to one of the model-based rule types addressed in Section II-C. Sniffed packets are provided to the IEEE C37.118 decoder which extracts all embedded information (from packets headers and payloads) using parsers of data, configuration, command and header messages. The extracted information along with the raw packet is provided to the analyzer/detector that detects malicious information/activity based on registered and active rules. During analysis, the analyzer communicates with the state manager to retrieve previous communication states or store new state information. The analyzer provides detected event (if any) information along with the raw packet to the event manager. The event manager communicates event information to management server as well as database server over UDP sockets. The console in current implementations is both local command line as well as network based (only accessible within management network).

The event manager at present is command line based and displays events information in the following format:

<TIMESTAMP> <SENSOR_AGENT_ID> <SEVERITY> <DEVICENAME>
<DEVICETYPE> <ALERT_TYPE> <ALERT_COUNT> <SRC_MAC>
<DST_MAC> <SRC_IP> <DST_IP> <SRC_PORT> <DST_PORT>
<EVENT_DESCRIPTION> <ACTION_TAKEN>

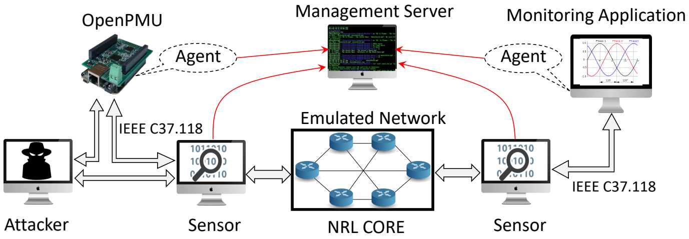

Figure 4. Experimental testbed for validation of SS-IDS features.

Current implementations have four SEVERITY levels: ultra, high, medium and low. DEVICENAME indicates PMU name, DEVICETYPE indicates PMU or PDC, ALERT_TYPE corresponds to rule name, and ALERT_COUNT is number of detections. ACTION_TAKEN is NULL and is for future use when prevention capabilities will also be implemented.

IV. Test-bed and Experimental Evaluation

This section addresses functional evaluation of the implemented SS-IDS in practical networking environment. The testbed for functional evaluation is depicted in Fig. 4. It consists of a real PMU (i.e., OpenPMU [1]), monitoring application (i.e., simply visualize synchrophasor measurements), two sensors for network based monitoring, two agents for host-based monitoring (i.e, one for PMU and one for monitoring application), a management server, an attacker PC (used to simulate attacks) and NRL CORE based emulated network. The management server receives events from sensors and agents and performs correlation. Multiple detection instances (i.e., sensors and agents) and correlation of events by management server help detect some malicious activities which could not be detected by a single sensor/agent alone e.g., packet or command injection attacks. Further, it also reduces false positives and false negatives.

NRL CORE is an open source and highly customizable emulated network tool that provides real-time connections to real-devices or real-networks. It runs applications and protocols without modifying them. The NRL CORE in Fig. 4 was configured on Ubuntu 14.04 using single router configuration which interconnects two different subnets. Each subnet has been mapped to a VLAN interface on a VLAN capable Netgear switch. The two sensors in Fig. 4 are connected to each VLAN interface.

The testbed in Fig. 4 was used to successfully validate the following SS-IDS functionalities:

- To detect GPS spoofing/blocking attacks, simulated data messages were injected with clock failure information set in the messages.
- For MITM attacks, simulated packets were injected with phasor values violating specified range based rule.
- For replay attacks, simulated data messages were injected with old GPS time-stamps.

- The importance of management server was analyzed in reducing false positives and false negatives. To this aim, a simulated command message requesting configurations was injected from an attacker PC to the PMU. It was a valid command but since the PMU's agent detects it but other sensors and agent could not detect it, the management server declares it suspicious.
- Synchrophasor applications normally have very high data transmission rate (normally 50+ packets per second) and packet drop attacks might not be tolerated. Further, synchrophasor measurements are time-stamped with GPS time and they must be received within a few milliseconds to be declared as valid. In the testbed, NRL CORE was used to demonstrate two attacks and detect them with SS-IDS: (i) packet drop attacks (which is analogous to introducing certain percentage of packet loss in NRL CORE) and (ii) packet delaying attacks (which is analogous to introducing certain link latency in NRL CORE).

V. Conclusions

IEEE C37.118 is highly vulnerable to cyber attacks and several attack cases have been demonstrated in literature. Due to involvement of synchrophasor-based systems in critical infrastructures, a SS-IDS is utmost necessary for early detection of malicious activity.

Previous related works [18], [19] lack comprehensive rules sets and face limitations such as expert IEEE C37.118 technical knowledge required to write rule, signature based rules written for one PMU/PDC cannot work other PMU/PDC of different configurations, lack to detect certain types of attacks (packet drop and injection, GPS spoofing etc) and lack management server and distributed deployment of agents and sensors.

This paper presented the design, implementation and validation of a very comprehensive and light-weight multi-threaded SS-IDS tool using optimized PCAP filters. Unlike previous works [18], [19] which uses general IDS tools for a single point/device, this paper implemented a SS-IDS from scratch following NIST recommendations and considered security of the entire system. Its comprehensive sets of model-based rules enable it to detect known as well as unknown attacks (including unintentional misuse). Further, the SS-IDS provides user friendly interface for registering rules and is flexible enough to simultaneously analyze traffic of more than one PMU/PDC while keeping their events and state information isolated. Unlike point-to-point connections [19], this paper validated the effectiveness of SS-IDS using emulated network with characteristics similar to the realistic network.

Acknowledgment

This work was funded by the EPSRC CAPRICA project (EP/M002837/1).

References

[1] D. M. Laverty, L. Vanfretti, I. A. Khatib, V. K. Applegreen, R. J. Best, and D. J. Morrow, "The OpenPMU Project: Challenges and Perspectives," in *2013 IEEE Power Energy Society General Meeting*, July 2013, pp. 1–5.

[2] I. M. Dragomir and S. S. Iliescu, "Synchrophasors Applications in Power System Monitoring, Protection and Control," in *2015 20th International Conference on Control Systems and Computer Science*, May 2015, pp. 978–983.

[3] E. O. Schweitzer, D. E. Whitehead, A. Guzmn, Y. Gong, M. Donolo, and R. Moxley, "Applied Synchrophasor Solutions and Advanced Possibilities," in *IEEE PES T D 2010*, April 2010, pp. 1–8.

[4] E. O. Schweitzer III, D. Whitehead, A. Guzman, Y. Gong, and M. Donolo, "Advanced Real-Time Synchrophasor Applications," in *proceedings of the 35th Annual Western Protective Relay Conference, Spokane, WA*, 2008.

[5] I. Friedberg, D. Laverty, K. McLaughlin, and P. Smith, "A cyber-physical security analysis of synchronous-islanded microgrid operation," in *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, ser. ICS-CSR '15. Swinton, UK, UK: British Computer Society, 2015, pp. 52–62. [Online]. Available: http://dx.doi.org/10.14236/ewic/ICS2015.6

[6] M. S. Almas, M. Baudette, L. Vanfretti, S. LŁvlund, and J. O. Gjerde, "Synchrophasor network, laboratory and software applications developed in the strong2rid project," in *2014 IEEE PES General Meeting — Conference Exposition*, July 2014, pp. 1–5.

[7] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "IEEE C37.118-2 Synchrophasor Communication Framework - Overview, Cyber Vulnerabilities Analysis and Performance Evaluation," in *2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), Rome, Italy*, 2016, pp. 167–178.

[8] K. E. Martin, "Synchrophasor Standards and Guides for the Smart Grid," in *2013 IEEE Power Energy Society General Meeting*, July 2013, pp. 1–5.

[9] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 807–816, March 2016.

[10] L. Coppolino, S. DAntonio, and L. Romano, "Exposing Vulnerabilities in Electric Power Grids: An Experimental Approach," in *International Journal of Critical Infrastructure Protection vol:7(1), pp:51-60*, 2014.

[11] S. D'Antonio, L. Coppolino, I. Elia, and V. Formicola, "Security Issues of a Phasor Data Concentrator for Smart Grid Infrastructure," in *13th ACM European Workshop on Dependable Computing*, 2011.

[12] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid," in *4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, August 2016, pp. 53–63.

[13] T. Zseby and J. Fabini, "Security challenges for wide area monitoring in smart grids," *e & i Elektrotechnik und Informationstechnik*, vol. 131, no. 3, pp. 105–111, 2014. [Online]. Available: http://dx.doi.org/10.1007/s00502-014-0203-3

[14] S. Paudel, P. Smith, and T. Zseby, "Data Integrity Attacks in Smart Grid Wide Area Monitoring," in *4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, August 2016, pp. 74–83.

[15] S. Pal, B. Sikdar, and J. Chow, "Real-time detection of packet drop attacks on synchrophasor data," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, Nov 2014, pp. 896–901.

[16] T. Morris *et al.*, "Cybersecurity Testing of Substation Phasor Measurement Units and Phasor Data Concentrators," in *ACM Annual Workshop on Cyber Security and Information Intelligence Research*, 2011.

[17] D. Shepard, T. Humphreys, and A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks," in *International Journal of Critical Infrastructure Protection*, 2012.

[18] R. Sprabery, T. H. Morris, S. Pan, U. Adhikari, and V. Madani, "Protocol mutation intrusion detection for synchrophasor communications," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, ser. CSIIRW '13. New York, NY, USA: ACM, 2013, pp. 41:1–41:4. [Online]. Available: http://doi.acm.org/10.1145/2459976.2460023

[19] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan, and H. F. Wang, "Intrusion detection system for network security in synchrophasor systems," in *Information and Communications Technologies (IETICT 2013), IET International Conference on*, April 2013, pp. 246–252.