Demonstrating Cyber-Physical Attacks and Defense for Synchrophasor Technology in Smart Grid

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

***Abstract*—Synchrophasor technology is used for real-time control and monitoring in smart grid. Previous works in literature identified critical vulnerabilities in IEEE C37.118.2 synchrophasor communication standard. To protect synchrophasor-based systems, stealthy cyber-attacks and effective defense mechanisms still need to be investigated.**

This paper investigates how an attacker can develop a custom tool to execute stealthy man-in-the-middle attacks against synchrophasor devices. In particular, four different types of attack capabilities have been demonstrated in a real synchrophasor-based synchronous islanding testbed in laboratory: (i) command injection attack, (ii) packet drop attack, (iii) replay attack and (iv) stealthy data manipulation attack. With deep technical understanding of the attack capabilities and potential physical impacts, this paper also develops and tests a distributed Intrusion Detection System (IDS) following NIST recommendations. The functionalities of the proposed IDS have been validated in the testbed for detecting aforementioned cyber-attacks. The paper identified that a distributed IDS with decentralized decision making capability and the ability to learn system behavior could effectively detect stealthy malicious activities and improve synchrophasor network security.

I. Introduction

Synchrophasor technology is used for real-time monitoring and control in modern power systems [1]. It consists of time-synchronized measurements of electrical quantities performed by Phasor Measurement Units (PMUs) at different points in the grid. For improved synchronization accuracy, PMUs perform time-stamping using a global precise time source i.e., GPS. The electrical measurements are transmitted in real-time to a control center using a suitable communication framework. The control center applications range from simple grid dynamics visualization to protection in distributed generation i.e., synchronous islanding [2], [3]. IEEE C37.118.2 is the most commonly used communication framework by commercially available PMU devices [4]. Due to involvement of critical infrastructure in synchrophasor applications and possible transmission over insecure network, a cyber-attack could result in devastating consequences [5], [6].

A. Related Work

Synchrophasor technology was introduced in the early 1980s with a limited view of emerging wide-area applications [7]. Most real-time control applications are still at the laboratory validation stage facing security as a major concern [8], [9]. Phasor devices integrated in power systems mainly use IEEE C37.118.2 communication framework which is susceptible to cyber-attacks due to lack of inherent security features [4]. Several publications have identified vulnerabilities in IEEE C37.118.2 which could be exploited in the form of cyber-attacks on synchrophasor applications [6], [10], [11].

Many research articles investigated a specific type of attack against a synchrophasor system e.g., packet drop [12], Denial of Service (DoS) [13], GPS spoofing [14], data manipulation [11], [15], etc. Authors in [16] investigated a GPS spoofing attack against PMU devices by injecting a counterfeit ensemble of GPS signals into the PMU antenna. It is identified that a timing error of only few microseconds can cause a PMU to violate the maximum phase angle error allowed by applicable standards leading to false perception of grid state by the automated controllers. Authors in [11] studied data integrity attacks for wide-area monitoring in smart grid. It is identified that the impact depends on attack scenario based on the hardware or software component compromised (e.g., PMU, PDC, gateway or network switch).

To protect synchrophasor communication, authors in [17], [18] proposed the concept of security gateway. Security gateway is a low cost device (e.g, Raspberry Pi) that encrypts the PMU communication before passing it through insecure network. However, gateways are ineffective in case of insider attacks (if a local device is compromised) that tamper with data prior to being secured by network gateways. An Intrusion Detection System (IDS) is the most feasible option to timely detect cyber-attacks. Several researchers have addressed IDS for synchrophasor-based systems [19]–[21]. Authors in [19] used SNORT IDS tool with 11 rules for detecting malicious activities in synchrophasor system. While authors in [20] used ITACA IDS tool for detecting attacks at network layer such as network scanning and ICMP based DoS. A single IDS instance is usually not effective enough to protect distributed PMU devices in a synchrophasor system. To this aim, authors in [21] identified that distributed IDS sensors provide better malicious events detection.

B. Paper Motivation and Contributions

Even though, IEEE C37.118.2 vulnerabilities have been identified by several researchers [4], [6] and attack cases have been studied (packet drop [12], DoS [13], GPS spoofing [14], data tampering [11], [15]), literature still lacks a clear technical specification for executing stealthy application layer cyber-attacks. Technical knowledge of the attack process could help security analysts develop effective threat detection and mitigation solutions. Further, threat detection using SNORT

IDS [19] and ITACA IDS [20] in literature have limited rules and bear limitations such as: (i) defined signature-based rules can work only for a specific PMU as IEEE C37.118.2 data messages format changes from one PMU to other, (ii) a single IDS instance usually has high false positive and false negative rates, and (iii) signature-based rules cannot detect (or hard to detect) certain attacks e.g., packet injection, packet drop, GPS spoofing, delayed or out-dated packets, stealthy data manipulation, etc. Thus, a new IDS needs to be implemented that can track PMU configurations and provide stateful behavior-based rules for effective detection of cyber-attacks (even if executed in stealthy manner) with significantly low false positives.

These limitations necessitate technical understanding of stealthy cyber-attacks against synchrophasor systems and consequently the development of an effective distributed IDS system. This paper investigates how an IEEE C37.118.2 compatible phasor device can be compromised by an expert attacker in a stealthy manner. It presents the development of an attack software prototype in Python language that features network scanning, reconnaissance, ARP poisoning based traffic diversion, packet sniffing and forwarding, stealthy attacker actions/manipulations and network restoring for concealment after acquiring malicious objectives. In particular, it demonstrates four types of attacks against a cyber physical synchrophasor testbed in the laboratory: (i) command injection, (ii) packet drop, (iii) replay and (iv) data manipulation. This paper studies the physical consequences and challenges in detection of such attacks if executed in stealthy manner. For effective detection, this paper identifies that a stateful system behavior tracking distributed IDS with decentralized malicious activities detection capability could detect stealthy cyber-attacks. The IDS is developed following NIST (National Institute of Standards and Technology) recommended architecture where a management server correlates events from distributed sensors. Events correlation by management server enhances detection and significantly reduces false positives (i.e., benign activities detected as malicious) and false negatives (i.e., malicious activities detected as benign). This paper also experimentally validates the effectiveness of IDS in detecting aforementioned cyber-attacks in a lab testbed consisting of real PMUs and an emulated communication network.

C. Paper Organization

The paper is organized as follows: Section II presents the anatomy of a cyber-attack and the development of attacker software prototype. Section III presents the implementation of the proposed IDS system, its features and capabilities. Section IV demonstrates aforementioned stealthy cyber-attacks, investigates their potential physical impact and analyzes the effectiveness of proposed IDS in detecting them. Section V provides a discussion based on IDS capabilities for detecting cyber-attacks. Finally, Section VI concludes the paper.

II. Attacking a Synchrophasor System

In a synchrophasor system, PMUs (deployed at different locations in power grid) communicate GPS timestamped data to a control center over Wide Area Network (WAN). The data represents electrical quantities for current/voltage waveform and used for real-time control, monitoring or simple visualization of the grid. Depending on the type of synchrophasor application, the consequences of a cyber-attack could be devastating including blackout, grid equipment damage and human injury. The process of executing a Man-In-The Middle (MITM) attack could be slightly different depending on the communication framework. This section first explains IEEE C37.118.2 standard which is widely used as a communication framework by most commercially available phasor devices. Based on the technical understanding of IEEE C37.118.2 standard, this section then describes the process of executing a successful MITM attack and retraction upon achieving malicious objectives.

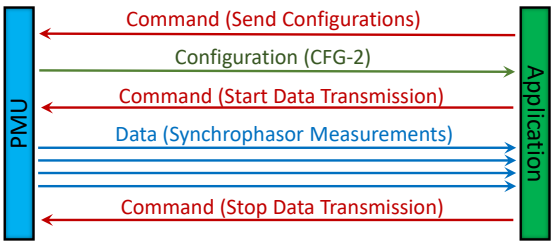


Figure 1. IEEE C37.118.2 communication scenario.

A. Overview of IEEE C37.118.2 Communication Framework

IEEE established a working group since the introduction of synchrophasor technology for developing a suitable communication standard. The group developed the IEEE 1344 standard in 1995 which has been improved and superseded by the C37.118 standard in 2005, and finally by the IEEE C37.118.2 standard in 2011. IEEE C37.118.2 offers a number of new features and also maintains full backward compatibility with the previous versions.

IEEE C37.118.2 has a compact message format and structure with simple communication semantics to keep the overhead and network bandwidth requirement at the minimum possible level. It consists of four types of messages, (i) Data, (ii) Configuration, (iii) Command and (iv) Header. Data, Configuration and Header messages are sent by phasor devices to control application while commands messages are received by phasor devices as instructions/orders. Data messages carry GPS timestamped real-time measurements known as synchrophasors. Synchrophasors contain information about electrical waveforms such as voltage/current values in rectangular or polar format, analog and digital values, frequency, Rate-Of-Change-Of-Frequency (ROCOF), etc. Configuration messages carry information about the data-source such as calibration factors, data types, meta data, processing parameters, etc. The IEEE C37.118.2 standard defines three types of configuration messages: CFG-1, CFG-2 and CFG-3. CFG-1 represents the capabilities of the data source. CFG-2 provides information to the receiver necessary for decoding Data messages. Whereas, CFG-3 is an extended version of CFG-2 with added

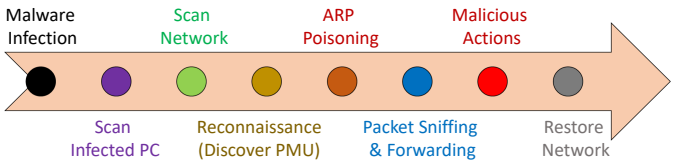


Figure 2. MITM attack process.

information and capability of flexible packet segmentation. Command messages are orders issued to phasor devices such as start/stop data transmission, send CFG-1, CFG-2 or CFG-3, send header message, etc. Whereas, header messages carry descriptive information in human readable format about the data source, filtering, scaling algorithm, etc. IEEE C37.118.2 does not put any restriction on the communication medium, communication mode and choice of the transport protocol. A basic communication scenario between the data source (i.e., PMU) and control application is depicted in Fig. 1.

B. Anatomy of MITM Attack Against a Substation

This section describes a basic cyber-attack model for a substation based on the behavior of IEEE C37.118.2 compliant phasor devices and communication semantics. The kill chain process has certain similarities with the recent cyber-attacks against ICS (e.g., Ukraine blackout) and has been tailored for synchrophasor systems. The attack execution steps are highlighted in Fig. 2 and described in the following.

1) Malware Infection: A cyber-attack starts from detecting and exploiting vulnerabilities in the target system including OS and firmware version, security credentials or any misconfiguration. A weapon or trojanized document is then prepared and injected into the target system. The most commonly used method for malware injection is spear phishing i.e., a link to a trojanized document in the email or trojanized document itself as an email attachment. Another common strategy is traffic redirection to a fraudulent website by exploiting DNS server vulnerabilities (known as pharming or driveby pharming). Once malware is injected, it normally conceals itself inside a victim machine for attack preparation and testing before final execution. Note, this step is excluded in the developed attacker software and it is assumed that one of the devices in the target network is compromised by malware.

2) Scan Infected/Compromised Device: The developed attacker software on infected host scans the device own network settings and configurations. This includes discovering IP address, MAC address and network mask. From IP and network mask, attacker gets an idea of how big is the network and what range of IP addresses are used in the network.

3) Scan Network: Based on the discovered network size and IP addresses range, the attacker software scans the presence of all IP addresses in the network and finds out their associated MAC addresses. It discovers what IP addresses are present or assigned to active devices. To achieve this, attacker software sends ARP request to all IP addresses in the network and marks an IP address as active or live if an ARP response is received. However, this will generate significant ARP traffic if the discovered network size is big. An alternative approach is to avoid sending ARP requests and silently sniff all ARP traffic in the promiscuous mode received at the Network Interface Card (NIC) of victim/compromised host (a network device normally receives lots of ARP traffic from other local devices). From the analysis of received ARP traffic, an attacker can discover what IP addresses are active and what are their associated MAC addresses. However, this approach of network scanning is slow but has less chances of being detected by network intrusion detection systems. The developed attacker software performs network scanning using the first approach i.e., sends ARP requests to all IP addresses.

4) Reconnaissance - Discover PMUs: The next step for attacker software is to find out what IP addresses in the list of discovered active IP addresses belong to phasor devices (i.e., PMUs). There are two possible ways to discover PMU devices in the network:

1) Send IEEE C37.118.2 command message (requesting CFG-2 configurations) to all discovered active network devices. The devices which respond to the command message over port 4712 or 4713 are the PMUs. In this approach, the attacker also discovers the PMU CFG-2 configurations. Note, the attacker needs to specify PMU IDCODE in the command message or else the PMU will not respond. This is a slow process and may generate huge amount of traffic as the attacker needs to try different possible values for 2-Byte IDCODE in order to discover a PMU. Another limitation is that the attacker does not know the device receiving traffic from the PMU.
2) A PMU is discovered by performing ARP poisoning (traffic diversion) one by one for all discovered active network devices for a short period of time and then restoring the network back to original state. During traffic diversion for each device, attacker software activates a packet sniffer in promiscuous mode on ports 4712 and 4713. If any IEEE C37.118.2 formatted packet is sniffed, attacker extracts the PMU and its receiver information. Note, the attacker software also forwards all sniffed packets to their original destinations to avoid any disruption in the usual network operations and keep network operators un-aware of the attack execution.

The developed attacker software supports both reconnaissance approaches which is pre-specified by the attacker as a software configuration option.

5) ARP Poisoning/Spoofing: The attacker software performs ARP poisoning in order to sniff and maliciously modify PMU traffic. ARP poisoning is used for achieving local traffic diversion and the process is illustrated in Fig. 3 as follows:

1) *Point:1* Normal operations before ARP poisoning.
2) *Point:2* The attacker broadcasts Gratuitous ARP and updates the ARP caches on all local network devices. Gratuitous ARP associates PMU IP address (one-way traffic diversion) or both PMU and gateway IP addresses (two-way traffic diversion) with the attacker's MAC address. To prevent deletion from ARP caches, ARP poisoning messages are sent periodically after every 10 seconds.

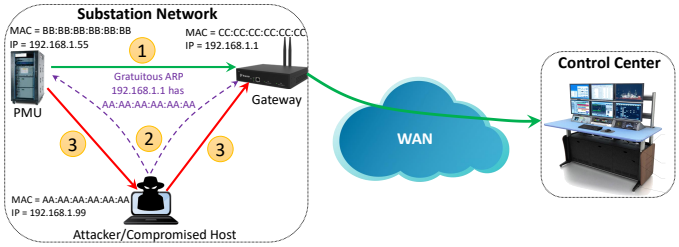


Figure 3. Network traffic diversion based on ARP poisoning.

3) *Point:3* Traffic direction after ARP poisoning.

6) Packet Sniffing and Forwarding: After ARP poisoning, all traffic to/from the target PMU redirects to the attacker host which needs to be forwarded to the correct destinations as shown in Fig. 3. The attacker software starts a packet sniffer in promiscuous mode to sniff packets and then forwards them to their original destinations. Forwarding is essential otherwise original receiver will have disruption of connectivity and will doubt MITM attack.

7) Malicious Actions: To identify and maliciously modify IEEE C37.118.2 packets in transit, attacker software creates a filter based on the transport layer port numbers (4712 and 4713). The basic scenario of hijacking IEEE C37.118.2 communication and performing malicious actions is depicted in Fig. 4. Since, attacker lies in the middle, it can drop packets, inject commands to the PMU or maliciously modify packets. Further details about attacker capabilities for performing stealthy malicious actions is described in Section IV-B.

8) Restore Network: When malicious objectives are achieved, the attacker software restores the network back to original configurations. This is achieved by sending gratuitous ARP reply packets to re-associate victim and gateway MAC addresses with their own IP addresses (to cancel the effect of ARP poisoning).

C. Implementation Tools

To implement attacker software, first IEEE C37.118.2 libraries were implemented in Python. These libraries provide encoding and decoding methods for different types of IEEE C37.118.2 messages. It enables attacker software to successfully parse and edit application layer payloads. Most MITM attack capabilities were implemented using Scapy. Scapy is a powerful packet manipulation tool in Python that provides functionalities for network scanning and discovery, probing, tracerouting, packet capturing, constructing and injecting maliciously modified packets.

III. Distributed Intrusion Detection System

Many synchrophasor applications are distributed in nature where geographically dispersed phasor devices communicate with the control center. To protect synchrophasor systems from cyber-attacks, a decentralized and highly distributed security approach is of paramount significance. This section addresses the development of an IDS for synchrophasor systems based on NIST recommendations. NIST provides practical guidance

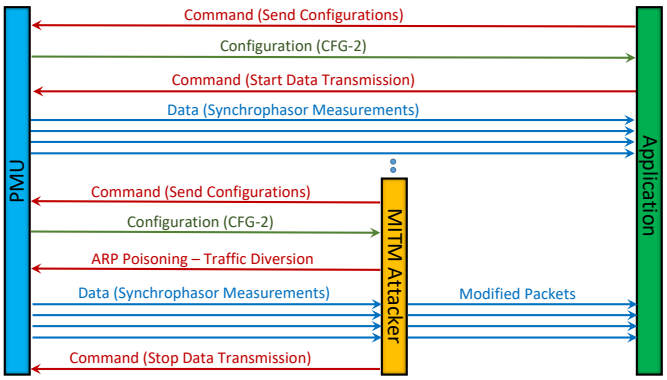


Figure 4. Active reconnaissance and attack execution.

to assist critical industries in designing, implementing, configuring and maintaining an IDS for better malicious activities detection. A network architecture adopting segregation alongside distributed IDS offers a best practice solution to cyber attack detection and mitigation.

A. NIST Recommended Architecture

Fig. 5 depicts the architecture of the proposed IDS based on NIST recommendations. All IDS components can be part of synchrophasor network or use a separate network i.e., management network. Management network is typically isolated from the main organization's network to protect IDS components from attackers. The proposed IDS consists of four types of components:

1) *Agents/Sensors:* An agent resides on a host, providing host-based monitoring for a specific device. Whereas, a sensor provides network-based monitoring for a group of devices.
2) *Management Server:* Its aim is to reduce false positives and false negatives by performing correlation of events received from agents and sensors.
3) *Database Server:* It is a repository of pre-processed events (from agents/sensors) and processed conclusions (from management server).
4) *Console:* It is a network interface to configure IDS components.

B. Supported Rules

The proposed IDS implements encoders and decoders for all types of IEEE C37.118.2 messages discussed in Section II-A. It supports four types of rules:

1) Signature-Based Rules (SBR): Signature-based rules look for a specific pattern in IEEE C37.118.2 packets and raise alert if a malicious pattern is detected or if a genuine pattern is violated. The pattern can be a network parameter (e.g., IP, MAC or port number) or any field of IEEE C37.118.2 packet (e.g., deviceID, protocol version, voltage, current, frequency, message type, data transmission rate, etc). These rules can detect simple attacks (e.g., port scanning, GPS spoofing, command injection, etc) but fail to detect complex behavior violations.

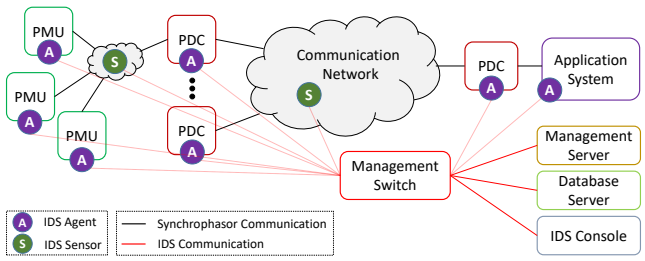


Figure 5. Distributed IDS architecture for synchrophasor systems.

2) Range-Based Rules (RBR): Range-based rules define an acceptable lower and upper bound for a parameter value (e.g., voltage value in the range of 230 V and 235 V). An alert is raised if a parameter value is outside a specified acceptable range. These rules are effective in detecting a MITM attack manipulating a parameter value.

3) Threshold-Based Rules (TBR): Threshold-based rules define the maximum acceptable variation in a parameter value (e.g., 1% variation in 230 V). An alert is raised if a parameter value violates the specified threshold. Like range-based rules, these rules are effective in detecting a MITM attack manipulating a parameter value.

4) Stateful Behavior-Based Rules (SBBR): Stateful behavior-based rules differentiate benign activity from malicious by tracking and storing previous state information of the system. Based on previous state information, it predicts next state and raises alert if the predicted state is different from received state information. These rules can detect packet drop attacks, command injection attacks, packet delaying or replay attacks, data manipulation attacks (e.g., malicious modifications in phasor values), violation in protocol semantics (e.g., sequence of packets exchanged in Fig. 1), etc. Stateful behavior-based rules are most effective in detecting stealthy cyber-attacks.

C. Implementation Tools

The proposed IDS was implemented in Linux OS using standard C/C++ programming language. It uses Boost libraries for implementing networking functionalities and PCAP libraries for sniffing, parsing and scrutinizing IEEE C37.118.2 packets. It consists of PCAP filters, set of rules and IEEE C37.118.2 decoders. A filter is created in promiscuous mode for each rule registered by the user. The IDS is capable to work simultaneously for multiple PMUs while keeping their events and state information isolated.

IV. Testbed and Experiments

This section demonstrates the capabilities of developed attacker software and proposed distributed IDS. For experimental validation, a real cyber physical synchronous islanding testbed facility is used in the laboratory.

A. Use Case: Synchronous Islanding Testbed

Synchronous islanding deals with distributed generation in smart grid. It ensures safe integration of microgrids into the main grid. A microgrid is a small geographical area where

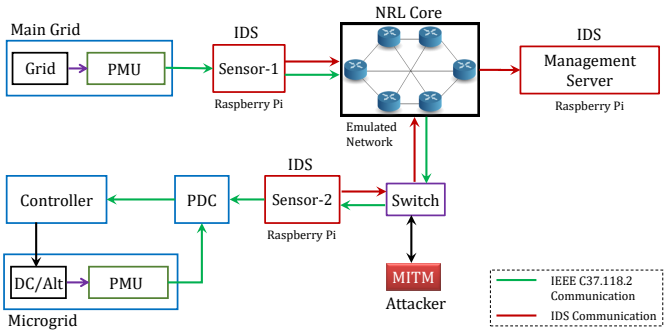


Figure 6. Secure testbed for synchronous-islanded microgrid operation using distributed IDS.

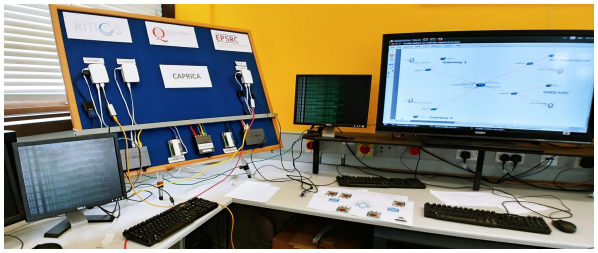
generation (e.g., solar panels, wind farms, etc), storage and load are in close proximity. It can dynamically connect and disconnect from the main grid. The synchronous islanded operation ensures safety in the re-connection by making microgrid synchronized with the main grid (same voltage magnitude, frequency and phase angle). Out of sync closure of a circuit breaker could severely damage components in the microgrid and/or main grid, causing loss of supply for the consumers.

Fig. 6 depicts the available laboratory based synchronous islanding testbed facility. The microgrid consists of a prime mover (DC machine) coupled with an alternator drive shaft. The PMUs measure electrical signals in real-time from both the microgrid and main grid (i.e., utility supply) and communicate them to the controller. Based on the PMUs data, the controller increases/decreases the speed of the DC machine (i.e., torque on the drive shaft of alternator) which in return controls the power output of the alternator. Once the phase angle of the microgrid synchronizes with the main grid, the controller issues a signal for the circuit breaker to be safely connected. NRL Core is used for emulating the wide-area network. Fig. 6 also depicts the host compromised by the attacker and IDS components. The attacker host is any device in the network compromised by a malware. For simplicity, two IDS sensors have been deployed which communicate detected malicious events to the management server over NRL Core based emulated network. Fig. 7 shows the pictorial view of testbed components.

B. Attack Experiments

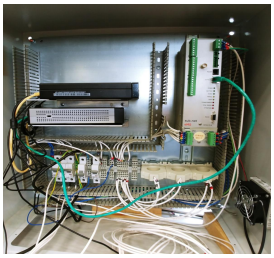
Fig. 8 depicts the interface of the attacker software with list of available commands. Before executing an attack, the attacker needs to specify certain rules. Based on the registered rules, the attacker software will inject commands to PMU devices, drop packets, replay packets or perform stealthy data manipulation.

1) Experiment 1: Command Injection: This experiment investigates an attacker's ability to issue commands to phasor devices and their potential impact. IEEE C37.118.2 compliant commercial PMU devices function based on the received commands. Most commonly supported commands by PMU devices include request for configurations (CFG-1, CFG-2 and CFG-3), header message, and starting or stopping data transmission.

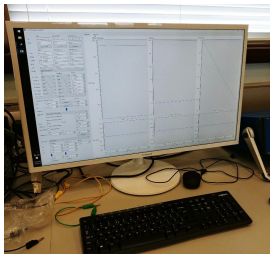


(a) NRL Core and IDS Components

(b) Microgrid and 3-Phase Transmission Load



(c) Connected PMU



(d) Microgrid Controller

Figure 7. Pictorial view of testbed components.

To issue a command to the PMU device, an attacker needs to know the PMU IDCODE. The attacker software discovers PMU IDCODE through reconnaissance as discussed in Section II-B. Observation of sniffed IEEE C37.118.2 traffic (through ARP poisoning) reveals IDCODE information to the attacker. By following the standard IEEE C37.118.2 message template, the attacker software crafts a requested command message and injects it to the PMU. The command injection attack has been validated in the testbed using eMS PMU (shown in Fig. 7).

a) Impact: The physical impact or consequences of a command injection attack could be minimal, especially for monitoring applications. For real-time control applications, a command injection attack could interrupt functionalities of control algorithms. In the synchronous islanding use case, issuing a 'stop data transmission' command to PMU leaves controller unable to synchronize microgrid to the main grid. This could lead to blackout if the microgrid is unable to meet its local demand. Even though other types of command messages have no impact on synchronous islanded operation, it could still reveal critical PMU configurations to the attacker. The revealed configurations may enable an attacker to properly decode and modify data messages in transit.

b) Detection: Fig. 9 depicts the interface of IDS sensor software with the list of available generalized rules. The sensor software supports blacklisting/whitelisting at the network and

```
Enter Command > help
-----------------------------------------------------------------------------------------
  COMMAND                    DESCRIPTION
-----------------------------------------------------------------------------------------
* help:                      Display all available commands
* scan:                      Scan entire network for active IP addresses
* discoverPMU:               Discover PMU and its IP address (if any)
* discoverGateway:           Discover IP address of gateway or receving device
* execute:                   Execute ARP poisoning / traffic diversion
* snlff:                     Sniff and print the diverted packets
* restore:                   Restore targets/network to original settings
* all:                       Execute all steps of the MITM attack
* printdevices:              Print all discovered active devices in the network
* exit/quit:                 Type exit or quit to close the application
-----------------------------------------------------------------------------------------
  ATTACKER ACTIONS
-----------------------------------------------------------------------------------------
* start:                     Send `Start Data Transmission' command to the PMU
* stop:                      Send `Stop Data Transmission' command to the PMU
* reqConfig:                 Request configurations from the PMU
* drop:                      Drop all PMU packets in transit
* drop      commands:        Drop command messages sent to the PMU
* drop      packets  time:   Randomly drop specified percentage of packets in specified
                             duration
* replay    time:            Store packets for specified time (seconds) and then replay
* magStep   value:           Step up/down the phasor magnitude by specified +/- value
* phaseStep value:           Step up/down the phase angle by specified +/- value
* freqStep  value:           Step up/down the phasor frequency by specified +/- value
* magRamp   value    time:   Increase/Decrease the phasor magnitude by specified +/- value
                             but slowly over the time (seconds) specified.
* phaseRamp value    time:   Increase/Decrease the phase angle by specified +/- value but
                             slowly over the time (seconds) specified.
* freqRamp  value    time:   Increase/Decrease the phasor frequency by specified +/- value
                             but slowly over the time (seconds) specified.
-----------------------------------------------------------------------------------------
Enter Command > phaseramp 180 86400
Enter Command >
```

Figure 8. Interface of attacker software.

transport layer. Whereas, it supports all the four categories of rules (discussed in Section III-B) at the application layer.

The effectiveness of developed distributed IDS sensors (see Fig. 6) in detecting command injection attack was validated with the following supported rules:

- *SBR-command:* Raises alert whenever a command message is sent to the PMU with code 1 (stop data transmission), 2 (start data transmission), 3 (header message), 4 (CFG-1), 5 (CFG-2) or 6 (CFG-3).
- *SBBR-semantics:* Raises alert whenever unnecessary message to/from PMU is detected that violates the semantics (see Fig. 1).

Based on the sensors deployment in Fig. 6, only Sensor-1 raises alert whenever a command message is sent to the grid/reference PMU. The IDS management server concludes the events as malicious due to not receiving them from Sensor-2. In case of a benign command issued by the controller, all agents/sensors (i.e., Sensor-1 and Sensor-2) raise alerts. Since, the management server receives events from all sensors lying along the end-to-end path, these benign activities are declared as false positives. The management server performs event correlation based on GPS timestamp which makes its decisions accurate enough to differentiate benign events from malicious.

2) Experiment 2: Packet Drop: Packet drop is an easily achievable function for MITM attacker software. The attacker can register three types of packet drop commands in the software: (i) drop all IEEE C37.118.2 traffic, (ii) drop only command messages, (iii) randomly drop X % packets for T duration. After registering packet drop, actual attack execution starts by giving commands in the order shown in Fig. 8. The attacker software starts sniffing all packets and based on the registered packet drop feature, either drops a specific IEEE C37.118.2 packet in transit or forwards it to the original destination.

```
==========================================================================================
                    SYNCHROPHASOR-SPECIFIC INTRUSION DETECTION AND PREVENTION SYSTEM
==========================================================================================
 Help: Enter 'Help' during runtime for commands information.
 EXIT: Enter 'exit' during runtime to quit.
------------------------------------------------------------------------------------------


>> help
------------------------------------------------------------------------------------------
AVAILABLE IDPS COMMANDS:
------------------------------------------------------------------------------------------
 *  Start
 *  Stop
 *  Reset
 *  Help
 *  Statistics
 *  Check   Configurations
 *  Update  Configurations NewConfigurations
 *  Load    Default        Commands
 *  Add     Device         IDCODE
 *  Delete  Device         IDCODE
 *  View    Device         IDCODE
 *  View    AllDevices
 *  Rule    Add            Device  IDCODE  SEVERITY  SBR   Parameter  Value
 *  Rule    Add            Device  IDCODE  SEVERITY  RBR   Parameter  MinValue  MaxValue
 *  Rule    Add            Device  IDCODE  SEVERITY  TBR   Parameter  Value     PercentageTolerance
 *  Rule    Add            Device  IDCODE  SEVERITY  SBBR  Parameter
 *  Rule    Delete         RuleID
 *  Exit
------------------------------------------------------------------------------------------
 NETWORK AND TRANSPORT LAYER RULES:
------------------------------------------------------------------------------------------
 *  Rule  Add  Whitelist  PROTOCOL  SRC_MAC  SRC_IP  SRC_PORT  OPERATOR  DST_MAC  DST_IP  DST_PORT  SEVERITY
 *  Rule  Add  Blacklist  PROTOCOL  SRC_MAC  SRC_IP  SRC_PORT  OPERATOR  DST_MAC  DST_IP  DST_PORT  SEVERITY
 *  View   Whitelists
 *  View   Blacklists
 *  View   Whitelist    PROTOCOL
 *  View   Blacklist    PROTOCOL
 *  Reset  Whitelists
 *  Reset  Blacklists
 *  Reset  Whitelist    PROTOCOL
 *  Reset  Blacklist    PROTOCOL
------------------------------------------------------------------------------------------
AVAILABLE COMMANDS FOR MORE DETAILED INFORMATION:
------------------------------------------------------------------------------------------
 *  Help  Long
 *  Help  Rules  SBR
 *  Help  Rules  RBR
 *  Help  Rules  TBR
 *  Help  Rules  SBBR
------------------------------------------------------------------------------------------

>>
```

Figure 9. Command line interface and capabilities of IDS sensor software.

a) Impact: The impact depends on the synchrophasor application and importance of the packet being dropped. Dropping all IEEE C37.118.2 traffic leaves controller unable to function as the reference main grid signal is missing. Such attack is easily detected by control algorithm and/or by operator through simple visualization of graphs on the controller's HMI. Dropping only command messages leaves the operator unable to instruct PMU. However, command messages are very rare and attacker software may not find any command message during the course of its operation. A wise attacker will drop X % packets for T duration to make it stealthy for control algorithms as well as operator. Smaller the number of packets being dropped, harder will be for controller or operator to detect the attack. In the use case example, dropping small number of packets does not seriously impact controller functionality but slightly reduces its effectiveness. However, dropping large number of packets leaves the controller unable to synchronize microgrid to the main grid.

b) Detection: Packet drop is hard to detect by IDS signature-based rules (especially if only certain data messages or command messages are dropped). The developed IDS sensors support a behavior based rule that keeps track of the data transmission rate for each PMU. When attacker dropped 10% of packets, IDS Sensor-2 raised alerts to the management server. Since, no alert was raised by IDS Sensor-1, management server concluded them as packet drop attack. Fig. 10 depicts the observed and expected data rate alerts/logs generated by IDS Sensor-2 when attacker software was configured to drop 10% packets in transit for 15 seconds duration. Note that the drop of command messages does not affect data messages transmission rate. To detect drop of command messages, same IDS rules were registered as in detecting command injection in experiment 1. However, only Sensor-2 raised alerts in this case which were concluded as malicious by the management server.

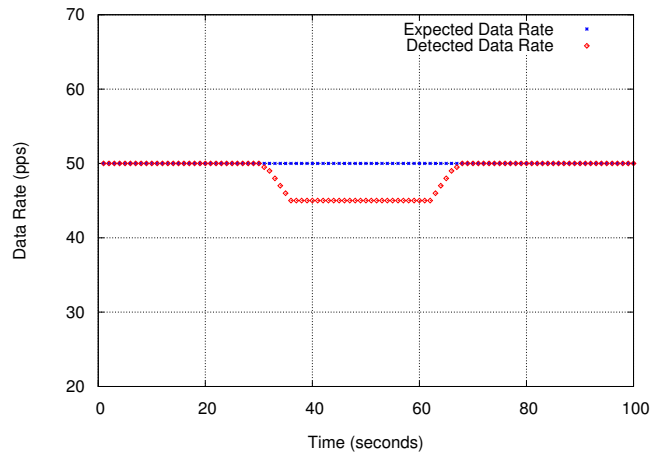


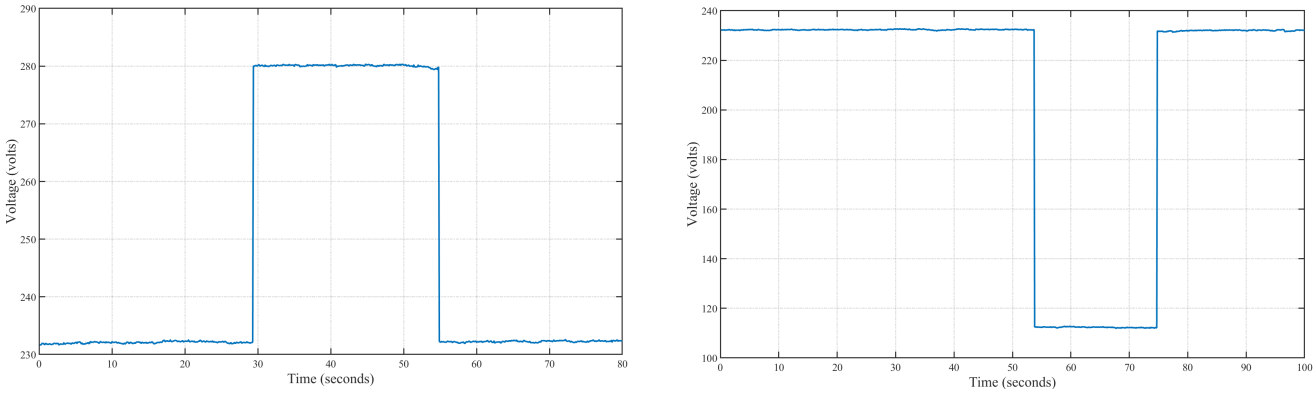
Figure 10. IDS detection of packet drop using a 5 seconds sliding window for data rate observation.

3) Experiment 3: Replay Attack: A replay attack can be the most favorable choice for a novice attacker as it is simple to execute (i.e., no protocol or domain knowledge required) and can cause significant damage. The aim of this attack is to capture and store IEEE C37.118.2 packets for a certain duration and replay them later against the target. While replaying out-dated packets, the attacker software drops real-time IEEE C37.118.2 traffic to trick the controller. The attacker software stores several complete cycles of the electrical waveform (based on frequency) to make the replay attack stealthy and prevent step change in values transmitted to the controller.

a) Impact: The replay attack is very harmful in synchronous islanded operation. It can leave controller trying indefinitely and fail to synchronize microgrid if executed on the microgrid PMU. It may cause blackout if the microgrid cannot handle its local load. If replayed traffic accidentally shows synchronization (while microgrid phase is different from the main grid), closing a circuit breaker could cause equipment damage (microgrid and/or main grid), blackout and/or human injury. However, it is hard to achieve out-of-sync closure of a circuit breaker in a replay attack compared to the stealthy packet manipulation attack.

b) Detection: Generally, replayed traffic exhibits safe limits for parameters set during the benign routine operation. To detect replay attack, both sensors were configured with a SBBR rule to analyze GPS timestamp inside each packet. Since GPS time is universal, IDS Sensor-2 raised alerts when detected packets with outdated measurement timestamps. The management server concluded replay attack from the received events. Since, no alert was raised by Sensor-1, location was quickly analyzed by the management server that replay attack took place between Sensor-1 and Sensor-2.

4) Experiment 4: Stealthy Data Manipulation: In this experiment, the attacker intercepts PMU traffic in transit and performs malicious modifications without being detected by the controller. The attacker software offers two types of data



(a) Step Up (b) Step Down

Figure 11. Step modification of the voltage magnitude.

modification features as shown in Fig. 8:

1) *Step Modification:* The phasor magnitude, frequency or phase angle is increased or decreased by the specified step value.
2) *Ramp Modification:* The phasor magnitude, frequency or phase angle is increased or decreased slowly by the specified value over a certain period of time. Longer the ramp duration, smaller will be the ramp slope and harder will be the detection of such attack by an operator/controller.

To execute a data manipulation attack, first relevant step and/or ramp modification rules must be registered by an attacker. The actual attack execution starts by giving commands in the order shown in Fig. 8. The attacker software starts sniffing all packets and forwards non-relevant traffic to the original destination without any modification. It identifies IEEE C37.118.2 traffic based on the transport protocol port number and passes to the relevant decoders based on the message type. The decoders are implemented using IEEE C37.118.2 library. The attacker software stores PMU state information and its full configurations. If IEEE C37.118.2 traffic does not contain a configuration message, it sends a command message to the PMU and requests configurations. Once PMU configurations are known, the attacker software becomes able to properly decode and manipulate phasor values in data messages. The attacker also re-calculates checksum in the modified packets to ensure they are accepted by the receiver.

Fig. 11 depicts step-up and step-down attacks executed on the voltage phasor magnitude for a certain duration. Normally, power system controllers do not inherent capability to detect malicious modifications and process any data received. However, visual inspection of the waveforms by an operator may raise suspicion for malicious modifications depending on the step size. For stealthy data manipulation, ramp modification will be the most favorable choice by an expert/wise attacker. Fig. 12 and Fig. 13 depicts the attacker's ramp modification of the voltage waveform frequency and phase angle, respectively. Ramp modifications will go undetected even with visual inspection if the ramp duration is long (i.e., ramp slope is very low). E.g., a wise attacker will manipulate phase angle by 180 degrees slowly over the duration of several days to make the modifications stealthy.

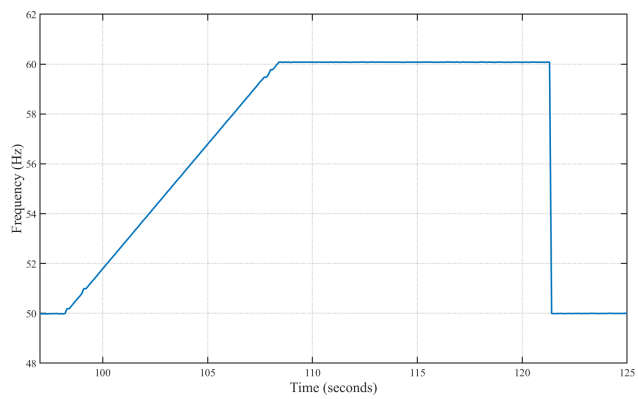


Figure 12. Ramp modification of the phasor frequency.

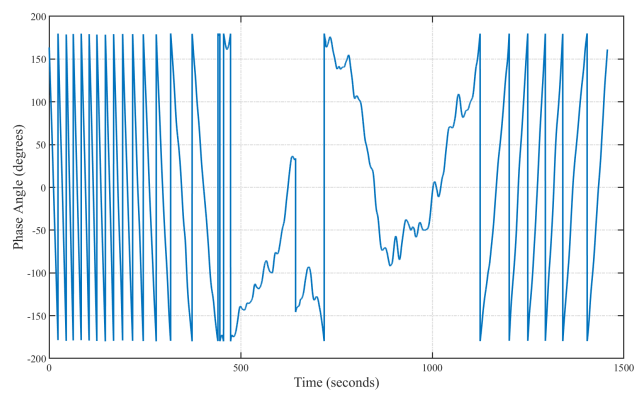


Figure 13. Ramp modification of the phase angle.

a) Impact: Stealthy data manipulation attacks are very harmful for synchrophasor-based real-time control and monitoring applications. They can trick controller performing incorrect decisions. The physical impact of such attacks depends on the synchrophasor application. For the use case under consideration, the controller can be tricked to assume synchronization (while the microgrid is not synchronized) and close the circuit breaker leading to equipment damage (microgrid and/or main grid) or blackout.

b) Detection: The developed IDS sensors support several SBR, RBR, TBR and SBBR rules for detecting malicious data modifications. The SBR rules are able to detect modifications for parameters which have fixed value e.g., IDCODE, data sorting method, breakers status, station name, number and format of phasors, etc. However, the attacks under consideration modify phasor values which could be easily detected by applying RBR and TBR rules with pre-defined safe operational limits. A wise attacker will modify phasor magnitude and frequency by a small value to evade unnoticed by the IDS RBR and TBR rules. Since phase angle is continuously varying in each packet, it cannot be detected by RBR and TBR rules. To this aim, IDS sensors support several SBBR rules for predicting phasor values in next upcoming packets based on the previously received values, frequency and transmission rate. Using basic power system equations and tracking phasor values over a prolonged time, IDS sensors were effective in correctly predicting phasor values in upcoming packets. To improve detection, IDS sensors were also configured with a SBBR rule to continuously keep track of packet inter-arrival times and transmission latencies using GPS time. Since communication latencies are not constant over a WAN, IDS sensors keep track of the minimum, average and maximum values observed (the SBBR rule engine is activated only after values have been recorded for at-least 10 minutes to reduce false positives). If a detected latency value is more than 5% higher than the maximum value, an alert is raised to the management server. Note that several milliseconds of additional latency is contributed by the attacker software for sniffing, decoding, modifying, calculating checksum and reconstructing the packet. During the experiment, only IDS Sensor-2 raised several alerts to the management server. The management server declared the events as malicious due to not receiving any such alerts from the IDS Sensor-1. Note that power system dynamics (e.g., load increase or decrease), which also fluctuate the phasor values, are hard to predict by IDS sensors. However, the management server quickly identified them as benign (false positives) due to receiving same alerts from both IDS sensors lying along end-to-end path. Fig. 14 shows the screenshot of IDS management server displaying the statistics of processed events.

```
>> statistics
-----------------------------------------------------------------------
Statistics:
-----------------------------------------------------------------------
 * Number of Events Processed by Management Server       :   207
 * Number of Pending SBR Events at Management Server     :   0
 * Number of Pending RBR Events at Management Server     :   0
 * Number of Pending TBR Events at Management Server     :   0
 * Number of Pending SBBR Events at Management Server    :   0
-----------------------------------------------------------------------


Statistics of all Registered PMUs:
-----------------------------------------------------------------------
PMU_ID  Sensor_ID   SBR   SBR_FP  RBR   RBR_FP  TBR   TBR_FP  SBBR   SBBR_FP
-----------------------------------------------------------------------
7734    1           4     0       0     0       0     0       4      17
7734    2           2     0       37    0       37    0       89     17
-----------------------------------------------------------------------


Statistics of all Registered Sensors:
-----------------------------------------------------------------------
Sensor_ID   SBR   SBR_FP  RBR   RBR_FP  TBR   TBR_FP  SBBR   SBBR_FP
-----------------------------------------------------------------------
1           4     0       0     0       0     0       4      17
2           2     0       37    0       37    0       89     17
-----------------------------------------------------------------------

>>
```

Figure 14. Statistics of received events by the IDS management server.

V. Discussion

The lack of authentication, encryption and cryptographic signature features in IEEE C37.118.2 communication framework make most commercially available PMU devices vulnerable to various types of cyber-attacks. The IEEE C37.118.2 standard has not been designed with information security in mind and does not address security aspects. Even though the packets include CRC checksum for assuring data integrity, it can be easily re-calculated by an attacker due to non-cryptographic nature. Due to lack of authentication, PMU devices cannot differentiate if a command message is received from the operator or from a malicious intruder. Since messages are not encrypted, the MITM attack can be launched against PMU devices in a synchrophasor system from an internal compromised device.

IEC 61850-90-5 has recently been published as a new communication standard for synchrophasor devices [22]. It has been designed with support for the Group Domain of Interpretation (GDOI) security mechanism. The GDOI ensures information security using certificate based authentication, encryption and cryptographic signature. It also provides protection against cryptanalysis attacks by using dynamic security credentials (i.e., security policies and keying material are refreshed periodically). However, the use of IEC 61850-90-5 in commercially available PMU devices is still very limited. Further, PMU devices deployed in power systems over last two decades are IEEE C37.118 compliant which are cost prohibitive to replace.

The experiments and attack scenarios presented in this paper have been designed from an expert attacker point of view. Basic packet drop or data manipulation attacks could be easily detected by an IDS or through visual inspection of graphs by an operator. An attacker may perform steady ramp based modifications (e.g., modify phase angle by 180 degrees over 48 hours) to make the attack stealthy for operators and evade security system. Detection of such stealthy attacks require an IDS with support for advanced stateful behavior-based rules that can continuously learn and track the system behavior. Centralized or single IDS instance is usually not effective enough to detect certain types of malicious activities in a highly distributed system. It has been validated in this paper that distributed IDS sensors with decentralized decision making improve the detection. Following NIST recommended architecture and correlation of events by the management server can help identify and isolate malicious events from the false positives. For better detection, IDS must perform analysis of network traffic at different layers of TCP/IP protocol stack. Depending on the compromised host and attack execution process, IDS rules for identifying network scanning and ARP poisoning traffic could help detect an attack at the early stage.

Further, keeping track of protocol semantics (see Fig. 4) could also help detect an attack if any unnecessary packet to/from the PMU is detected. The stateful analysis of application layer data is useful for detection of sophisticated and stealthy cyber-attacks. Real synchrophasor systems in general have poor observability in terms of threats. The presented work in this paper can contribute to better system visibility and cyber situational awareness.

VI. Conclusions

Security for synchrophasor applications is vital for safe and secure wide-area monitoring and control operations in smart grid. Previous works [4], [6] have identified that IEEE C37.118.2 communication framework (used by most commercially available phasor devices) is susceptible to cyber-attacks. Thus, the development of an effective IDS tool based on technical anatomy of cyber-attacks is paramount for early detection of malicious activities in synchrophasor systems.

In comparison to previous related works (packet drop [12], DoS [13], GPS spoofing [14], data tampering [11], [15]), this paper provided clear technical specification for investigating a cyber-attack and primarily focused on making the attack execution stealthy for operators and power system controllers. This paper demonstrated the developed attacker tool for executing four types of cyber-attacks in a stealthy manner against a physical testbed consisting of real phasor devices in the laboratory: (i) command injection, (ii) packet drop, (iii) replay, and (iv) data manipulation. It has been identified that attacks execution in stealthy manner go undetected by the automated controllers as well as through visual inspection by an operator. Furthermore, signature-based IDS tools in previous works [19], [20] are ineffective in detecting stealthy cyber-attacks. Both, SNORT-based IDS [19] and ITACA-based IDS [20] lack stateful behavior-based rules and have limitations such as (i) require technical knowledge of IEEE C37.118.2 to write rules, (ii) specified signature-based rules can work for one PMU but cannot work for other PMUs with different configurations, (iii) have high false positives due to single IDS instance, and (iv) cannot detect stealthy cyber-attacks studied in this paper.

To effectively detect stealthy cyber-attacks, this paper developed a distributed IDS following NIST recommended architecture. Due to multiple distributed sensors and events correlation by a management server, the proposed IDS offers improved detection of known as well as unknown cyber-attacks with much lower false positives. It has a comprehensive stateful behavior-based rules set for continuously learning and analyzing the system behavior. Through demonstrations in the real testbed using developed attacker tool, IDS effectiveness has been proven in detecting stealthy malicious activities to improve synchrophasor network security. The objective of presented attack cases and IDS features is to provide technical insights of stealthy cyber-attacks from an expert attacker point of view to power system operators and security analysts. This could lead to the development of effective security tools for ensuring trustworthy real-time operations in synchrophasor systems.

References

[1] M. S. Prabhu and P. K. Nayak, "A State-of-the-Art Review on Synchrophasor Applications to Power Network Protection," in *Advances in Power Systems and Energy Management, vol. 436*, 2018.

[2] A. G. Phadke and J. S. Thorp, "Synchronized Phasor Measurements and Their Applications," in *Springer Power Electronics and Power Systems book series (PEPS)*, 2017.

[3] L. Meegahapola, D. Laverty, and M. R. Jacobsen, "Synchronous Islanded Operation of an Inverter Interfaced Renewable Rich Microgrid using Synchrophasors," in *IET Renewable Power Generation, vol. 12, issue. 4*, March 2018.

[4] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "IEEE C37.118-2 Synchrophasor Communication Framework - Overview, Cyber Vulnerabilities Analysis and Performance Evaluation," in *ICISSP*, 2016.

[5] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications," in *IEEE Systems Journal*, 2017.

[6] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based Threat Modeling for Cyber-Physical Systems," in *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017.

[7] T. Becejac and M. Kezunovic, "Synchrophasor Technology: Powerful Tool that Increases Grid Reliability and Advances Electrical Safety," in *2017 IEEE IAS Electrical Safety Workshop (ESW)*, 2017.

[8] I. Friedberg, D. Laverty, K. McLaughlin, and P. Smith, "A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation," in *3rd International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, 2015.

[9] 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.

[10] 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 ICS-CSR*, August 2016.

[11] 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.

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

[13] T. Morris *et al.*, "Cybersecurity Testing of Substation Phasor Measurement Units and Phasor Data Concentrators," in *ACM CSIIRW*, 2011.

[14] X. Fan, L. Du, and D. Duan, "Synchrophasor Data Correction under GPS Spoofing Attack: A State Estimation Based Approach," *IEEE Transactions on Smart Grid*, 2017.

[15] V. K. Singh *et al.*, "Stealthy Cyber Attacks and Impact Analysis on Wide-Area Protection of Smart Grid," in *NAPS*, 2016.

[16] 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.

[17] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and Implementation of Security Gateway for Synchrophasor Based Real-Time Control and Monitoring in Smart Grid," *IEEE Access*, 2017.

[18] S. R. Firouzi *et al.*, "Interpreting and Implementing IEC 61850-90-5 Routed-Sampled Value and Routed-GOOSE Protocols for IEEE C37.118.2 Compliant Wide-Area Synchrophasor Data Transfer," in *Elsevier Journal on Electric Power Systems Research*, 2017.

[19] 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, 2013.

[20] 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*, 2013.

[21] R. Khan, A. Albalushi, K. McLaughlin, D. Laverty, and S. Sezer, "Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid," in *IEEE PES-GM*, July 2017.

[22] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 Synchrophasor Communication Frameworks," in *IEEE PES-GM*, July 2016.