Evaluation of Anomaly Detection for Wide-Area Protection Using Cyber Federation Testbed

Vivek Kumar Singh, and Manimaran Govindarasu
School of Electrical and Computer Engineering
Iowa State University, Ames, IA 50011
Email: vsingh@iastate.edu, gmani@iastate.edu

Donald Porschet, Edward Shaffer, and Morris Berman
US Army Research Laboratory
Adelphi, MD 20783

***Abstract*—Cyber physical security research for smart grid is currently one of the nation's top R&D priorities. The existing vulnerabilities in the legacy grid infrastructure make it particularly susceptible to countless cyber-attacks. There is a growing emphasis towards building interconnected, sophisticated federated testbeds to perform realistic experiments by allowing the integration of geographically-dispersed resources in the dynamic cyber-physical environment. In this paper, we present a cyber (network) based federation testbed to validate the performance of an anomaly detector in context of a Wide Area Protection (WAP) security. Specifically, we have utilized the resources available at the Iowa State University Power Cyber (ISU PCL) Laboratory to emulate the substation and local center networks; and the US Army Research Laboratory (ARL); to emulate the regional control center network. Initially, we describe a hardware-in-the loop based experimental setup for implementing data integrity attacks on an IEEE 39 bus system. We then perform network packet analysis focusing on latency and bandwidth as well as evaluate the performance of a decision tree based anomaly detector in measuring its ability to identify different attacks. Our experimental results reveal the computed wide area network latency; bandwidth requirement for minimum packet loss; and successful performance of the anomaly detector. Our studies also highlight the conceptual architecture necessary for developing the federated testbed, inspired by the NASPI network.**

I. Introduction

Today's power grid is evolving into a highly complex, interconnected, cyber-physical system to meet the real-time demand response where numerous controllers are performing different operations to maintain the stability and reliability of the power system. In earlier days, the traditional power system relied on SCADA communications for system protection and control, which provided limited capability in capturing a comprehensive dynamic view as well as providing appropriate control actions to mitigate power quality disturbances. However, with significant advancements in the application of synchrophasor technology, and communication infrastructure, wide-area measurements based protection scheme, also known as Remedial Action Scheme (RAS), can be implemented with the objectives of detecting disturbances, and providing automated, intelligent control actions to enhance the system stability and reliability with system wide information [1]. Based on the NERC document, the Synchrophasor based RAS (SP RAS) is also considered a "do no harm" scheme as it does not take corrective action that can have a negative impact on the system stability [2]. As wide-area protection schemes evolve, serious challenges exist to ensure a robust security profile. The published literature, government documents, and surveys have reported numerous malicious incidents targeting industrial control systems (ICSs) including Stuxnet and the Ukraine grid hack [3]. The papers in [4], [5] discuss the vulnerability assessment on SCADA communications and shows how a coordinated cyber-attack can affect the normal operation of the RAS. Given the amount of conventional security measures deployed, coupled with legacy infrastructure, it is not the matter of "if" but a matter of "when" in regards to these existing applications becoming exploited by cyber attacks. Thus, there is a compelling urge to develop attack-resilient RAS schemes. Existing state-of-the-art research is often constrained by its real-world practical application as the current operational systems cannot be used to perform cyber physical security related experiments. The Cyber Physical System (CPS) security testbed plays a vital role in the development, evaluation, and validation of novel technologies and tools. Most of the published work in the past are based on the traditionally isolated CPS testbed which does not provide a realistic platform to emulate the real power grid. Since the power system substations are geographically dispersed; and are controlled and monitored through high-speed communications, the resources available at geographically dispersed multiple testbeds can be shared through the common network like internet or intranet to develop an interconnected testbed, also known as the federated testbed. It can provide a high fidelity representation of the real-world grid architecture.

In an earlier effort, we have presented the notion of decision tree based anomaly detection using differential PMU features for detecting a data integrity attack (malicious tripping) in the context of WAP security [6]. In this work, we have proposed the cyber(network) based federated testbed architecture, inspired by the NASPInet architecture, to analyze the wide-area network traffic, and to evaluate the performance of the anomaly detector using a realistic platform for detecting cyber-attacks. For developing the federated testbed, we have leveraged the resources available at Iowa State University's Power Cyber Laboratory (ISU PCL) and the US Army Research Laboratory (ARL) testbeds, where the regional control center

[1]Acknowledgement: This research is funded in part by NSF CPS and DOE CEDS programs.

is operating at the ARL testbed, and the substation and local center networks are operating at the ISU PC testbed. ARL's control center receives the PMU data measurements which are further processed by the anomaly detector to identify possible anomalies in real-time. Apart from the malicious tripping attack, we have also considered other data integrity attacks including ramp and pulse attacks, which are implemented in the hardware-in-the-loop based cyber-physical environment at the ISU PCL testbed.

II. OVERVIEW AND RELATED WORKS

A. Attack Surface on RAS

1) Background on RAS : In this work, we have considered the response based generation rejection scheme, where, the centralized, control center based controller, (RAS controller), checks the maximum operation transfer capability (OTC_{max}) of the transmission lines during single line contingency. It then determines how much generation has to be reduced to prevent thermal overloading on the remaining connected lines. Specifically, we have focused on the SCADA-Synchrophasor integrated, control center based remedial action scheme, which receives PMU measurements including line flows, relay status and generator output to detect disturbances, and SCADA based, closed loop control signals are employed to reduce the generation, if necessary, to prevent the thermal overloading. More details are provided in [6].

2) Attack Vectors on WAP: Previous research efforts have shown how the attacker can strategically modify the sensor measurements and control signals to inject disturbances in the generation rejection based RAS scheme. In our previous works, we have shown how stealthy cyber-attacks, which includes malicious tripping followed by pulse or ramp attack on the generator can affect the system and generator stability [5], [12]. Specifically, as a part of the attack experiment, we have considered three different attack vectors, which are defined as:

1) Malicious tripping attack: It involves tripping the physical relay maliciously. We have performed this attack by replaying the tripping packets through the Man-in-the Middle (MITM) over wide-area network.
2) Pulse attack:This attack vector involves periodically changing the input control signal by adding the pulse attack parameter, λ_{pulse}, for a small interval (t1) and retaining back the original input for the remaining interval (T- t1) for the given time period, (T), as shown in equation 1.
3) Ramp attack: This attack vector involves adding a time varying ramp signal to the input control signal based on a ramp signal parameter, λ_{ramp}, as shown in equation 2.

$$P_{pulse} = \begin{cases} P_i(1 + \lambda_{pulse})(t = t_1) \\ P_i(t = T - t_1) \end{cases} \quad (1)$$

$$P_{ramp} = P_i + \lambda_{ramp} * t \quad (2)$$

B. Why Federation CPS based Testbed?

The concept of a federation can be defined as the integration of multi-domain specific testbeds to leverage individual resources to achieve synergy among geographically dispersed components without exposing their individual properties. It can be used for different applications such as solving research-oriented problems, developing novel CPS security tools, providing scaling capability to simulate the large-scale system, and capturing real-time communication networks to emulate the real-grid network. There exist few works, which capture the flavor of a federation in some specific applications. Previously, the ISU PowerCyber testbed successfully federated with the DETER testbed at the University of Southern California's Information Science Institute to demonstrate different cyber-attack experiments on wide area controllers [7]. The paper in [8] shows how the two real-time digital simulators (RTDS) can be connected to perform distributed simulations. The project report in [9] addresses the NIST's effort in developing a cross-sector CPS testbed to enhance the interoperability among multiple testbeds. Bryan et al. shows the power hardware-in-the-loop (PHIL) based closed loop co-simulation for the distributed system by using resources available at PNNL and NREL [10]. In a similar work, the press article in [11] mentions the real-time connection between multiple real-time simulators, available at a distance in NREL and INL, with an average delay of 28 milliseconds. Although good works, there is a strong need to develop a robust platform for experimental testing and validation at the federation level for cyber physical security. This paper shows our research-in-progress work towards developing the sophisticated, federated testbed. We do not explicitly solve the issues related to the federation including packet loss or communication latency. However, we have utilized this platform for the network analysis, testing and validating the applied anomaly detection in the context of WAP security.

III. FEDERATION ARCHITECTURE & DETECTION METHODOLOGY

A. Proposed Federation Architecture

Figure 1 depicts the proposed high-level view of federation architecture using multiple testbeds for the CPS security. We have followed the NASPI network (NASPInet) conceptual architecture's guideline to develop the industry-grade CPS federated testbed infrastructure. Generally, the NASPInet consists of phasor gateways (PGs) and a data bus (DB), where PMU data is shared among multiple utilities/centers in the standard, and decentralized fashion. In this architecture, two testbeds are connected through the common data bus and user end gateways to facilitate the bi-directional streaming of real-time data including the SCADA and PMU measurements in a realistic way. Specifically, we are proposing a network-based federated architecture between two testbeds, where the substation and local control center networks operate in testbed 1; and the regional control center network is located in testbed 2. For developing the common data bus between two phasor/SCADA

gateways for testbed1 and testbed 2, the IPSec virtual private network (VPN) tunnel is configured using the UDP protocol by exchanging internal and end points certificates, to allow the secure, real-time communication between the two networks. Since PMU based applications have a timing constraint as the latency is an important factor, UDP is preferred at the transport layer over the TCP. The pfSense software can be used as the phasor-SCADA gateway to provide the access point to the PMU and SCADA data. It can also work as a firewall and router to whitelist the configured devices, monitor the network packets, and provide Quality of services (QoSs). It is important to note that, based on the possible attack surfaces (as shown with a red arrow in figure 1), testbed 1 can work as the cyber security experimental station, where, different types of attacks can be implemented on the SCADA and synchrophasor network. In this work, we assume that the attacker has access to the substation and local control network in the testbed 1, and the regional control center is operating in the secure environment in testbed 2. The anomaly detector operates at the regional control center to detect anomalies based on the applied detection methodology

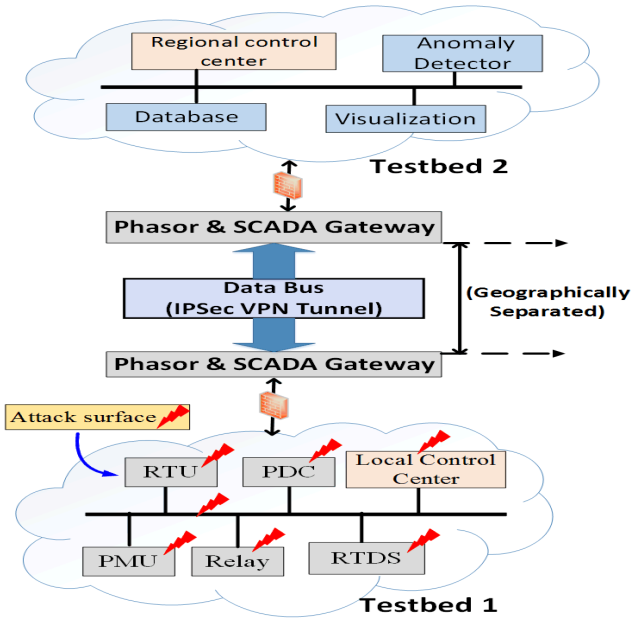


Fig. 1: High-level network-based Federated architecture for attack-detection experiment.

B. Anomaly Detection Methodology

Figure 2 shows the anomaly detection methodology for detecting different classes of data integrity attacks. We have extended the previous methodology by also addressing generation altering attacks through the ramp and pulse attacks; to target the generator, which is controlled by a protection controller. We have applied the decision tree (J45) based data mining technique to build the classification model. For building the classification model, the PMU measurements including generator bus voltages (Vg), line bus voltages (Vi, Vj), where subscripts i and j represent the sending and receiving end of the transmission lines, and the generator frequency (F), are collected from deployed PMUs for computing the derived features, where, ΔX includes difference in sending and receiving ends line voltage (ΔV_{ij}), change in generator bus voltages (ΔV_g) and change in generator frequency (ΔF). $\frac{dX}{dt}$ includes the derivate of line bus voltages ($\frac{dV_{ij}}{dt}$) , generator bus voltage ($\frac{dV_g}{dt}$), and generator frequency ($\frac{dF}{dt}$). As part of the supervised learning, we have generated a dataset library of various events, including cyber-attacks and line faults, and labelled them in the integer format. The generated dataset library is used for training the model. Finally, the trained model is deployed for testing multi-events classification, and later for sending the alert messages and possible corrective actions.

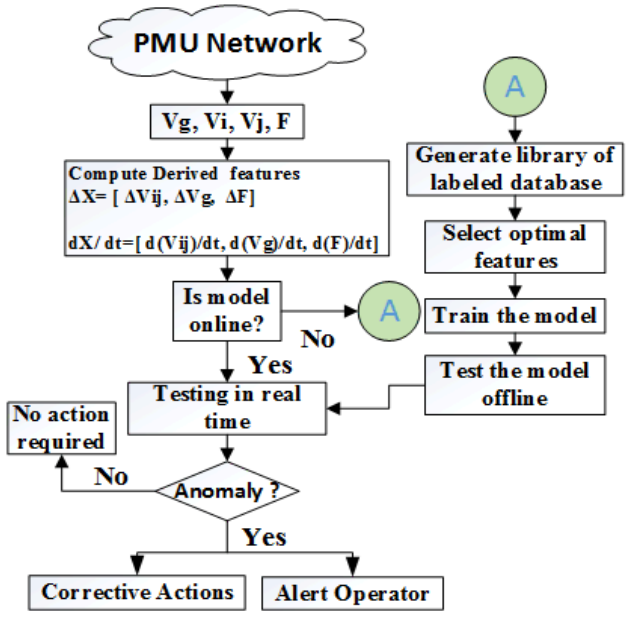


Fig. 2: Anomaly detection methodology for WAP.

IV. EXPERIMENTAL SETUP AND CASE STUDY

Figure 3 shows the hardware in the loop (HIL) based federated testbed for attack-detection experiments. We have modeled the IEEE 39 bus system in ARTEMiS/SSN (eMEGASIM), and simulated it in real-time using real time digital simulator (OPAL-RT). We have deployed virtual PMU models to generate synthetic phasors, and later to compute the derived features inside the simulator. The computed features are sent to the hardware PDC; at the ISU PC network, which forwards the data to software super PDC (Open PDC) at the ARL control center over the VPN network. The super PDC saves the data in a local csv historian and a MySQL database. The stored data is used for generating the labeled database, and further training and testing of the decision tree based algorithm. The WAP controller is running in a python script

which is communicating with the substation RTU; in the ISU PC testbed, through Kepserver's OPC Unified Architecture (UA) client-server tunneling. The substation RTU, as shown with pink box, is communicating with the simulator using the DNP3 (OPC server) protocol for SCADA communication. The software PDC at ARL collects the measurements and forwards them to the anomaly detector and RAS (WAPS) controller. The protection controller receives the measurements from MySQL in real-time, and sends the control signal back to the ISU substation through the OPC UA client-server SCADA communication to provide the appropriate response, if necessary, to close the loop.

Figure 3 also shows the IEEE 39 bus system, which is divided into two major areas, where area 2, operating as a generation area, is supplying power to the area 1 through tie-lines L15-16 and L16-17. If the breaker for line L16-17 is tripped then line L15-16 will present an overloaded condition. Accordingly, the WAP controller will shed the generation (Gen 6) at bus 35, as shown in colored circle, and equal amount of load is shed at bus 18 to maintain the system stability. To simulate the HIL experiment, relays 1 and 2 are mapped to lines L15-16, and L16-17 respectively. For the attack implementation, we have performed a malicious tripping attack on the relay 2 to trip the line L16-17, by replaying the tripping packet using a python script with Man-in-the-Middle (MITM) technique between the substation and local control center. For executing ramp and pulse attacks on generator (Gen 6) at bus 35, a Trojan horse malware is installed in the OPC server based substation RTU, providing backdoor access to the attacker. The attacker closes the legitimate RTU program and initiates a python scripted malicious logic routine which periodically sends control signals to the simulator targeting the generator (Gen 6) to initiate ramp and pulse attacks. We have also simulated three phase to ground faults followed by the normal tripping of the line L16-17 to simulate physical disturbances; and multiple simulations are performed for different cases as discussed in [6]. It is appropriate to note that the due to the space limitation, we are not discussing the details of different scenarios required for generating the labeled datasets. Overall, we have generated datasets for the four events: 3 phase to ground fault (0), malicious tripping (1), ramp attack (2) and; pulse attack (3), with the detection results provided in the next section.

V. RESULTS AND DISCUSSIONS

In order to address the challenges of Quality of Service (QoS), we have analyzed the PMU packets in terms of network latency, communication bandwidth; and detection rate. Based on the network analysis using Wireshark, we have computed the average value of the computed bandwidth to be around 15,250 bytes/sec, with a minimum value of 15,000 bytes/sec, and a maximum value of 15300 bytes/sec for 17 phasors with sampling rate of 60 samples per second. We did not observe any dropped packets during the real-data streaming, which shows that the given bandwidth is adequate to ensure that the PMU data is transferred over the VPN network.

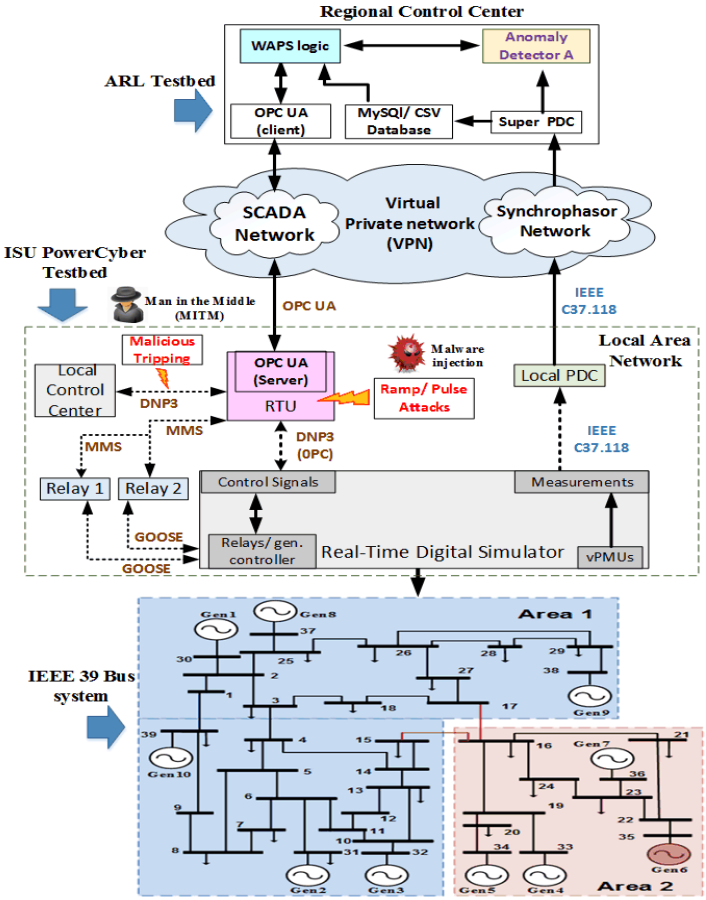
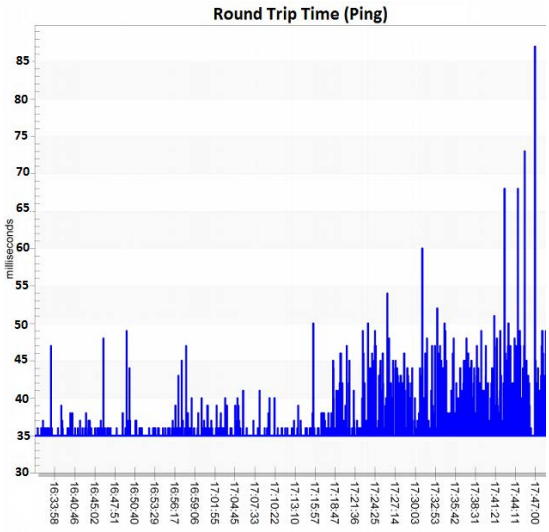


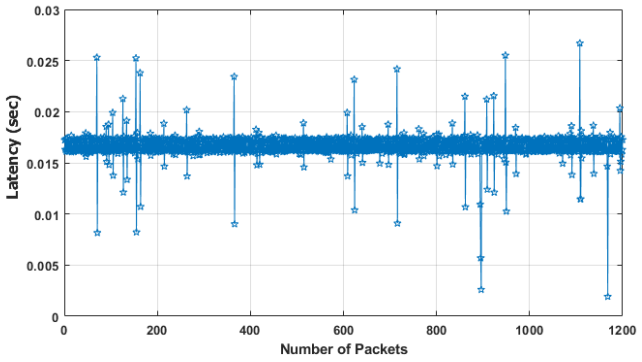
Fig. 3: Federated Testbed based Experimental Setup for attack-detection experiment

1) Network Packet Analysis : The total time for receiving the network packets depends on various factors such as sampling rate, communication latency, additional communication system delays, processing and computation times. In this experiment, we have computed the round trip time (RTT) during ping scanning, which is the length of time between the transfer of TCP/IP network packets to reach to its destination, and the arrival of an acknowledgement before sending the new packet. Figure 4(a) shows the ping latency distribution, where the regional control center is pinged every 0.5 *seconds*. It can be observed that the maximum latency is computed around 87 *milli-seconds*, while the minimum is approximately 35 *milli-seconds*. As a major latency factor, we have computed the data delay, which is the time delay from when measurements leave the substation PDC and reaches to the regional control center PDC. We have observed that the average value of computed delay is 16.6 *milli-seconds*, with a minimum of 1.9 *milli-seconds* and maximum of 26.7 *milli-seconds*.

2) Detection Rate Analysis : Based on the generated datasets at the regional control center, we have evaluated the performance of the anomaly detector in terms of accuracy, sensitivity, specificity, and precision to provide a comprehensive picture of how the classifiers are classifying the four



(a) Round Trip Time (RTT) delay



(b) PMU packets delay

Fig. 4: Latency for Round Trip Time (RTT) and PMU packets delay during live-streaming

events {0,1,2,3}. Sensitivity, also known as recall, defines the true positive rate (TPR), specificity defines the true negative rates (TNR), and the precision measures the positive predictive value. It can be observed that J48 decision tree (J48 DT) consistently performs better than the other classifiers including support vector machine (SVM), K-nearest neighbors (KNN), and Bayesian networks (Bayes Net). J48 DT exhibits an accuracy rate of 99.6%, precision rate of 98.38%, specificity of 99.89% and a sensitivity of 99.03%.

VI. CONCLUSION

The cyber physical system (CPS) federated testbed works as a driving force to enable the pipeline from state-of-the art research work through the transition to industry by experimental testing and validation. In this work, we have presented a cyber (network) based federated testbed; inspired by the NASPINet architecture, to evaluate the applied anomaly detector, as proposed in [6], in terms of network latency, communication bandwidth, and accuracy rate. We have implemented the realistic data integrity attacks targeting physical

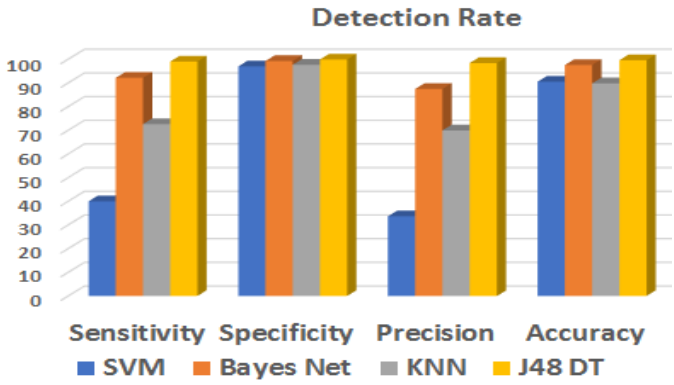


Fig. 5: Accuracy rate for different classifiers.

relays and substation RTUs, located at the ISU Power Cyber lab. We then validated the performance of a decision tree (J48) based anomaly detector, located at the ARL regional control center; for detecting tripping attacks, ramp and pulse attacks. Our experimental results showed that the computed maximum latency for incoming synchrophasor data packets is around 26.7 *milli-seconds*, with a round trip time of (RTT) 87 *milli-seconds*. This is well within the requirement of overloading based WAP scheme that has timing constraints in the order of seconds (1-100 seconds), however, it may affect the detection time for the applied anomaly detector. The decision tree based anomaly detection algorithm is shown to be consistently outperform the other machine learning classifiers. Future work will extend the cyber federation to a cyber-physical federation thus allowing distributed level system interaction and cyber security realted experiments on multiple testbeds.

REFERENCES

[1] M. Begovic et al., "Wide-Area Protection and Emergency Control," in Proceedings of the IEEE, vol. 93, no. 5, pp. 876-891, May 2005.
[2] NERC Draft, "Reliability Guide, PMU Placement and Installation", May 2016.
[3] Industrial Control System Cyber Emergency Response Team (ICSCERT), "Monitor (ICS-MM201212)", January 2012 [Online].
[4] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, Cyber-physical security testbeds: Architecture, application and evaluation for smart grid, Smart Grid, IEEE Transactions on, vol. 4, no. 2, pp. 847855, 2013.
[5] V. Kumar Singh, A. Ozen and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," 2016 North American Power Symposium (NAPS), Denver, CO, 2016, pp. 1-6.
[6] V. K. Singh, M. Govindarasu, "Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data," IEEE Power and Energy Society 2018 General Meeting, August 5-9, 2018, Portland, Oregon, USA, 2018.
[7] Iowa State University, "Iowa State awarded NSF Global City Teams Challenge project," September 2015.
[8] K. G. Ravikumar et al., "Distributed simulation of power systems using real-time digital simulator," 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, 2009, pp. 1-6.
[9] NIST, Cyber-physical Systems for Testbed Design, March 09.2016.
[10] B. Palmintier et al., "A Power-Hardware-in-the-Loop Platform with Remote Distribution Circuit Co-simulation," IEEE Trans. Ind. Electron., vol. 62, no. 4, pp. 2236–2245, Apr. 2015.
[11] Heather Lammers, INL and NREL Demonstrate Power Grid Simulation at a Distance URL, May 4, 2015.
[12] V. K. Singh, A. Ozen and M. Govindarasu, "A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid," 2018 Resilience Week (RWS), Denver, CO, 2018, pp. 63-69.