Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid

R. Liu, *Student Member, IEEE*, C. Vellaithurai, *Member, IEEE*, S. Biswas, *Student Member, IEEE*, T. Gamage, *Member, IEEE*, A. Srivastava, *Senior Member, IEEE*

***Abstract*—With ongoing smart grid activities, advancements in Information and Communication Technology (ICT) coupled with development of sensors are utilized for better situational awareness, decision support, and control of the power grid. However, it is critical to understand the complex interdependencies between cyber and power domains, and also the potential impacts of cyber events on the power grid. In this paper, the impact of three different possible cyber events on physical power grid have been analyzed using an integrated cyber-power modeling and simulation testbed. Real-time modeling of end-to-end cyber-power systems have been developed with hardware-in-the-loop capabilities. Real-Time Digital Simulator (RTDS), synchrophasor devices, DeterLab, and Network Simulator-3 (NS-3) are utilized in this developed testbed with a wide-area control algorithm and associated closed-loop control. DeterLab can be used to model real-life cyber events in the developed cyber-physical testbed. Man-in-the-middle and denial-of-service attacks have been modeled as specific cases for IEEE standard test cases. Additionally, communication failure impact on the power grid has been analyzed using the testbed.**

***Index Terms*—Cyber-Power, Real-Time Simulation, NS-3, DeterLab, RTDS, Wide-Area Control, Cyber Security, Synchrophasor Devices**

I. Introduction

The impact of cyber attacks on power systems has been at the forefront of research in recent years. Smart grids – traditional electric power grids augmented with highly integrated communication and computational capabilities – depend significantly more on data transfers, with higher quality of service (QoS), than their traditional counterparts [1], [2]. Due to their highly integrated nature, smart grids are also more vulnerable to cyber threats and attacks. However, the true *cyber-physical* impact of such attacks is not always clear, and needs to be analyzed. An integrated cyber-physical testbed provides an excellent platform to understand the intricate relationship between the power system and the associated cyber system through real-time modeling and simulation, and to directly observe the in-depth impact of cyber events on the simulated power system.

This research was funded in part by Department of Energy (DoE) Award Number DE-OE0000097 (Trustworthy Cyber Infrastructure for the Power Grid).

R. Liu, A. Srivastava are with the School of Electrical Engineering and Computer Science, Washington State University, Pullman WA 99164 USA, e-mail: asrivast@eecs.wsu.edu.

T. Gamage is with the Southern Illinois University, Edwardsville, IL 62026 USA

C. Vellaithurai is with Schweizer Engineering Laboratories (SEL), Pullman, WA 99163 USA.

S. Biswas is with the ALSTOM, Redmond, WA, USA

Most of the existing research work have explored either cyber system or power system vulnerabilities, but not both in a comprehensive and truly integrated manner. In [3], the authors present the impact of data integrity attacks on voltage control loop. In [4], the impact of cyber attacks on transient stability of smart grids with voltage support devices is discussed. A framework that models a class of cyber-physical switching vulnerabilities in smart grid systems is found in [5]. An address resolution protocol (ARP) spoofing based man-in-the-middle attack has been shown in [6].

Most recent testbed development efforts suggest to have one or more of the following disadvantages: (i) lack of hardware interface to integrate the real hardware-in-the-loop; (ii) lack of end-to-end system modeling; and (iii) lack of real time dynamic unbalanced system simulation. For example, the national SCADA testbed (NSTB) [7] utilizes actual physical grid components including generation, transmission, and communication networks, in addition to incorporating real world data from industry collaborators[1]. Virtual control system environment (VCSE) [8] uses OPNET as the network simulator and PowerWorld as power system simulator, and provides a platform for creating a large-scale control system test environment. SCADA CST [9] is similar to VCSE except that it uses the real-time immersive network simulation environment (RINSE) to simulate the communication network. A virtual power system testbed that utilizes RINSE and PowerWorld is found in [10]. A hardware-in-the-loop testbed that uses the real-time digital simulator (RTDS) as the power system simulator is found in [11]. GECO testbed [12] utilizes GE's positive sequence load flow (PSLF) and network simulator-2 (NS-2). The Iown State University testbed [13] uses RTDS and the internet-scale event and attack generation environment (ISEAGE).

In this work, our goal is to analyze the direct cyber-physical impact of specific cyber attacks on the power system not limited by the observed cyber vulnerabilities of the given power system. To reach this goal, a comprehensive and reconfigurable cyber-physical testbed that can be used to model and simulate most practical cyber events is required. Towards this end, we've developed a comprehensive cyber-physical testbed for real-time end-to-end system simulation that integrates a simulated power grid, hardware sensors and controllers, industry grade substation and control center level data concentrators, emulated communication network, and

[1]NSTB has helped in identifying several cyber vulnerabilities and developed cost-effective methods for secure communication between control centers and remote devices

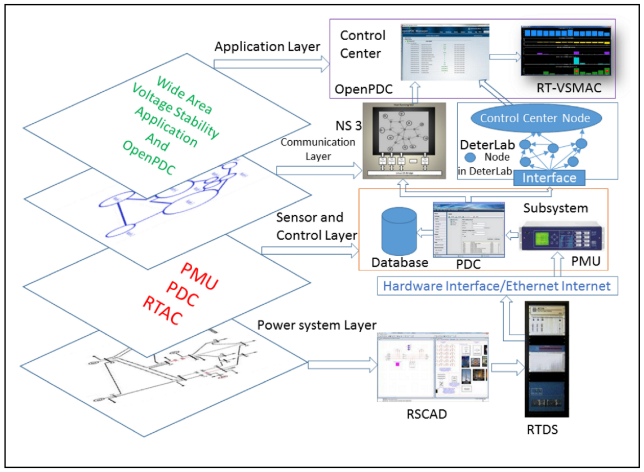


Fig. 1. Cyber-Physical TestBed Architecture

industry grade wide-area voltage stability applications. Our contribution also includes a high-level system cyber-physical security analysis framework. Standard IEEE test systems have been modeled and three different possible cyber attacks have been simulated to analyze their cyber-physical impact on the power system.

II. The Testbed Architecture

Four different layers have been modeled in the developed testbed. These are, (i) the power systems layer, (ii) the sensors and control layer, (iii) the communication layer, and (iv) the application layer. The data flow and the interconnection between different layers are shown in Figure 1.

A. The Power System Layer

The power system and associated control is modeled and simulated using RTDS and RSCAD®. RTDS is a fully digital power system simulator capable of continuous real-time operation, and is capable of digital and analog signal exchange through numerous dedicated high speed I/O ports. The physical protection, control, and measurement devices are interfaced with RTDS to interact with the simulated power system [14].

B. The Sensor Layer

The physical power system simulated by RTDS may have a number of substations where each substation may have multiple phasor measurement units (PMU) and phasor data concentrator (PDC) to collect local phasor measurements. Local substation databases are used to archive data to prevent any loss of data due to communication failures and to retrieve data once the communication is re-established. Satellite-synchronized clock provides a high accurate time synchronization signal to all the synchrophasor devices and simulators, such as RTDS, PMU, and PDC.

Four Schweizer Engineering Laboratories (SEL) devices and one giga-transceiver network communication card (GTNET) based simulated device are integrated into the testbed to monitor bus voltage phasors. Each SEL device has two PMU modules and the GTNET card is used to simulate additional software PMUs needs. The hardware PMUs are connected to RTDS through a giga-transceiver analog output (GTAO) Card. The connection between PMUs and the PDC is an ethernet connection. The connection channels built between the PDC and each PMU is based on the PMU ID, PMU port number, and the IP address. Synchrophasor data transmitted in the testbed are based on the IEEE C37.118-2005 protocol at a rate of 60Hz.

C. The Communication Layer

1) Network Simulator-3: The Network Simulator-3 (NS-3) is used to emulate the communication network that overlays the simulated power system. For the purpose of emulation, two kinds of net devices[2] are used in NS-3: emulation net devices; and tap net devices. An emulation net device allows NS-3 simulations to send data on a real network. A tap net device allows real or virtual host systems, which support virtual-network kernel devices, to participate in NS-3 simulations.

In NS-3, the protocol entities are designed to be similar to that of the real world protocols and the packet implementations are written similar to that of real world packets. With these features, the NS-3 simulated communication network is able to communicate with the external real networks, if necessary. The real-time implementation of NS-3 schedules events by using the time synchronization signal from the SEL satellite-synchronized clock which also supports the time signal to all other synchrophasor devices in the testbed.

All data transfers between the control center and substations will pass through emulated communication network in real-time. The emulated communication network also needs to emulate the delays that occur in real world communication networks. NS-3 provides network processing delay, signal propagation delay, transmission delay, and queuing delay as a result of communication network emulation [15].

2) DeterLab: DeterLab is another optional communication network simulator which can be integrated into the developed cyber-physical testbed. The architecture of the cyber-physical testbed integrated with DeterLab is shown in the Figure 2. DeterLab is a shared testbed facility designed for repeatable, controlled experiments on networking and cyber-physical research. In the DeterLab, hundreds of processors, several special hardware tools, and some software tools are integrated to create dynamically reconfigurable cyber security experiment [16]. DeterLab also provides the Security Experimentation EnviRonment (SEER), which integrates number of tools and agents to assist in setting up, performing, monitoring, and analyzing an experiment in the DeterLab environment. SEER consists of traffic tools, attack tools, traffic monitoring, and analysis tools.

D. The Application Layer

Several power engineering applications have been integrated with the developed cyber-physical testbed. One of these applications, the "RT-VSMAC tool" [17] has been discussed here

[2]A node in NS-3 is equivalent to a process of a computer, while a net device represents the network cards and network device drivers.

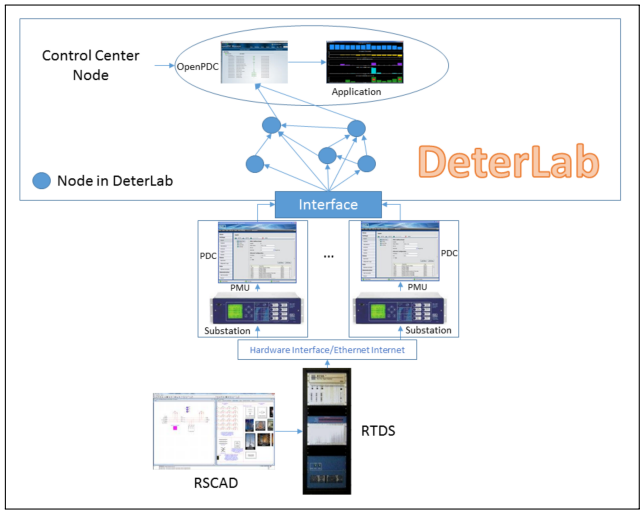


Fig. 2. Cyber-Physical Testbed Architecture with DeterLab

for real-time voltage stability monitoring and adaptive control. The RT-VSMAC tool is utilized as an energy management system (EMS) application in the testbed. Voltage measurements and breaker status data are collected from the power system using SCADA and/or synchrophasor technology and fed to the state estimator (SE) in the control center. The RT-VSMAC tool gets its input data from the SE output. The RT-VSMAC tool has the following major modules:

1) Real-time Voltage Stability Monitoring Engine: This module computes the "voltage stability assessment index" (VSAI) non-iteratively for a given power system, every time a new set of measurement data is obtained from the SE. The governing equation used to calculate VSAI for each bus is given by:

$$VSAI_{Load(i)} = Z_{Load(i)}/Z_{SCTh(i)}$$

where $0 \leq VSAI_{Load(i)} \leq 1$. Here, $Z_{SCTh(i)}$ is the system centric thevenin's equivalent impedance w.r.t. load bus 'i' and $Z_{Load(i)}$ is the impedance of the load bus 'i'. These quantities are based on phasor measurements at load bus and system topology information. Futher deatils are available in [18] [17] and not provided here due to page limitiation.

If the VSAI value at a particular load bus is close to '0', it indicates that the load bus is highly voltage stable. On the other hand, a VSAI is close to '1' indicates that the load bus is near the point of voltage collapse. The system VSAI is given by the VSAI of the weakest bus in the system.

2) Control Resource Status Information Database: This module archives the real-time status information of the different control devices / equipments available in the monitored system for the purpose of voltage stability control. This may include the status based on availability of installed control devices/mechanism:

(i) Line switching
(ii) Transformer automatic load tap changer blocking
(iii) Shunt reactive power compensation
(iv) Series reactive power compensation
(v) Generator reactive power control
(vi) Load priority for load shedding

3) Voltage Stability Controller - Normal Mode: This aims at generating minimum set of control actions at once to improve the voltage stability of a power system, if the real-time voltage stability monitoring engine detects one or more buses violating the VSAI alarm limit set by the operator. The normal mode internally strategizes the different types of coordinated wide-area control actions and estimates their effects at each internal stage using an internal voltage stability estimating engine, before finally listing the set of effective control actions that need to be generated. While performing the control strategies at each internal stage, this mode takes into account the coordinated decisions made by the control action activation sub-module (CAAS) and/or control action deactivation sub-module (CADS) along with the automatic hunting detection sub-module (AHDS). CAAS aims at strategizing the activation of coordinated control actions at each internal stage involving individual control blocks as per their availability that is archived and updated in the control resource information database. CADS aims at deactivating the excess control actions that have been previously activated by CAAS, thus ensuring that efficient use of system control resources are made at all times. There may arise situations when CAAS and CADS contradict each other, resulting in hunting between their actions. These kind of situations are automatically detected by AHDS, resulting in prevailing control actions decided by the CAAS.

4) Voltage Stability Controller - Emergency Mode: If the SE computation timestep is lower than the timestep of the normal mode, or if the system voltage stability is critical enough to require immediate control actions, the RT-VSMAC tool switches to the voltage stability controller mode - emergency mode. This generates multiple sets of control actions in multiple steps, each set at a time based on the feedback from SE, to improve the voltage stability of the power system, if the engine (refer Sec. II-D1) detects one or more buses violating the VSAI alarm limit set by the operator. At each step, the emergency mode strategizes and generates the different types of coordinated wide-area control actions in a completely non-iterative manner, thus involving minimal computational time. While performing the control strategies at each step, this mode takes into account the coordinated decisions made by CAAS and/or CADS along with AHDS. The individual roles of these sub-modules remain exactly the same as that in the voltage stability controller - normal mode. As the emergency mode strategizes control action set for each step based on feedback from the SE at the beginning of that step, hence this mode is inherently self-corrective in nature.

Although, this mode has the capability to rapidly strategize necessary control actions, when operating in this mode, more number of control actions will be eventually required to improve the system voltage stability as compared to just one set of control actions required by the normal mode.

III. Applications of the Developed Testbed

The developed cyber-physical testbed is able to perform real-time, end-to-end system simulations with hardware-in-the-loop capability in flexible manner. This developed cyber-

physical testbed can be used for multiple applications as listed here.

A. Vulnerability Assessment

A typical cyber-physical system consists of many different hardware, software, communication protocols, and protection control, each with vulnerabilities specific to them. However, system level vulnerability analysis and assessment require an integrated approach, instead of a piecemeal assessment. Vulnerability assessment, vulnerability scanning, and software test could be conducted using the approach for a cyber-physical testbed in [19]. Another testbed [20] shows the cyber security vulnerability of the control system using NSTB, which can be easily extended to this testbed. In [21], [22], authors of these papers presented an integrated cyber-physical vulnerability analysis and utilized for the real time modeling.

B. Real World Cyber Events Simulation and Impact Analysis

Our two different communication network simulators offer various options to simulate real world cyber events. With the ability of real world cyber events simulation, impact can be easily realized. Possible cyber attacks which could be simulated in the DeterLab and extended in this paper are discussed in [23]. Impact of different cyber events listed in [13] can be analyzed using the developed testbed. This paper has demonstrated impact of communication outage, MITM and DoS attacks on the physical system.

C. Security Control Validation

Since both cyber system and physical system are simulated in the testbed, different security controls could be integrated into the testbed, such as SSL/TLS, secure key storage, key distribution, and key escrow. The performance of these security controls against various cyber attacks could be directly observed from the testbed.

D. Testing of New Applications

Cyber-physical testbed is a great platform to test new smart grid applications. The performance of these new applications in different operating conditions can be tested and the performance of these new applications under various cyber or physical incidents can also be validated.

E. Hardware Device Testing

With the hardware in-the-loop, end-to-end features, the cyber-physical testbed could also be used to test the emerging hardware devices, such as PMU and PDC [24] [25].

F. Operators Training and Education

Normally, power system operators gain experience and expertise through working with an actual system. A better training and transfer of experience is needed to make sure that inexperienced operators can acquire experience without any damage to the grid. Cyber-physical testbed could simulate and demonstrate different situations and possible cyber attacks in the real world. Operators could gain the experience of many realistic conditions from both power and cyber systems. In [26], authors utilize cyber-physical co-simulation platform for the education and the training.

IV. Cyber Event Categorization

Recent R&D efforts have placed a heavy emphasis on improving the *situational awareness* of the power grid operators. Power grid WAN applications, especially those based on PMU technology, play a pivotal role in these efforts as they provide the ability to make control decisions based on (near) real-time, accurate state of the system. Consequently, the stringent availability and communication latency requirements of these applications make QoS [2] of the delivered data an implicit aspect of *cyber-physical security* analysis. For example, untimely data, inputs, or outputs, even though not tampered, can potentially lead to erroneous decisions. Such aspects are beyond the traditional notion of security that revolves around the concepts of Confidentiality, Integrity, and Availability.

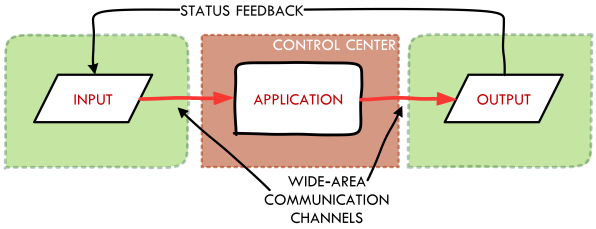


Fig. 3. The Wide-Area Closed-Loop Cyber Events Analysis Engine

The end-to-end cyber-physical security of the smart grid can be conceptualized using the wide-area closed-loop cyber events analysis engine depicted in Figure 3. Here, hardware field devices at substation level, such as PMUs and various control actuators, are represented by input and output respectively. The communication network is represented by the wide-area communication channels and status feedback channels. Application represents power grid WAN applications (such as those described in Section II-D) and the associated software and hardware components.

Cyber events – both intentional acts of sabotage and random hardware or software failures – can impact the proper operation of the wide-area closed-loop decision engine. These events can be broadly categorized into four categories as follows:

(i) events that affect physical equipment;
(ii) events that affect communication channels;
(iii) events that affect applications; and
(iv) events that affect data.

A. Cyber Events on Physical Equipment

Physical equipment, as they are inherently exposed, provide malicious entities with the opportunity to launch attacks with relatively low effort but with substantially high impact, thus is considered one of the most trivial attacks on any cyber-physical system. Disabling or tampering with physical equipment can easily render them unavailable at critical times of

operation. Compromised physical equipment is much more dangerous than ones that have been maliciously disabled as they will continue to produce and feed ambiguous input to the system. The Stuxnet virus [27] is one such example. Attacks on physical equipment can lead to attacks on availability and integrity of signals, therein compromising the integrity of the system's overall operation. Beyond these, physical equipment are prone to attacks on the QoS of the signals they generate. For example, a compromised critical device may continue to operate slowly than what's required by the corresponding application, even though the signals produced are reflective of the actual system, which triggers usability concerns of the signals.

B. Cyber Events on Communication

Many classic cyber attacks – man-in-the-middle, black-hole, etc.– target communication channels of the system with the objective of compromising the confidentiality, integrity, availability, or a combination of those. Given that WAN applications place a heavy reliance on wide-area communication channels, cyber events that can affect tight delivery guarantee requirements or latency requirements can also have serious impact on the overall system operation. Even when the underlying physical equipment is operating as intended by their design, a carefully crafted attack on communication channels can leave the operator left in a state of ambiguity of the true state of mission critical equipment.

C. Cyber Events on Applications

Compared to the previous two categories, attacks on applications are much more complex to execute in nature and needs significant coordination. These attacks usually encompass attacks on physical equipment and communication channels including exploiting software bugs, open ports and other points of intrusion, exploiting known vulnerabilities and limitations in any dependent technologies, software, and underlying hardware, etc. False data injection attacks – which exploit a mathematical weakness in the state estimation algorithm –, buffer over flow attacks, buffer over read attacks (such as the recent Heartbleed vulnerability) are some examples of attacks on applications.

D. Cyber Events on Data

Attacks on data can be considered as a generalization of all three attack categories described above as there are tight interdependencies between data, equipment, communication, and applications. For example, critical physical equipment can be manipulated to produce useless or unusable data. Communication channels can be exploited to produce data that does not meet the corresponding application's QoS requirements. Applications can be exploited to force them to use data outside their specifications. Beyond these, there are also other attack avenues such as exploiting critical storage limitations.

Our testbed is specifically developed to provide critical analysis capabilities of the impact of each of the these cyber event categories. More specifically, cyber events that affect physical equipment can be modeled in the power system and sensors layers (Sections II-A and II-B) so that their real-time impact can be analyzed as well as visualized. Cyber events that affect communication can be modeled in the communication layer (Section II-C), and cyber events that affect applications and data can be modeled in the application layer (Section II-D).

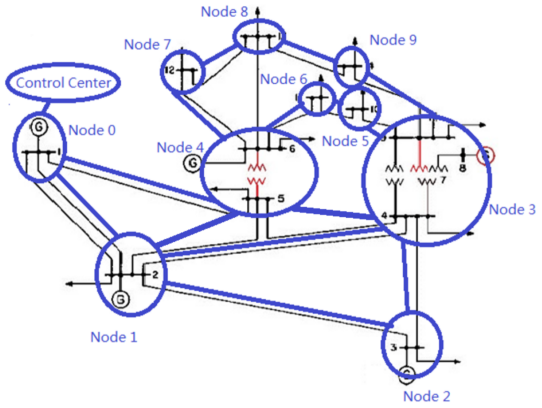


Fig. 4. Communication Model for the IEEE 14-Bus Test System

V. Testbed Capabilities in Analyzing Cyber Events

As proof of concept, we present cyber-physical impact analysis of three cyber events as follows. The IEEE 14-bus test system is used the model physical power system with the communication overlay model depicted in Figure 4. Without loss of generality, we consider these three case studies as intentional acts of sabotage, hence cyber attacks.

A. Physical Attack: Communication Line Outage

The objective of this attack is to exploit a critical path in the communication network and to induce significant communication delay by rendering it unavailable during a critical data transmission corridor. We consider the communication delay is proportional to the length of the transmission line.

Consider Figure 4. Under normal operating conditions, the communication link between $node_0$ and $node_1$ serve as the critical path as it offers the shortest path (hence, least communication delay) between $node_0$ and $node_4$. When the aforementioned link is not available, the data has to take a much longer route through $node_3$ and $node_0$ to reach the control center, which can potentially induce a significant delay.

B. Data Attack: Denial of Service

In the wide area network, there are several possible vulnerabilities to access PMU communication network. For example, attacker can install malware on the router located at substation. Another possibility is devices with default password (which is often the case) allowing attacker to get the access into the communication network by guessing the default password. In this DoS attack, the attacker is assumed to target the communication interface on the $node_9$ with a TCP SYN flood

attack. To cause SYN flood attack, an attacker can send a succession of SYN requests to consume server resources as much as possible and to make the system unresponsive to legitimate traffic. Attacker can cause malicious client to simply not send the expected ACK, or attacker can spoof the source IP address and send the SYN-ACK to a falsified IP address. Results are shown in the Section VI. The impact of DoS attack on the power system and wide-area voltage stability monitoring and control application is also analyzed.

A denial-of-service (DoS) attack is an attempt to make a critical resource unavailable to its intended users in a useful capacity when required. In the power system, it is important that all communication channels in the system are available as much as possible especially when the power system is operating near a point of instability where an important control action needs to be taken. If the DoS attack is successful in such a situation, it is quite hard to maintain the level of reliability that is deemed required by the modern power grids.

C. Communication Attack: Man-in-the-Middle

The man-in-the-middle (MITM) attack is a form of active eavesdropping in which the attacker makes independent connections with both endpoints of a compromised communication and relays information between them, so the victims are led to believe that they are talking directly to each other over their private connection. In the real world, some of the utilities still use normal UDP protocol following IEEE Std C37.118.1a-2014 to transmit PMU measurement data, and there is no other cyber protection controls, such as SSL. This can give an attacker a chance to do the MITM attack. On the other hand, for the wide area network from substation to control center, some of the utilities use the public communication line and other utilities use the private communication line. For the public communication line, it is easy to find vulnerabilities which could be used to let the attacker get into the network. For the private communication line, the attacker also could find these communication line and use the hardware access to get into this private communication network. A successful comprehensive MITM attack will give the attacker the same observations made by the control center operators, which he could use to exploit critical components of the system for future attacks (such as the one described in section V-A). The attacker could also use a MITM attack to corrupt information including control command, measurement value, price signal, etc., in the transmitted packets.

Figure 5 shows the architecture of the MITM attack. Under normal operating conditions, the local PDC directly sends the synchrophasor data to the control center, but during the attack, it is assumed that the attacker uses ARP spoofing [6] to poison the two communication endpoints in such a way that the local PDC sends data, which was originally intended to the control center, to the attacker's computer. Thus, the attacker can silently sit between the local PDC and the control center. The attacker manipulates each IEEE C37.118 based data packets by changing the payload, which in this case is the synchrophasor data related to the VSAI calculation.

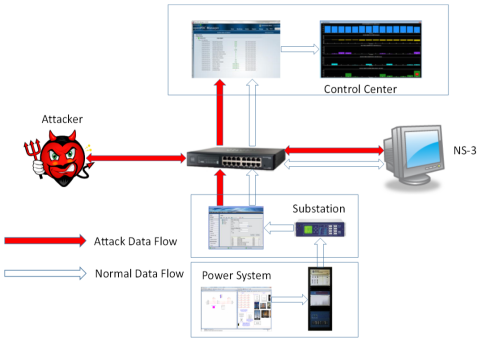


Fig. 5. Man-in-the-Middle Attack Setup

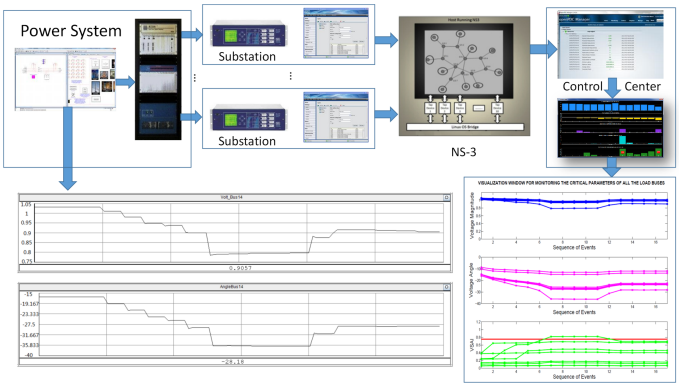


Fig. 6. Simulation Architecture

VI. Simulation Results

The testbed setup consists of a modified IEEE 14-bus system that is made completely observable using PMUs, and automated closed-loop control is used with the RT-VSMAC tool as the controller application. The simulation architecture is shown in Figure 6.

TABLE I
SEQUENCE OF EVENTS LEADING TO A POSSIBLE VOLTAGE COLLAPSE

Event	Timestamp	Event Description
1	t=5s	Base Case.
2	t=10s	Load at bus_9 increase to real power consumption 59MW and reactive power consumption is 33.2MVAR. (Base Case: 29.5MW and 16.6MVAR)
3	t=15s	Load at bus_{14} increase to real power consumption 29.8MW and reactive power consumption is 10MVAR. (Base Case: 14.9MW and 5MVAR)
4	t=20s	Load at bus_{14} increase to real power consumption 44.7MW and reactive power consumption is 15MVAR.
5	t=25s	Load at bus_{13} increase to real power consumption 27.6MW and reactive power consumption is 11.6MVAR. (Base Case: 13.5MW and 5.8MVAR)
6	t=30s	Load at bus_{14} increase to real power consumption 59.6MW and reactive power consumption is 20MVAR.
7	t=35s	Load at bus_{14} increase to real power consumption 89.4MW and reactive power consumption is 30MVAR.

A. Stressed System Operation without Cyber Events

In the normal system operation with stressed condition, the timeline of several events for load increase is shown in the Table I. The time interval between each event is 5s. When the wide-area monitoring and control application detects VSAI goes over the threshold 0.75, it calculates the control action based on possible control component and system status. All the control actions have been modeled using the RTDS. All the simulation results shown are created in the MATLAB® based on the real-time values obtained from RTDS.

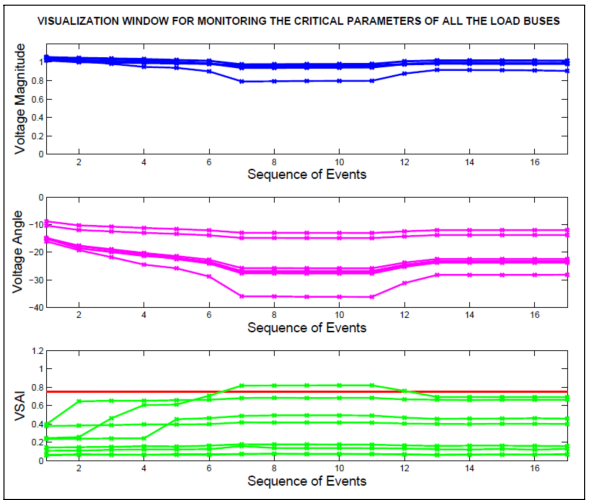


Fig. 7. Wide-Area VSAI and Voltage Phasor Data for Normal Condition

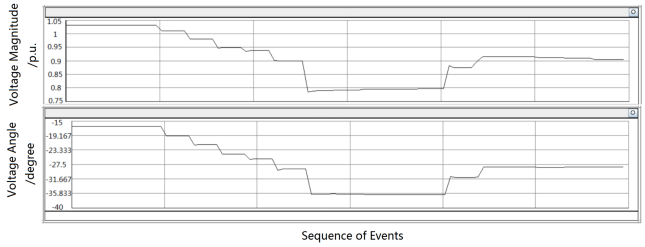


Fig. 8. The Changes in Voltage Magnitude and Angle on bus_{14} for Substation View

The changes in voltage data and VSAI have been shown in Figure 7. Control actions is taken by RT-VSMAC from $event_7$ onwards. All the control actions made by RT-VSMAC Tool are shown in the Table II. The first four control actions from $event_8$ to $event_{11}$ relates to inserting shunt capacitor banks on bus_9 and on bus_{14}. These control actions do not change the VSAI to the desired value, next two control actions at $event_{12}$ and $event_{13}$ are local load shedding. which brings VSAI below the threshold. To keep the availability of the control resource, RT-VSMAC automatically deactivates the ineffective controls. The performance of these control actions are also shown in the Figure 8, which is the voltage magnitude and angle at the bus 14 from RTDS. Both of the voltage magnitude and angle increases, when the control actions are taken by RT-VSMAC on bus_{14} as shown in Figure 8.

TABLE II
SEQUENCE OF EVENTS WITH RELATED CONTROL ACTIONS FOR NORMAL CONDITION

Event	Time	Event Description
8	t=40s	Control Action by RT-VSMAC Tool: Capacitor rated 1 MVAR connected at Bus-14
9	t=45s	Control Action by RT-VSMAC Tool: Capacitor rated 2 MVAR connected at Bus-14
10	t=50s	Control Action by RT-VSMAC Tool: Capacitor rated 1 MVAR connected at Bus-9
11	t=55s	Control Action by RT-VSMAC Tool: Capacitor rated 2 MVAR connected at Bus-9
12	t=60s	Control Action by RT-VSMAC Tool: Load-shedding at Bus-14: Real Power Loading at Bus-14 to 70.775 MW Reactive Power Loading at Bus-14 to 21.8706 MVAR
13	t=65s	Control Action by RT-VSMAC Tool: Load-shedding at Bus-14: Real Power Loading at Bus-14 to 56.8063 MW Reactive Power Loading at Bus-14 to 17.1831 MVAR
14	t=70s	Control Action by RT-VSMAC Tool: Capacitor rated 1 MVAR disconnected at Bus-9
15	t=75s	Control Action by RT-VSMAC Tool: Capacitor rated 2 MVAR disconnected at Bus-9
16	t=80s	Control Action by RT-VSMAC Tool: Capacitor rated 1 MVAR disconnected at Bus-14
17	t=85s	Control Action by RT-VSMAC Tool: Capacitor rated 2 MVAR disconnected at Bus-14

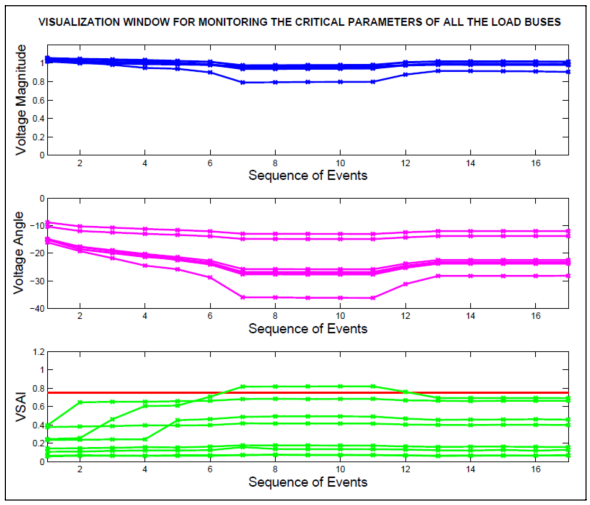


Fig. 9. Wide-Area VSAI and Voltage Phasor Data for Communication Line Outage Attack

B. Stressed System Operation with Cyber Events

1) Impact of Communication Line Outage: In the communication line outage simulation (refer section V-A), the attacker causes a communication line outage at $event_4$. The resulting observations are shown in Figure 9. As seen, there are no obvious delays that would be large enough to cause a substantial error in either control action generation or actuation. Thus, for this specific case study, the communication line outage attack does not have a substantial impact on the power system. The reasoning for this lies in the large bandwidth defined for each communication link in NS-3 being 50Mbps and the normal packet traffic from all nodes to the control center is just ˜50KBps, thus losing one communication line does not

sufficiently cause data congestions or delays. On the other hand, the delay on the communication line between $node_0$ and $node_4$ is 1.1469ms, which is relatively large in the simulated communication network, but this delay will not impact real time voltage stability control operation.

Given that the PMU-based applications are still in their infancy, dedicated fiber optics for PMU communication will be under utilized (a lot of free bandwidth) in the short term. but is anticipated to pick up in the near future. Furthermore, PMU technology is still quite expensive, thus, their deployment not intensive in most places in the national power grid. This further justifies why a small portion of the available bandwidth is currently occupied in our testbed setup. Since communication line is part of the cyber infrastructure of the power system, this test shows that N-1 criterion can also be applied for communication system.

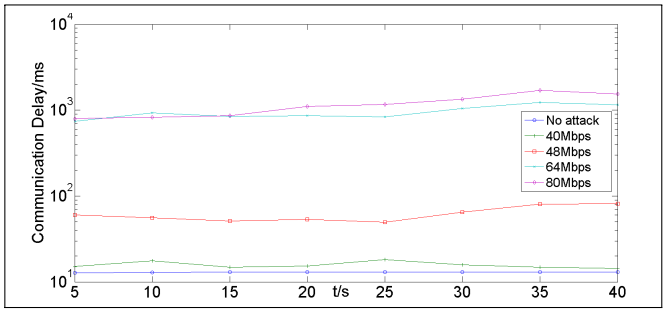


Fig. 10. Communication Delay on $node_9$ for DoS Attack

2) Impact of Denial of Service: In the DoS attack simulation (refer section V-B), the attacker floods the communication interfaces on $node_9$ in order to disrupt the PMU data from $node_9$. Because of the DoS attack, traffic congestion happens on the $node_9$, communication delay and small amount of packet loss appear on data stream sent from $node_9$. Figure 10 shows the impact of the DoS attack on the $node_9$ data stream communication delay from 5 situations. X-axis represents the length of the attack and y-axis shows the $node_9$ packets communication delay. From Figure 10, for 40 Mbps attack rate, the communication delay increases a little on $node_9$ data stream compared with no attack situation. When the attack rate reaches 64 Mbps, the serious communication delay, which is almost 100 times than no attack situation, is added to all the packets sent from $node_9$. During the attack, RT-VSMAC detects that one of the phasor data streams has large communication delay compared with other phasor data streams, which could indicate (from the control centers pespective) either a communication failure, a power system failure, or some other benign failure. In order to prevent making wrong control actions based on the bad data, RTVSMAC keeps using previous VSAI data until all phasor data streams recover back to the normal condition. In this DoS attack, bad input let the application enter the safety mode and the application gives the bad output according to the bad input, finally bad control action is sent back to power system, which may lead to a blackout, such as the 2011 San Diego blackout. If the attacker misled the control center to cut 500kV transmission line, this may lead to a blackout.

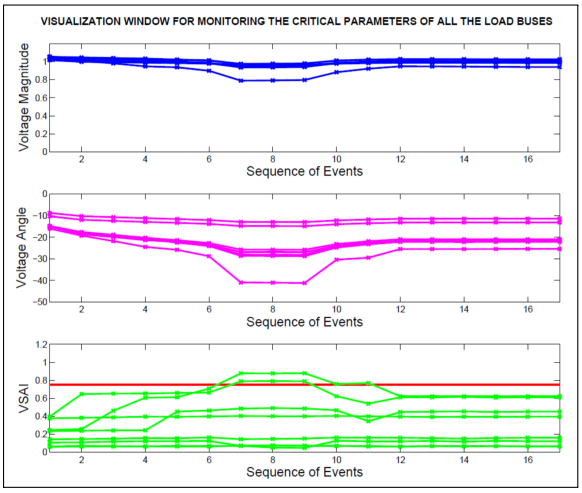


Fig. 11. Wide-Area VSAI and Voltage Phasor Data for MITM Attack

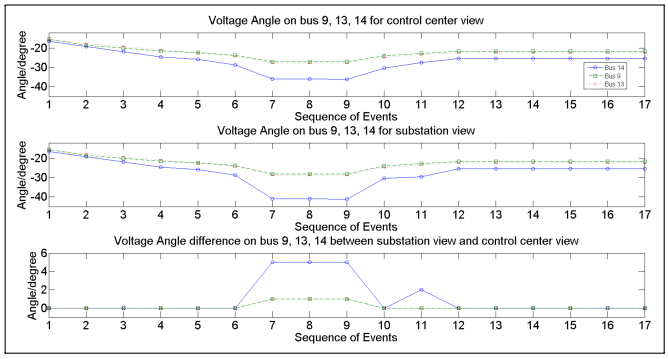


Fig. 12. Voltage Angle Value at $buses_{9,13,14}$ for MITM Attack

3) Impact of Man-in-the-Middle Attack: In the MITM attack (refer section V-C), the attacker silently sits between the substation and control center (communication) and at $event_6$ initiates the false data injection attack in two different methods. In the first method, the attacker hides the real system status from the control center by dropping all the data and only sending data at $event_6$, so that RT-VSMAC could not detect that the system VSAI has already breached the VSAI threshold. Thus, the initial observations of this attack are similar to that of the DoS attack.

In the second method, the attacker manipulates the phasor data on multiple buses, as shown in the Table III. Based on the false data, control center considers the power system as more stressed than its true status. From Figure 12 and Table III, there are two more load shedding control actions than that of the no cyber events condition. The first excess control action is remote load shedding at bus_9 and the second excess control action is local load shedding at bus_{14}. With these two extra control actions, there are 36% additional load shedding at bus_{14} and 51.625 MW additional load shedding at bus_9 compared to the normal condition. From Figure 12, it is also obvious that the voltage angle is different from the substation data and control center data due to the manipulation from the attacker. Under this condition, the attacker successfully manipulated the input data to mislead the application to generate inaccurate output signals.

TABLE III
SEQUENCE OF EVENTS WITH RELATED CONTROL ACTIONS FOR MITM CONDITION

Event	Time	Event Description
7	t=35s	Increasing the loading at Bus-14: Real Power Loading at Bus-14 to 89.4 MW Reactive Power Loading at bus-14 to 30 MVAR The voltage phasor data corresponding to this updated data is changed by cyber attack (man-in-the-middle attack) and hence this changed data is fed to the input of the RT-VSMAC Tool. Changed data are: [1] Decrease in Bus Voltage Angle at Bus-9 by 1 ° [2] Decrease in Bus Voltage Angle at Bus-13 by 1 ° [3] Decrease in Bus Voltage Angle at Bus-14 by 5 °
8	t=40s	Control Action by RT-VSMAC Tool: [1] Capacitor rated 1 MVAR connected at Bus-9 [2] Capacitor rated 1 MVAR connected at Bus-14 MITM changed data are: [1] Decrease in Bus Voltage Angle at Bus-9 by 1 ° [2] Decrease in Bus Voltage Angle at Bus-13 by 1 ° [3] Decrease in Bus Voltage Angle at Bus-14 by 5 °
9	t=45s	Control Action by RT-VSMAC Tool: [1] Capacitor rated 2 MVAR connected at Bus-9 [2] Capacitor rated 2 MVAR connected at Bus-14 MITM changed data are: [1] Decrease in Bus Voltage Angle at Bus-9 by 1 ° [2] Decrease in Bus Voltage Angle at Bus-13 by 1 ° [3] Decrease in Bus Voltage Angle at Bus-14 by 5 °
10	t=50s	Control Action by RT-VSMAC Tool: [1] Load-shedding at Bus-9: Real Power Loading at Bus-9 to 51.625 MW Reactive Power Loading at Bus-9 to 21.8674 MVA (This is an excess amount of load-shedding performed due to cyber-attack) [2] Load-shedding at Bus-14 - Real Power Loading at Bus-14 to 70.775 MW Reactive Power Loading at Bus-14 to 21.8706 MVAR
11	t=55s	Control Action by RT-VSMAC Tool: [1] Load-shedding at Bus-14 - Real Power Loading at Bus-14 to 56.8063 MW Reactive Power Loading at Bus-14 to 17.1799 MVAR MITM changed data is: [1] Decrease in Bus Voltage Angle at Bus-14 by 2 °
12	t=60s	Control Action by RT-VSMAC Tool: [1] Load-shedding at Bus-14 - Real Power Loading at Bus-14 to 46.3297 MW Reactive Power Loading at Bus-14 to 13.6643 MVAR (This is an excess amount of load-shedding performed due to cyber-attack)
13	t=65s	Control Action by RT-VSMAC Tool: [1] Capacitor rated 1 MVAR disconnected at Bus-9
14	t=70s	Control Action by RT-VSMAC Tool: [1] Capacitor rated 2 MVAR disconnected at Bus-9
15	t=75s	Control Action by RT-VSMAC Tool: [1] Capacitor rated 1 MVAR disconnected at Bus-14
16	t=80s	Control Action by RT-VSMAC Tool: [1] Capacitor rated 2 MVAR disconnected at Bus-14

VII. CONCLUSIONS

In this paper, an end-to-end, real-time, hardware-in-the-loop cyber-physical testbed using Real-time Digital Simulator (RTDS), synchrophasor devices, NS-3, DeterLab and voltage stability applications has been presented. The developed testbed is used to demonstrate the impact of three possible different kinds of real-life cyber-attacks, which are communication line outage attack, denial-of-service attack, and man-in-the-middle attack, on the power system, specifically for wide-area voltage stability control algorithm. The developed testbed is much closer to the future realistic smart grid and will enable to understand the complex relationship between power system and cyber systems. Standard IEEE power system test cases are modeled and simulated to analyze the cyber-power interdependencies for specific cases and can be extended easily for additional test cases. Results demonstrate that the real-time, end-to-end comprehensive system model is required to analyze the impact of cyber events on the power grid dynamics and performance.

In our future work, we will analyze the effect of the different security control against the specific cyber attack and validate on our testbed. We will identify the critical defensive tools or mechanisms to improve the cyber-physical security of the power system.

REFERENCES

[1] U.S. Department of Energy, "National Electric Delivery Technologies Roadmap," Jan. 2004.

[2] D. Bakken, A. Bose, C. Hauser, D. Whitehead, and G. Zweigle, "Smart Generation and Transmission With Coherent, Real-Time Data," *Proc. of the IEEE*, vol. 99, no. 6, pp. 928–951, Jun. 2011.

[3] S. Sridhar and G. Manimaran, "Data Integrity Attack and Its Impacts on Voltage Control Loop in Power Grid," in *IEEE Power and Energy Society General Meeting*, July 2011, pp. 1–6.

[4] B. Chen, S. Mashayekh, K. Butler-Purry, and D. Kundur, "Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices," in *IEEE Power and Energy Society General Meeting (PES)*, July 2013, pp. 1–5.

[5] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A Framework for Modeling Cyber-Physical Switching Attacks in Smart Grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273–285, Dec 2013.

[6] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono, and H. Wang, "Man-In-The-Middle Attack Test-Bed Investigating Cyber-Security Vulnerabilities in Smart Grid SCADA Systems," in *International Conference on Sustainable Power Generation and Supply (SUPERGEN)*, Sept 2012, pp. 1–8.

[7] Idaho National Laboratory, "National SCADA Test Bed: Fact Sheet," 2007.

[8] M. McDonald and G. Conrad, "TC Service, and RH Cassidy. Cyber Effects Analysis Using Vcse," Tech. Rep. SAND2008-5954, Sandia National Laboratories, Tech. Rep., 2008.

[9] C. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development," in *38th North American power symposium (NAPS)*, 2006, pp. 483–488.

[10] D. C. Bergman, D. Jin, D. M. Nicol, and T. Yardley, "The virtual Power System Testbed and Inter-Testbed Integration," in *Conference on Cyber Security Experimentation and Test (CSET), USENIX Association*, 2009, pp. 1–6.

[11] M. Stanovich, I. Leonard, K. Sanjeev, M. Steurer, T. Roth, S. Jackson, and M. Bruce, "Development of A Smart-Grid Cyber-Physical Systems Testbed," in *IEEE PES Innovative Smart Grid Technologies (ISGT)*, Feb 2013, pp. 1–6.

[12] H. Lin, S. Veda, S. Shukla, L. Mili, and J. Thorp, "GECO: Global Event-Driven Co-Simulation Framework for Interconnected Power System and Communication Network," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1444–1456, Sept 2012.

[13] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, June 2013.

[14] A. Srivastava and N. Schulz, "Applications of Real Time Digital Simulator in Power System Education and Research," in *American Society for Engineering Education*. American Society for Engineering Education, 2009.

[15] S. S. Biswas, F. Shariatzadeh, R. Beckstrom, and A. K. Srivastava, "Real Time Testing and Validation of Smart Grid Devices and Algorithms," in *IEEE Power and Energy Society General Meeting (PES)*, 2013, pp. 1–5.

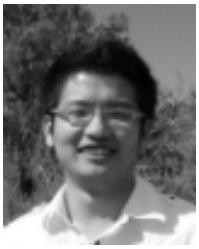
[16] The deter project. [Online]. Available: http://www.deter-project.org

[17] S. S. Biswas and A. K. Srivastava, "RT-VSMAC Tool: A Real Time Voltage Stability Monitoring and Adaptive Control Tool For Electric Power Grids," provisional U.S. patent filed, Washington State University, Pullman.

[18] S. S. Biswas and A. K. Srivastava, "Voltage Stability Monitoring in Power Systems," Patent U.S. 27 158.8052. US01 filed, 02 25, 2014.

[19] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec 2011.

[20] Idaho National Laboratory, "Common cyber security vulnerabilities observed in control system assessments by the INL NSTB program," Nov. 2008.
[21] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, March 2013.
[22] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "Cpindex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2014.
[23] J. Mirkovic and T. Benzel, "Teaching cybersecurity with deterlab," *Security Privacy, IEEE*, vol. 10, no. 1, pp. 73–76, Jan 2012.
[24] S. Biswas, J. H. Kim, and A. Srivastava, "Development of a smart grid test bed and applications in pmu and pdc testing," in *North American Power Symposium (NAPS), 2012*, Sept 2012, pp. 1–6.
[25] S. Biswas and A. Srivastava, "Tool for testing of phasor measurement units: Pmu performance analyser," *IET Generation, Transmission and Distribution*, August 2014.
[26] C. Vellaithurai, A. Srivastava, and S. Zonouz, "SECPSIM : A Training Simulator for cyber-power infrastructure security," in *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, Oct 2013, pp. 61–66.
[27] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec Security, Nov. 2010, http://goo.gl/dC8VT.



Ren Liu received his B.S. degree at Huazhong University of Science and Technology, China, in 2011 and the M.S. degree at Arizona State University in 2012. He is a Ph.D. student at Washington State University since 2013. His research interests are cyber-physical simulation and computational analysis for cyber-physical security.

Ceeman Vellaithurai received his B.E. degree in Electrical and Electronics Engineering from Anna University Tiruchirappalli, India, in 2011. He received his M.S. in Electrical Engineering with specialization in power systems from Washington State University, Pullman, Washington, USA in 2013. His research interests include real time modeling and simulation of cyber-power system. He is currently working at Schweitzer Engineering Laboratories Inc., Pullman, Washington, USA as a protection engineer. He received the Best Outgoing Student award from Anna University Tiruchirappalli for his academic achievements.

Saugata S Biswas received his B.E. degree in Electrical Engineering from Nagpur University, Maharashtra, India, in 2007. From 2009 to 2010, he was in the Mississippi State University as a PhD student. From 2011 to 2014, he continued as a PhD student at Washington State University. His research interests include synchrophasor device testing, real time voltage stability monitoring and control using synchrophasor technology, and substation automation technology for component level diagnostics and prognostics of substation health monitoring. He worked in the Design and Development Department of a Switchgear industry in India from 2007 to 2009. He received his Ph.D. degree in 2014 and is currently working at Alstom. He is the recipient of several Gold Medal awards from Nagpur University for his academic achievements during 2003-2007. He is the recipient of the 2013 EECS Outstanding PhD Student in Electrical Engineering award from Washington State University, Pullman.

Thoshitha Gamage is an Assistant Professor of Computer Science at the Southern Illinois University Edwardsville. He holds a B.Eng. in Computer Engineering (2006) from the University of Peradeniya, Sri Lanka, M.S. in Computer Science (2008) from the St. Cloud State University, and a Ph.D. in Computer Science (2011) from the Missouri University of Science and Technology. Dr. Gamages primary research interest is in cyber-physical systems and their overlap with computer security, distributed computing, and wide-area communication. In particular, Dr. Gamage is actively engaged in cyber security research for for critical infrastructure systems.

Anurag K. Srivastava received his Ph.D. from Illinois Institute of Technology (IIT), Chicago, in 2005. He joined Washington State University as Assistant Professor in August 2010. He worked as an Assistant Research Professor at Mississippi State University from 2005-2010. Before that, he worked as a Research Assistant and Teaching Assistant at IIT, Chicago; as a Senior Research Associate at the Indian Institute of Technology, Kanpur, India; and as a Research Fellow at the Asian Institute of Technology, Bangkok, Thailand. His research interests include power system operation, control, security, and stability within smart grid and micro grid. Dr. Srivastava is a senior member of the IEEE, past-chair of the IEEE PES career promotion subcommittee and chair of the IEEE PES student activities subcommittee. He is active in several other IEEE PES technical committees, serves as associate editor of IEEE Transactions on Smart Grid and IEEE distinguished lecturer.