Integrated Simulation to Analyze the Impact of Cyber-Attacks on the Power Grid

R. Liu, *Student Member, IEEE*, A. Srivastava, *Senior Member, IEEE*

***Abstract*—With the development of the smart grid technology, Information and Communication Technology (ICT) plays a significant role in the smart grid. ICT enables to realize the smart grid, but also brings cyber vulnerabilities. It is important to analyze the impact of possible cyber-attacks on the power grid. In this paper, a real-time, cyber-physical co-simulation testbed with hardware-in-the-loop capability is discussed. Real-time Digital Simulator (RTDS), Synchrophasor devices, DeterLab, and a wide-area monitoring application with closed-loop control are utilized in the developed testbed. Two different real life cyber-attacks, including TCP SYN flood attack, and man-in-the-middle attack, are simulated on an IEEE standard power system test case to analyze the the impact of these cyber-attacks on the power grid.**

***Keywords*—Cyber-Physical, Real-Time Co-Simulation, DeterLab, RTDS, Cyber Security, Synchrophasor Devices**

I. Introduction

In the last couple of years, the number of smart grid projects have been growing fast [1]–[3]. According to IEEE definition of smart grid, the main difference between smart grid and conventional electrical power grid is the increased use of communication and information technology [4], [5], which leads to a more reliable and efficient power grid. However, this new feature also brings several disadvantages, such as complex interdependencies between cyber and power domains, and additional vulnerabilities into the power grid. An integrated cyber-physical testbed allows to understand the intricate relationship between the power system and the associated cyber system through real-time modeling and simulation. There are number of efforts by other researchers to develop cyber-physical testbed to analyze the interdependencies of different domains within the smart grid. Each of these testbeds has their own unique advantages and limitations. The Experimentation Platform for Internet Contingencies (EPIC) is a testbed that can provide assessment of the impact from cyber-attack on both cyber and power domain. In EPIC, MatLab is used to simulate the power system and emulab is utilized to emulate the communication network [6]. Another testbed designed at Royal Institute of Technology (Sweden) is used for to analyze the ICT architecture impact on the power monitoring and control system's reliability. The MatLab Simulink is used for the power system simulation and the communication network is simulated by OPNET [7]. In order to make the assessment of power system wide area measurement and control schemes, a Global Event-driven Co-simulation framework (GECO) is developed at Virginia Tech. PSLF is used to simulate the power system and NS2 is the simulator for the communication network [8]. Researchers at the Austrian Institute of Technology have developed a co-simulation training platform for education and training. In this platform, GribLAB-D is utilized to simulate the power system and NetSim has been used for communication network simulation [9]. In order to evaluate the real-time performance of Cyber-Physical system, a co-simulation platform called INSPIRE is presented in [10]. In this paper, DIgSILENT Power Factory is used to simulate electromechanical dynamics of the power systems and OPNET is used to simulate the communication network. The Substation Data Processing Unit has been implemented into the platform for time synchronization. Comparing with these testbed, the cyber-physical co-simulation testbed presented in this paper has hardware-in-the-loop capability, ability of real-time simulation, ease of cyber-attack modeling, and end-to-end system modeling. With the real industry power system hardwares involved into the cyber-physical testbed, there is a opportunity to test whether the attacker can manipulate those devices and which function can be controlled by the attacker.

In this paper, a developed real-time cyber-physical co-simulation testbed has been used to analyze the impact of specific cyber-attack examples on the power grid. Preliminary work for integrated simulation and applications have been reported by authors in [11]–[13]. None of these papers directly addresses cyber-security aspects.

II. Cyber-Physical Co-Simulation Testbed

In order to simulate the different components in the smart grid and get closer to the real environment as much as possible, the developed cyber-physical co-simulation testbed consists of three major parts: (i) Power system simulation and sensors (ii) Communication network (iii) Smart grid application. The interconnection and data flow between different parts are shown in the Figure 1.

A. Power System Simulation and Sensors

As shown in the Figure 1, Real Time Digital Simulator (RTDS) and RSCAD ® are utilized to model and simulate power system and related control components. RTDS is designed to simulate the power system and to interface with various hardware devices, such as measurement, protection, and control devices. With number of hardware interface, RTDS is capable of doing synchronized real-time simulation, involving

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.

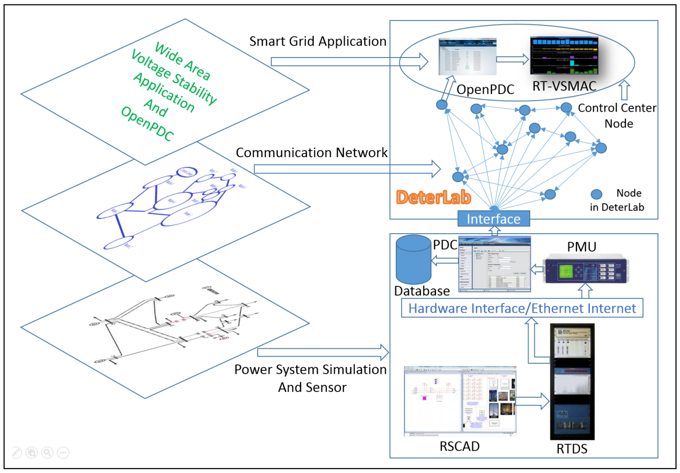

Fig. 1. Cyber-Physical Co-Simulation Testbed Architecture

real industry hardware into the simulation, and testing user developed application with different types of custom I/O port. RSCAD, which is used to model, simulate, and analyze the power system, is the main interface of RTDS hardware.

In this work, there are multiple substations modeled in the RTDS simulated power system. In each of these modeled substations, several PMUs are used to measure the synchrophasor data and a PDC is utilized to archive the data from PMUs. A small amount of database is installed in each substation to temporarily store the synchrophasor data from PDC in case of data loss caused by communication failures. And when communication connection recovers, the database can also re-send the data automatically to control center. In order to synchronize the cyber-physical testbed, the high resolution time stamp is provided by satellite-synchronized clock to all the synchronized devices and simulator, such as RTDS, PMU and PDC.

In the developed testbed, four hardware PMUs and eight GTNET software PMUs from RTDS are connected by Giga-Transceiver Analogue (GTAO) Card to capture the phasor data from each bus. The hardware PMUs also have the relay function, which can send the control command back to RTDS through Giga-Transceiver Digital Input (GTDI) Card for control action in the simulated power system. Software PDC is used to archive the phasor data from all the PMUs and send the synchrophasor data through interface to the control center node in the emulated communication network. The PDC communicates with PMU by fiber optics connection using PMU ID, IP address, PMU Port Number, and Transport layer protocol. All the synchrophasor data transmitted in cyber-physical testbed meets the IEEE C37.118-2011 protocol.

B. Communication Network Simulation

DeterLab is a shared testbed facility designed for repeatable and controllable cyber-security experiment. The basic architecture of DeterLab is shown in Figure 2. All the operation in the DeterLab should go through a web-based interface in order to protect the security of the experiment and keep the separation with outside Internet experiment. The web-based interface is connected with two different network: Hardware Control Network and Control Network. The hardware control network is connected with switch management interfaces and power controllers which are used to configure the experimental network and control testbed nodes in user defined experiment. The control network is connected with all the testbed nodes to support imaging traffic, file system traffic, experiment booting, and interaction between user and testbed nodes. The testbed nodes are hundreds of real high-performance PCs. The experiment network is dynamically configured to each specific experiment to support the network communication.

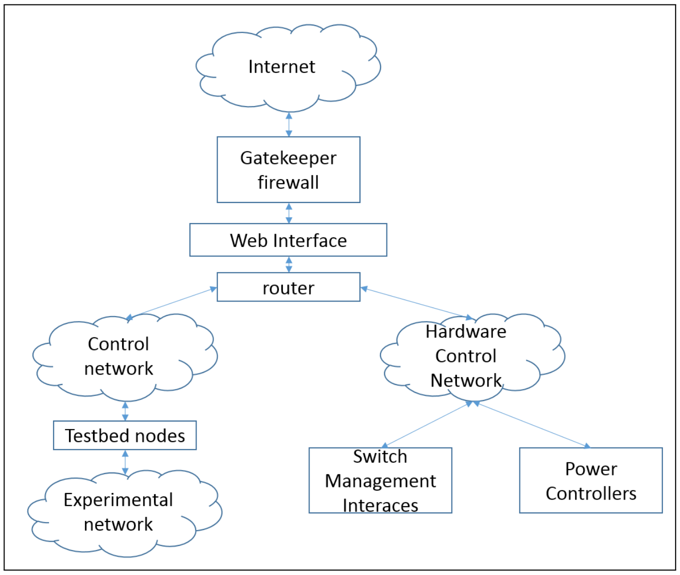

Fig. 2. Basic Architecture of DeterLab

Simulated power system and DeterLab are needed to be integrated together for cyber-physical co-simulation. To reach this research goal, DeterLab offers the Deter Federation Architecture (DFA). The DFA allows researcher to connect the resource from DeterLab testbed with other testbed. In the developed testbed, the experiment controller is installed in one of the Lab PC. The PMU data streams from all the substations go from this interface to experiment network, created inside the DeterLab. The basic architecture of the federated experiment is shown in Figure 3.

In the DeterLab, there is an advanced tool called Security Experimentation EnviRonment (SEER), which allows the users to create, plan, monitor, and analyze the cyber-security experiment in a relative simple way. SEER has a user-friendly graphical user interface (GUI) and includes many different types of tools, such as attack tools, traffic generation tools, and analysis tools. Another feature of SEER is the extensible interfaces, which can be used to operate user-developed attack or protection control in the DeterLab experiment [14].

C. Smart Grid Application

Several smart grid applications have been integrated into the developed testbed, such as voltage stability, Remedial Action

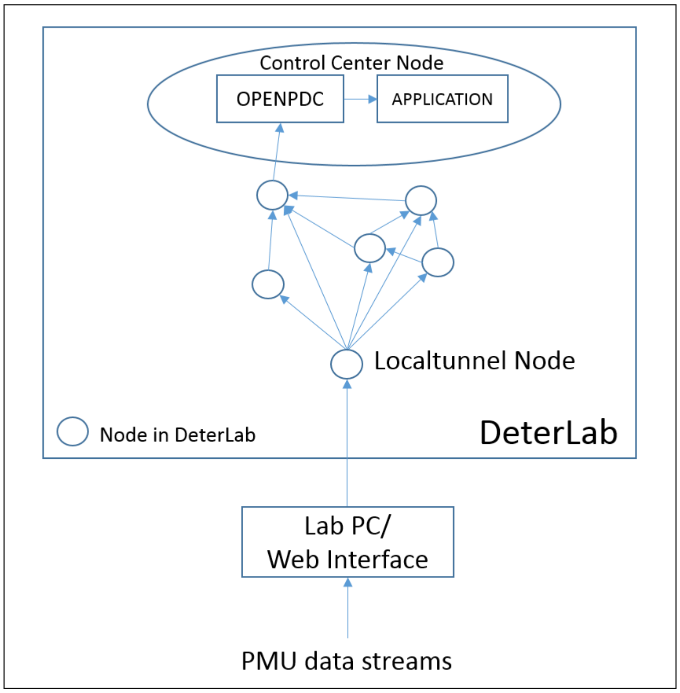

Fig. 3. Basic Architecture of Federated Experiment in DeterLab

Schemes (RAS), and state estimation. In this paper, the "RT-VSMAC tool" [15] designed for voltage stability is presented as an example. The RT-VSMAC is a real-time voltage stability monitoring and control tool, which monitors the wide-area voltage stability condition for the whole system and gives the appropriate control command based on the available control resource when it finds out the voltage instability condition. The RT-VSMAC tool computes the "voltage stability assessment index" (VSAI), which represent the voltage stability condition for the given power system. The range of the VSAI is from 0 to 1. When VSAI is near 0, it represents a voltage stable system. When VSAI is near 1, it indicates the given power system is less voltage stable. Based on the VSAI and available control resource, the RT-VSMAC tool will give the appropriate control command when needed based on the voltage stability status.

III. Real Life Cyber-Attacks Analysis

In recent years, the impact of cyber events on the power grid is gaining more attention from both industry sector and academicians. With the ability to do real-time cyber-physical co-simulation and capability of hardware-in-the-loop, the developed cyber-physical testbed is a great tool to analyze the cyber-physical impact of cyber-attacks on the power grid. To show the ability of cyber-physical testbed, two different real life cyber-attacks are listed here as examples.

A. *Denial of Service Attack*

A denial-of-service (DoS) attack is to attempt to make the critical resource unavailable for intended user when the resource is required. In the modern power system, it is very important to maintain all the communication connections available especially in critical time, when the system is subjected to disturbances or operates near the instability point. If the DoS attack succeeds during the critical time, it may be very hard to keep the reliability of the modern power grid. A specific type of real life DoS attack is presented as below.

TCP SYN flood attack utilizes the vulnerability of three-way handshake mechanism, which is used to establish the TCP connection. The attacker forges the fake IP address and use it to send the TCP/SYN packets to the selected server. Each of these packets is considered as a TCP connection request, which leads the selected server to send ACK packets with its own SYN request to the fake IP address. Since the IP address is forged, the selected server can not receive ACK packets and keeps waiting until the request is timed out. During the waiting time, the TCP request keeps wasting the resource of the processor. If the huge amount of the fake TCP SYN requests are continuously sent to the selected server, it will lead to consuming all the resources on the selected server. And other requests from legal users will not be able to get respond [16]. The simulation results are shown in the Section IV. The impact of TCP SYN Flood Attack on the power system and RT-VSMAC is also analyzed.

B. *Man-In-The-Middle Attack*

The MITM attack is a form of active eavesdropping. The attacker makes the independent connection with both ends of the communication, and relays message between them to make them believe that they are communicating through a private connection. In the power grid, a successful MITM attack gives the attacker opportunities to have almost the same observation with control center operator, which helps the attacker find out the critical information for other attacks. With the MITM attack, the attack can also manipulate the critical information, such as measurement data, real-time price signal, and control command, in the transmitted packets.

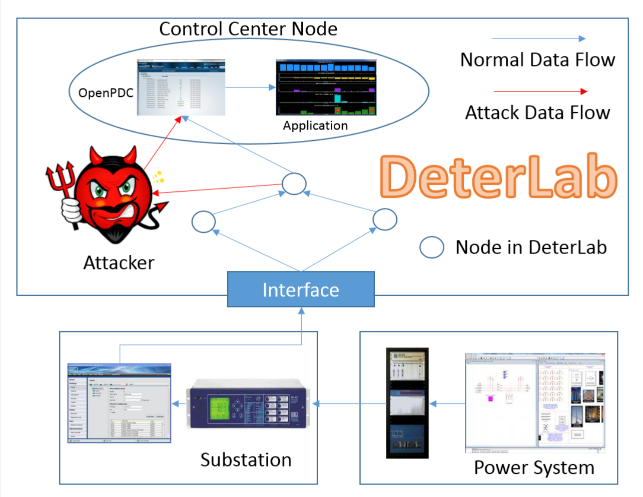

Fig. 4. Man-in-the-Middle Attack Setup

The architecture of the MITM attack is shown in the Figure

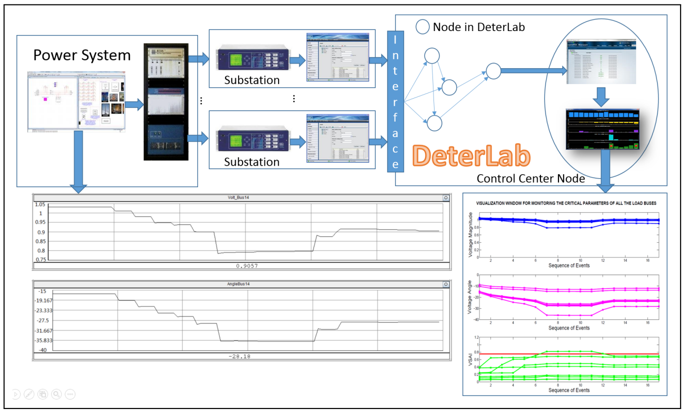

Fig. 5. Simulation Architecture

4. Under normal operation, the synchrophasor data is sent to the control center node following the blue arrow. During the MITM attack, the attacker uses ARP spoofing [17] to poison the selected node and the control center node so that the selected node sends data, which is originally sent to the control center node, to the attacker. Thus, the attacker can silently sit between the control center node and the selected node. The attacker manipulates all the synchrophasor data packets by modify the payload, which is required for the VSAI calculation.

IV. Simulation Results

The developed testbed is validated by simulation of the modified IEEE 14 bus system fully observed by the PMUs. RT-VSMAC is integrated as the controller application. The simulation architecture is shown in the Figure 5.

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. Normal Operating Scenario

In the normal stressed situation, the sequence of events, which may lead to a possible voltage collapse, is shown in the Table I. The time interval between each event is 5 seconds. When RT-VSMAC detects that the VSAI goes beyond the threshold 0.75, it gives the appropriate control command based on the VSAI and the available control components. All the control commands are modeled in the RTDS based on the real-time values obtained from RT-VSMAC.

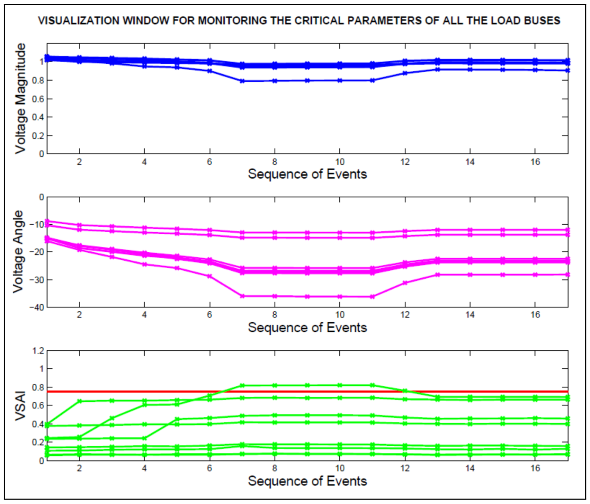

Fig. 6. Wide-Area VSAI and Voltage Phasor Data for Normal Condition

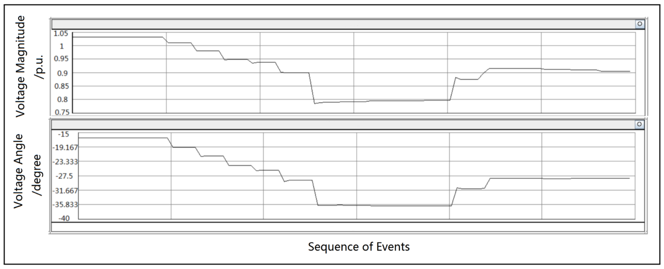

Fig. 7. The Changes in Voltage Magnitude and Angle on bus_{14} for Substation View

The VSAI and related voltage data area shown in Figure 6. Control actions are given by RT-VSMAC from $event_7$. All the control actions are shown in Table II. The first four control actions are inserting the shunt capacitor banks on bus_9 and on bus_{14}. However, these control actions don't change the VSAI lower than the threshold. The next two control actions are load shedding. After these two control actions, the VSAI drops below the threshold. To keep availability of the control components, RT-VSMAC automatically revokes the ineffective control actions. The voltage data at bus_{14} from RTDS is shown in the Figure 7. When the control actions are taken on bus_{14}, both of the voltage magnitude and voltage angle increase.

B. TCP SYN Flood Attack

In the TCP SYN flood attack simulation (refer section III-A), the attacker floods TCP SYN packets to $node_9$ in order to disrupt the PMU data from $node_9$. Due to TCP SYN flood attack, the resource of $node_9$ is consumed by attack. Communication delay and packet loss appear on the data streams from $node_9$. Figure 8 shows the impact of TCP SYN flood attack on the communication delay of $node_9$ data

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

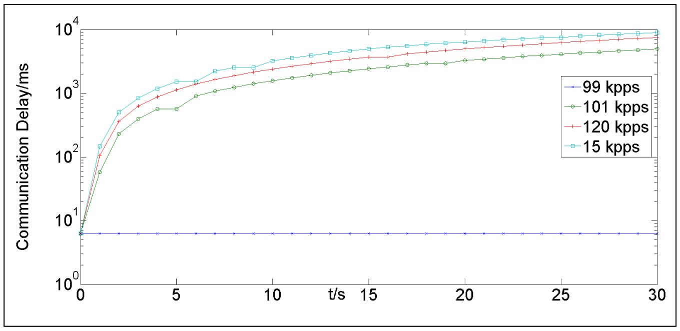

Fig. 8. Communication Delay on $node_9$ for TCP SYN Flood Attack

stream from four situations. X-axis represents the length of the attack and Y-axis represents the communication delay on $node_9$ data stream. From the results, for the 99 kilo packets per seconds (Kpps) attack, the communication delay is still at the normal level. When the attack increases to 101 Kpps, huge communication delay appears on the $node_9$ data stream. The ability of the $node_9$ processor to deal with the TCP communication request is around 100 Kpps. With the increase of the attack rate, the communication delay also keeps increasing. When the attack rate is over 100 Kpps, RT-VSMAC detects that one synchrophasor data stream has large communication delay compared to other data streams. This situation may be caused by the occurrence of communication failure or power system failure. In order to avoid incorrect control command based on the bad data, RT-VSMAC keeps using previous VSAI data until all the phasor data streams come back to the normal condition. In the TCP SYN flood attack, since the application enters the safety mode caused by the bad input data, it can not observe that the system is operating near the instability condition, and there is no control action going back to power system, which may finally lead to a blackout.

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

C. MITM attack

In the MITM attack, the attacker silently sits between the substation and control center. At the $event_6$, the attacker starts to manipulate the phasor data on multiple buses shown in the Table III. Based on manipulated data, control center considers the power grid being more stressful than its real condition. From the Table III and Figure 9, there are two more load shedding control actions, which are local load shedding at bus_{14} and remote load shedding at bus_9, compared to normal situation. Comparing with the normal situation, there are 46.329MW additional load shedding at bus_{14} and 51.625MW additional load shedding at bus_9. Figure 10 also shows that the voltage difference between control center data and substation data.

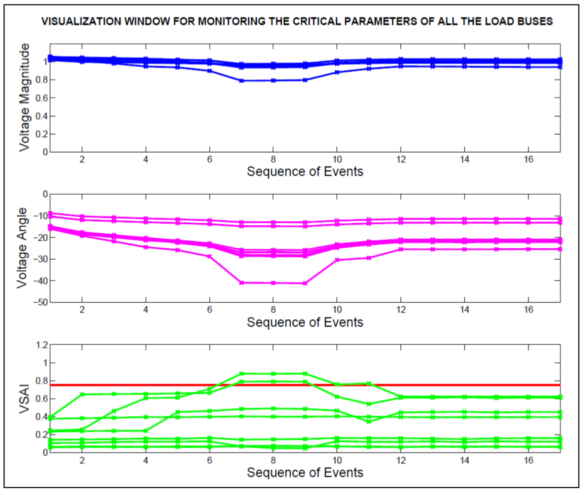

Fig. 9. Wide-Area VSAI and Voltage Phasor Data for MITM Attack

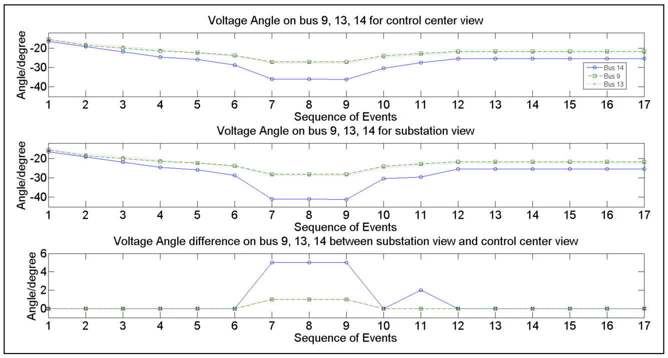

Fig. 10. Voltage Angle Value at $buses_{9,13,14}$ for MITM Attack

V. Conclusion

In this paper, a developed real-time, hardware-in-the-loop, cyber-physical co-simulation testbed using RTDS, PMU, PDC, satellite-synchronized clock, DeterLab, and RT-VSMAC has been presented. Since the developed cyber-physical testbed is close to real life smart gird environment, the developed cyber-physical testbed is used to show the ability of testbed for simulation and analyze the impact of different real life cyber-attacks on the power grid. Two different cyber-attacks, which are TCP SYN flood attack, and MITM attack, are demonstrated as examples. To analyze the interdependency between cyber events and power grid, standard IEEE power system test case is modeled and simulated. Results demonstrate that cyber-physical co-simulation testbed is useful to analyze the impact of cyber-attacks on the power grid.

In our future work, we will integrate the cyber protection control into the developed cyber-physical testbed and test the effect of the cyber protection control against different cyber-attacks.

References

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

[2] S. Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34–41, 2005.

[3] S. Chen, S. Song, L. Li, and J. Shen,, "Survey on smart grid technology," *Power System Technology*, vol. 33, no. 8, pp. 1–7, 2009.

[4] H. Farhangi, "The path of the smart grid," *Power and Energy Magazine, IEEE*, vol. 8, no. 1, pp. 18–28, January 2010.

[5] IEEE & Smart Grid. [Online]. Available: http://smartgrid.ieee.org/ieee-smart-grid

[6] C. Siaterlis, B. Genge, and M. Hohenadel, "EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation," *Emerging Topics in Computing, IEEE Transactions on*, vol. 1, no. 2, pp. 319–330, Dec 2013.

[7] K. Zhu, M. Chenine, and L. Nordstrom, "ICT Architecture Impact on Wide Area Monitoring and Control Systems' Reliability," *Power Delivery, IEEE Transactions on*, vol. 26, no. 4, pp. 2801–2808, Oct 2011.

[8] 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," *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1444–1456, Sept 2012.

[9] T. Strasser, M. Stifter, F. Andren, and P. Palensky, "Co-simulation training platform for smart grids," *Power Systems, IEEE Transactions on*, vol. 29, no. 4, pp. 1989–1997, July 2014.

[10] H. Georg, S. Muller, N. Dorsch, C. Rehtanz, and C. Wietfeld, "INSPIRE: Integrated co-simulation of power and ICT systems for real-time evaluation," in *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, Oct 2013, pp. 576–581.

[11] C. Vellaithurai, S. Biswas, R. Liu, and A. Srivastava, "Real Time Modeling and Simulation of Cyber-Power System," in *Cyber Physical Systems Approach to Smart Electric Power Grid*, ser. Power Systems, S. K. Khaitan, J. D. McCalley, and C. C. Liu, Eds. Springer Berlin Heidelberg, 2015, pp. 43–74. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-45928-7_3

[12] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPINDEX: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2014.

[13] 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.

[14] S. Schwab, B. Wilson, C. Ko, and A. Hussain, "SEER: A security experimentation environment for DETER," in *Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test*, Aug 2007.

[15] 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.

[16] D. Erhan, E. Anarim, G. Kurt, and R. Kosar, "Effect of DDoS attacks on traffic features," in *Signal Processing and Communications Applications Conference (SIU), 2013 21st*, April 2013, pp. 1–4.

[17] 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.