# Co-Simulation Platform For Characterizing Cyber Attacks in Cyber Physical Systems

Mohammad Ashraf Hossain Sadi[1]
Mohd. Hassan Ali[2]
Electrical and Computing Engineering Department
University of Memphis
Memphis, TN 38152 USA
masadi@memphis.edu[1], mhali@memphis.edu[2]

Robert K. Abercrombie[4] *
Computational Sciences & Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831 USA
abercrombier@ornl.gov[4]

Dipankar Dasgupta[3]
Department of Computer Science
University of Memphis
Memphis, TN 38152 USA
dasgupta@memphis.edu[3]

Shubhalaxmi Kher[5]
Electrical Engineering Department
Arkansas State University
State University, AR 72467 USA
skher@astate.edu[5]

***Abstract*—Smart grid is a complex cyber physical system containing numerous and variety of sources, devices, controllers and loads. Communication/Information infrastructure is the backbone of the smart grid system where different grid components are connected with each other through this structure. Therefore, the drawbacks of the information technology related issues are also becoming a part of the smart grid. Further, smart grid is also vulnerable to the grid related disturbances. For such a dynamic system, disturbance and intrusion detection is a paramount issue. This paper presents a Simulink and OPNET based co-simulated platform to carry out a cyber-intrusion in a cyber-network for modern power systems and smart grids. The cyber-attack effect is also characterized for the physical power system. The effectiveness of the co-simulated platform is demonstrated by the IEEE 30 bus power system model. The distributed denial of service attack, in terms of tampering with the circuit breaker reclosing signal was carried out in the cyber network to see its effect on the physical network. Different physical fault situations in the test system are considered and the results indicate the effectiveness of the proposed co-simulated scheme.**



* Robert K. Abercrombie is also an Adjunct Professor, Department of Computer Science, University of Memphis, Memphis, TN 38152 robert.abercrcombie@memphis.edu.

## I. Introduction

Smart grid is a complex cyber physical power system network containing a large penetration of distributed generators, variety of interaction between utility and customers, and customers' participation into energy market [1]. Smart grid will accommodate the integration of renewable energy sources located in diverse locations along with suitable energy storage devices. Two way digital communication of data and signals are the heart of smart grid, where, both the utility and customers can participate into energy and load management [2]. Smart grid will be able to self-assess the status of the power system and estimate the flow of the power through self-management. The customers will be allowed to decide about their power usage, choose suitable appliances and offers from the utilities [1, 2]. Therefore, with advent of the smart grid, the healthy competition between the power utilities will increase among the power companies. Thus, the quality of the power delivered to the customers will improve.

Supervisory Control and Data Acquisition (SCADA) is widely used for industrial process control. In power systems, SCADA network is used to interconnect the field devices, sensors, actuators, etc. [3]. Moreover, these devices are controlled and monitored through the SCADA architecture from the system floor. They were initially designed to work separately with connectivity to external networks [4]. However, for making the power system more efficient and reliable, SCADA system is adopting the ideas of communication technologies. Therefore, there is increased use of internet, corporate network, protocols, hardware's and software's in the advanced SCADA system. As a consequence, the smart grid becomes prone to external intrusion and grid related cyber-attacks and disturbances [5]. So, a successful cyber intrusion in SCADA system may cause huge sociological and economical negative impact.

978-1-4799-7560-0/15 $31.00 © 2015 IEEE
DOI 10.1109/SSCI.2015.178

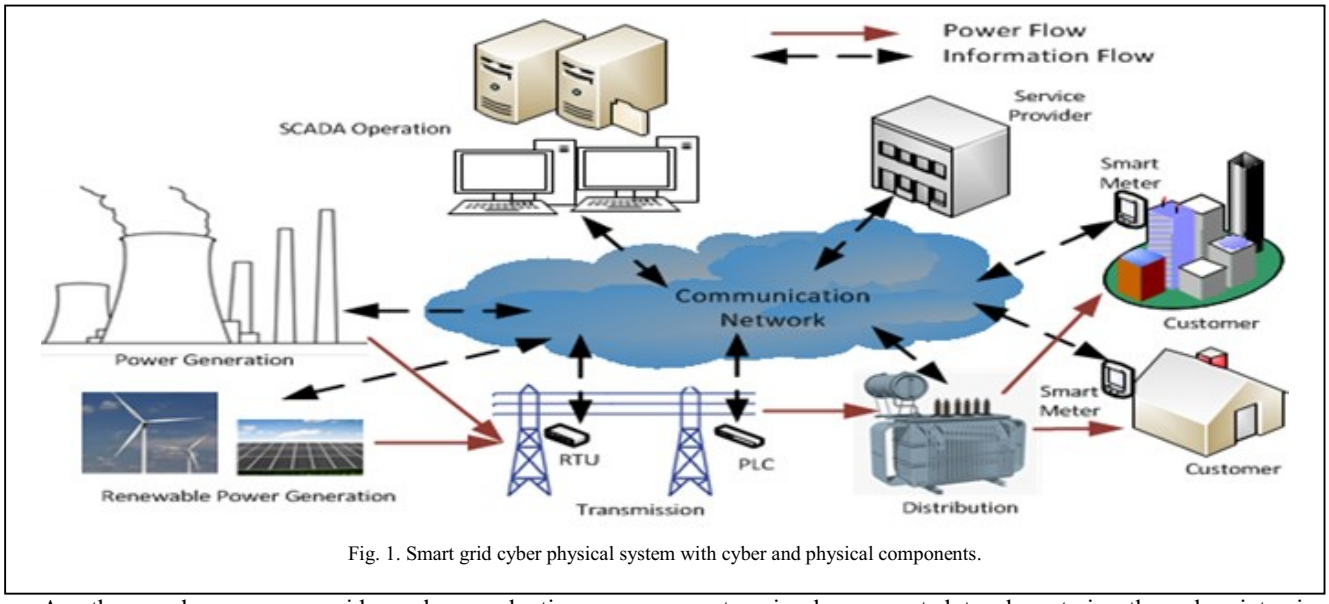



Fig. 1. Smart grid cyber physical system with cyber and physical components.

As the modern power grid evolves, adopting new technologies and subsequent availability to new connections, its vulnerability is also increasing. Further, recent studies and reports indicate increasing cyber security incidents and risks associated with the electric power grid and SCADA systems [6]. There are examples of cyber-attack on nuclear power plant, industrial control system and sewerage treatment systems too [7]. U.S. Department of Energy (DOE) has listed the cyber security vulnerability assessment and resilience efforts for smart grid as the top priority [8]. So, the researchers are investigating the cyber security related complexities in different environments.

To protect the smart grid from external cyber-attack, it is paramount to understand and analyze the security risks and vulnerabilities of the system. The existing works on cyber security of smart grid are mostly related to the testbed based disturbance detection procedures of smart grid [9]. Different testbeds in different environment are designed and evaluated by the researchers. However, the designed testbeds lack proper modeling tools to analyze the security of the smart grid. In these testbeds it is difficult to incorporate the complexity between the cyber system and physical system. Also the operating dynamics, modeling strategies and security scenarios are difficult to present in these designed testbeds.

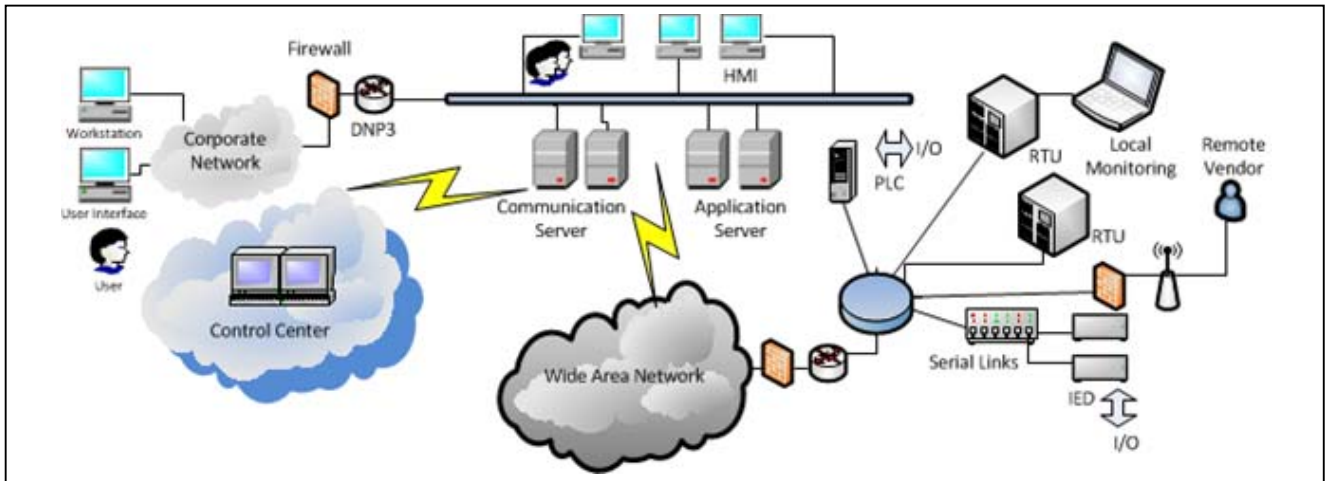
In this work, we present a scheme to represent the cyber physical system (CPS) through a co-simulated platform. There is an example of co-simulated Matlab/Simulink and OPNET based model for a wireless network control system study [10]. There is also work on the effect of communication channel in the power network [11]. To the best of our knowledge, there is no work available on the effect of cyber-attack on physical power system network carried out in the SCADA system. Therefore, we are proposing a Matlab/Simulink and OPNET based co-simulation platform to represent the cyber physical system (CPS), which is another salient contribution of this work. Moreover, a correlation between the cyber-attack in the cyber system and the corresponding impact on the physical system is also presented to characterize the cyber intrusion impacts. The cyber network is presented as a SCADA system through OPNET platform and the physical power system is presented through MATLAB/SIMULINK platform. The cyber intrusion is carried out in the SCADA network to see its effect on the physical power network.

For validating the proposed scheme, a co-simulated Matlab/Simulink™ and OPNET™ based intrusion detection model was designed. For demonstrating the effect of the scheme, the IEEE 30 bus power system is used to simulate a physical system with the Matlab/Simulink platform [12]. In the event of a fault, the reclosing time signals of circuit breakers from a central controller are considered to be manipulated due to cyber-attack. The effect of the manipulated signal on the physical network is presented in this work.

## II. Smart Grid Security Threats

Smart grid provides a dynamic and interactive infrastructure to intelligent control of the distributed energy resources and enhances the energy management capabilities. The entire smart grid may be connected through an information network. Fig. 1 represents the smart grid cyber physical system. The physical system is represented by the power grid and field devices, whereas, the cyber system is represented by the control center, electronic devices and communication architecture embedded throughout the physical system. The smart grid can be subject to either physical attacks by humans or cyber-attacks into the information infrastructure [8]. Some critical cyber security issues of the smart grid system are discussed below.

In smart grid, numerous critical equipment's and field devices will be used in the remote locations to effectively and efficiently collect the customer operating conditions. Moreover, smart meters will also allow the customers to actively participate into the energy management. The field devices: PLCs, IEDs, RTUs, PMUs and smart meters have algorithms which can be manipulated by either customers or




Fig, 2. SCADA system with different layers and components.

cyber intruders [5]. By hampering and tampering with the data collection process in these devices, the operators of the utilities can get misleading feedback and thus can cause interruptions which may ultimately result in a blackout.

The communication network in the smart grid can be exploited by the intruders to damage different layers present in the grid. There can be eavesdropping both in the wired network and wireless network in the smart grid. The network layer can be easily jammed by traffic injection. However, wireless and wired networks are vulnerable to traffic flooding and worm propagation attacks [3]. Certain applications can be built in the communication network which can deliberately change the MAC parameters that can lead to spoofing attack and fake information passing. Distributed denial of service (DDoS) and malicious malwares in the internet also presents a huge threat to the smart grid security.

In smart grid, several micro grids can operate independently. Those micro grids have local SCADA system. Even for substations and field devices, there may be local SCADA system. For all those micro grids, there will be a master SCADA system, where, every local SCADA system will be connected. The SCADA system for the micro grids will be controlled by the master SCADA system [8]. However, traditionally, the local SCADA systems can operate independently. The angry operator or the previous employee of this SCADA system can put the SCADA system into danger by putting and initiating bug into the system. Intercepting or forging the access logs of this SCADA system can damage the grid [13]. The state estimation data for the power system can be tampered in the SCADA database. That may initiate a misleading operation of the smart grid. One of the primary functions of the smart grid will be energy management and efficient load forecasting while different distributed energy sources will be in operation. Thus, false load forecasting due to database attack can misguide the decision of the distributed management system (DMS).

## III. SCADA System

SCADA system plays the core role in controlling and monitoring the power system. It is the backbone of power systems for automated and reliable operation. The complex interaction and decentralization of SCADA system has exposed power system to numerous vulnerabilities. The SCADA system has three main components and other sub components into these main components [13]. Fig. 2 represents the scheme and components of a SCADA system. The basic components for SCADA system are discussed below.

The field devices consisting of Remote Terminal Units (RTUs), Programmable Logic Controls (PLCs) and Intelligent Electronic Devices (IEDs) are connected to the physical devices and collects secure and reliable data. They collect the data from the field devices and send them to the SCADA terminals through communication network. Normally, field devices send the log data and alarm signal to the SCADA through Master Terminal Units (MTUs). Recently, the smart meters also perform as a field device. The data collected from the field devices are presented to the operator through Human Machine Interface (HMI), so that supervisory actions can be taken in the control center. These data are formatted and compiled before presenting to the HMI, and are stored in a database management system for further analysis, forecasting and study purpose [14].

The MTU consists of servers and software's and communicates with the field devices for requesting data. The MTU performs as a master and field devices perform as a slave. In a SCADA system, there must be a central MTU and there may be several SUB-MTUs connected to the master MTU. The HMI is responsible for interacting with the operator for supervisory actions and that happens through a graphical interface.

Finally, in the SCADA system, there must be a static communication network. The field devices, RTUs, MTUs and HMIs should be connected through the wired or wireless communication structure. Even field devices (e.g., different RTUs), can also communicate through a communication

network. The HMIs and MTUs are located in the same place, and there is TCP/IP protocol based communication between them.

In SCADA system, numerous devices will be used, which need to be authenticated. All users in the system should be authenticated to keep the integrity of the system. Signal transmission between nodes should be authenticated and encrypted. Devices should be able to inspect the deep packets. The application software's used in the SCADA system should have firewalls and be free from viruses [14]. This software and operating systems should be able to auto update.

The SCADA system performs as a node, where, variety of data is collected and delivered. Therefore, different DDoS attacks can be initiated in different layers of the SCADA system [5]. Consequently, different security measures should be taken to protect the SCADA center. The basic security measures for SCADA system are discussed below.

The SCADA control center will be divided into zones through switches. Zone based security policies are also needed. The switches should have encryption and decryption properties [14]. Further, the divided zones should have certain unified security policies.

The network components and protocols should be maintained and protected through proper security measures. Moreover, network traffic should be monitored and maintained to check any intrusion in the system.

## IV. Background and Related Works

Determining the vulnerabilities of a SCADA system in real time is a complicated process because of the complex hardware and software interactions that must be considered. Developing a simple system that captures the complexity of the whole system will be more appropriate for that particular study. This simple system is called a Test Bed for SCADA system. Various agencies and institutions have developed different Test Beds for SCADA systems [15]. The recent and notable lists of test beds developed are given bellow:

Cyber Physical Test Bed was developed by Iowa State University by using real time digital simulation (RTDS) and DIgSILIENT power factory software [16]. Sandia National Laboratories developed a Virtual Control System Environment (VCSE) by utilizing OPNET, Power World simulator and by using centralized model/simulation management tool [17]. Virtual Power System Test Bed (VPST) and Real Time Immersive (RINSE) network integration was developed at University of Illinois, which utilizes Power World simulator [16]. The University of Arizona developed a Test Bed for Analyzing Security of SCADA control system (TASSCS) by utilizing OPNET and Power World simulators and by using Modbus R Sim software [18]. SCADA Sim Test Bed has been developed at Royal Melbourne Institute of Technology (RMIT) to study the network performance under cyber-attack [16]. European CRUTIAL projects have developed two different SCADA test beds. University College Dublin (UCD) developed a test bed based on industry standard software/hardware with a DIgSILENT power system simulator [16]. A collaborative work of three universities developed an integrated software based testbed. That testbed adopts the software emulation approach. For detecting network based intrusions a testbed is developed in Washington State University [19].

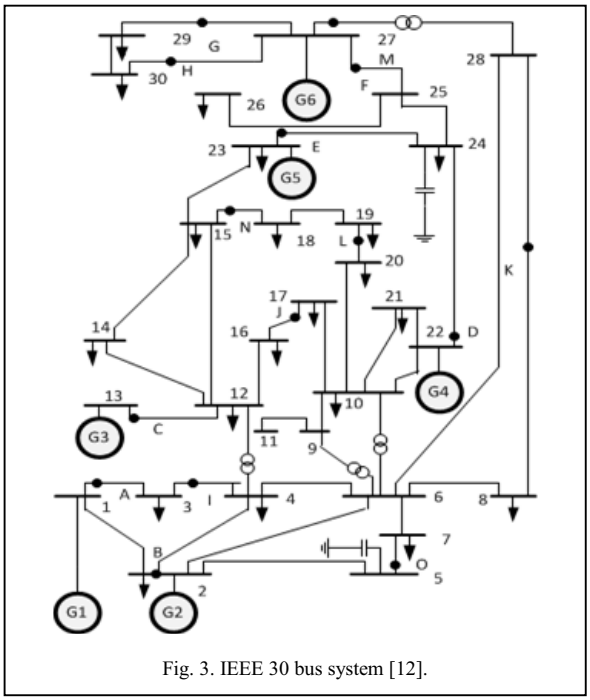


Fig. 3. IEEE 30 bus system [12].

## V. System Design and Implementation

The IEEE 30 bus power grid system model [12, 20] shown in Fig. 3 is used in this paper to check the effect of the cyber intrusion on the power system. This test system consists of six generating units interconnected with 41 branches of a transmission network to serve a total load of 189.2 MW and 107.2 MVAR. There are 24 loads and 4 transformers in the whole system. We considered 15 fault points (A to M) in the test system. For all the fault situations, we considered the total kinetic energy based optimal reclosing for the circuit breakers [21-24].

It is noteworthy that, the considered test system is a conventional power system having synchronous generators only. According to the smart grid concept, the present power grid will adopt the smart functionality. The considered system follows an intelligent technique to calculate the optimal reclosing time as presented in Fig. 4 [12]. Therefore, though only synchronous generators are used in the system proposed the system uses intelligent and smart techniques for its operation.

The OPtimised Network Engineering Tool (OPNET) uses discrete event-driven mechanism. It has very high simulation efficiency [25, 26]. In this work, a simple SCADA network is designed in OPNET for supervisory control of the model power grid. The Simulink and OPNET were adopted to simulate the real time control and network performance separately.

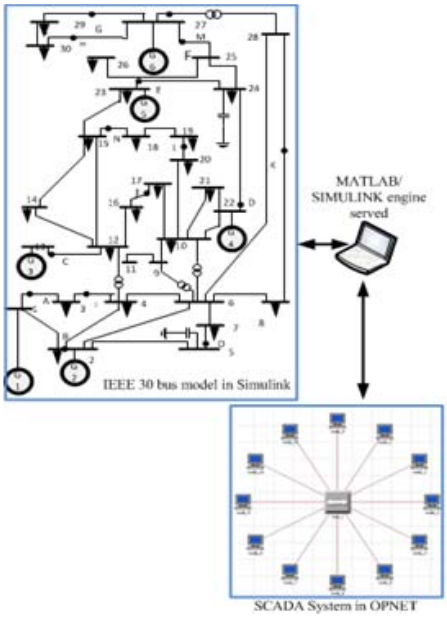



Fig. 4. MATLAB/SIMULINK and OPNET integration scheme.

## VI. Simulation Tools and Environment

Simulation of both the power systems and SCADA systems are important part of the intrusion detection schemes for the power system. Simulation of only the designed power system will not incorporate the behavior of SCADA systems. Therefore, simultaneous combination between power systems simulation and SCADA systems simulation is required.

However, to the best of our knowledge, there is no software available to support the functionality of these two areas of simulation. The Matlab/Simulink is a well-known platform for modeling, characterizing and analyzing the performance of power systems. It is a powerful software platform for modelling system and implementing control algorithms. However, it is difficult to implement the computer networks in the Simulink. On the other hand, OPNET is an object oriented network modeling approach providing a graphical user interface. OPNET provides a detailed computer network simulation platform. In OPNET, the packet drop, node movements, data rate etc. are easy to simulate. So, co simulated Simulink and OPNET based overall design can provide a powerful simulation environment. Combining the strengths of both the simulation platforms can produce more realistic simulation results. Therefore, in this work, the combined functionality of Matlab/Simulink and OPNET software's are used to constitute the operation of both power system simulation and network simulation.

In the co-simulation platform, there is a provision for Simulink to invoke the OPNET plant node via MATLAB engine server as presented in Fig. 5. However, the state of any circuit breakers can be read by the OPNET from the Simulink model and it can generate corresponding state signal. Moreover, any control state data /signal can arrive to the circuit

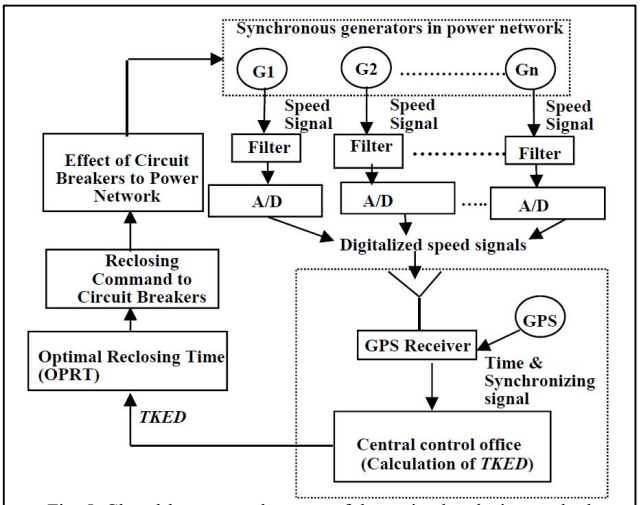



Fig. 5. Closed-loop control system of the optimal reclosing method including GPS function.

breakers from the OPNET model in this co-simulation platform.

## VII. Simulation Scenario

There are three types of cyber-attacks which can significantly affect smart grid operation.

### A. Packet Drop Attack

This problem can be caused at various choke points in the communication path (links, firewalls, proxy servers, encryption device, routers, switches, etc.), when a queue within these network points reaches its maximum capacity. While there are some obvious reasons for packet drop, there are also some targeted cyber-attacks which can cause packets to drop before reaching the intended destination (e.g. SCADA or field units) [5]. Moreover, the technologies and protocols used currently like Modbus, DNP3, etc. were designed for connectivity with cyber security issues. Therefore, they are vulnerable and cause packet drop attack. Backdoor entry to the system registry can also cause packet drop attack.

### B. Distributed Denial of Service (DDoS) Attack

These attacks are mainly used for disrupting, blocking or jamming the flow of information through control and communication networks. Jamming attack on the wireless network can launch DDoS attacks on the physical layer. The circuit breaker reclosing time signal is a time critical signal and if it is delayed then it initiates DDoS attack [8]. The deliberate modification or the spoofing of the MAC parameters in any communication layer can also initiate the DDoS attack. In the HMI, the flooding of the commutation requests can exhaust or overwhelm the computers and thus initiate the DDoS attack. Recently, there has been an increase in DDoS attacks (with shorter attack duration, but a bigger packet-per-second attack volume) which not only exploit bandwidth, but also attack applications that focus on sending bad traffic using those applications protocols. This type of attack can significantly

disrupt the communication in the smart grid cyber infrastructure.

### C. Tampering Communication Data/Signal

This type of cyber-attack not only delays communication but also contaminates the data in the communication. Such an attack can target a specific type of command and control signal which for example activate or deactivate critical field devices for hostile purpose. This data corruption attack can manifest in many different ways: a malware (like *Flame*) can make such changes in communication data causing devastating damage to smart grid components including equipment damage, power outage and misreading of smart meter data. If the software and enterprise security are not proper, it can lead to the data stealing from the database for tampering.

For combining the operational characteristics of SIMULINK and OPNET, high level architecture synchronization is required. This synchronization technique is out of scope of this paper and will be described in our future work. Three common types of attack have been identified above. In this work, the tampering of communication signal is implemented to see its effect on the physical power grid. The other two types of attack will be part of our future work.

When any fault happens in the power grid, the circuit breakers opens and then reclose to minimize the effect of this fault into the power system. For circuit breakers optimal reclosing, we used the Total Kinetic Energy (TKE) based reclosing technique [5, 27] in the IEEE 30 bus power system as represented in Fig. 3. For implementing the TKE based optimal reclosing, the kinetic energy of all the six generators in the IEEE 30 bus system is collected in SCADA system. In the IEEE 30 bus power system, we considered three phase to ground (3LG) fault in fifteen fault locations. The circuit breakers near the considered fault locations are opened and then reclosed according to the TKE reclosing method. But in this work, a cyber-attack in the collection and application of this TKE reclosing signal from SCADA system to the IEEE 30 bus power system is considered. The tampering delays the reclosing signal from the SCADA system to the circuit breakers operating near any considered fault location. Consequently, the normal and steady operation of generator at the corresponding buses near the fault location hampers.

## VIII. Simulation Results

In the test system, we considered three-phase-to-ground (3LG) fault at fifteen fault locations and observed the speed and terminal voltage response of the generators and corresponding buses. We observed those responses in case of cyber-attack and no cyber-attack scenarios in the SCADA system. Fig. 6 represents the speed response of the generator G3 considering both cyber-attack and no cyber-attack for 3LG permanent fault at point C. Similarly, Fig. 7 represents the terminal voltage response at bus 13 of the generator G3 at bus 13 considering both cyber-attack and no cyber-attack for 3LG permanent fault at point C. Moreover, Fig. 8 and Fig. 9 represents the speed of generator G5 and terminal voltage response at bus 23 considering both cyber-attack and no cyber-attack for 3LG permanent fault at point E. From the responses,

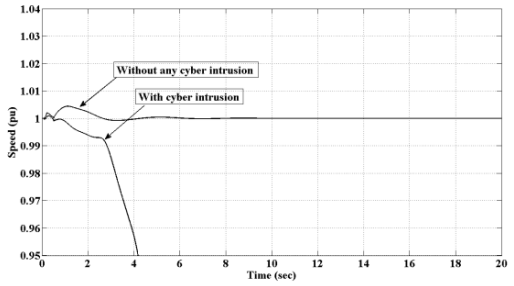


Fig. 6. Speed response of generator 3 for 3LG permanent fault at position C considering cyber-attack and no cyber-attack.

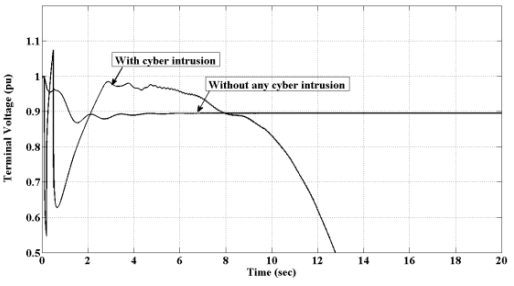


Fig 7. Terminal voltage response of generator 3 for 3LG permanent fault at position C considering cyber-attack and no cyber-attack.

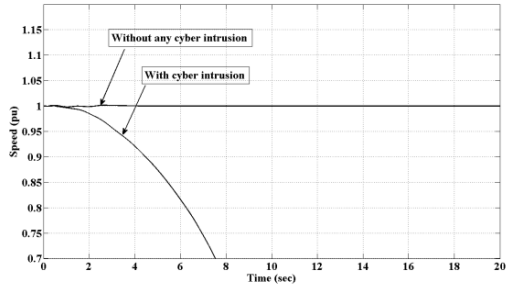


Fig 8. Speed response of generator 5 for 3LG permanent fault at position E considering cyber-attack and no cyber-attack.

it is clear that without any cyber intrusion on the circuit breakers reclosing signal collection, generators speed and terminal voltage returns to steady operating state for any fault in the IEEE 30 bus power system. However, with delayed reclosing signal from cyber intrusion, the speed and terminal voltage goes out of step and control. So, any physical fault without cyber intrusion on the power system will hamper the stability of the nearest generator but it may heal itself depending upon the fault condition. But with physical fault and cyber intrusion on circuit breakers reclosing signal accumulation, the generators will be out of control and it will adversely affect the whole systems operation. Therefore, it is clear that the delayed reclosing signal from the SCADA has adverse effect on the operation of the system. Moreover, the co-simulated system can easily translate the delayed traffic signal and represents the system performance.

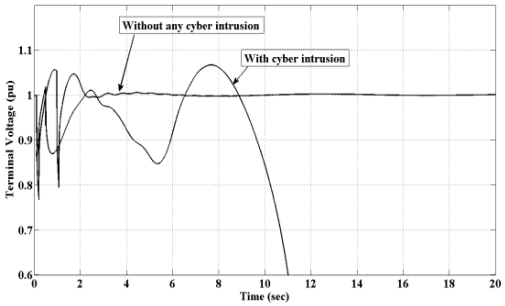


Fig. 9. Terminal voltage response of generator 5 for 3LG permanent fault at position E considering cyber-attack and no cyber-attack.

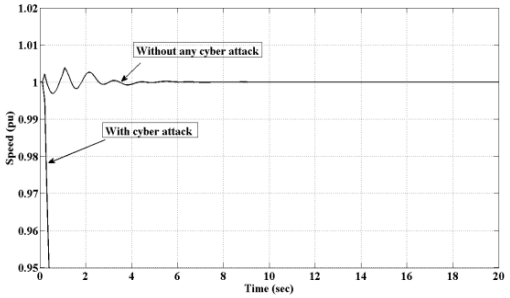


Fig. 10. Speed response of generator 2 for 3LG permanent fault at position B considering cyber-attack and no cyber-attack.

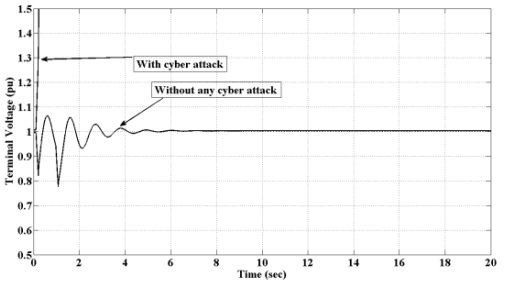


Fig. 11. Terminal voltage response of generator 2 for 3LG permanent fault at position B considering cyber-attack and no cyber-attack.

Fig. 10 and Fig. 11 represent the speed of generator G2 and terminal voltage at bus 2 considering both cyber-attack and no cyber-attack for 3LG permanent fault at point B.

## IX. Critical Clearing Time (CCT)

In this work, the critical clearing time (CCT) has been considered and adopted as a stability limit for the smart grid from a practical point of view. The CCT presents the maximum allowable time at which a fault and cyber-attack must be cleared to preserve and maintain the stability of the whole system [12]. Therefore, it is used for quantifying the effect of a cyber-attack in the considered system. With proper CCT information, a better coordination between the protective devices in a power system can be established in case of a cyber-attack. Lower CCT indicates less stable situation for smart grid stability studies [12].

For this study, a time domain simulation method is used to calculate the CCT. For the time domain simulation, a predefined step size is used for clearing time, and the stability of the system is observed. Table I represents the critical clearing times with and without cyber-attacks for 3LG permanent fault at different fault locations in the IEEE 30 bus test system. From Table I, it is clear that the CCT values with a cyber-attack in the system are less than the CCT values without a cyber-attack in the system. This is an indication of the effect of cyber-attack in the stability of the smart grid.

TABLE I. Critical Clearing Time With Cyber Attack And Without Cyber Attack For Different Fault Location

| Fault Type | Fault point | CCT values without any cyber-attack (sec) | CCT values with cyber-attack (sec) |
|---|---|---|---|
| 3LG | A | 0.121 | 0.052 |
| | B | 0.542 | 0.073 |
| | C | 0.402 | 0.068 |
| | D | 0.565 | 0.075 |
| | E | 0.572 | 0.074 |
| | F | 0.132 | 0.055 |
| | G | 0.614 | 0.077 |
| | H | 0.632 | 0.078 |
| | I | 0.513 | 0.072 |
| | J | 0.511 | 0.070 |
| | K | 0.712 | 0.083 |
| | L | 0.488 | 0.068 |
| | M | 0.723 | 0.085 |
| | N | 0.431 | 0.069 |
| | O | 0.505 | 0.071 |

## X. Conclusion and Future Research

In this paper, a Simulink and OPNET based co-simulated platform for observing the effect of cyber intrusion in modern power systems and smart grid is presented. In order to demonstrate the effectiveness of the proposed co-simulation scheme, the IEEE 30 bus power system model is considered. The experimental test system was designed and implemented in Simulink environment. A simple SCADA system was designed in the OPNET environment. The optimal reclosing signal of the circuit breakers is delayed to represent a cyber-attack. The effect of the cyber-attack on the responses of the generators near the fault locations was observed. Different disturbance situations in the IEEE 30 bus test system were considered and the co-simulated results and the critical clearing time indicate the adverse effect of cyber intrusion on the physical systems response.

In our future studies, a large smart grid network consisting of various generation sources (photovoltaic, wind and synchronous generators), smart loads and energy storage system will be considered and analyzed by observing the effect of tampered communication signal. Moreover, we will consider packet drop and DDoS attacks. Also, we plan to investigate the effect of unsuccessful cyber-attacks on the smart grid performance.

## XI. ACKNOWLEDGMENT

The views expressed in this paper are those of the authors and do not reflect the official policy or position of our respective academic institutions (University of Memphis, Arkansas State University), Oak Ridge National Laboratory, the Department of Energy, or the U.S. Government.

## REFERENCES

[1] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," Proceedings of the IEEE, vol. 100, pp. 210-224, 2012.

[2] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," IEEE Communications Magazine, vol. 50, pp. 38-45, 2012.

[3] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," IEEE Transactions on Power Delivery, vol. 25, pp. 1501-1507, 2010.

[4] C. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, "SCADA cyber security testbed development," in Proceedings of the 38th North American power symposium (NAPS 2006), 2006, pp. 483-488.

[5] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," IEEE Communications Surveys & Tutorials, vol. 14, pp. 981-997, 2012.

[6] Z. Mohajerani, F. Farzan, M. Jafary, Y. Lu, D. Wei, N. Kalenchits, et al., "Cyber-related risk assessment and critical asset identification within the power grid," in 2010 IEEE PES Transmission and Distribution Conference and Exposition, 2010, pp. 1-4.

[7] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim—A framework for building SCADA simulations," IEEE Transactions on Smart Grid, vol. 2, pp. 589-597, 2011.

[8] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol. 57, pp. 1344-1371, 2013.

[9] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," IEEE Transactions on Smart Grid, vol. 2, pp. 796-808, 2011.

[10] M. S. Hasan, H. Yu, A. Carrington, and T. C. Yang, "Co-simulation of wireless networked control systems over mobile ad hoc network using SIMULINK and OPNET," IET communications, vol. 3, pp. 1297-1310, 2009.

[11] W. Li, A. Monti, M. Luo, and R. A. Dougal, "VPNET: A co-simulation framework for analyzing communication channel effects on power systems," in Electric Ship Technologies Symposium (ESTS), 2011 IEEE, 2011, pp. 143-149.

[12] M. A. H. Sadi and M. H. Ali, "A Fuzzy Logic Controlled Bridge Type Fault Current Limiter For Transient Stability Augmentation of Multi-Machine Power System," Accepted for publication in the IEEE Transactions on Power Systems, 2015.

[13] D. Choi, S. Lee, D. Won, and S. Kim, "Efficient secure group communications for SCADA," IEEE Transactions on Power Delivery, vol. 25, pp. 714-722, 2010.

[14] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," Computers & Security, vol. 25, pp. 498-506, 2006.

[15] NIST. Guidelines for smart grid cyber security: Privacy and the Smart Grid, NISTIR 7628. 2.

[16] 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, pp. 847-855, 2013.

[17] M. J. McDonald, G. N. Conrad, T. C. Service, and R. H. Cassidy, "Cyber Effects Analysis Using VCSE Promoting Control System Reliability (Report No. SAND2008-5954)," Sandia National Laboratories, Albuquerque 2008.

[18] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in 2011 IEEE PES Innovative Smart Grid Technologies (ISGT), 2011, pp. 1-7.

[19] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in 2014 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), 2014, pp. 1-5.

[20] M. A. H. Sadi and M. H. Ali, "A Comprehensive Analysis of Transient Stability Enhancement Methods of Electric Power System," Paper number 1085, Accepted for Lecture presentation at The 47th North American Power Symposium, The University of North Carolina at Charlotte, 2015.

[21] M. A. H. Sadi and M. H. Ali, "Combined Operation of SFCL and Optimal Reclosing of Circuit Breakers for Power System Transient Stability Enhancement," in 2013 IEEE SoutheasrCon, Jacksonville, FL., 2013.

[22] M. A. H. Sadi and H. Ali, "Combined operation of SVC and optimal reclosing of circuit breakers for power system transient stability enhancement," Electric Power Systems Research, vol. 106, pp. 241-248, 2014.

[23] M. A. H. Sadi and M. H. Ali, "Transient stability enhancement by bridge type fault current limiter considering coordination with optimal reclosing of circuit breakers," Electric Power Systems Research, vol. 124, pp. 160-172, 2015.

[24] M. H. Ali, T. Murata, and J. Tamura, "Effect of Coordination of Optimal Reclosing & Fuzzy Controlled Braking Resistor on Transient Stability During Unsuccessful Reclosing," IEEE Transaction on Power System, vol. 21, pp. 1321-1330, August 2006.

[25] X. Chang, "Network simulations with OPNET," in Proceedings of the 31st conference on Winter simulation: Simulation---a bridge to the future-Volume 1, 1999, pp. 307-314.

[26] M. A. H. Sadi, M. H. Ali, D. Dasgupta, and R. K. Abercrombie, "OPNET/Simulink Based Testbed for Disturbance Detection in the Smart Grid," in Proceedings of the 10th Annual Cyber and Information Security Research Conference, 2015, Article No.: 17.

[27] M. A. H. Sadi and M. H. Ali, "Transient Stability Enhancement of Multi-Machine Power System by Parallel Resonance Type Fault Current Limiter," Paper number 1217, Accepted for Lecture presentation at The 47th North American Power Symposium., The University of North Carolina at Charlotte, 2015.