Smart Grid Co-Simulation Tools: Review and Cybersecurity Case Study

Tan Duy Le[1,2], Adnan Anwar[2], Razvan Beuran[1] and Seng W. Loke[2]
[1]*Japan Advanced Institute of Science and Technology* - [2]*School of IT, Deakin University, Geelong*
Ishikawa, Japan - Victoria, Australia
tanld@jaist.ac.jp

***Abstract*—The smart grid is a complicated system consisting of communication network and power grid components. There are various powerful simulation tools for communication networks, as well as power systems. However, co-simulation tools are required to reproduce the interaction between cyber-physical components. We conducted a survey overview of various co-simulation tools and their characteristics applicable to smart grid research. We determined that the combination of FCNS, GridLAB-D and ns-3 is a promising direction for smart grid study, improving co-simulation speed by 20%. By applying these tools and the IEEE 13 Node Test Feeder Model, we conducted a case study on the impact of security threats on smart grid demand/response and dynamic pricing applications. The impact of fake data injection and jamming attacks are obvious as a result of our simulation. The findings support related research in the field and can be used for cybersecurity training.**

***Index Terms*—smart grid, co-simulation, framework, network simulation, fake data injection, jamming attacks, test feeder model**

I. Introduction

The smart grid is a complex system that includes two independent parts: communication networks and the power grid. In recent years, there has been an expansion in the number of cyber-attacks on the smart grid system, which leads to various consequences, ranging from blackouts, loss of confidential information or even physical damage to power devices. Therefore, understanding the impact of security threats and network performance on smart grid applications is critical.

Simulation, which provides the ability to solve real-world problems safely and efficiently, has advantages compared to the physical systems for cybersecurity research. There are various powerful simulation tools for each smart grid component. For example, OMNET++ and ns-3 are the most well-known communication network simulation tools. Moreover, GridLAB-D and OpenDSS are widely applied for power system simulation.

However, these simulation tools do not provide the capability to track and monitor the interaction between the communication network and physical power grid factors. There is a lack of design tools that are efficient in simulating the smart grid system within a single environment. Co-simulation is the solution to overcome these barriers for smart grid research.

Although some work has already been done in this area, much of this has utilized with specific scenarios, in a limited scope, and is hard to expand. In this research, we make the following contributions. First, we introduce each smart grid component and piece of network architecture. We provide an analytical literature review state of the art in smart grid co-simulation technologies. Our research indicates that the combination of FNCS, GridLAB-D, and ns-3 is a promising direction towards smart grid co-simulation with the dedicated messaging system and time synchronization, useful not only for analysis but for cybersecurity training. Second, to demonstrate the usefulness of grid co-simulation for understanding cybersecurity, we explore a case study with FNCS by using the IEEE 13 Node Test Feeder Model. Demand/response and dynamic pricing applications are investigated under false data injection and jamming attack circumstances. The results make clear the impact of security threats on smart grid applications, and are supported by related research in the field. Finally, this type of modeling can be helpful for smart grid cybersecurity training because the impact and implications of attacks can be easily demonstrated.

The remainder of this research is structured as follows. The smart grid system will be described in Section II. Smart grid co-simulation tools, including power system simulation, network simulation, and co-simulation, will be discussed in Section III. Section IV describes a case study that we implemented using FNCS. Finally, we conclude our research in Section V.

II. Smart Grid System

Built since the 1890s, the traditional electrical grid, or "the grid", consists of a network of transmission lines, transformers, distribution substations and all of its accessories. Its primary function is to deliver electricity from producers to consumers. To move forward, this grid has been strengthened by applying advanced technologies. Nowadays, in the era of Society 5.0, there is a need for a new type of electrical grid, the one which has been developed from the bottom up to manage the groundswell of digital and computerized equipment, and technology-dependent on it. Furthermore, the new technique should also automate and handle the growing complexity and energy requirements in the 21^{st} century. The "Smart Grid" is emerging as a potential technology to resolve these problems.

The smart grid is an automation system that allows two-way communications between utility and consumers. Such a grid consists of advance digital systems, automation, computers, and controls. There are two essentially independent components of a smart grid system: the power grid and communica-

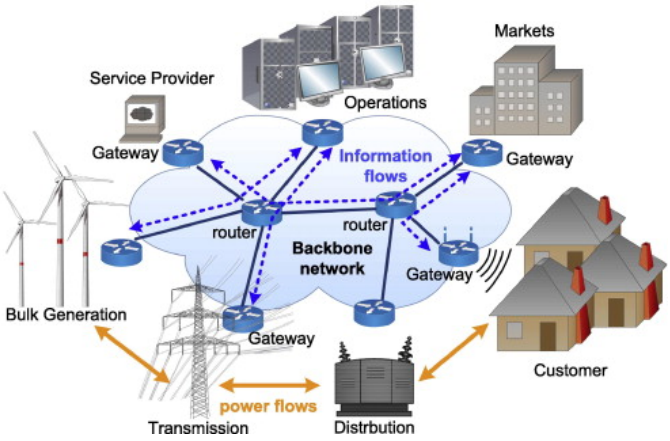


Fig. 1: The network architecture in the Smart Grid: backbone and local-area networks. [2]

tion network. The interaction between these technologies and the electrical grid allows the system to digitally respond to the quickly changing electric demand and power failure. In short, a smart grid can be defined as a power network using modern computer and communication technology to achieve a system that can better deal with potential failures.

The U.S. Department of Energy has indentified four advanced technologies that turn a traditional electrical grid into a smart grid, as follows:

- Fully automated and integrated two-way communication between the overall components of an electric grid.
- Automatic control for power distribution, faults, and repairs.
- Advance management panel, decision support software, and mechanism.
- Accurate sensing and measurement technologies.

According to the conceptual model proposed by NIST [1], there are seven logical domains in a smart grid system which can be divided into two types based on their features:

- Support the two-way power and information flow:
  - Bulk Generation
  - Transmission
  - Distribution
  - Customer
- Support information collection and power management:
  - Markets
  - Service Provider
  - Operations

The communication network must be highly-distributed and hierarchical in order to interconnect all these domains. Figure 1 is proposed by the research in [2], which represents a smart grid communication network onto a hybrid and hierarchical network, including the backbone network and millions of local-area networks.

A smart grid is a complex system in which network communication and the physical power grid are the two essential components. For further system study and development, researchers need to understand the interaction between these factors. However, it is difficult to apply a real smart grid system for testing and validation purposes. Therefore, system-level modeling and tools for smart grid simulation are essential. These tools also allow researchers to evaluate the impact and effectiveness of proposed approaches in the system.

III. Smart Grid Co-simulation tools

Obviously, there are various powerful simulation tools for power systems as well as communication networks. In this section, we briefly introduce some popular simulation tools. The co-simulation tools are surveyed and discussed.

A. Power System Simulation

For the power grid simulation, there are abundant open-source tools. However, GridLAB-D and OpenDSS are emerging as powerful tools for power grid simulation. These power distribution system simulation and analysis tools provide valuable information to utilities wanting to exploit the latest energy technologies and to users who design and operate distribution systems.

GridLAB-D [3] is an open-source power distribution system simulation and analysis tool that was developed by Pacific Northwest National Laboratory - the U.S. Department of Energy in collaboration with academia and industry. GridLAB-D incorporates the most sophisticated simulation methodologies and high-performance algorithms to provide the latest end-use modeling. In addition, GridLAB-D is combined with software integration tools and distribution automation models for developers of a wide variety of power analysis tools. GridLAB-D can be combined with a range of data management and analysis tools from third parties. It is valuable for utility engineers, regulators, various stakeholders, and consumers. GridLAB-D provides a wide range of tools for designing, handling, and evaluating findings.

The Open Distribution System Simulator (OpenDSS, or simply, DSS) [4] is an open-source project developed by the Electric Power Research Institute (EPRI) since 1997. OpenDSS is a powerful simulation tool for electrical systems, especially for electricity distribution systems. This supports not only most frequency-domain analyses (sinusoidal steady-state analyses) typically conducted on power distribution systems but also many new types of analysis designed to support future needs relevant to smart grid, grid optimization, and renewable energy studies. The OpenDSS is developed to be continuously expandable to meet future requirements. Developers can externally add other solution modes and features via the COM interface and perform simulator functions, including model data definition.

B. Network Simulation

For the network communication simulation, there are various tools such as OMNET++ and ns-3, whereby a software program models the behavior of the network by calculating the interaction between the different network entities.

No	Last update	Name	Power Simulator	Network Simulator	Operating system
1	2006	EPOCHS	PSLF	ns-2	Linux
2	2011	Hybrid Simulator	OpenDSS	ns-2	Windows
3	2011	VPNET	Virtual Test Bed (VTB)	OPNET	Windows
4	2011	PowerNet	Modelica	ns-2	N/A
5	2011	TASSCS	PowerWorld	RINSE	Windows
6	2012	GECO	PSLF	ns-2	N/A
7	2013	Nessi2	Built-in	Built-in	Windows
8	2014	SGsim	OpenDSS	OMNeT++	Windows 7
9	2014	GridSpice	MATPOWER and GridLAB-D	N/A	Windows and Linux
10	2015	ScorePlus	GridLAB-D (Built-in)	CORE	Linux
11	2015	InterPSS	Built-in	N/A	Windows and Cloud
12	2015	Simulating Smart Grid	GridLAB-D	ns-2	Linux
13	2016	ASTORIA	Mosaik 2.4.0	NS-3	Linux
14	2017	CPSA	MATLAB, PowerWorld,	GridSim	Windows
15	2018	FNCS	GridLaB-D	ns-3	Linux
16	2019	SimApi	EnergyPlus	Built-in	Cloud
17	2019	ERIGrid	PowerFactory, MATLAB	ns-3 and mosaik	Mainly on Windows
18	2019	HELICS	GridLaB-D	ns-3	Linux, Windows, and Mac OS X

TABLE I: Co-simulation tools for Smart Grid

OMNeT++ [5] is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators. Instead of building a specialized simulator, OMNeT++ was designed to be as general as possible. Developed since 1997, this open-source tool has been widely used by researchers for network simulation. OMNeT++ can be employed in numerous domains from sensor networks, wireless ad-hoc networks, Internet protocols, and performance modeling to photonic networks. The objective of OMNeT++ is to support network simulation on a large scale.

ns-3 [6] is an open, extensible network simulation platform specifically for networking research and education. First introduced in 2008, following its predecessor - ns-2, ns-3 has been widely adopted as a simulator for the Internet and other network systems. The simulator consists of a robust network models library, including multicast protocols, IP-based applications (TCP, UDP), routing, wire, and wireless networks. Although the core of ns-3 is created by using the C++ programming language, ns-3 not only supports the OTcl interface but also CMDENV, TKENV, TVENV, and a Python scripting interface. Therefore, developers can develop and modify simulations without understadning the C++ language or recompiling ns-3. Further, by supporting Python language, ns-3 provides the ability to improve scalability and better software integration. There are four major components of ns-3 to support all other simulator components, including core, simulator, common, and node modules.

C. Co-Simulation Tools

Co-simulation is the co-ordinated operation of two or more simulation models that vary in their representation and runtime. This allows the interaction and reciprocal effect between physical power grids and communication networks to be recorded. Multiple specialized simulation environments are connected into a single distributed environment instead of developing and constructing a new combined simulation environment. By combination, the well-validated existing libraries of models and frameworks can be reused. However, the integration also introduces various challenges in co-simulation, for example, time synchronization, differences in time scales, messages delivery delays, and reasonable models reuse.

Extensive efforts have been made and various co-simulation platforms have been introduced into the energy domain in recent years, which are shown in Table I.

The electric power and communication synchronizing simulator (EPOCHS) [7] is one of the pioneers in smart grid co-simulation. The framework is a combination of PSLF, a commercial electric simulator, with ns-2, an open-source communication-network simulator. This distributed simulation environment was developed to understand the impacts of communication systems on electromechanical circumstances. The major applications of EPOCHS are relevant to wide-area

monitoring, security, and management. It should be noted that the last update of this partial open-source project was in 2006.

NeSSi2 [8] is a network simulation environment based on the service-centric agent platform JIAC. NeSSi2 concentrates on security-related scenarios, for example, attack analysis and evaluation of countermeasures. Chinnow et al. [9] extended NeSSi2 to provide the security paradigm and relevant attack scenarios specific for Smart Metering or AMIs Network. An open ring topology, which is commonly deployed in larger cities in Germany, is defined for both the energy network and IP network. However, the research only simulated and evaluated the impact of the DDoS attacks on critical infrastructure.

SGsim [10] is a real-time simulation framework to simulate different smart grid applications. The researchers have applied OMNET++ and OpenDSS as the backend for communication and power simulation, respectively. SGsim aims to assess the effects of communications on control actions. Furthermore, smart grid related standards, for instance, IEEE C37.118 and standard smart grid tools such as openPDC are supported. This open-source framework has been widely respected in the research community. However, there are limitations in supported standards, components, and case studies.

There are various other frameworks that have been mainly designed for high usability. For example, the theoretical research has been conducted by Dugan et al. [11] by utilizing the combination of OpenDSS and ns-2.

Although these simulation tools can carry out power flow and communication studies, they are usually used with a minimal scope that has been tested in small networks. The tools are mainly designed for specific scenarios. Therefore, it is difficult to extend. However, current simulation approaches are quite complicated for implementation and usage. They require the proprietary software adoption or the construction of the network model in the engineer's unusual platforms, for example, new GUI.

Fenix Framework for Network Co-Simulation (FNCS) [12] is a High-Performance Computing (HPC) simulation platform. FNCS supports co-simulation for multiple platforms, including a single node, multiple nodes, clusters, and clouds. On the one hand, ns-3 is used to simulate data communication networks and to control the operation of the components. On the other hand, GridLAB-D is applied to simulate the power grid. FNCS broker is structured in the middle to manage the interaction between cyber-physical components. Each simulator that is going to be federated by FNCS needs to register with the FNCS broker. This enables centralized control of simulator processes. FNCS's design goal is to reuse existing simulators as much as possible to provide the environment for real-time co-simulation development. The time steps for synchronization is determined according to the next time steps of the simulators and whether in-transit messages exist. By applying two synchronization strategies that make thoughtful decisions about when the simulators are going to exchange messages, FNCS can improve co-simulation speed by 20%.

FNCS is a promising direction towards smart grid co-simulation with a dedicated messaging system and time synchronization. Currently, there are few research efforts that evaluate the consequences of cyber-attacks on the smart grid system using FNCS.

IV. A CASE STUDY USING FNCS

There are various smart grid applications including demand response (DR), dynamic pricing, wide-area monitoring, protection, and control (WAMPAC), phasor measurement units (PMU) and advanced metering infrastructures (AMI). High bandwidth communications are required to enable high-speed, wide-area control and protection in numerous applications including demand response and dynamic pricing applications. However, these requirements are not applied for all applications; for example, AMI just needs to update billing information once every 24 hours. Therefore, previous work in the field has assumed that different elements exchange information near-instantaneously and communication delays do not exist.

Peak demand reduction is an emerging issue in the energy industry. The research in [13] indicated that 25% of the distribution and 10% of generation assets as well as transmission, which are worth of 100s of billions of dollars, are needed less than 400 hours a year. Achieving peak demand reduction requires a smart grid with demand response and dynamic pricing functions. To fulfill our needs to understand the interaction between cyber-physical components in the context of cybersecurity, we applied the FNCS framework to simulate demand response and dynamic pricing applications.

Few researchers in the field have done work related to this. The study by Fuller et al. [14] pioneers the development of a transactive demand response system by using FNCS to conduct the Olympic Peninsula and AEP gridSMART demonstrations. This simple case study used the IEEE 13 Node Test Feeder Model as the power grid model. The result figured out the effect of communication delays on the smart grid system. Moulema et al. [15] applied FNCS to implement extensive case studies to understand the interaction between each smart grid component. However, the standard test feeder model is not applied in this research. Our case study is needed to bridge this gap.

A. Smart Grid Applications

Demand/Response aims to ensure stable energy supply during times of peak demand by providing the ability for end-users to dynamically reduce or shift their energy consumption. Instead of adjusting the supply, demand/response objects to adjust the energy demand of the consumers. Therefore, unlike in the traditional energy grid system, consumers can take an significant part in electric grid service. Consequently, there are various benefits to a utility such as a peak load reduction, regulating services, and emergency operations.

Dynamic pricing is an efficient methodology to empower demand/response function. Time-of-Use (TOU), Critical Peak Price (CPP), and Real Time Price (RTP) are three methods of doing pricing. Real Time Pricing of electricity has facilitated the estimation of price elasticity over different periods. Therefore, it is commonplace in developed economies. In this

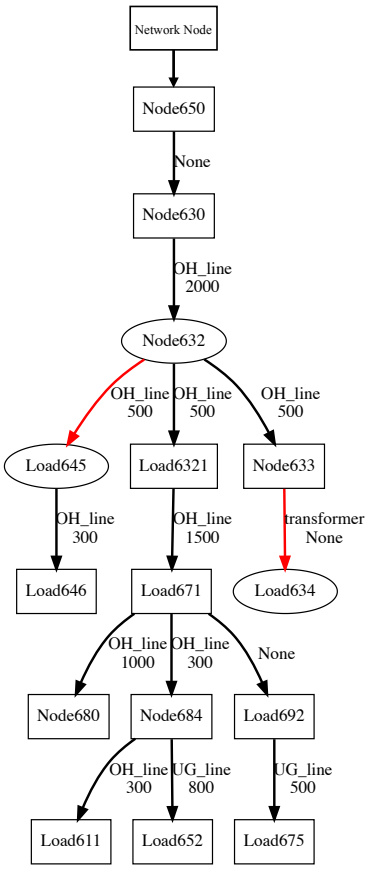


Fig. 2: IEEE 13 Node Test Feeder Model

approach, control signals or a reference bids price are sent to the controller by both suppliers and demanders in a finite time interval. The supplier bid power they can provide at a given time while demanders bid power they can forgo at a given price. After the defined time interval, usually from 5 to 15 minutes, the bidding process is stopped, and market-clearing begins. Both demand and supply components have been sorted. Demand bids are sorted from the highest price to the lowest price, while supply bids are sorted from the lowest price to the highest price. Their curves are then created by the total quantities associated with these sorted prices. Principally, the intersection of curves is the clearing price and quantity of the market. This process repeats for every time interval.

B. Smart Grid Model

A Gridlab-D power system was developed based on the IEEE 13 Node Test Feeder Model [16]. This test feeder is applied to evaluate common distribution analysis software characteristics. It is distinguished by being short, relatively highly loaded, and having a single voltage regulator at the substation, two shunt capacitors, overhead and underground lines, an inline transformer, and a total of 9 unbalanced loads. Figure 2 illustrates the IEEE 13 Node Test Feeder Model. The static loads were replaced with 73 individual residential building objects connected via triplex meters to the power line. Every house had Heating, Ventilation, and Air Conditioning (HVAC) system. A passive controller is defined to control this HVAC system. After receiving clearing quantity from the market for each interval, the passive controller adjusts the thermostat control band, by increasing the hysteresis or by moving the temperature band as the feature of demand/response.

The substation comprises a three-phase swing bus 2401 V nominal voltage and 5 MAV power rating. One meter between the substation transformer and the loads monitors the total load and senses the electricity demand. This meter allows the substation to modify its power supply. In this model, the substation is represented as the energy provider. It sets the energy market's maximum power capacity and determines energy reference prices depending on the time during the day, as well as current electricity demand. The default maximum capacity bid quantity and price cap are set as 150 kW and $3.78, respectively.

For the communication network, there are 73 nodes representing smart meters equipped in each house. These smart meters are arranged and clustered into 20 nodes that construct local networks. Through a point-to-point communication connection, an edge network node in each group routes the data to a data aggregator. The communication model relies on the transport protocol CSMA (Carrier-sense multi-access), which includes a data rate of 4 Mbps and a transmission delay of 2 milliseconds for point-to-point connectivity, and a transmission delay of 10 Gbps for local area networks with a data rate of 3 milliseconds.

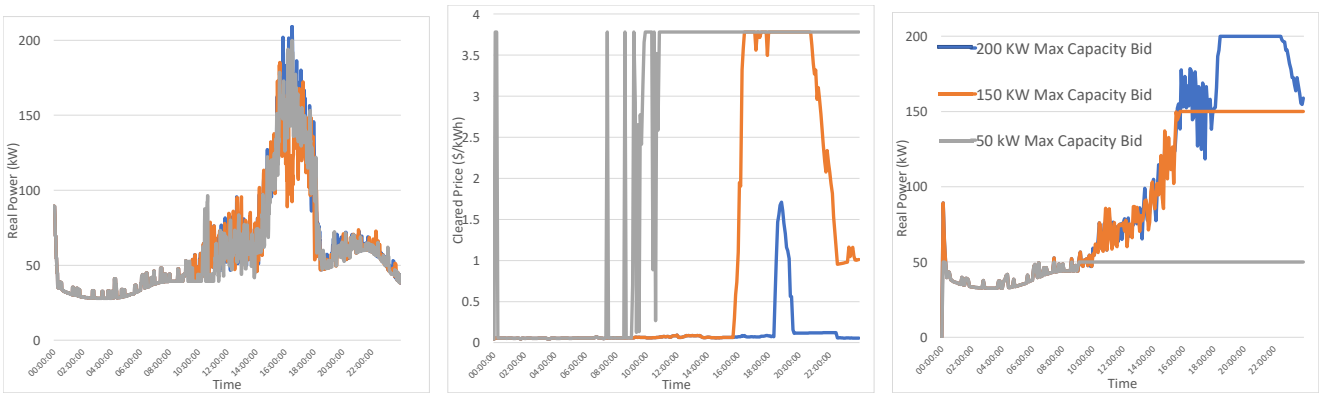
C. Co-Simulation Scenarios

By using FNCS, Gridlab-D, and ns-3, we simulated two different scenarios to understand the impact of security threats and network performance on smart grid applications.

(1) False Data Injection: Intending to disrupt system operations, attackers exploit system vulnerabilities then manipulate the data collected from the network in a false data injection attack. In this scenario, we made the assumption that the attackers injected incorrect data into the system, which changed the maximum bid quantity from 150 KW to unexpectedly higher at 250 KW and lower at 50 KW. This circumstance aims to evaluate the overall performance of the dynamic pricing and the effectiveness of the demand/response function under security attacks.

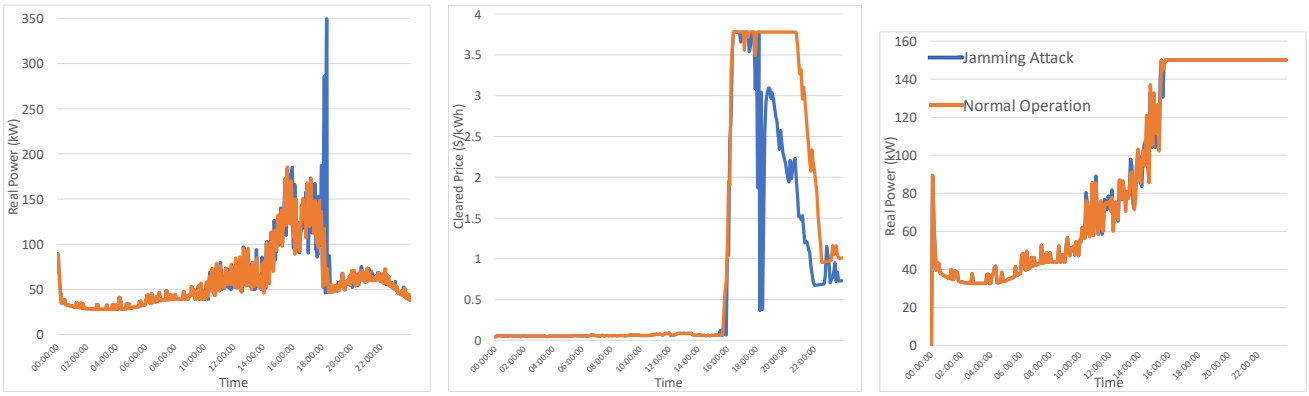
(2) Jamming Attack: Data rate, throughput, and delay affect the general operation and efficiency of the system. A jamming attack is a kind of Denial of Service attack where an attacker transmits a high-range signal to interrupt the communication. To simulate the attack, communication delays were increased until the cleared market price was noticeably affected. Finally, the data rate were shifted from 4 Mbps to 1 Mbps while the delay has been adjusted from 3 ms to 100 ms, which is the worst-case scenario for the delay. The goal of this scenario is to demonstrate the impact of a faulty network environment on the market.

Under these conditions, the system behavior will be observed and data, including (a) total load metrics, (b) market-



(a) (b) (c)

Fig. 3: False Data Injection Attack



(a) (b) (c)

Fig. 4: Jamming Attack

clearing price, and (c) market-clearing quantity will also be collected. Based on our available database, the simulation duration is 24 hours from 00:00:00 July 21^{st}, 2009 to 00:00:00 July 22^{nd}, 2009, using the National Solar Radiation Data Base of Seattle City - Washington.

It is noted that other fake data, data rates, and delay values have significant effects on the system. However, the scope of this research focuses on the aforementioned values.

D. Performance Evaluation

We developed an experimental setup on Intel Core i7 CPU 3.1 GHz, Linux 64-bit operation system and equipped it with 16 GB DDR3 memory. FNCS relies on the additional software libraries including ZeroMQ, and its higher-level C binding CZMQ. Therefore, GridLAB-D (ticket 797), ns-3 3.26 specific version for FNCS, and prerequisite libraries must be installed properly. We next present our experimental results for the smart grid model. It should be noted that error bars were omitted in all figures since these simulations run premeditatedly.

(1) False Data Injection: The variation of (a) the total load, (b) market-clearing price, and (c) market-clearing quantity in 24 hours for a normal capacity bid of 150 kW, false high capacity bid of 200 kW, and low capacity bid of 50 kW are respectively shown in Figure 3. In normal operation, the highest clearing price is during peak hours, which are from the late afternoon to the evening. The typical maximum total load is 186 kW. The three total load curves are similar in the morning periods for low consumption. However, the differences are noticeable when energy consumption increases from the afternoon.

By injecting a fake, large maximum capacity bid at 200 kW, we supply more energy to the market. As expected, the price is always low and independent from the time of use. Figure 3(b) shows that the clearing price is almost the same when energy demand is typically low and remains below $1.7 during peak hours. Consequently, customers can afford to use more power without being too concerned about their monthly bills even during peak hours. The maximum total load jumped to 210 kW in these circumstances.

Less energy is available in the market by injecting a false,

small maximum capacity bid at 50 kW. Therefore, there is a great effect on the clearing price, which jumps to the price cap $3.78. In this scenario, the customers' efforts to adapt their energy consumption has minimal effect and demand/response is less efficient. The maximum total load is 200 kW.

Therefore, the maximum capacity bid and the quantity of energy supplied to the market should be defined optimally in order to achieve a fair market as well as a win-win condition between suppliers and consumers. Manipulating and forging capacity bids on the market can cause enormous consequences.

(2) Jamming Attack: The variation of (a) the total load, (b) market-clearing price, and (c) market-clearing quantity in 24 hours for normal operation and network congestion are illustrated in Figure 4. Although the clearing quantity curves are similar, as shown in Figure 4(c), the clearing price curves are quite different as represented in Figure 4(b). Under network congestion conditions, the clearing price curves fluctuated and the customers can pay less money. Therefore, they can demand more energy during peak hours. Figure 4(a) shows that the total load in jamming attack conditions reaches over 350 kW.

The packet distribution ratio is very poor since more packets are lost in jamming attack scenarios. The lack of real-time information exchange between controller and consumers results in a malfunctioning market, which does not make the impact of demand response application noticeable. This is because a large number of the bids are delayed, especially the re-bids later in the market cycle. Since the re-bids within the cycle do not actually reach the auction before clearing, the auction utilizes obsolete information to formulate the bid curve. Therefore, the performance of demand/response and dynamic pricing was poor. This scenario gives a substantial profit for the end-users; however, there are notable losses for energy suppliers. To achieve the win-win situation between end-users and suppliers, jamming attack issues should be considered.

It is noted that the impact (quantitative and qualitative) of fake data injection and jamming attack are not obvious without such simulation, and can only be understood via co-simulation, due to the inter-play of network and power factors. Understanding such impact when designing solutions to detect attacks and to manage attacks, and for smartgrid cybersecurity training purposes.

V. Conclusions and future work

In this research, we provided a comprehensive survey of various co-simulation tools and their features, and functionalities for smart grid study. Among the tools, FNCS is a successful solution to co-simulate the smart grid with a dedicated messaging system and time synchronization. We implemented two distinct scenarios using FNCS, GridLAB-D, and ns-3, to comprehend the effect of security threats on smart grid applications. This knowledge can be used for cybersecurity training of end-users. For example, via visualizing graphics, the customers can easily understand the economic impact of cyber-physical attacks on the smart grid system. Thanks to the co-simulation tool, IT experts can recognize and evaluate the effects of false data injection and jamming attack on the system. In addition, this tool can be applied to identify the most economical methods of implementing smart grid technology, particularly with regards to communication requirements for efficient system operation. Moreover, this co-simulation environment can help system planners to calculate the inherent cost of the proposed demand/response and dynamic pricing technology. For future work, more applications, attack types, IEEE test feeder models, network models, and scenarios will be investigated.

References

[1] Greer, C., Wollman, D. A., Prochaska, D. E., Boynton, P. A., Mazer, J. A., Nguyen, C. T., ... & Pillitteri, V. Y. (2014). NIST framework and roadmap for smart grid interoperability standards, release 3.0 (No. Special Publication (NIST SP)-1108r3).

[2] Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. Computer networks, 57(5), 1344-1371.

[3] Chassin, D. P., Schneider, K., & Gerkensmeyer, C. (2008, April). GridLAB-D: An open-source power systems modeling and simulation environment. In 2008 IEEE/PES Transmission and Distribution Conference and Exposition (pp. 1-5). IEEE.

[4] Montenegro, D., Hernandez, M., & Ramos, G. A. (2012, September). Real time OpenDSS framework for distribution systems simulation and analysis. In 2012 Sixth IEEE/PES Transmission and Distribution: Latin America Conference and Exposition (T&D-LA) (pp. 1-5). IEEE.

[5] OMNeT Discrete Event Simulator. (n.d.). Retrieved April 30, 2019, from https://omnetpp.org/

[6] Henderson, T. R., Lacage, M., Riley, G. F., Dowell, C., & Kopena, J. (2008). Network simulations with the ns-3 simulator. SIGCOMM demonstration, 14(14), 527.

[7] Hopkinson, K., Wang, X., Giovanini, R., Thorp, J., Birman, K., & Coury, D. (2006). EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. IEEE Transactions on Power Systems, 21(2), 548-558.

[8] Grunewald, D., Ltzenberger, M., Chinnow, J., Bye, R., Bsufka, K., & Albayrak, S. (2011, May). Agent-based network security simulation. In The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 3 (pp. 1325-1326). International Foundation for Autonomous Agents and Multiagent Systems.

[9] Chinnow, J., Bsufka, K., Schmidt, A. D., Bye, R., Camtepe, A., & Albayrak, S. (2011, November). A simulation framework for smart meter security evaluation. In 2011 IEEE International Conference on Smart Measurements of Future Grids (SMFG) Proceedings (pp. 1-9). IEEE.

[10] Awad, A., Bazan, P., & German, R. (2014, May). SGsim: A simulation framework for smart grid applications. In 2014 IEEE International Energy Conference (ENERGYCON) (pp. 730-736). IEEE.

[11] Dugan, R., Mullen, S., Godfrey, T., & Rodine, C. (2011, June). Hybrid simulation of power distribution and communications networks. In Proc. CIRED (pp. 1-4).

[12] Ciraci, S., Daily, J., Fuller, J., Fisher, A., Marinovici, L., & Agarwal, K. (2014, April). FNCS: a framework for power system and communication networks co-simulation. In Proceedings of the symposium on theory of modeling & simulation-DEVS integrative (p. 36). Society for Computer Simulation International.

[13] Chu, S. (2009). Investing in our energy future. Presentation of Grid Week, Washington, DC, Sep, 21.

[14] Fuller, J. C., Ciraci, S., Daily, J. A., Fisher, A. R., & Hauer, M. (2013, May). Communication simulations for power system applications. In 2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES) (pp. 1-6). IEEE.

[15] Moulema, P., Yu, W., Griffith, D., & Golmie, N. (2015, August). On effectiveness of smart grid applications using co-simulation. In 2015 24th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-8). IEEE.

[16] Schneider, K. P., Mather, B. A., Pal, B. C., Ten, C. W., Shirek, G. J., Zhu, H., & Dugan, R. C. (2017). Analytic considerations and design basis for the IEEE distribution test feeders. IEEE Transactions on Power Systems, 33(3), 3181-3188.