CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid

Anonymous Author(s)

ABSTRACT

It has now become critical and important to understanding the nature of cyber-attacks and their impact on the physical operation of emerging smart electricity grids. Modeling and simulation provide a cost-effective means to develop frameworks and algorithms that address cyber-physical security challenges facing the smart grid. Existing simulation tools support either the communication network or the power system, but not both together. Thus, it is difficult to explore the effects of cyber-physical attacks on power system dynamics and operations. In order to bridge this gap, a cyber-physical co-simulator is required.

In this paper, we present a novel integrated cyber-physical security co-simulator tool capable of cyber-physical security assessment (CPSA), which simulates the communication network and the power system together. The tool identifies future vulnerable states and bad measurements and guides the operator at the control center on taking appropriate action to minimize disruption of the physical power system operation due to cyber-attack. The developed tool can be used in understanding of power system monitoring, analyzing the nature of cyber-attacks, detecting bad measurement data, bad command, disabled devices and understand their impact on the operation of the power system.

CCS CONCEPTS

•**Security and privacy** → *Distributed systems security;* •**Computer systems organization** → *Embedded and cyber-physical systems;*

KEYWORDS

Cyber-physical system, cyber-attack, impact monitoring, smart grid

ACM Reference format:
Anonymous Author(s). 2017. CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid. In *Proceedings of ACM Conference on Computer and Communications Security, Dallas, Texas, Due 19 May 2017 (Anonymous Submission to ACM CCS 2017),* 11 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

A reliable, trustworthy, and secure smart grid requires continuous, efficient, real-time monitoring and cyber-physical security assessment for increased situational awareness. It should also have the ability to detect various types of cyber-physical attacks and be able to quantify, characterize, and mitigate the impact of such attacks [12]. In recent years, there has been an increase in the number of cyber-attacks on the smart grid, with these attacks having severe consequences, such as blackouts and loss of confidential information in certain instances [2]. Cyber-attacks can affect the normal operation of power system applications, such as demand response, voltage control, device control over wide area network, etc. It can also affect the decision making capability of an Independent System Operator (ISO) or Regional Transmission Organization (RTO)'s Energy Management System (EMS), which can lead to cascading failures and instability in the grid. Compromised confidential power system information can trigger inappropriate actions by the operators. Ultimately, cyber-physical attacks can results in permanent physical damage to power devices in the field.

1.1 Context and Motivation

The power system is cyber-controlled through a combination of communications networks, embedded systems, computing resources and software applications. It is therefore important to understand the interdependencies between the cyber-elements used for control, and the operation of the power grid [11]. Different attack situations need to be monitored and analyzed as they take place in the underlying communication network. Malicious attacks or system misbehavior on the power or communication network system may compromise power system data and may disrupt control devices and apparatus [19].

Cyber-physical attacks typically compromise the cyber layer by incapacitating communications devices and/or making communications resources unavailable [21]. This can cause disruptions in the topology of the network, communication and controlling devices in the network and field, and communication performance (such as link baud rate, propagation time or delay, maximum number of packets that can be sent without major collision or packet dropping, and maximum allowable size of each packet). However, the effect of these attacks transcends the cyber layer, as cyber-physical attacks can incapacitate actual power system devices. Cyber-attacks on the smart grid range from traditional cyber-attacks, such as man-in-the-middle [24], denial-of-service [23], replay [22] and impersonation [3] to attacks that are cyber-physcial in nature and more specific to the smart grid, such as bad data injection, malicious command injection, and coordinated denial-of-service on Remote Terminal Units (RTUs).

The current state and overall health of the power system can also be affected by attacks over the communication network, such as delay attacks, synchronous flood attacks, distributed denial-of-service attacks on devices. During these attacks, the power system may undergo various state transitions and eventually become insecure. The modern smart grid is controlled using several latest wired and wireless communication technologies, such as WiMAX and LTE, to ensure the availability of information in an efficient manner, as well as to monitor critical components of the entire power system, such as , such as power equipment located in remote substations. In

DOI: 10.1145/nnnnnnn.nnnnnnn

order to analyze the interdependencies of cyber and physical power infrastructure, a cyber-physical security assessment co-simulator must be developed.

1.2 Scope and Challenges

Existing simulators on the market independently simulate either the power system or the communications network [18]. For example, PowerWorld [15] is a dedicated power systems simulator that simulates power systems dynamics and operations but assumes ideal communication conditions in the communications layer. NS2/3 on the other hand are dedicated communication network simulators that simulates communication network dynamics, but is incapable of simulating power systems devices [10]. An integrated cyber-physical co-simulator must be able to model and simulate the power system as well as the communication system simultaneously in addition to providing functionalities for assessing cyber-physical security. The co-simulator is able to perform an assessment on future vulnerable states, evolution of system states, and provide situational awareness in the presence of different cyber-attacks [13]. Accurate modeling and simulation of the dynamic behavior of the smart grid is quite challenging since the grid is a large and complex system comprised of thousands of sensors and power devices, such as generators, and transformers, etc., tied together by transmission and distribution lines. In addition, the smart grid communications network generally comprises thousands of communication nodes, several communication routers, and communication and authentication servers. Hence, it is quite difficult to model and characterize the dynamic behavior and inter-dependencies between the communication and the power systems. Moreover, the co-simulator tool must also include mechanisms to detect inaccurate behavior of the cyber-physical system. Outlined below are the challenges associated with modeling the detection of malicious behavior and the incorrect operation in a cyber-physical system such as the smart grid:

(1) Existing simulators address different scenarios of either the communication system or the power system, but not both system simultaneously taken together as a cyber-physical system.
(2) It is hard to extend the functionality of the existing simulators as most of them either do not support such an interface or are not scalable.
(3) Existing simulation tools are not capable to detect misbehavior of the cyber-physical systems and their impacts.

1.3 Objective and Contributions

Our main objective in this work is to develop a fast real-time simulator for the cyber-physical smart grid that can provide:

(a) A cyber-aware state estimator considering system-level communication.
(b) Security assessment of steady-state cyber-attack impact.
(c) Overall system simulation for cyber-security assessment.

We develop a "Cyber-Physical Security Assessment (CPSA)" co-simulator that performs real-time simulation. The approaches used in the co-simulator are able to detect the misbehavior and anomalies in the cyber-physical electric power system. This simulation tool can be utilized by operators at the control center for CPSA-related decision-making. We also develop a predictive global state estimator at the system level that enables very fast modeling and simulation at timescales relevant to modern and emerging power systems. The co-simulator tool provides system level simulation to understand the impact of cyber-attack on the power system.

1.4 Paper Organization

The rest of the paper is organized as follows. Section 2 presents the existing relevant literature on co-simulation and cyber-attacks' impact. Section 3 presents the proposed system architecture along with functional requirements and various modules of the proposed co-simulator. Section 4 describes the overall design and implementation strategy with suitable technological platform to implement the co-simulator. Thereafter, Section 5 discusses various applications of the developed co-simulator in the smart grid. Finally, Section 6 presents the conclusion of this work.

2 RELATED WORK

This section presents literature work related to the co-simulator and cyber-attack analysis.

The area of smart grid cyber-physical co-simulators and testbeds have not been fully explored. In this direction, Davis et al. [8] presented a survey of cyber ranges and categorize these ranges as: (i) modeling and simulation, where models of each component exist, (ii) ad-hoc or overlay where tests are run on production network hardware with some level of test isolation provided by a software overlay, and (iii) emulation, which maps a desired experimental network topology and software configuration onto a physical infrastructure. Gluhak et al. [5] provided a survey on testbeds for experimental Internet-of-Things (IoT) research. These testbeds have a different scope than what is presented in [8] in the sense that they focus on specific networking technologies, such as wireless sensor networks. Leblanc et al. [10] provided a snapshot of different tools and testbeds for simulating and modeling cyber-attacks as well as defensive responses to those.

Researchers have also identified different categories of attacks as well as their defense strategies. In this direction, Chen et al. [3] discussed different categories of attacks: vulnerability, data injection and intentional attacks, and analyzed network robustness. Tran et al. [22] proposed a detection scheme for replay attacks in the smart grid. Yang et al. [24] discussed Address Resolution Protocol (ARP) spoof-based Man-in-the-Middle (MITM) attacks. Wei et al. [23] performed a study on modeling Denial-of-Service (DoS)-resilient communication routing in the smart grid. Liu et al. [13] presented a framework that models a class of cyber-physical switching vulnerabilities. Etigowni et al. [4] presented a cyber-physical access control solution by using information flow analysis based on mathematical models of the physical grid to generate policies enforced through verifiable logic. Sgouras et al. [19] made an attempt to assess the impact of cyber attacks on Advanced Metering Infrastructure (AMI), especially considering DoS and Distributed DoS (DDoS) attacks.

Researchers have developed security models and testbed setups to simulate the behavior of cyber-attacks. In this direction, Hahn et al. [6] introduced a security model to represent privilege states and evaluated viable attack paths. Liu et al. [12] analyzed the impacts of a line outage attack, DoS attack and MITM attack on the

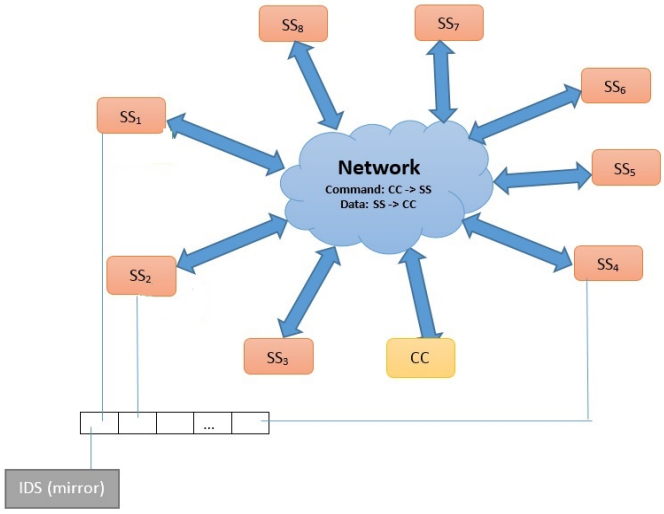

Figure 1: Overview of a cyber-physical power system that consists of eight substations (SS) connected to a control center (CC) over the wireless network and is monitored by a global state estimator.

physical power grid using an integrated cyber-power modeling and simulation testbed. This testbed was developed using devices, NS3, and DeterLab with hardware components. However, the scalability of their software is not discussed and the simulation was performed on the IEEE 14-bus test system.

The above mentioned solutions have limitations, which could be further improved. In [3], [24], [19], [25], [6] and [4], the impact of attacks on the power system was not studied, whereas the scheme in [22] does not consider the source of the cyber-attacks as being from the communication network, rather directly injected into the power system.The simulation work in [23] only included a 3-generator system, which is too small to fully understand the impact of these attacks on real power systems. The communication network is not considered when quantifying the cyber-physical system impact in [13] and [20].

In order to accurately evaluate the current security of the power system, a cyber-physical security assessment of the joint communication and power system is required, rather than simply examining the cyber security concerns in purely the communication network or the impact of physical events on the power system. However, research in this area has not been fully explored. We tackle the issue of monitoring the entire cyber-physical system by using a cyber-physical co-simulator.

3 PROPOSED SYSTEM ARCHITECTURE

In this section, we present the overall system architecture for a novel CPSA co-simulator that overcomes the research challenges mentioned in the "Introduction" section and provides security assessment, attack impact, and situational awareness of the cyber-physical electricity power system.

3.1 CPSA Co-Simulator Functional Requirements

In this section, we present CPSA functional requirements that represent the overall actions performed by the CPSA co-simulator. We summarize these features as follows. The CPSA can:

(1) Detect real-time cyber security situations.
(2) Provide visualization and control capabilities to the operators and EMS administrator.
(3) Detect plausible contingencies that can occur in the system as a result of cyber-attack.
(4) Enhance the security and resilience of the power system by suggesting appropriate CPSA-driven operator actions.
(5) Generate historical logs and a trust metric(s) for different components and identify weak elements, which helps operators to respond quickly when a similar situation occurs at repeated locations.
(6) Apply user-generated rules for what is considered the normal operating range.
(7) Identify and assesses the current health of the cyber-physical system by performing cyber-physical contingency analysis.
(8) Enables hashing/encryption of operator-initiated commands and/or critical measurements.

3.2 CPSA System Module

In this section, we describe various sub-modules of the CPSA system. Figure 1 presents an overview of the considered cyber-physical power system consisting of eight substations connected to a control center over the wireless network. An Intrusion Detection System (IDS) has been mirrored at the connected port of each substation as well as at the control center. The sub-modules of the CPSA system are as follows:

(1) **Data Management Module:** This module stores all the measurement values, legitimate as well as rogue values, received in text files (extracted from the DNP3 packets). It stores rogue values with a flag "up" in order to distinguish them from legitimate data values. This module extracts measurement values from each packet or file, and passes them to the next module, known as the logic module. We assume that this module can use buffer storage available at the control center for storing the packets. We presume that the IDS can provide measurement values to the control center in a csv file using a converter.
(2) **Setup Module:** This module specifies the user defined rules, such as acceptable operational limits. It also provides a component-criticality metric, which clearly defines different components of the cyber-physical system with their severe criticality of loss.
(3) **Logic Module:** The logic modules verifies the boundary limits of each measurement value. If the module identifies bad measurement values, it separates out those values, and sets flag "up" for those values, but still passes those bad values in order to assess their effect on the power system under the bad measurement injection attack scenario to verify how much these values would impact the current state of the system.

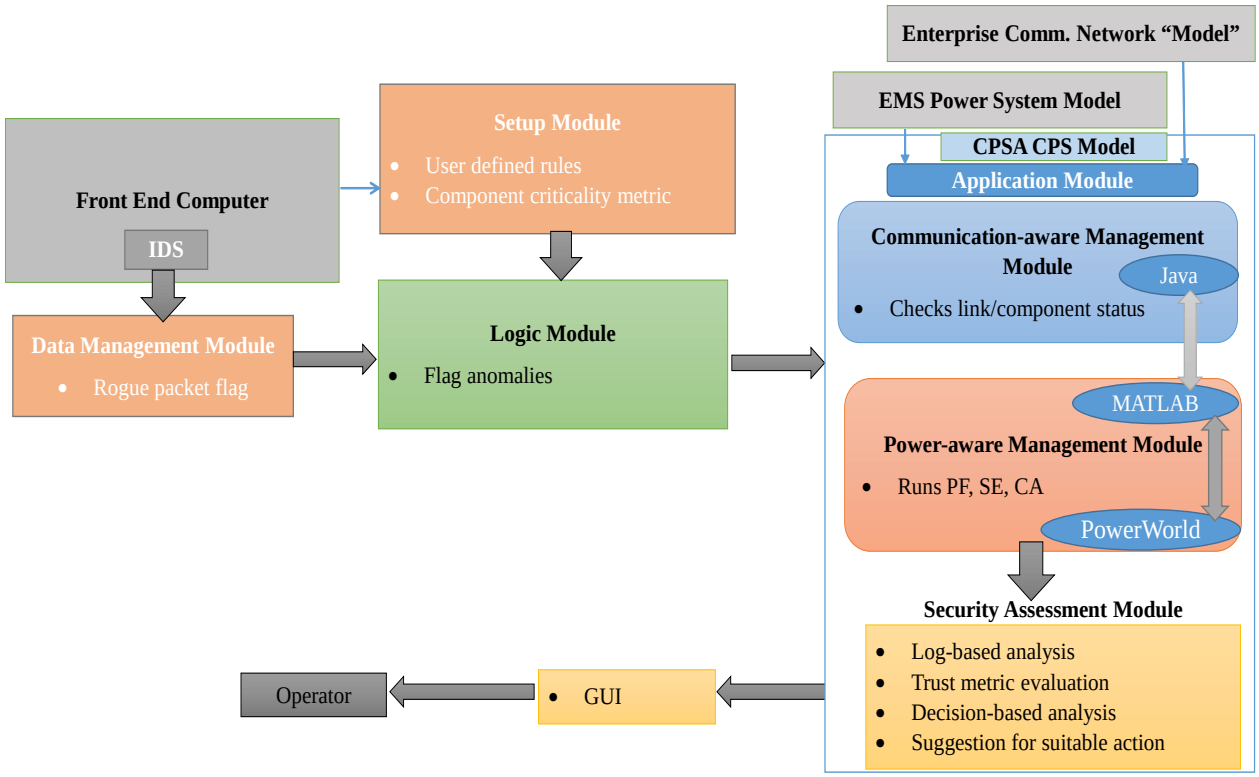

Figure 2: Overall CPSA system module.

(4) **Cyber-Physical System Input Modules:** This module is comprised of the enterprise communication network model as well as the EMS power system model for the existing cyber-physical electricity system.
   (a) **Enterprise Communication Network Model:** It provides input to the co-simulator regarding various communication components. This includes the communication network topology, number of connected devices in the network, baud rate, packet size, Maximum Transmission Unit (MTU) size, and propagation delay over the communication channel.
   (b) **EMS Power System Model:** It provides power system input to the co-simulator, which includes the power system topology, different parameters (with the actual value as well as acceptance ranges) for different components, such as transmission lines, buses, generators, loads, shunts, and transformers, and the configuration of the power system at the time of data acquisition.

(5) **Cyber-Physical System Application Module:** This module is the main functional and application driven module. It runs every few (4-5) minutes to check the current health of the system. All cyber-physical operations of the CPS module will be performed by the application module. This module generates a component trust metric based on the system behavior observed by its sub-modules. Basically, a trust metric reflects the frequency of the cyber-attack attempts on different components of the communication as well as the power system. Based on the analysis and observations of this module, instructions for appropriate actions are forwarded to the security assessment module (discussed in the next subsection) along with the component trust metric. This module consists of two sub-modules:
   (a) **Communication-Aware Management Module:** It is responsible for managing different components of the communication system along with the statistics of cyber-attack impact. Normal operations performed by this module include frequent pings to different communication devices to verify whether they are active and up, maintaining log records of the communications at the control center, RTUs, and intermediate devices, such as routers. We describe this module in detail as follows:
      (i) **Communications between Different Components:** In order to make the simulation real-time, communications between the control center and RTUs through routers are provided, where the sender can send multiple messages with specified MTU size at one time and the receiver responds with an acknowledge for each message along with the action that needs to be performed. The communication system also

includes a propagation delay and the delay at components for computations.

(ii) **Log Records of Communication Components:** The communication system maintains log records at the control center, at all RTUs and at routers. The logs include messages sent and received by the sender and the receiver, enqueue and dequeue timing of each packet at each router along with sender and receiver information, and the route followed by each message from the source.

(iii) **Evaluate System Behavior with Cyber-Attacks Scenarios:** The communication system is simulated in the presence of different cyber-attacks scenarios so that the overall impact and the behavior of the cyber-physical system can be observed. Some of these attacks include man-in-the-middle attack, denial-of-service (disabled) attack, and delay at devices, such as routers and RTUs. Each such attack affects the communication system components and as a results the system behaves differently than in normal operations.

(iv) **Evaluate System Behavior with Future Demands Scenarios:** Based on future forecasts, such as the predicted load profile and generation dispatch (say for example, the next 30 minutes), future states of the cyber-physical system are observed. This enables the co-simulator to run and evaluate system states faster than real-time. After each co-simulator run of 2 minutes for 30 iterations, the system states for the next 30 minutes can be accurately predicted and analyzed.

(b) **Power-Aware Management Module:** This module analyzes the current state of the power system by comparing legitimate and malicious or suspicious measurement values to evaluate their impact on the overall CPS security. It then simulates the what-if scenarios using contingency analysis. It also verifies whether the suspicious measurements should be forwarded to other applications, if the system is still secure. This module contains enhanced versions of three core power system functions typically performed by the EMS: global state estimation, power flow, and contingency analysis.

(i) **Global State Estimation:** The global state estimator uses measurements from all of the RTUs to perform observability analysis. If the entire system or a part of the system is found to be unobservable, then the worst case scenario is assumed for the unobservable portion(s). Thereafter, the measurements (both legitimate as well as malicious) are sent to the global state estimator for the observable part of the system, which assigns different weights to them based on their legitimacy, identifies the most likely state of the system, and then it attempts to detect and identify bad measurements. Finally, the processed measurements are sent on to the power flow function.

(ii) **Power Flow:** The processed measurements from the global state estimator are used to determine the actual state of the system. These results serve as the pre-contingency scenario for the subsequent contingency analysis.

(iii) **Contingency Analysis:** A list of cyber-physical contingencies is generated. Then, several different simulation scenarios are performed to determine the potential impact of each contingency on the power system. The worst contingencies (above a user-defined threshold) are identified and flagged for the power system operator.

(6) **Security Assessment Module:** This module is specifically designed for operators to analyze the CPS system behavior based on the different observations provided by other modules. This module evaluates a trust metric to figure out the critical components of the cyber-physical system, and also performs log-based analysis to verify secure operation. It can investigate if finds unexpected behavior in any communication or power system component. Finally, the operator concludes with decision-based analysis and takes suitable actions in order to maintain the secure and stable operation of the power system.

4 DESIGNING AND IMPLEMENTING THE CPSA CO-SIMULATOR

Simulation is an effective way of working with very large problems that would otherwise require involvement of a large number of active users and resources, which is difficult to coordinate and build in a large-scale research environment for the purpose of investigation. Our CPSA co-simulator implements the power and the communication systems using PowerWorld and Java (with APIs). The interface between the power system and the communication system is governed by MATLAB (Java ⇔ MATLAB ⇔ PowerWorld). There is an active connection for the interface between Java and MATLAB, which further calls MATLAB-PowerWorld interface.

(1) **Connection for the Interface between Java-MATLAB:** We use special Java APIs, such as GridSim, Matlabcontrol, and Java Agent DEvelopment Framework (JADE) for this work. We provide a brief description of these APIs below:

(a) **GridSim:** The GridSim toolkit allows modeling and simulation of entities in parallel and distributed computing systems. It provides a comprehensive facility for creating different classes of heterogeneous resources for solving compute and data intensive applications. The processing nodes within a resource can be heterogeneous in terms of processing capability, configuration, and availability [16].

(b) **Matlabcontrol:** Matlabcontrol is a Java API that enables calling MATLAB from Java [9]. It provides the ability to evaluate a variable (eval), a function (feval),

and allows get and set variables from Java to MATLAB.

(c) **JADE:** JADE is used to provide an interface between the communication network (in Java) and the power system (in PowerWorld) through an interface using MATLAB. JADE is an open source middleware and a Java-based framework that facilitates the creation of agent based simulations by providing basic functionalities, such as agent and behavior classes that can easily be extended [7]. Although many other multi-agent frameworks are available, JADE is the most commonly used for power system applications.

(2) **Connection for the Interface between MATLAB-PowerWorld:**

(a) **MATLAB:** MATLAB is a powerful software that provides a programming environment to perform complex numerical computations and data analysis [14]. We use MATLAB as an interface between Java and PowerWorld.

(b) **PowerWorld:** PowerWorld is a popular simulation tool used to analyze power systems [15]. Using this tool, we can perform power flow analysis on a system with up to 100,000 buses. It also provides an interface to perform other analysis, such as transient stability, optimal power flow, voltage stability, and contingency analysis. We use SimAuto as a COM object to control the simulator from MATLAB and Java.

MATLAB-PowerWorld Interface: Through this interface, PowerWorld can be requested to run instructions such as the following:

(a) Open, save and close a case (network).
(b) List the devices of each type (buses, branches, generators, loads, etc.) present in the case.
(c) Get the parameters (status, MW and MVAR rating, nominal voltage, etc.) of different elements or all elements of a given type.
(d) Change the parameters of an element or all elements of a given type.
(e) Run a power flow using a specific algorithm, such as Newton-Raphson.

JADE-PowerWorld Interface: JADE cannot directly interface with PowerWorld. It must be done through MATLAB. There is no Java documentation available to directly connect Java with PowerWorld as a COM object. A Transmission Control Protocol (TCP) connection is established to enable communication between JADE and MATLAB. A TCP/IP connection enables running all software on a single computer or using a remote computer for running MATLAB and PowerWorld. The connection between MATLAB and PowerWorld is established with a COM object through SimAuto. Single agent in JADE handles all communications with MATLAB using InterfaceAgent. On initialization, a TCP connection is established between InterfaceAgent and MATLAB, and is open throughout the entire simulation duration. JADE agent sends a message with desired action information to InterfaceAgent using the standard Message Transport Protocol (MTP). InterfaceAgent processes the content of the message and sends it to MATLAB through TCP. MATLAB receives the message, processes respective parameters, and requests PowerWorld to run the appropriate instructions. After executing the instructions, PowerWorld returns the result to MATLAB through the COM interface. MATLAB then reprocesses the answer and sends it through TCP back to InterfaceAgent. Finally, InterfaceAgent processes the answer it received and sends the final answer to the agent that issues the initial request [17].

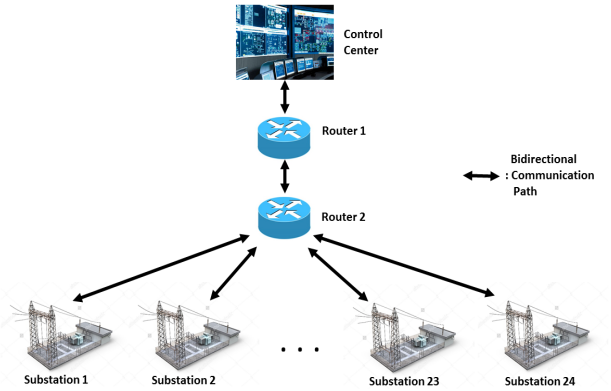

Figure 3: Topology for the communication network.

(3) **The Communication-Aware Management Module:** The communications module is implemented using Java with GridSim. In GridSim, all components communicate with each other using message passing operations defined by SimJava. We adopt a star topology with two intermediate routers for routing information/messages from the control center to the RTUs. The Communications network simulations are modeled on GridSim core elements namely grid resources, such as network links. We can specify the baud rate for the different links between the control centers and the RTUs. Routing tables stored in each router are used to route power system information from the control center to the RTUs and back. Figure 3 shows the topology of the communications network in our system model.

(4) **The Power-Aware Management Module:** This module provides the functionalities for global state estimation, power flow, and contingency analysis.

(a) **Global State Estimation:** Currently the state estimator has been implemented in MATLAB and tested on several small power systems. The purpose of state estimation is to identify the most likely state (bus voltage magnitudes and angles) of the power system using raw measurements coming from RTUs in the field. The formulation of the state estimation problem is as follows:
Let z represent a set of power system measurements. Then,

$$z = h(x) + e,$$

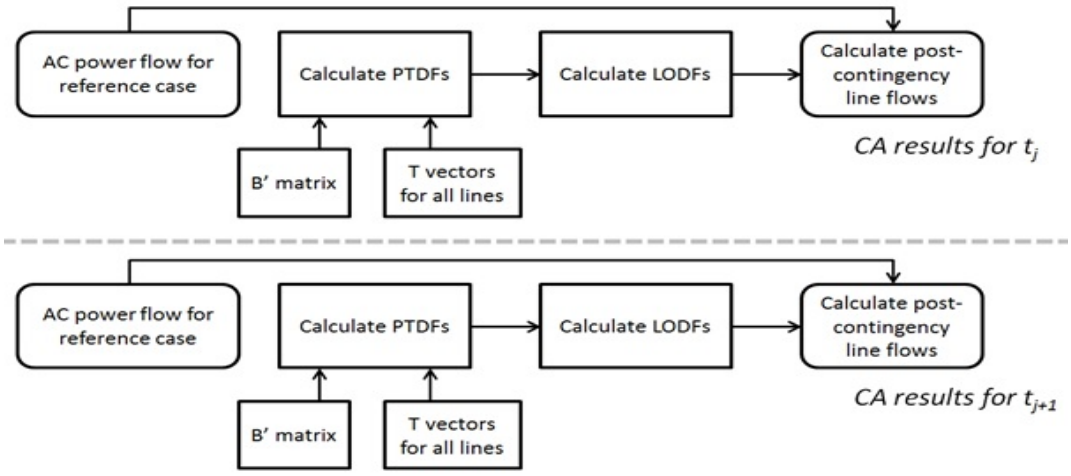

Figure 4: Algorithm flowchart for DC contingency analysis.

where x is the estimated state vector (bus voltages and angles), $h()$ is the vector of functions relating the state variables to the error-free measurements, and e is a vector of Gaussian measurement errors with mean of zero and variance σ^2. The Weighted Least Sqaure (WLS) estimator minimizes the objective function:

$$J(x) = [z - h(x)]^T R^{-1} [z - h(x)].$$

where R is a diagonal matrix of the measurement error variances. To obtain the minimum x, we take the partial derivative of the objective function and obtain

$$g(x^{(k)}) = -H(x^{(k)})^T R^{-1} (z - h(x^k))$$

Here, $x^{(k)}$ is the state vector at iteration k. H is the measurement Jacobian and the partial derivative of h. By applying the Gauss-Newton method [1], we obtain the Normal Equations

$$[G(x^{(k)})] \triangle x^{(k+1)} = -g(x^{(k)}),$$

where the gain matrix G is the derivative of g and is equal to

$$G(x^{(k)}) = H(x^{(k)})^T R^{-1} H(x^{(k)}).$$

Then the state x is solved iteratively until a convergence tolerance is reached.

(b) **Power Flow:** Currently power flow results are obtained through PowerWorld via MATLAB. The purpose of power flow is to determine the system state based on bus injections. These results serve as the base scenario for subsequent contingency analysis.

(c) **Contingency Analysis:** Currently a DC contingency analysis sub-module has been implemented in MATLAB and tested on several small power systems for a list of automatically generated physical contingencies. The purpose of contingency analysis is to evaluate the impact of possible physical contingencies on the power system in terms of line thermal overload. See Figure 4 for the flowchart of the DC contingency analysis algorithm, where AC, DC, PTDF, LODF and CA are acronyms for alternating current, direct current, power transfer distribution factors, line outage distribution factors and contingency analysis, respectively.

The CPSA GUI in Figure 5 presents a scenario of a polling request initialed by the CC. The CC sends the command "Send Measurement Values" to the RTUs with different setting preferences, and the RTUs respond with the current measurement values of various components. Similarly, the CPSA GUI in Figure 6 presents a scenario where the CC sends one or more commands to the respective RTU with different setting preferences, and the respective RTU updates the changes for the respective power system component.

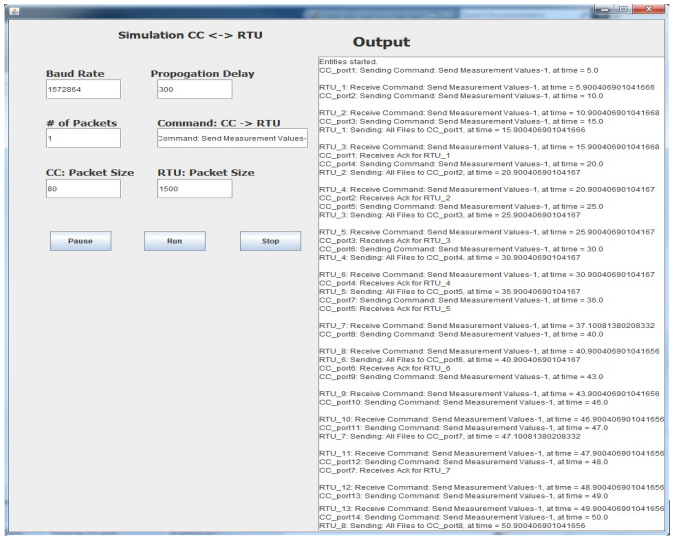

Figure 5: A polling request initialed by the CC and RTUs reply with the current measurement values.

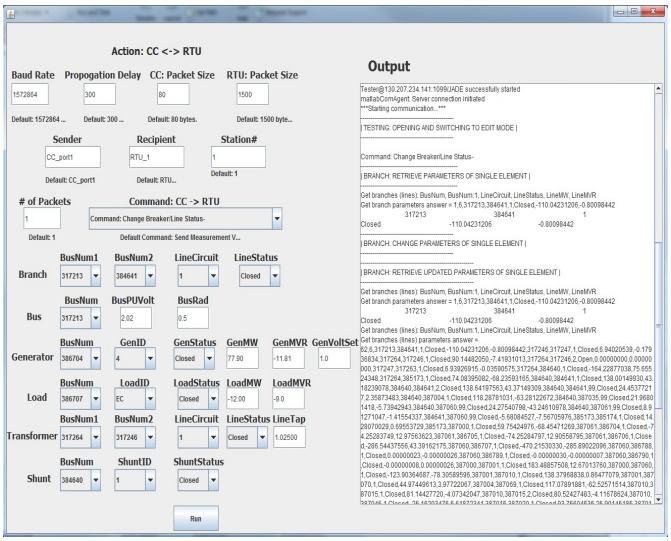

Figure 6: Actions performed by the CC by sending one/more commands to the respective RTU.

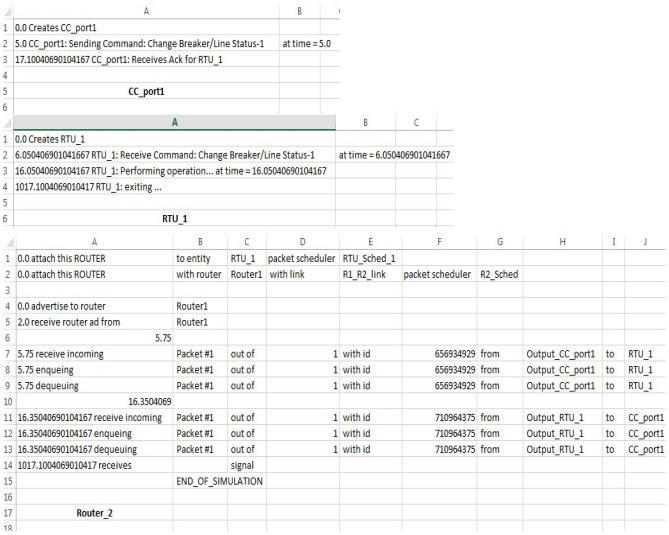

Figure 7: Maintaining log records of the communication network statistics.

Figure 7 presents an overview of the log records for the communication network statistics at the CC, the RTUs, and the routers. Figure 8 presents an overview of the power system measurement values for the co-simulator in a specific format in files received from the RTUs, current state and values of the power system components, and after running power flow and contingency analysis.

5 APPLICATIONS OF THE DEVELOPED CO-SIMULATOR

The co-simulator was made scalable by design. It can handle a small power system case with a few tens of buses to a large system with

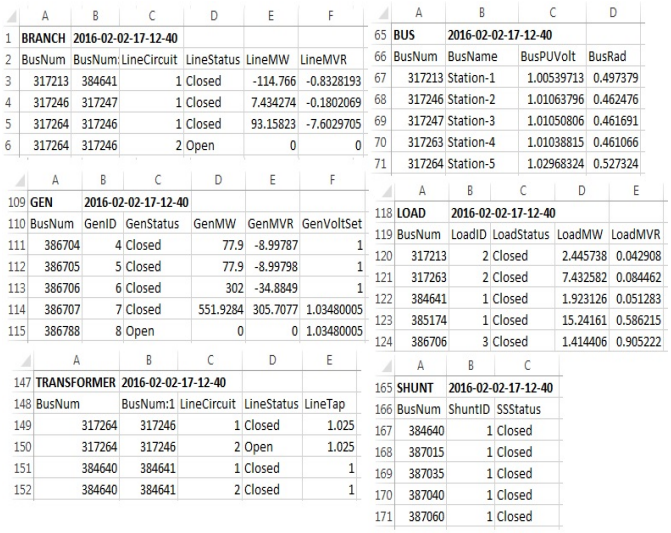

Figure 8: Maintaining power system measurement values in a specific format receiving from the RTUs.

ten thousand buses. The simulator is capable of monitoring the real-time system behavior as well as the impact of cyber-attacks on the power system. In general, this tool is relevant to the following power system applications:

5.1 Power System Monitoring

The developed tool provides the operator with an interface to monitor real-time behavior of the power system. The tool also generates system residuals and Aggregate MW Contingency Overload (AMWCO) matrices in order to evaluate the security and health of the power system. The tool can support dynamic power system topology having power components ranged from several hundreds to a thousand. We consider a 24-substation power system with 42 buses, 62 transmission lines, 8 generators, 27 loads, 6 transformers, and 9 shunt capacitor banks. A visual representation of this case is shown in Figure 9, where the blue dotted lines indicate the communication channels and solid orange lines indicate the power lines.

5.2 Cyber-Attack Impact Evaluation

Recent cyber-attacks targeting power systems around the world have increased the concern over the security of the grid as well as the privacy of the information (data and commands) transmitted over the grid's communication network. Currently, an operator at the control center can monitor power system statistics and line outages of different substations. However, the operator has no knowledge of the security of the communication network. The adversary can perform cyber-attacks over the communication network to alter the transmitted measurement data or the critical command, and in most cases the operator will unable to detect the attacks. Therefore, we need smarter tools and techniques to detect cyber and physical attacks over the communication network as well as on the power system. The tool presented in the paper continuously pings the communication devices deployed in the network and

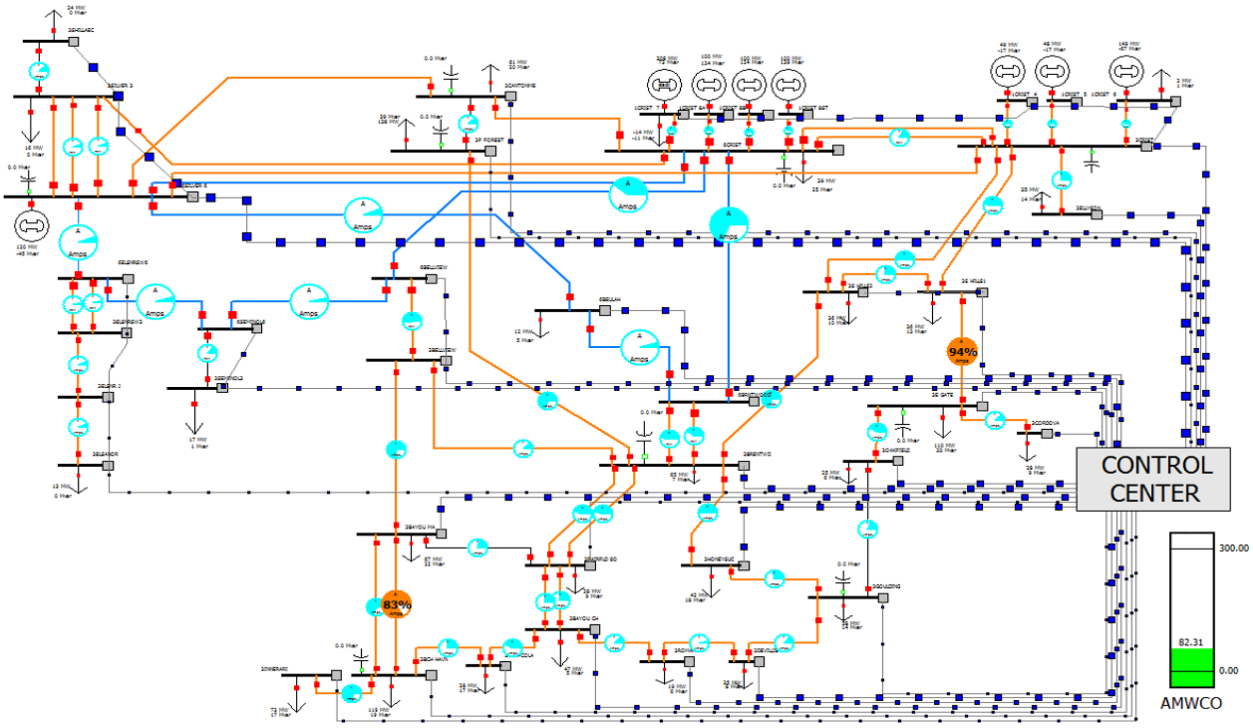

Figure 9: Visual representation of our 42-bus case.

Figure 10: Evaluating power system health under normal operation vs. under attack scenaio.

monitor them by modeling an identical topology in software. The tool is capable of identifying the situations under attacks, and is also able to understand the worst-case impact of cyber-attacks on the power system as shown in Figure 10.

5.3 Detecting and Ensuring Measurement Data Under Limit

During data acquisition, the control center sends a poll request to the substation RTU. As a response, the RTU transmits its measurement data in a series of DNP3 packets to the control center. An adversary located between the substation RTU and the control center can compromise the transmitted information of the packets, a scenario of which is presented in Figure 11 where the measurements of a specific bus (with attached generators and loads) are altered under an attack. As a result, the power system may become insecure. In a real world scenario, the utilities either protect their communication networks using Virtual Private Network (VPN) or simply do not include any protection due to the large deployment cost. Even in the presence of a VPN network, the adversary can modify the measurement values or the commands just before the starting points of the VPN at the substation. The developed tool can be easily extended and used to simulate a secure scheme applied to the data transmitted over the insecure network.

5.4 Detecting and Ensuring Transmission of Accurate and Authentic Command Delivery

The operator at the control center is responsible for making decisions based on the operating conditions of the power system. The operator sends control commands to different power components at the substation as part of its routine and emergency operations. An adversary can affect the power system dynamics by modifying the malicious yet valid commands over an insecure network. If the

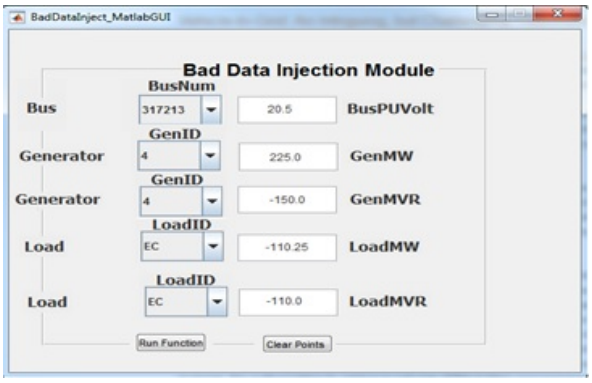

Figure 11: Bad measurement attack scenaio.

adversary has access to the control center, it can also send a malicious command to execute an inappropriate action in the present scenario to the substation device. These actions can include opening a circuit breaker, shedding load, etc. A scenario of malicious command injection is shown in Figure 12 where the IDS alerts the system about a bad command and the co-simulator simulates the command before executing on the real power system. A scheme supporting accurate and authentic command delivery can be simulated and implemented using our tool. A module at the control center generates a fresh command and sends the command to the respective control node with fresh information. A module at the substation RTU is immediately activated after receiving a command from the control center, which could verify whether the received command is legitimate or malicious.

5.5 Detecting a Disabled RTU Attack or Communication Delay at a Substation RTU

Assume one or more RTUs are subject to a DoS attack, under which an attacker delays the communication at each RTU or even blocks the communication entirely between the CC and the RTU. Hence, measurements for one or more substations are unavailable for state estimation. If only one RTU is lost due to a DoS attack, the EMS state estimator may still have global observability using CPSA, since it may have sufficient measurements in other parts of the system to

Figure 12: Bad command attack scenaio.

infer the behavior of the substation under attack. However, there are cases where a disabled RTU will result in loss of observability for some system states. Also, if several substation RTUs are under DoS attacks, the state estimator will lose observability into at least a portion of, if not the entire system. In this situation, it is difficult to provide any input to other downstream EMS functions, such as power flow, contingency analysis, and optimal power flow. The operator at the control center can see these effects using the CPSA co-simulator visualizations, as shown in Figure 9. The CPSA is able to detect such an attack and guide operators to take immediate action in order to mitigate the impact of such an attack on the power system.

5.6 A Training Resource for Operators

The developed tool is an important and useful resource for training control center staff, especially power system operators. Better training on cyber-physical security will provide them with an enriched experience and improve their understanding of the power system's behavior in the presence of potential cyber-attacks. It will also enable the operator to further develop their decision making skills.

6 CONCLUSION

In this paper, we presented and described a novel integrated cyber-physical security co-simulator, CPSA, which can assess the impact of the cyber-attacks on the power system. We proposed a system architecture covering the functional requirements and system modules of the developed co-simulator, and described the dependencies and implementation of the co-simulator using Java, MATLAB and PowerWorld. The developed co-simulator supports the transmission of measurement data through polling request and response, triggering a control command to a power component deployed at a substation, and updating power system values: voltage, active power, reactive power, and angle. At the end, we also described various power system security applications that can utilize the developed co-simulator.

REFERENCES

[1] Abur, A., Ed. *Power System State Estimation: Theory and Implementation.* CRC Press, Boca Raton, Florida, USA, 2004.
[2] Comprehensive analysis report on ukraine power system attacks, 2016. http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-powersystem-attacks.
[3] Chen, P.-Y., Cheng, S.-M., and Chen, K.-C. Smart attacks in smart grid communication networks. *IEEE Communications Magazine 63*, 1 (2014), 3–18.
[4] Etigowni, S., Tian, D. J., Hernandez, G., Zonouz, S., and Butler, K. Cpac: Securing critical infrastructure with cyber-physical access control. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (Los Angeles, California, USA, 2016), ACSA, pp. 139–152.
[5] Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., and Razafindralambo, T. A survey on facilities for experimental internet of things research. *IEEE Communications Magazine 49*, 11 (2011), 58–67.
[6] Hahn, A., and Govindarasu, M. Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid 2*, 4 (2011), 835–843.
[7] Java agent development framework, 2015. http://jade.tilab.com/.
[8] A survey of cyber ranges and testbeds, tech. rep, dtic document, 2013. http://www.dtic.mil/docs/citations/ADA594524.
[9] matlabcontrol: Walkthrough, 2015. https://github.com/jakaplan/matlabcontrol/wiki/Walkthrough.
[10] Leblanc, S. P., Partington, A., Chapman, I., and Bernier, M. An overview of cyber attack and computer network operations simulation. In *Proceedings of the Military Modeling & Simulation Symposium (MMS)* (Boston, Massachusetts, USA, 2011), SCSI, pp. 92–100.

[11] Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., and Mili, L. Power system and communication network co-simulation for smart grid applications. In *Proceedings of the Innovative Smart Grid Technologies (ISGT)* (Anaheim, CA, USA, 2011), IEEE, pp. 1–6.

[12] Liu, R., Vellaithura, C., Biswas, S. S., Gamage, T. T., and Srivastava, A. K. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Transactions on Smart Grid 6*, 5 (2015), 2444–2453.

[13] Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., and Butler-Purry, K. A framework for modeling cyber-physical switching attacks in smart grid. *IEEE Transactions on Emerging Topics in Computing 1*, 2 (2014), 273–285.

[14] System requirements for matlab r2017a, 2017. https://www.mathworks.com/support/sysreq.html.

[15] The visual approach to electric power systems, 2016. https://www.powerworld.com/.

[16] Gridsim: A grid simulation toolkit for resource modelling and application scheduling for parallel and distributed computing, 2010. http://www.buyya.com/gridsim/.

[17] Agent-based architectures and algorithms for energy management in smart grids, 2012. PhD Thesis, University of Technology of Belfort-Montbliard.

[18] Roche, R., Natarajan, S., Bhattacharyya, A., and Suryanarayanan, S. A framework for co-simulation of ai tools with power systems analysis software. In *Proceedings of the International Workshop on Database and Expert Systems Applications (DEXA)* (Vienna, Austria, 2010), IEEE, pp. 350–354.

[19] Sgouras, K. I., Birda, A. D., and Labridis, D. P. Cyber attack impact on critical smart grid infrastructures. In *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference (ISGT)* (Washington, USA, 2014), IEEE, pp. 1–5.

[20] Srikantha, P., and Kundur, D. Denial of service attacks and mitigation for stability in cyber-enabled power grid. In *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference* (Washington, USA, 2015), IEEE, pp. 1–5.

[21] Ten, C.-W., Manimaran, G., and Liu, C.-C. Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 40*, 4 (2010), 853–865.

[22] Tran, T.-T., Shin, O.-S., and Lee, J.-H. Detection of replay attacks in smart grid systems. In *Proceedings of the International Conference on Computing, Management and Telecommunications* (Ho Chi Minh, Vietnam, 2013), IEEE, pp. 298–302.

[23] Wei, J., and Kundur, D. A flocking-based model for dos-resilient communication routing in smart grid. In *Proceedings of the International Conference Globecom* (California, USA, 2012), IEEE, pp. 3519–3524.

[24] Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Im, E. G., Yao, Z. Q., Pranggono, B., and Wang, H. F. Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems. In *Proceedings of the International Conference on Sustainable Power Generation and Supply (SUPERGEN)* (Hangzhou, China, 2012), IEEE, pp. 1–8.

[25] Yi, P., Zhu, T., Zhang, Q., Wu, Y., and Li, J. A denial of service attack in advanced metering infrastructure network. In *Proceedings of the IEEE ICC* (Sydney, Australia, 2014), IEEE, pp. 1029–1034.