# An Integrated Control and Intrusion Detection System for Smart Grid Security

Eniye Tebekaemi, Duminda Wijesekera, Paulo Costa

Chapter 13

# AN INTEGRATED CONTROL AND INTRUSION DETECTION SYSTEM FOR SMART GRID SECURITY

Eniye Tebekaemi, Duminda Wijesekera and Paulo Costa

**Abstract** Several control architectures have been proposed for smart grids based on centralized, decentralized or hybrid models. This chapter describes the Secure Overlay Communications and Control Model, a peer-to-peer, decentralized control and communications model with its own communications protocols and intrusion detection mechanisms that integrate a physical power system and its communications and control systems. This chapter also demonstrates how the model can help mitigate cyber attacks on a power system.

**Keywords:** Smart grid, communications, control, security, intrusion detection

## 1. Introduction

A networked control system uses a feedback control loop that requires control and feedback signals to be exchanged between its components over a communications network. The feedback signals contain periodic sensor measurements of the system that may vary during each iteration. The central controllers use the signals to estimate the current state of the system and, when necessary, the controllers send signals to actuators to adjust the behavior of the system. Traditionally, the communications network of a control system has been isolated from the Internet, with all the components (sensors, actuators and controllers) residing in the same physical location. However, the components of a smart grid are not co-located and the communications network is not isolated, making the resulting cyber-physical system highly vulnerable to cyber and physical attacks.

A modern power grid is centrally managed using the communications and control architecture shown in Figure 1. The central controller obtains telemetry data from all the locations and attempts to estimate the current state of the distributed system. The control and automation functions make control decisions

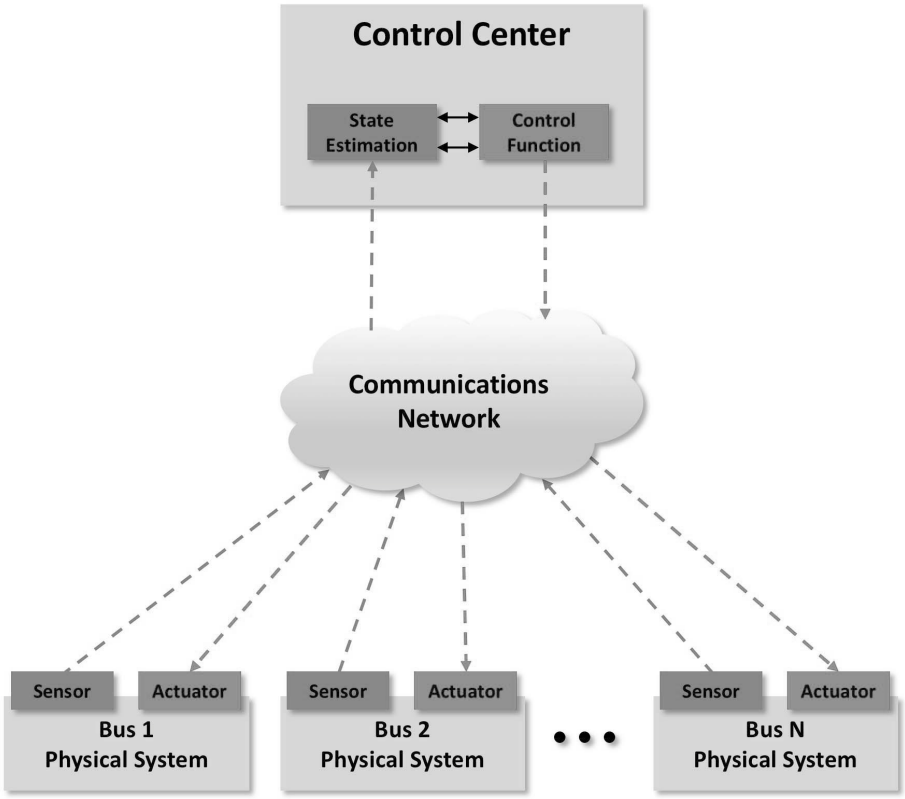



*Figure 1.* Cyber-physical system.

based on the estimated system state. Grid components use remote terminal units to send telemetry data and receive control commands from the central controller housed in a supervisory control and data acquisition (SCADA) system. The remote terminal units may be equipped with cryptographic tools and intrusion detection systems that validate messages purportedly sent by the central controller.

## 1.1 State Estimation

The objective of state estimation is to compute (with sufficient accuracy) the operational state of the power grid from measurements (bus voltage magnitudes and angles, branch currents and branch real and reactive power values) taken by sensors and communicated over the distributed communications network. The state estimator, which is an important component of the control center, computes the system state from sensor measurements. The relationship between the measurements and the system state is given by:

$$z = h(s) + e \tag{1}$$

where $z = (z_i, z_2, \cdots, z_k)$ is the measurement data vector; $s = (s_1, s_2, \cdots, s_n)$ is the true state vector; $e$ is the measurement error (usually white Gaussian noise); and $h$ is a non-linear scalar function that relates the measured data $z$ to the state variables in $s$. The equation is typically solved using the weighted least squares method as described in [12] to obtain the estimated state vector $\hat{s}$.

## 1.2 Control Function

The objective of power system control functions is to constrain system behavior (by controlling power regulation transformers, capacitor banks, circuit breakers, etc.) to meet objectives such as optimal power flow, voltage regulation, power quality and/or economic dispatch. In the case of a smart grid, the objective functions are automation functions such as self-healing and restoration [8, 9, 22, 26], dynamic volt/var optimization [1, 25, 27] and priority load management [2–4, 18], among others. The control functions rely primarily on the state estimator to obtain the current state of the power system in order to determine the optimal control vector that constrains the behavior of the power system.

## 1.3 Communications

Two communications protocols – distributed network protocol (DNP3) [6] and IEC Power Utility Automation Standard (IEC 61850) [7] – are predominantly used in power systems communications and control. DNP3 is a centralized master/slave protocol used by most SCADA systems to control field devices at remote locations. Each location is polled by the master (SCADA central controller) and the information obtained is used to make control decisions that are enforced by actuators at remote locations. IEC 61850 is a layered standard that defines three protocols: (i) manufacturing messaging service (MMS) protocol; (ii) generic object-oriented substation event (GOOSE) protocol; and (iii) sampled value (SV) protocol. Manufacturing messaging service is a centralized connection-oriented client/server protocol used by a central controller to control lower-level devices in SCADA-based substations. GOOSE and sampled value are multicast subscriber/publisher protocols used to interact with and control field devices such as sensors and circuit breakers. The GOOSE and sampled value protocols are inherently insecure and used only for communications that originate and terminate in the same physical location.

## 1.4 False Data Injection Attacks

The smart grid attacks considered in this work fall broadly in the false data injection attack category. False data injection attacks seek to corrupt system state estimation by injecting false data in the messages sent from sensors in

remote locations to the central controller or directly controlling actuators by injecting false commands from the control controller to actuators in remote locations.

The architecture in Figure 1 has the following attack entry points:

- **Communications Channel:** An attacker with access to the network communications channel may be able to observe and inject data into the communications stream between the central controller and buses. An attacker located at the control center side could gain global visibility of the network and attack any remote bus.

- **Remote Bus:** An attacker with physical access to remote bus sensors could physically alter the sensors to produce incorrect measurements that result in erroneous system states computed by the state estimator [23].

- **Control Center:** The control center houses the management network that is connected to the Internet. This makes the control center vulnerable to traditional cyber attacks that could be leveraged to gain access to the power grid communications network and perform false data injection attacks. The 2015 attack on the Ukrainian power grid [11] exemplifies the use of a traditional cyber attack on a centrally-managed power system followed by false data injection attacks.

## 1.5 Research Objective

Cyber security controls for computer networks seek to meet some or all of the traditional goals of confidentiality, integrity and availability. While confidentiality retains its original meaning, the concepts of integrity and availability are defined a little differently for the smart grid. In this context, integrity means that the data does not violate the operational constraints of the physical system and availability means that the physical system operates predictably and reliably in an optimal manner even when data is compromised.

Integrity and availability together define the resilience of a cyber-physical system. The most important cyber security objective for the smart grid is resilience. This is because it is impossible to provide absolute guarantees about defeating all cyber attack activity. Therefore, the resilience goal is to ensure that the smart grid operates reliably and predictably under cyber attacks, even when portions of the grid are already compromised.

This work focuses on mitigating cyber attacks using a resilient communications and control architecture. Specifically, it employs the Secure Overlay Communications and Control Model (SOCOM), a novel peer-to-peer, decentralized control and communications model with its own communications protocols and intrusion detection mechanisms that integrate a physical power system and its communications and control systems. A power grid intrusion detection system (SOCOM-IDS) is designed specifically for SOCOM. SOCOM-IDS integrates the coupling characteristics of the smart grid – physical system properties, au-

tomation/control function behavioral properties and communications network properties.

## 2. Related Work

Three aspects should be considered when designing intrusion detection and prevention systems for decentralized cyber-physical systems such as the smart grid: (i) data integrity; (ii) state integrity; and (iii) process integrity. Data integrity, which ensures that data has not been tampered with when it transits from node to node; is usually enforced using cryptographic solutions. The global system state is estimated using data obtained from various points (buses) in the system, and it is imperative that the integrity of system state estimation is maintained for the automation functions to work correctly. Each automation function makes a control decision based on its perception of the global system state relative to the local states and is governed by a process. The process involves a series of actions and interactions between the physical system, nodes (controllers and intelligent electronic devices) and the communications network required to implement the automation function. Most research in this area focuses on one or two of these three aspects.

Yang et al. [24] have designed an encryption-based system that detects false data injection in smart grids during data aggregation (state estimation). Hong and Lin [5] have presented a collaborative intrusion detection system that detects false data injection in sampled values and GOOSE messages based on the semantic anomalies in the sampled value and GOOSE packet header information. Li et al. [10] have designed a rule-based collaborative false data detection method, where the nodes share and compare measured data collected from sensors. Talha and Ray [19] have proposed a framework for MAC-layer wireless intrusion detection and response for smart grid applications; in their system, nodes collaboratively detect flooding attacks at the MAC layer that may result in denial of service and switch the wireless transmission channel as a countermeasure. Zhang et al. [28] have proposed a distributed intrusion detection system that engages intelligent multilayer analysis modules positioned at each network level of the grid to detect and classify malicious data and possible cyber attacks.

Lin et al. [13] have proposed a method for detecting and mitigating control-related attacks on power grids using runtime semantic security analysis of control messages sent over the communications network. Mashima et al. [14] have designed a concrete command mediation scheme called autonomous command-delaying to enhance grid resilience. They introduce artificial delays between intelligent electronic devices and the control center to provide the control center with a time buffer to detect attacks and subsequently cancel malicious commands. Sakis Meliopoulos et al. [17] have developed a cyber-physical co-model for detecting data and control-related attacks. They created a distributed dynamic state estimator that decentralizes the state estimation process, thereby reducing the cyber attack points and the processing overhead at the control center.

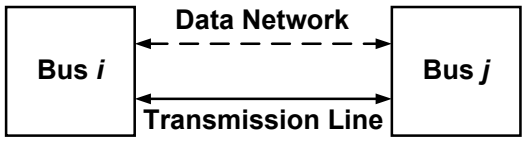



*Figure 2.* Double coupling property.

## 3. Proposed Model

A smart grid incorporates automation functions that coordinate the widely distributed components of the grid to ensure reliable, efficient and safe delivery of power. Attacks on the smart grid target the correct operation of automation functions by: (i) corrupting data exchanged over the communications network; and/or (ii) attacking physical equipment so that it is unable to operate correctly. The objective of SOCOM-IDS is to detect and mitigate the cyber and physical attacks on automation functions and their corresponding processes. In order for SOCOM-IDS to adequately protect the automation functions that control physical power distribution, it has to understand the physical distribution system, control system and network system behavior that define the automation/control process.

The power grid communications/control architecture discussed in Section 1 has an obvious flaw – an attacker can maximize the attack impact by focusing on the control center; if the control center, is compromised then the whole system may be compromised. To address this flaw, several architectures have been proposed that employ a decentralized communications/control model or a hybrid centralized-decentralized model. These new architectures often fall short for the following reasons:

- They focus mainly on control and rely on an existing centralized communications model.
- They do not incorporate cyber security as a major factor in their models and designs.
- They rely on high-level decentralized communications protocols (e.g., JADE [21]) that cannot be readily implemented on low-level field devices.

### 3.1 SOCOM Overview

The physical power system is inherently decentralized. Power transmission lines provide point-to-point connections between the distributed components and power flows only between directly connected terminals. SOCOM has been designed to mirror the natural behavior of power systems.

Consider the configuration in Figure 2 where buses $i$ and $j$ are also directly connected by a power transmission line modeled as:

$$\begin{bmatrix} V_{i,j} \\ I_{i,j} \end{bmatrix} = \begin{bmatrix} A_{j,i} & B_{j,i} \\ C_{j,i} & D_{j,i} \end{bmatrix} \begin{bmatrix} V_{j,i} \\ I_{j,i} \end{bmatrix} \tag{2}$$

where the matrix $\begin{bmatrix} A_{j,i} & B_{j,i} \\ C_{j,i} & D_{j,i} \end{bmatrix}$ is the characteristic impedance or power transfer characteristics of the transmission line; $A = V_S/V_R$ is the voltage ratio; $B = V_S/I_R$ is the short circuit resistance; $C = I_S/V_R$ is the open circuit conductance; and $D = I_S/I_R$ is the current ratio. Buses $i$ and $j$ are directly connected by a data network and exchange state information.

Consider two neighboring buses $i$ and $j$ where $x_{i,j} = \begin{bmatrix} A_{i,j} & B_{i,j} \\ C_{i,j} & D_{i,j} \end{bmatrix}$ denotes the power transfer characteristics from bus $i$ to bus $j$; $s_{i,j} = \begin{bmatrix} V_{i,j} \\ I_{i,j} \end{bmatrix}$ is the state of the line $\{i, j\}$ at bus $i$; $Z^*_{RVI_{i,j}} = x_{i,j} \cdot Z_{LVI_{i,j}} = x_{i,j} \cdot (h(s_{i,j}) + e_i)$ is the line state measurement of bus $j$ estimated at bus $i$; and $Z_{RVI_{i,j}} = Z_{LVI_{j,i}} = h(s_{j,i}) + e_j$ is the line state measurement sent over the network from bus $j$ to bus $i$.
Under normal operating conditions:

$$\begin{aligned} Z^*_{RVI_{i,j}} &\stackrel{?}{=} Z_{RVI_{i,j}} \\ x_{i,j} \cdot h(s_{i,j}) - h(s_{j,i}) &= e_j - x_{i,j} \cdot e_i \end{aligned} \tag{3}$$

where $e_j - x_{i,j} \cdot e_i$ is the estimation error. Therefore:

$$|e_j - x_{i,j} \cdot e_i| = |Z^*_{RVI_{i,j}} - Z_{RVI_{i,j}}| < \zeta \tag{4}$$

where $\zeta$ is the error detection threshold or estimation error threshold.

SOCOM uses the characteristic impedance of power transmission lines to model the physical power grid system as a sparse matrix of pairs of directly connected nodes. Each node holds a subset of the system state information matrix that is used to estimate the system state and make control decisions.

**SOCOM Architecture.** Decentralized autonomous functions for smart grid can benefit from using decentralized communication protocols. However, a major challenge is the reluctance of utility providers to make the necessary investments because they already have older but functional technology. SOCOM runs as middleware on the existing TCP/IP communications infrastructure employed by utilities. This creates a logically decentralized network for the efficient operation of decentralized automation functions.

SOCOM offers the following advantages:

- **Administration:** Engineers are reluctant to cede control of power systems to autonomous intelligent electronic devices (IEDs). Because the SOCOM overlay model is only logical, utility managers can still have direct access to the underlying communications network and retain the ability to observe and intercede in administering the power system.

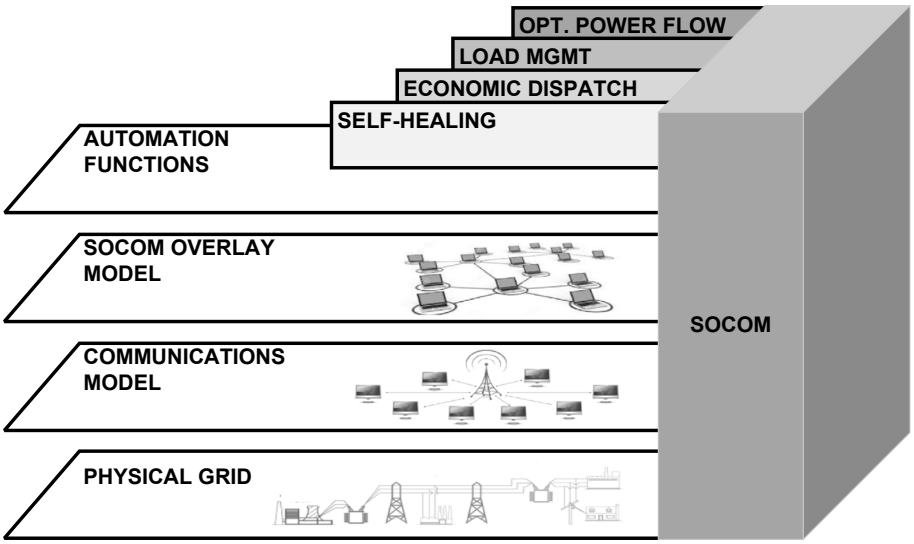



*Figure 3.* SOCOM architecture.

- **Cost:** No structural modifications to the existing communications infrastructure are required. The overlay middleware is implemented between the automation functions and physical communications network as shown in Figure 3.

- **Portability:** The overlay model executes in the network, Internet, transport or application layers of the TCP/IP network. The implementation would, of course, depend on user objectives and requirements.

- **Ease of Use:** Automation functions are oblivious to the physical communications layer and vice versa. Consequently, regardless of the communications protocols, automation functions can be adapted to run on the overlay model.

- **Implementation:** The overlay is lightweight and suitable for direct hardware implementation on field electronic devices and field programmable gate array (FPGA) based controllers.

**SOCOM Protocol.** The SOCOM protocol is a lightweight asynchronous messaging platform designed for decentralized automation and control in cyber-physical systems [20]. The SOCOM protocol (Figure 4) executes as middleware (overlay network) between the smart grid automation functions and the physical communications network as shown in Figure 3. The overlay network layer is structured to mirror the physical system layer (bus network), where each node

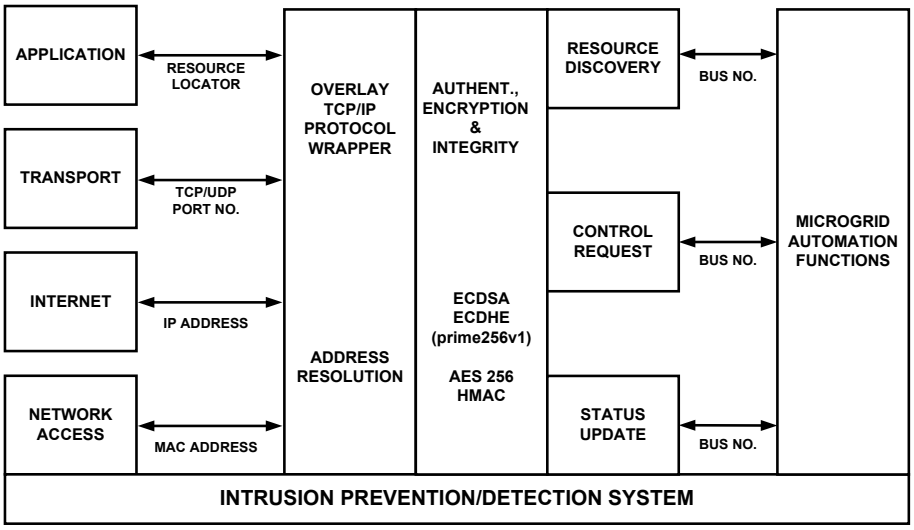



*Figure 4.* SOCOM protocol.

represents a local (bus) controller that can communicate only with its physically connected peers.

SOCOM uses three major protocols: (i) resource discovery protocol; (ii) control request protocol; and (iii) status update protocol. SOCOM has a security layer that provides communications confidentiality, integrity and authentication if needed, and a TCP/IP wrapper for address resolution. Using these protocols, local controllers in the smart grid can locate resources, update their status and initiate control operations in response to optimization objectives in a secure and logically decentralized manner.

The SOCOM protocols have various features:

- **Resource Discovery Protocol (RDP):** This gossip-like protocol is used to locate resources in the smart grid. A resource may be an energy source, storage component, electric load or any other device that may provide, transform or consume energy in the smart grid.
- **Control Request Protocol (CRP):** This request/response protocol remotely executes control actions on resources that are directly connected to peer buses. For example, a bus controller can request a peer bus controller to connect or disconnect a power line to alter the flow of power, possibly in response to a disturbance in order to recover from line faults.
- **Status Update Protocol (SUP):** This point-to-point protocol sends and receives bus information to and from directly connected buses. Each bus sends bus status messages at set time intervals or immediately when specific bus information changes.

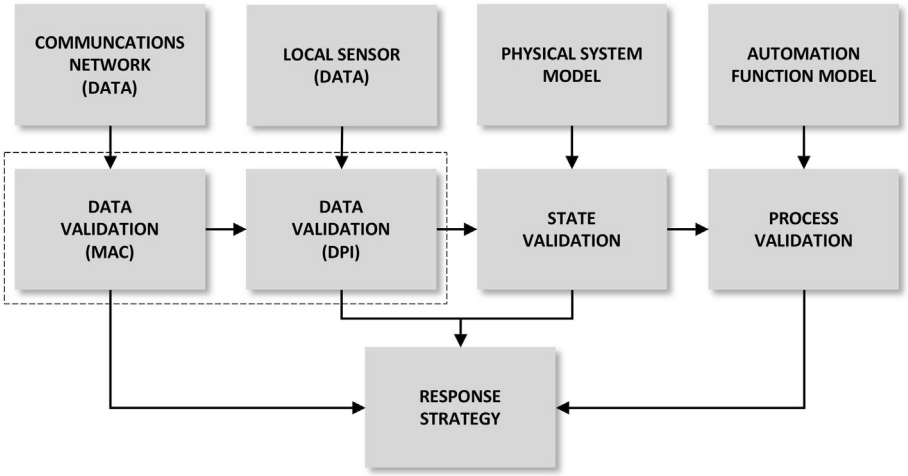



*Figure 5.* SOCOM-IDS model.

## 3.2 SOCOM-IDS Model

The SOCOM-IDS model employs a modular strategy for attack detection and response in a microgrid (i.e., part of a smart grid). It incorporates three detection modules, each of which is compartmentalized to run independently of the other modules. Figure 5 shows the structural layout of SOCOM-IDS.

**Data Validation Module.** The goal of the data validation module is to detect false data injection attacks on the nodes in a microgrid. The module has two components. The first component, data validation (MAC), uses cryptographic controls to validate network data received from neighboring nodes. Each bus controller has a hard-coded (permanent) private/public key pair that initiates the ephemeral elliptic curve Diffie-Hellman (ECDHE) key exchange process with other peer bus controllers to generate session keys. After the session keys are generated, a symmetric algorithm (AES) is used for encryption and the keyed hash message authentication code (HMAC) is used to ensure message integrity.

The second component, data validation (DPI), uses deep packet inspection to check for voltage and current values that exceed predetermined values. The detection problem is formulated as a binary decision:

$$\begin{aligned} FALSE &: |Z^*_{RVI_{i,j}} - Z_{RVI_{i,j}}| \leq \zeta \\ TRUE &: |Z^*_{RVI_{i,j}} - Z_{RVI_{i,j}}| > \zeta \end{aligned} \tag{5}$$

where the claim that the data has been modified is verified when the equation evaluates to true. The data validation module estimates the neighbor node bus voltage magnitudes and phase angles, branch currents and direct and reactive power values from local sensor measurements. These values are compared against the neighbor node state measurements obtained over the network. Potential bad data is detected when the variation exceeds the bad data detection threshold.

**State Validation Module.** Each node estimates the state of the microgrid using information obtained from SOCOM messages exchanged with neighboring nodes. The estimated state is evaluated against the constraints and guarding conditions of the modeled physical system. The constraints are obtained from the physical laws that govern electric power systems.

The state validation module is based on three laws of electricity:

- Let $Z_{RVI_i}^{I \leftarrow in} = \left[ Z_{RVI_{i,j}}^{I \rightarrow out} : \{j \in J \subset M_i\} \right]_{J \times 1}$ denote the current measurements from all the neighboring buses from which bus $i$ draws current. Let $Z_{RVI_i}^{I \rightarrow out} = \left[ Z_{RVI_{i,k}}^{I \rightarrow out} : \{k \in K \subset M_i\} \right]_{K \times 1}$ denote the current measurements from all the neighboring buses that draw current from bus $i$. Then, the sum of currents flowing into a node is equal to the sum of currents flowing out:

$$\sum_{j=1}^{J} Z_{RVI_{i,j}}^{I \leftarrow in} \stackrel{?}{=} \sum_{k=1}^{K} Z_{RVI_{i,k}}^{I \rightarrow out} \tag{6}$$

- The voltage $Z_{RVI_{i,j}}^{V}$ and current $Z_{RVI_{i,j}}^{I}$ measurements received from bus $j$ should be equal to the estimated branch power $x_{i,j} \cdot Z_{LVI_{i,j}}^{V} * x_{i,j} \cdot Z_{LVI_{i,j}}^{I}$ measured locally at bus $i$ for line $\{i, j\}$:

$$x_{i,j} \cdot Z_{LVI_{i,j}}^{V} * x_{i,j} \cdot Z_{LVI_{i,j}}^{I} \stackrel{?}{=} Z_{RVI_{i,j}}^{V} * Z_{RVI_{i,j}}^{I} \tag{7}$$

- Let $LD_u$ be the consumer load that is directly connected to bus $u$ and let $GEN_v$ be the power generator that is directly connected to bus $v$. In a closed system, the total power used by the load is equal to the total power drawn from the power source. Each node estimates the total power used by loads in the microgrid and the total power drawn from all the sources using resource discovery protocol message exchanges:

$$\sum_{q=1}^{u} LD_q + \varpi = \sum_{r=1}^{v} GEN_r^{used} \tag{8}$$

where $\sum_{q=1}^{u} LD_q$ is the sum of the bus loads in the grid; $\sum_{r=1}^{v} GEN_r^{used}$ is the total power generated by all the sources in the grid; bus $u$ and bus

$v$ are the load bus and source bus, respectively; and $\varpi$ is the estimated maximum power loss in the grid.

**Process Validation Module.** The process validation module is unique to each automation function. A process is a series of actions and interactions between physical system components, intelligent controllers (or intelligent electronic devices) and communications network devices that are needed to implement an automation function under normal operating conditions. Each automation function has distinct process behavior that is useful in designing security solutions that are tailored to meet its unique requirements.

For example, consider the self-healing automation function described by the state diagram in Figure 6. The goal of the healing function is to ensure that a failed bus $i$ can independently generate a new grid configuration, which restores power to satisfy the following constraints:

- The load on bus $i$, which has to be restored, must be less than the sum of the available capacity of all the available power generation sources in the power grid.
- The bus voltage at bus $i$ after power restoration must not violate the bus voltage constraints.
- The load on transmission lines must not be less than its maximum capacity.
- The switching overhead must be minimized. For example, the least number of number of switchgear device configuration changes should be performed to restore power.

The self-healing automation function is described by the state diagram in Figure 6. The goal of the healing function is to ensure that the failed bus $i$ can independently generate local configuration changes to restore power in a manner that satisfies the constraints listed above. The new configuration, which is generated by the failed bus, is sent to neighboring buses.

The self-healing process has four states: (i) NORMAL; (ii) FAIL; (iii) RECOVER; and (iv) BAD:

- **NORMAL:** During the normal operating state, the bus continuously monitors its voltage state (using local sensors) and the voltage states of its neighboring nodes.
- **FAIL:** Power lines incorporate relays that detect faults and trigger circuit breakers in response to faults. The triggering of these protective relays may result in power failures that affect one or more buses in the microgrid.
- **RECOVER:** If a failure occurs and the self-healing function is enabled, then the affected bus $i$ independently generates a new configuration to control local and neighboring switchgear devices in order to restore power based on the self-healing algorithm.

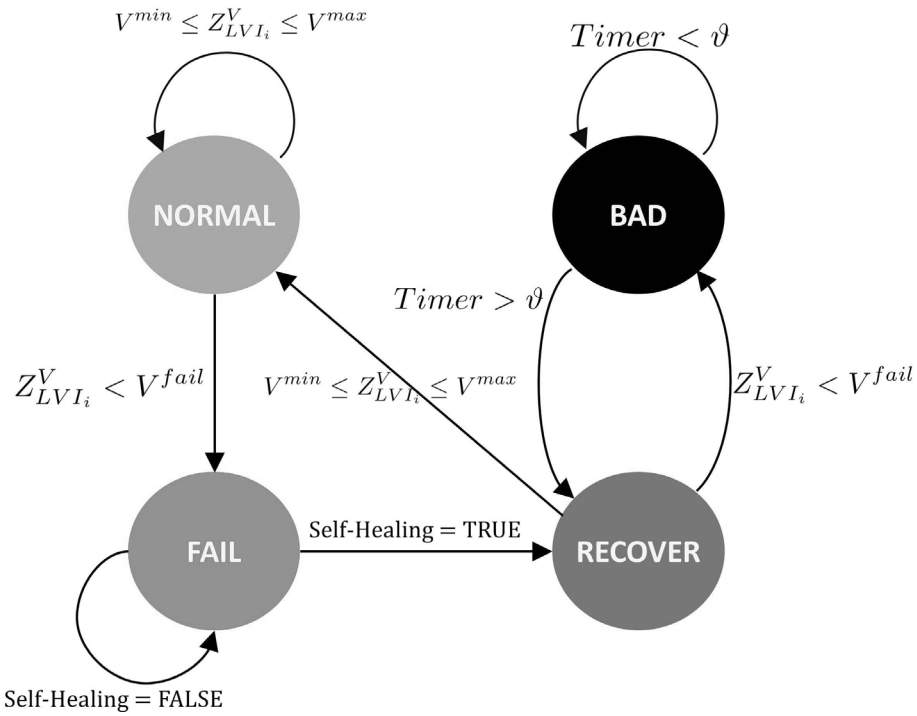



*Figure 6.* Self-healing state diagram.

- **BAD:** The bus enters the bad state when no configuration solution is found that restores power in a manner that satisfies the self-healing function constraints.

The self-healing process follows the following sequence of messages from a failure to service restoration:

$$SUP_{NORMAL} \rightarrow SUP_{FAIL} \rightarrow RDP \rightarrow CRP_{HEAL} \rightarrow SUP_{NORMAL} \quad (9)$$

**Response Strategy.** Upon detecting an intrusion, SOCOM-IDS attempts to stop the attack by performing the following tasks in order:

- **Change the Implementation Layer:** SOCOM can run on the MAC layer, network layer, transport layer (UDP) or application layer. When an intrusion is detected by a node, a change layer message is sent by the detecting node to all its neighboring nodes.

- **Change Cryptographic Keys:** If the intrusion persists, then the node generates new cryptographic keys and initiates a key exchange procedure.

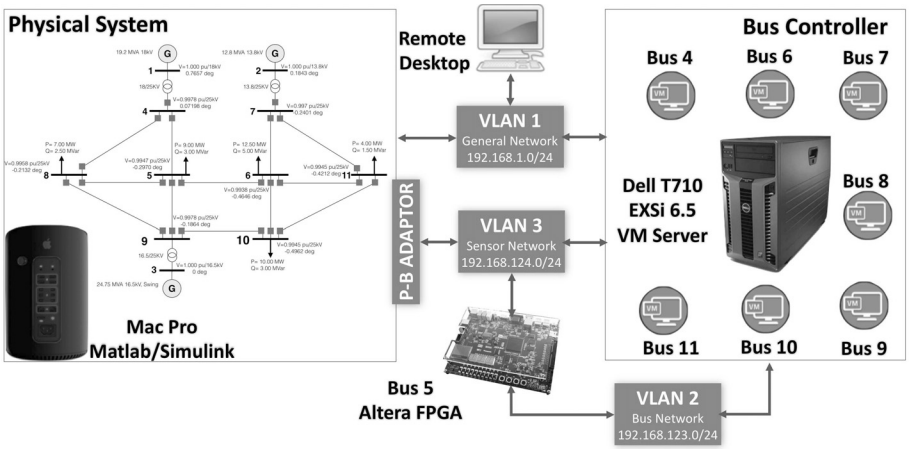



*Figure 7.* Experimental testbed.

- **Discard Communications from Compromised Node(s):** If the intrusion continues to persist, then it is most likely that the originating node may have been compromised. Messages from the compromised node are discarded.

- **Disable Secondary Control Functions:** Discarding network messages may have an adverse effect on secondary control functions. If more than a predetermined number of neighboring nodes are compromised or the secondary control function is unable to run effectively, then the secondary control function is disabled.

## 4. Implementation and Results

Figure 7 shows the experimental testbed. The physical power grid was simulated using Matlab/Simulink, Simscape Power Systems [15] and Simulink Real-Time [16] applications. Simscape Power Systems provided component libraries and analysis tools for modeling and simulating electrical power systems. Simulink Real-Time enabled the creation of real-time applications from Simulink models. The applications supported the implementation and execution of an eleven-bus physical power grid in real-time on a Mac Pro server (3 GHz 8-Core Intel Xeon E5, 64 GB RAM). The physical power grid comprised three power generator sources, three transformers (one for each source), five load buses and current/voltage sensors and switchgear devices.

Eight bus controllers were developed based on the SOCOM communications and control protocol. Seven of the eight buses were implemented as virtual machines and the remaining bus was implemented on an FPGA device. The seven virtual machines ran on a Dell T710 server (2.66 GHz 6-Core x2 Intel Xeon X5650, 64 GB RAM). Each bus controller received sensor measurements and sent control messages to the corresponding physical bus over UDP messages

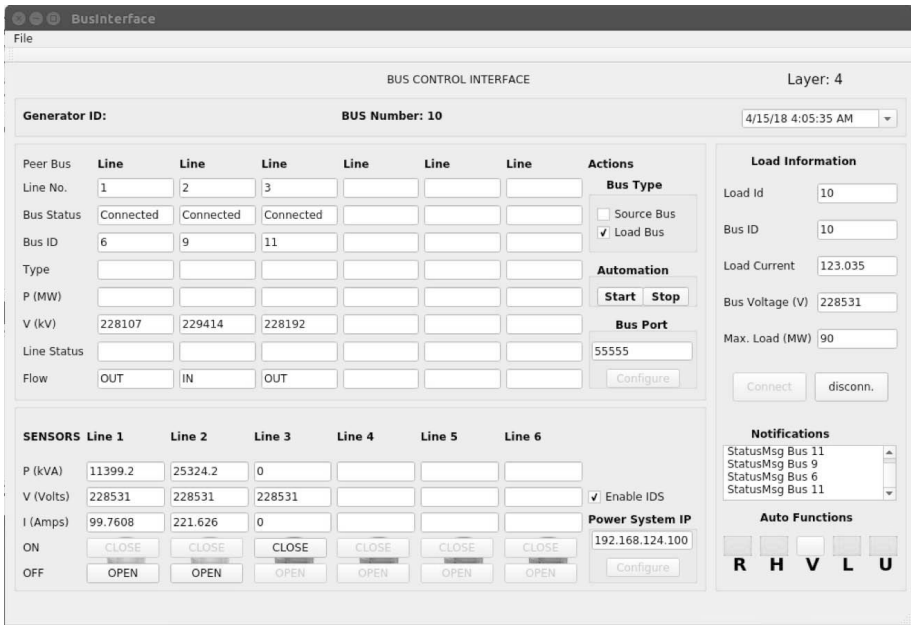



*Figure 8.* SOCOM bus interface.

through the physical-bus (P-B) controller adaptor. The adaptor routed UDP packets from the physical buses to the corresponding bus controller, and from the bus controllers to the corresponding physical buses. Figure 8 shows the bus control and configuration interface.

## 4.1 FPGA Implementation

The implementation employed a Cyclone IV-E EP4CE115F29C7 FPGA and an Altera DE2-115 Development and Education Board. The model comprised a Nios II processor that executed application programs, a JTAG UART component for supporting communications between the processor and host computer, a Triple-Speed Ethernet IP Core for implementing the MAC sublayer and a partial physical layer, a synchronous dynamic random-access memory (SDRAM) for program code and data, and two scatter-gather direct memory access (SGDMA) controllers for data transmission and receiving functions to and from the MAC sublayer. The model also incorporated flash memory for storing MAC and IP addresses, input/output peripherals used as output indicators and control inputs for the bus controller.

## 4.2 Attack Scenarios

Three attack scenarios were developed to evaluate the performance of the SOCOM-IDS in protecting a smart grid The scenarios involved disruptions of

smart grid operations and its automation functions. In the attack scenarios, cryptographic controls were disabled on all the bus controllers (i.e., data was sent and received as plaintext). Intrusion detection was performed by the SOCOM-IDS model.

The following three attack scenarios were evaluated:

- **Scenario 1:** In this scenario, the attacker intercepted messages sent between buses 4 and 5. The attacker's goal was to corrupt the state estimation at bus 5 by injecting false current and voltage information into messages sent by bus 4.

- **Scenario 2:** In this scenario, the attacker generated and sent control messages from bus 5 to neighboring buses using the control vector $a_4 = \{0,0\}_i^M$ to force switchgear device configuration changes to the neighbors of bus 5. The goal of this attack was to disconnect bus 5 from the smart grid to cause a power failure at bus 5.

- **Scenario 3:** In this scenario, the attacker generated a series of messages that mimicked the self-healing automation function process in order to initiate a switchgear connection request from bus 6 to bus 5. It was assumed that the switchgear device state between bus 5 and 6 was not connected and that the attacker understood how the self-healing process worked. The goal of the attacker was to force a disruption in the power flow of the smart grid by routing power in an unauthorized manner.

Attackers have varying knowledge about power systems, SOCOM operational behavior and physical access. This impacts their ability to disrupt the smart grid. The experiments assumed the following three categories of attackers:

- **Category 1:** Attackers in this category have limited knowledge about smart grid network protocols. They can sniff and modify network traffic, but have no understanding of how power systems and automation functions work. The attackers are basically script-kiddies who launch random attacks without clear objectives.

- **Category 2:** Attackers in this category have basic knowledge of smart grid network protocols and can sniff and modify network traffic. They have a basic understanding of power systems, but no understanding of the automation functions. The attackers can craft valid messages in order to deceive state estimators in the smart grid and trigger switchgear devices.

- **Category 3:** Attacker in this category have complete understanding of smart grid network protocols and detailed knowledge of power system functionality. The attackers also have an expert understanding of smart grid automation functions and the underlying processes and network behavior. The attackers in this category can craft sequences of messages to manipulate automation functions.

Scenario 2 assumed the presence of a Category 2 attacker. The attacker spoofed bus 5 and sent valid control request protocol messages to buses 4, 6, 8 and 9 to disconnect their switchgear device connections to bus 5. The malicious messages were detected by the SOCOM-IDS process validation module. The data validation module discovered that the malicious messages did not belong to an automation function process running on the smart grid and, therefore, flagged them as false messages.

## 4.3 Results

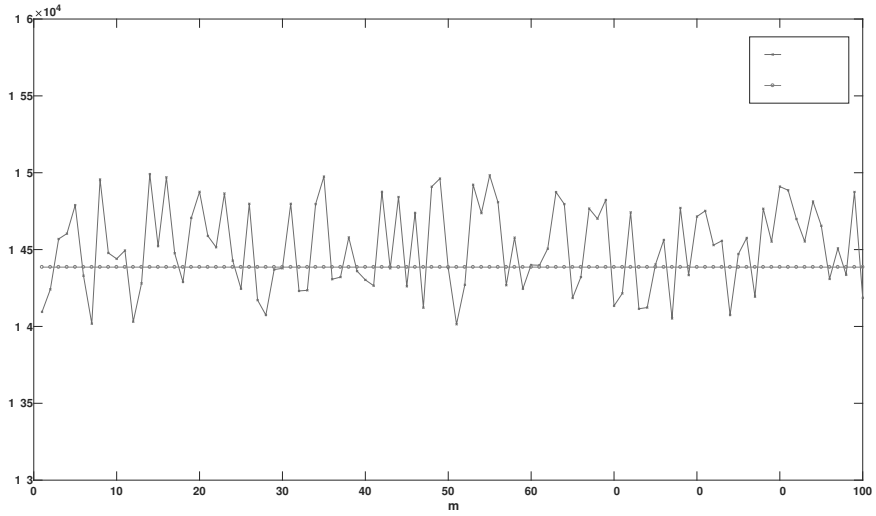
SOCOM-IDS was tested against attacks in Scenario 1. The attacker, who was assumed to be in Category 1, generated random status messages. One hundred status update protocol messages were generated with random voltages and currents in the ranges 24 kV to 25 kV and 300 A to 400 A, respectively. Figure 9 shows the random measurement values sent every five seconds by the attacker (who spoofed bus 4) to bus 5 compared against the expected measurements at bus 5. The SOCOM-IDS data validation module detected all the false messages with no false alarms or missed detections.

An attacker in Scenario 3 would generally be in Category 3. The corresponding attack was detected by the SOCOM-IDS state validation module. Figure 10 shows the sequence of messages received by bus 5 during a self-healing process initiated by bus 6. As discussed above, buses 4, 6, 8 and 9 sent duplicated resource discovery protocol messages to bus 5 reflecting the same changes in the source and load information. These messages were used in Equation (8) to verify if a failure actually occurred. A significant drop in total power drawn from source buses (bus failure causing load disconnection) indicated that a power failure had occurred.

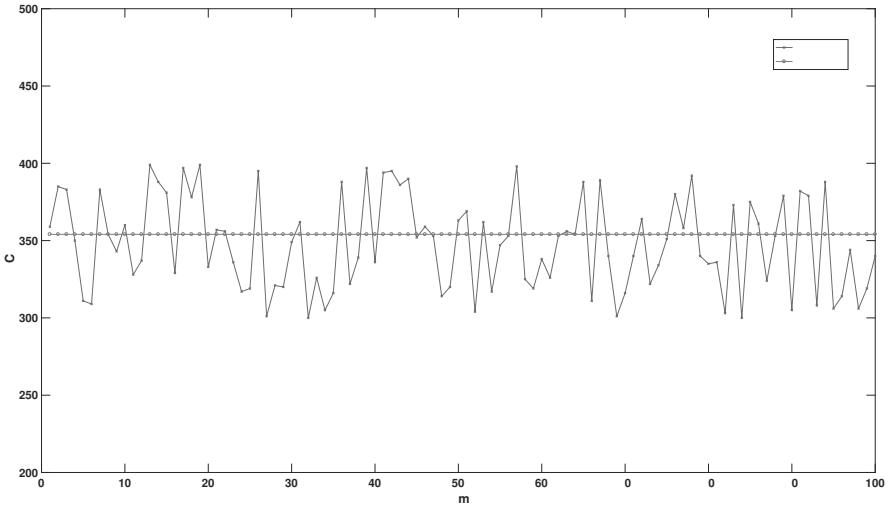
The data validation module and the process validation module are designed for on-line operation. Figure 11 shows the runtime performance of the SOCOM-IDS data validation and process validation modules.

# 5. Conclusions

This chapter has presented the Secure Overlay Communications and Control Model Intrusion Detection System (SOCOM-IDS) for smart grid security. SOCOM-IDS provides an extra layer of security over traditional network security controls by integrating the physical and behavioral properties of a power system. Its primary objective is to ensure the resilient operation of a smart grid under cyber attacks. The intrusion detection modules in SOCOM-IDS constantly validate the communications between buses in a smart grid to ensure that operational constraints are not violated. The modules were evaluated using a self-healing automation function developed for smart grids and the results demonstrate that SOCOM-IDS is able to detect a variety of control-related and state-estimation cyber attacks on a simulated smart grid.



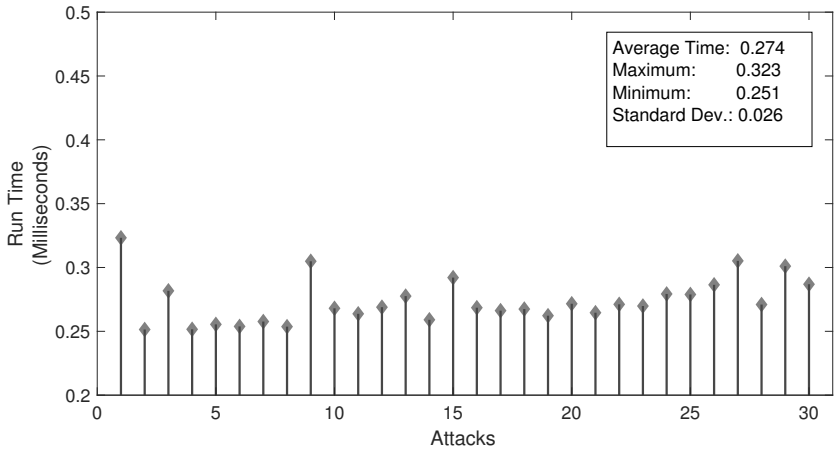

(a) Bus 4 voltage measurements.



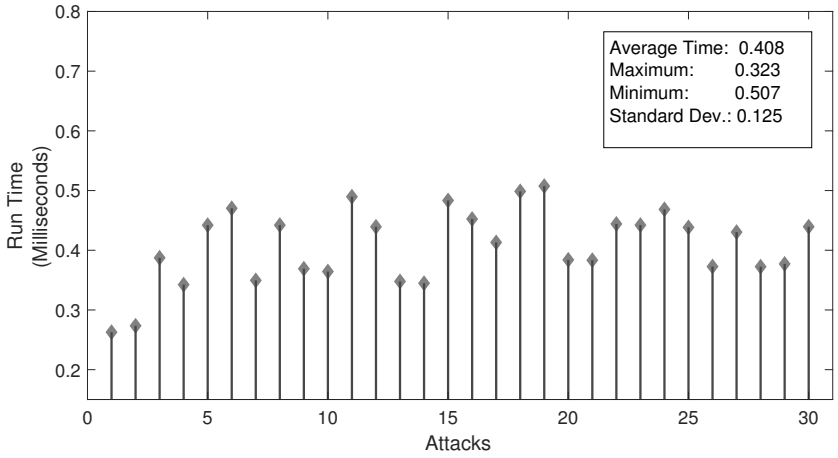

(b) Bus 4–5 line current measurements.

*Figure 9.* Random attack values vs. expected state measurement values.


*Figure 10.* Self-healing message sequence.




(a) Data validation module performance.




(b) Process validation module performance.

*Figure 11.* Runtime performance of the SOCOM-IDS validation modules.

This chapter also demonstrates the importance of communications/control architectures for implementing cyber security in cyber-physical systems such as a power grid. The SOCOM architecture provides a framework that integrates physical system properties and behavior into cyber security controls in an intuitively-appealing manner. The SOCOM framework is extensible and its application extends beyond power systems. Indeed, it is easily adapted to any cyber-physical system for which secure decentralized automation is a requirement.

## References

[1] H. Cho, T. Hai, I. Chung, J. Cho and J. Kim, Distributed and autonomous control system for voltage regulation in low-voltage DC distribution systems, *Proceedings of the International Conference on Condition Monitoring and Diagnosis*, pp. 806–810, 2016.

[2] A. Clausen, A. Umair, Z. Ma and B. Norregaard Jorgensen, Demand response integration through agent-based coordination of consumers in virtual power plants, in *PRIMA 2016: Principles and Practice of Multi-Agent Systems*, M. Baldoni, A. Chopra, T. Son, K. Hirayama and P. Torroni (Eds.), Springer, Cham, Switzerland, pp. 313–322, 2016.

[3] L. Gomes, P. Faria, H. Morais, Z. Vale and C. Ramos, Distributed, agent-based intelligent system for demand response program simulation in smart grids, *IEEE Intelligent Systems*, vol. 29(1), pp. 56–65, 2014.

[4] L. Hernandez, C. Baladron, J. Aguiar, B. Carro, A. Sanchez-Esguevillas, J. Lloret, D. Chinarro, J. Gomez-Sanz and D. Cook, A multi-agent system architecture for smart grid management and forecasting of energy demand in virtual power plants, *IEEE Communications*, vol. 51(1), pp. 106–113, 2013.

[5] J. Hong and C. Liu, Intelligent electronic devices with collaborative intrusion detection systems, to appear in *IEEE Transactions on Smart Grid*.

[6] Institute of Electrical and Electronics Engineers, IEEE 1815-2012 – IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3), Piscataway, New Jersey, 2012.

[7] International Electrotechnical Commission, IEC 61850 Power Utility Automation, Geneva, Switzerland, 2013.

[8] X. Ji, J. Liu, X. Yan and H. Wang, Research on self-healing technology of smart distribution network based on multi-agent system, *Proceedings of the Chinese Control and Decision Conference*, pp. 6132–6137, 2016.

[9] Y. Kumar and R. Bhimasingu, Enabling self-healing microgrids by the improvement of resiliency using closed loop virtual DC motor and induction generator control scheme, *Proceedings of the IEEE Power and Energy Society General Meeting*, 2016.

[10] B. Li, R. Lu, W. Wang and K. Choo, Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical systems, *Journal of Parallel and Distributed Computing*, vol. 103, pp. 32–41, 2017.

[11] G. Liang, S. Weller, J. Zhao, F. Luo and Z. Dong, The 2015 Ukraine Blackout: Implications for false data injection attacks, *IEEE Transactions on Power Systems*, vol. 32(4), pp. 3317–3318, 2017.

[12] G. Liang, J. Zhao, F. Luo, S. Weller and Z. Dong, A review of false data injection attacks against modern power systems, *IEEE Transactions on Smart Grid*, vol. 8(4), pp. 1630–1638, 2017.

[13] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer and R. Iyer, Runtime semantic security analysis to detect and mitigate control-related attacks in power grids, *IEEE Transactions on Smart Grid*, vol. 9(1), pp. 163–178, 2018.

[14] D. Mashima, P. Gunathilaka and B. Chen, Artificial command delaying for secure substation remote control: Design and implementation, to appear in *IEEE Transactions on Smart Grid*.

[15] MathWorks, Simscape Power Systems, Natick, Massachusetts (`www.mathworks.com/products/simpower.html`), 2018.

[16] MathWorks, Simulink Real-Time, Natick, Massachusetts (`www.mathworks.com/products/simulink-real-time.html`), 2018.

[17] A. Sakis Meliopoulos, G. Cokkinides, R. Fan and L. Sun, Data attack detection and command authentication via cyber-physical co-modeling, *IEEE Design and Test*, vol. 34(4), pp. 34–43, 2017.

[18] V. Singh, N. Kishor and P. Samuel, Distributed multi-agent-system-based load frequency control for multi-area power systems in smart grids, *IEEE Transactions on Industrial Electronics*, vol. 64(6), pp. 5151–5160, 2017.

[19] B. Talha and A. Ray, A framework for MAC layer wireless intrusion detection and response for smart grid applications, *Proceedings of the Fourteenth International Conference on Industrial Informatics*, pp. 598–605, 2016.

[20] E. Tebekaemi and D. Wijesekera, A communications model for decentralized autonomous control of the power grid, *IEEE International Conference on Communications*, 2018.

[21] Telecom Italia Lab, Java Agent Development Framework (JADE), Telecom Italia Group, Turin, Italy (`jade.tilab.com`), 2018.

[22] Z. Wang, B. Chen, J. Wang and C. Chen, Networked microgrids for self-healing power systems, *IEEE Transactions on Smart Grid*, vol. 7(1), pp. 310–319, 2016.

[23] K. Weaver, Smart meter deployments result in a cyber attack surface of "unprecedented scale," *Smart Grid Awareness*, SkyVision Solutions, Naperville, Illinois (`smartgridawareness.org/2017/01/07/cyber-attack-surface-of-unprecedented-scale`), January 7, 2017.

[24] L. Yang and F. Li, Detecting false data injection in smart grid in-network aggregation, *Proceedings of the Fourth IEEE International Conference on Smart Grid Communications*, pp. 408–413, 2013.

[25] N. Yorino, Y. Zoka, M. Watanabe and T. Kurushima, An optimal autonomous decentralized control method for voltage control devices using a multi-agent system, *IEEE Transactions on Power Systems*, vol. 30(5), pp. 2225–2233, 2015.

[26] M. Zaki El-Sharafy and H. Farag, Self-healing restoration of smart microgrids in islanded mode of operation, in *Smart City* 360°, A. Leon-Garcia, R. Lenort, D. Holman, D. Stas, V. Krutilova, P. Wicher, D. Caganova, D. Spirkova, J. Golej and K. Nguyen (Eds.), Springer, Cham, Switzerland, pp. 395–407, 2016.

[27] X. Zhang, A. Flueck and C. Nguyen, Agent-based distributed volt/var control with distributed power flow solver in smart grid, *IEEE Transactions on Smart Grid*, vol. 7(2), pp. 600–607, 2016.

[28] Y. Zhang, L. Wang, W. Sun, R. Green II and M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smart grids, *IEEE Transactions on Smart Grid*, vol. 2(4), pp. 796–808, 2011.