Impact Evaluation of Malicious Control Commands in Cyber-Physical Smart Grids

Neetesh Saxena *Senior Member, IEEE,* Leilei Xiong *Member, IEEE,*
Victor Chukwuka *Member, IEEE,* and Santiago Grijalva *Senior Member, IEEE*

Abstract—The Smart Grid (SG) is vulnerable to cyber-attacks due to its integration with a variety of information, communication and control technologies. If undetected by deployed security systems, cyber-attacks could damage critical power system infrastructure and disrupt service to a very large number of energy customers. In particular, cyber attackers could hijack the smart grid by injecting malicious commands. To provide insight into these concerns, we propose an approach that develops a new tool for the real-time Cyber-Physical Security Assessment (CPSA) of malicious control commands that target physical SG components. The tool is able to detect and protect the system against known Trojans (such as BlackEnergy). It also efficiently and effectively monitors the health of the power system in real-time and detects the presence of malicious commands. The security analysis of our approach includes a look at three system-generated metrics: system susceptibility, access points, and threat capability. The performance analysis includes a look at the system overhead, scalability, accuracy, robustness, and execution and response time. Our proposed approach was tested on a 42-bus power system with 24 substations. The developed tool could be extended and used by power system operators to assess and mitigate the impact of cyber-attacks on the smart grid.

Index Terms—Cyber-physical system, malicious control command, smart grid.

1 Introduction

Over the past few years, cyber-physical security of the Smart Grid (SG) has become an increasingly critical research direction due to several recent cyber-attack attempts on the SG in different countries and successful cyber-attacks such as the attack on the Ukranian power system[2]. Today, the SG is more vulnerable to cyber-attacks due to its integration with different communication technologies, including in some applications, the Internet. Despite how important power system cyber-security is, today's system don't have a capability to develop real-time cyber-physical security situational awareness. Cyber-Physical Security Assessment (CPSA) is necessary in order to examine the impact of failure or attack through cyber-elements on the physical operation of the power system. This can be accomplished through modeling and simulation of cyber events on the power system using a real-time co-simulator or through a hardware testbed setup.

The best practice for CPSA is to analyze the direct cyber-physical impact of specific cyber-attacks on the power system, which is not limited to previously observed cyber vulnerabilities of the given power system. To achieve this goal, a comprehensive and re-configurable cyber-physical co-simulator that can be used to model and simulate cyber events is required. In this paper, we describe a cyber-physical co-simulator for real-time communication and power system simulation. Our co-simulator is then used to evaluate the impact of malicious control commands on a test power system. The considered power system contains a central Control Center (CC), which communicates with downstream substation Remote Terminal Units (RTUs) through intermediate routers. Generators, buses, loads, transformers, and capacitor banks are present at the various substations.

- *N. Saxena is with the Department of Computing and Informatics, Bournemouth University, UK.*
  E-mail: nsaxena@ieee.org
- *L. Xiong, V. Chukwuka and S. Grijalva are with the School of Electrical & Computer Engineering, Georgia Institute of Technology, USA.*
  E-mail: leileix@gatech.edu, vchukwuka3@gatech.edu, sgrijalva@ece.gatech.edu

Manuscript received XXXX XX, 20XX; revised XXX XX, 20XX.

1.1 Motivation and Research Problem

The power industry is facing potential cyber-attacks that can impact the power grid with serious implications. Our work is motivated by recent cyber-attacks on real power systems (such as the Ukraine attacks in December 2015 and February 2016 [2]). The Ukraine power grid was brought down by cyber-attacks, which left 80,000 people in dark for six hours, and more than two months after the attack, the control centers were still not fully operational [2]. The attacks targeted IT staff and system administrators of companies responsible for distributing electricity. They delivered email to workers with a malicious Word document attached. Clicking on and selecting the attachment enabled macros for the document injected BlackEnergy (which have infected other systems in Europe and the US) into workers' machines. The attackers accessed the Supervisory Control and Data Acquisition (SCADA) networks through the hijacked Virtual Private Networks (VPNs), sent commands to disable the Uninterruptible Power Supply (UPS) systems, and opened up transmission lines breakers at numerous substations. This causes a broad power blackout. It is evident that well-planned and well-executed cyber-attacks through malicious control commands can potentially disconnect power devices and leave hundreds of thousands of energy consumers in the dark. Therefore, it is very important to evaluate and

understand the resiliency of the power grid against cyber-attacks to develop new solutions to safeguard the system.

Incident responses, security risk evaluation, and vulnerability analysis have not been standardized in the smart grid environment. Although there are certain standards assessing security aspects of the smart grid, such as by the European Commission [10], EU Distribution System Operators (DSO) [23], European Union Agency for Network and Information Security (ENISA) [8], European Telecommunications Standards Institute (ETSI) Smart Grid Coordination Group [5], National Institute of Science and Technology's NISTIR 7628 [21], and NIST framework [20]. However, some of them are either not enough to handle Advance Persistent Threat (APT) in the smart grid environment or not fully implemented by the service providers inline with the compliance. In fact, the cyber and physical interactions of power components and devices interactions are not well understood. A cyber threat may lead to damage of critical power infrastructure or significantly impact, potentially even disable critical functions of the Energy Management System (EMS) due to inappropriate responses. With the knowledge that cyber-physical insecurities exist in the power system and cannot be completely eliminated, our goal is to reduce these insecurities to an acceptable level. Existing tools are not capable of effectively evaluating the health of the power system in the presence of cyber-attacks.

1.2 Challenges

In order to gain insight and better understanding on the inter-dependencies of cyber and power elements in the smart grid, an integrated co-simulator is developed. The co-simulator model overall cyber-physical control loop including operator decisions under attack scenarios. It will provide the security and performance assessment on the overall health of the entire system. The assessment on future vulnerable states and situational awareness in the presence of different cyber-attacks can also be achieved by a co-simulator. Implications of cyber-physical system under different communication scenarios, such as reliable, unreliable, limited bandwidth and limited allowed data size can also be studied. However, accurate and correct modeling and simulation of the dynamic behavior of the smart grid is quite challenging as the smart grid is a large and complex structure comprises with millions of the components, such as loads, generators and transformer tied together by hundreds of thousands of miles of transmission and distribution wires and integrated with a large number of control devices. In addition, the communication network connected to the smart grid generally comprises of thousands of communication nodes, several communication routers, computation and communication servers, and authentication servers. Hence, it is quite difficult to clearly understand the dynamic behavior and inter-dependencies between the both systems.

1.3 Contributions

Our contributions are as follows:
1) Development of a tool for cyber-physical security assessment of cyber-attacks targeting physical SG components. This tool would help operators make an appropriate control decision by simulating the impact of the potentially malicious commands on the power system in real-time.
2) A method that helps operators to detect and protect the system thhrough an IDS against known malicious software (Trojans) used for spamming and attacking the power grid.
3) Introduction of a specific and system wide security metric for real-time situational awareness. Simulation of a set of relevant use cases in a realistic but small system.
4) Efficiently and securely monitoring of the power system security in real-time and output logs generation for the operator in 5 sec. to evaluate if any malicious commands target power system components.

The remainder of this paper is organized as follows. Section II discusses the existing work related to cyber-attacks on the power system. Section III describes the system model, the threat model, and our goals to be achieved. We propose an approach towards simulating the malicious control command cyber-attack and monitoring its impact on the power system in Section IV. Section V presents a discussion about security and performance analysis of the proposed approach along with its limitations. Finally, Section VI concludes this work and highlights future directions.

2 Related Work

In order to accurately evaluate the current security of the power system, a cyber-physical security assessment of the joint communication-power system is required, rather than simply examining the cyber-security concerns in only the communication network or the impact of physical events on the power system. However, research in this area has not been fully explored. First, we discuss the works related to cyber security followed by the research on cyber-physical system security in the SG.

Chen et al. [6] discussed different categories of attacks: vulnerability, data injection and intentional attacks, and analyzed network robustness. Tran et al. [29] proposed a detection scheme for replay attacks in the SG. Yang et al. [32] discussed Address Resolution Protocol (ARP) spoofing-based Man-in-the-Middle (MITM) attacks. Wei et al. [30] performed a study on modeling Denial-of-Service (DoS)-resilient communication routing in the SG. Liu et al. [19] presented a framework that models a class of cyber-physical switching vulnerabilities. Etigowni et al. [9] presents 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. [26] made an attempt to assess the impact of cyber-attacks on the Advanced Metering Infrastructure (AMI), specifically considering DoS and Distributed DoS (DDoS) attacks. Yi et al. [33] presented a DoS attack scenario that lowers packet delivery rate by 10-20% in the AMI network. Srikantha et al. [27] considered the effect of a DoS attack on the power system. Hahn et al. [13] introduced a security model to represent privilege states and evaluated viable attack paths in the AMI network. Liu et al. [18] analyzed the impacts of a line outage attack, DoS attack, and MITM attack on the physical power grid using an integrated cyber-power modeling and simulation testbed.

The above mentioned solutions have limitations, which could be further improved. In [6], [32], [26], [33], [13] and

[9], the impact of attacks on the power system was not studied, whereas the scheme in [29] 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 [30] only included a 3-generator system, which is small to fully understand the impact of these attacks on real power systems. The communication network is not considered in quantifying the cyber-physical system impact in [19] and [27].

TABLE 1: Communication Attacks Targeted on Smart Grid

Attack Type	Authors Work	Studied Power System Impact?
Data injection	Chen et al. [6]	No
Replay	Tran et al. [29]	Yes
ARP spoofing MITM	Yang et al. [32]	No
DoS	Wei et al. [30]	Yes
Switching vulnerabilities	Liu et al. [19]	Yes
Access control	Etigowni et al. [9]	No
DoS and DDoS	Sgouras et al. [26]	No
DoS	Yi et al. [33]	No
DoS	Srikantha et al. [27]	Yes
Viable attacks paths	Hahn et al. [13]	No
Line outage, DoS, MITM	Liu et al. [18]	Yes

Hahn et al. [12] described a cyber-physical testbed. Yan et al. [31] summarized the cyber security requirements and the possible vulnerabilities in smart grid communications and proposed solutions. However, neither of these work model cyber-attacks to understand the physical impact of cyber-attacks on the power system. Godfrey et al. [11] represented an analytical model of the communication network to examine the effect of communication failures as a function of the radio frequency (RF) transmission power level. The paper discusses the transmission of various messages with power quantities and observe the communication delay. However, it does not detect or alert any malicious message and also does not measure the impact of such change on the power system behavior. Kundur et al. [17] focused on the model synthesis stage for both cyber and physical grid entity relationships as directed graphs to derive a framework for cyber-attack impact analysis of a smart grid with a case study. However, the work does not perform any simulation and also does not consider physical impact on the power system. The paper [33] performs a simulation of packet rate, but it does study the impact of the attack on the power system. Aditya et al. [3] proposed a game-theoretic framework to model cyber-physical security for Wide-Area Monitoring, Protection and Control (WAMPAC) applications, whereas the proposed work in this paper is more analytical and is dependent on the outcomes of each timestep iteration and the current state of the power system. The advantages of the approach in [3] include articulation and understanding of cyber-attacks (threat timing, data integrity, and replay attacks) and coordinated attacks. However, our work targets malicious command (injection or forgery) attacks on the power system. The work in [3] focuses potential attacks on the communication network without considering their impact on the power system. In summary, none of these papers actually determine the physical impact of the attacks on the system and do not provide a security assessment metric. This is a big difference on impact between stealing a credit card or a billing record, and disconnecting a power plant. We tackled this challenge in the proposed work, as we believe that the future smart grid must be resilient and support fault-tolerant system.

The studies of cyber-physical systems found in literature are based on traditional attacks, such as MITM, DoS, and DDoS as mentioned in Table 1. These attacks are achieved by injecting false data or targeting the device to stop its functionality. However, there is no study carried out for malicious/false command injection in the SG, where an adversary can potentially isolate the critical power components by disconnecting them from the rest of the power system. We tackle this issue of impact monitoring of the cyber-physical system by using a cyber-physical co-simulator.

3 System Model, Threat Model, and Goals

In this section, we present a smart grid system model, a threat model, and the specific goals of this research.

3.1 System Model

We introduced a smart grid system model as shown in Figure 1 that consists of a single control center with an EMS, where a power systems operator makes operation and control decisions, and numerous downstream substations, each of which contains an RTU. The communication between the RTUs and the control center is provided through two routers (Router 1 and Router 2). The smart grid power systems layer consists of multiple stages: electricity generation, transmission, distribution, and consumption by the end users (known as loads). Electricity is typically produced by large-scale generation, which can include nuclear power plants, thermal power plants (fueled by coal, oil, or natural gas), hydroelectric plants, and nondispatchable renewables (such as wind and solar farms). In order to reduce resistive losses that can occur during long-distance transmission, electricity is stepped up to a high voltage at nearby substations by power transformers before it is sent across a network of transmission lines. Once it reaches substations near the end customers, it is stepped down in voltage by a series of transformers before it is ultimately used by industrial, commercial, or residential loads.

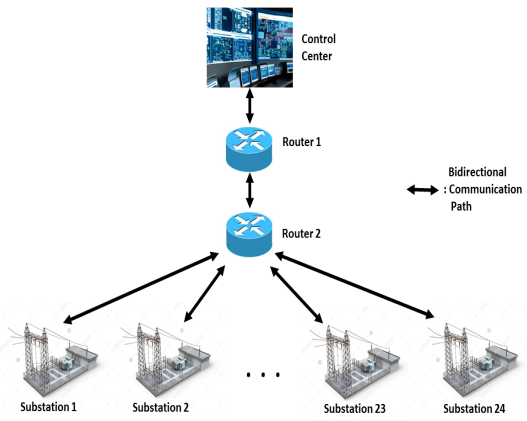


Fig. 1: Power system model consisting of a single control center and multiple substations, each consists with an RTU.

Substations serve as transition points between generation and load. In addition to power transformers, substations also contain circuit breakers that provide the ability to connect or disconnect equipment as well as busbar (hereafter referred to as buses), which are metal bars that connect high voltage equipment in the substation switchyard. They may also contain capacitor banks, which are used to correct power factor issues caused by inductive loads in the system, improve voltage stability, and reduce network losses. One of the key assumptions behind the design of the smart grid is that the amount of electricity generated and the amount of electricity consumed are balanced at any given time. The alternating current electricity operates at 60 or 50Hz. Thus, the balancing of power is very delicate and fast. For instance loss of a large generating unit is felt almost immediately throughout the system and actions to balance the system are initiated in milliseconds and balancing usually takes a few seconds. Cyber-attacks that seek to drastically disrupt this balance have the potential to cause widespread cascading power outages. Also, cyber-attacks could seek to destroy critical equipment such as generators and bulk power transformers, which are costly to replace and typically have very long lead times. Power systems are operated with physical security in mind so as to avoid large blackouts that can happen under equipment failure, weather events, physical or cyber-attacks. In this paper, we study the impact of malicious control commands that have the potential to reduce the security of the power system. These commands could include opening generator circuit breakers, which may create a sudden imbalance between generation and load that could cause system-wide problems. Each substation contains multiple buses, power transformers, circuit breakers, and capacitor banks.

In the power system we consider that there are 24 substations, each equipped with one RTU. During the polling request, the control center asks each substation RTU to send its available measurement data. All polled RTUs send their data back to the control center as a response. In a real scenario, this communication takes place either over an insecure network or via VPN. However, there is still a chance that an adversary could modify the measurement data before it leaves the substation. In real operation, the power system operator can also send control commands to the substation RTU in order to take an appropriate action to mitigate the impact of events on the overall power system. These commands include: setting a generator operating point, opening/closing a circuit breaker, and connecting/ disconnecting a capacitor bank.

Power system measurements are modeled as follows. Let z represent a set of available measurements. Then $z = h(x)+e$, where x is the estimated state vector (bus voltages represented in phasor form as magnitudes and angles), h is the vector of functions relating the state variables to the error-free measurements, and e is a vector of measurement errors, which are assumed to have a Gaussian distribution with mean 0 and variance σ^2. There are five types of measurements considered in h: real and reactive injection measurements, real and reactive power flow measurements, and voltage measurements. The expressions for real and reactive power injection at bus i are [1]:

$$P_i = V_i \sum_{j \in N_i} V_j \ (G_{ij}\ cos\theta_{ij} + B_{ij}\ sin\theta_{ij})$$
$$Q_i = V_i \sum_{j \in N_i} V_j \ (G_{ij}\ sin\theta_{ij} - B_{ij}\ cos\theta_{ij})$$

where V_i denotes the voltage at bus i, N_i represents the set of buses adjacent to bus i, G_{ij} and B_{ij} are the real and imaginary components of the admittance matrix, and θ_{ij} is the difference of the angles between buses i and j. The expressions for real and reactive power flow from bus i to bus j are:

$$P_{ij} = V_i^2(g_{si} + g_{ij}) - V_i\ V_j(g_{ij}\ cos\theta_{ij} + b_{ij}\ sin\theta_{ij})$$
$$Q_{ij} = -V_i^2(b_{si} + b_{ij}) - V_i\ V_j(g_{ij}\ sin\theta_{ij} - b_{ij}\ cos\theta_{ij})$$

where $g_{ij} + j\ b_{ij}$ represents the series impedance and $g_{si} + j\ b_{si}$ represents the shunt impedance of a line from bus i to bus j based on the two-port π-model of a transmission line. If there is no communication error and no adversarial manipulation, a power system measurement would be exactly equal to $h(x)$. If there was only noise and no adversarial manipulation, state estimation could filter out the Gaussian error from z. However, in the presence of an attack where an adversary does modify a measurement, then z would no longer be equal to the correct $h(x)$ plus a random Gaussian error.

3.2 Threat Model

We describe our cyber security threat model with respect to the SG system as follows:
1) System Susceptibility: The adversary can perform suspicious and/or malicious activities including attempts to access the login credentials of the operator and/or device, transmission of fake/bad commands, such as opening a circuit breaker connected to a substation device, and disturbing network communications and packet data. The adversary will attempt to discover and exploit these susceptibilities in order to compromise (modify or control) critical power system infrastructure, information and operations.
2) Adversary's Capability: We assume that the adversary is capable of performing a MITM attack by altering or replacing a legitimate command, injecting a malicious command, or accessing the control center to send a legitimate command as an insider attacker.
3) Adversary's Accessibility: We assume that the adversary has knowledge of the communication network topology as well as the power system topology. The adversary also has enough resources to perform the required malicious or suspicious actions and has accessibility to the system.

We have considered three attack scenarios as follows: In first attack scenario, the attacker sends a false but legitimate command from a location other than the control center to the generator breaker over an insecure network. In second attack scenario, the adversary modifies a legitimate command transmitted from the control center to the generator breaker over an insecure network. In third attack scenario, the adversary acts as an insider attacker who has access privileges for sending a legitimate command to the generator breaker.

3.3 Goals

We present the following goals to be achieved in this cyber-physical SG system:
1) *Critical Components:* The primary goal of the adversary is to target critical power components, such as generators and transformers, in order to damage the power system or cause a service interruption. The adversary could also target the routers to explore and access the communication system and exploit vulnerabilities. Our goals are to perform a regular security analysis, detect any such suspicious activity and attempt to deny illegitimate access.
2) *Key Assets:* Key assets are the pieces of critical information that the adversary will seek. These key assets could be information about a regular schedule for polling operations at a specific substation or the IP address and other communications related information for the control center. With these assets the adversary can later spoof the control center and try to inject a malicious command. Our goal is to identify this malicious activity and prevent such injections in the real power system.
3) *Detection, Reaction, and Adaptation:* In the worst case, the adversary successfully performs an undetected malicious action, such as injecting a malicious command. Our goal is to simulate the worst case scenario and analyze the potential impact of malicious command on the power system either in study mode, or upon detection of a suspicious command.

4 Our Approach

In this section, we present our approach, discuss specific use cases for malicious command injection, describe the behavior on and impact monitoring of the cyber-physical power system, design malicious command countermeasure, and evaluate the impact of control operation on the cyber-physical power system.

4.1 Use Case Scenarios

An adversary can perform a malicious command injection attack by sending a false control command to a substation RTU. If the adversary does not have complete knowledge of the system and simply injects a false command at random, the operator should be able to identify and stop the execution of the malicious command on the power system. Also, if the adversary has complete or partial knowledge of the system, it can purposefully inject a specific malicious command to damage the system at large. If an adversary targets a command from a malicious source, such as a fabricated command to detach a generator, the IDS will be able to detect the command and prevent its execution on the power system. If an adversary models a smart command, which is legitimate but unwanted and seems to be a routine operation, such as slightly reduce power generation at any specific point in time, the IDS probably will not be correctly able to detect it. However, it will alert and send a notification of suspicious behavior (considering threshold values and % of change in values) to the operator. We also note that there are automatic commands issued by the control center, without the involvement of the operator, such as those generated by the Automatic Generation Control (AGC) function. These commends are sent to all the generating units in a power system every few seconds. While all the commands pass through the IDS, which is very fast, only those suspect will be blocked and sent to the operator for simulation. One example of a malicious command that could significantly impact the power system is the opening of the circuit breaker connected to the largest generator in the system. We discuss three specific scenarios as follows:

Use Case 1: Adversary impersonates the network and sends a false (unwanted) but legitimate command outside of the control center to breaker of the largest generator.

Effects on the Communication Network: Under this attack, we can observe and monitor several effects on the communication system, such as: (i) the Intrusion Detection System (IDS) notifies the control center operator what command it received. The operator verifies whether the command is legitimate, and (ii) a false command was issued to the substation RTU connected to the breaker of the targeted generator.

Effects on the Power System: If this attack is successful, we can observe the following impacts on the power system: (i) insecure operation(s) of the power system, and (ii) possible shedding of electrical load.

Use Case Steps: 1) The attacker targets a command as mentioned as (a) in threat model.
2) IDS detects a suspicious malicious command (based on its rules engine, such as IP address, port number, etc.) and notifies the operator. The operator verifies that the control center did not issue this command.
3) CPSA performs power flow and cyber-physical contingency analysis to evaluate the effect of the command on the power system if it was allowed to go through and discovers that the system is insecure, indicating that the command was malicious.
4) The operator discards the command. Secure system operation is restored.

Use Case 2: Adversary fabricates or modifies a legitimate command sent to a generator breaker over an insecure network.

Effects on the Communication Network: Same as in use case 1, except the legitimate command was modified over the network.

Effects on the Power System: Same as in use case 1.

Use Case Steps: 1) The attacker sends a command as mentioned as (b) in threat model.
2) The IDS does not detect the command modification, but still sends a notification to the operator. The operator verifies that the control center did not issue the command.
3) Same as use case 1 step 3.
4) CPSA asks IT personnel for attack information with a response that there is suspicion of a MITM attack.
5) Same as use case 1 step 4.

Use Case 3: Adversary as an insider attacker (other person) at the control center sends a legitimate but unwanted command to the generator breaker.

Effects on the Communication Network: The operator receives a command notification from the IDS and finds the transmitted legitimate command was not issued by him/her. In the worst case scenario, the operator ignores the notification and allows the execution of the command on the power system.

Effects on the Power System: Same as in use case 1.

Use Case Steps: 1) The attacker sends a command as mentioned as (c) in threat model.
2) The IDS does not detect the insider attack and notifies the operator that it is a legitimate command. The operator verifies that the received command is the same as what was issued from the control center.
3) Generator breaker receives a false command and trips.
4) CPSA runs contingency analysis and discovers that the system is insecure, indicating that the command was legitimate but false (unwanted).
5) CPSA asks the IT personnel for attack information with the response that there is suspicion of an insider attack. Thus CPSA prompts the operator to reclose the breaker.
6) If the breaker does not respond after 20 seconds, CPSA will prompt the operator to initiate the appropriate remedial action after which secure system operation is restored.

4.2 Cyber-Physical Behavior Impact Monitoring

In this section, we discuss cyber-physical attack impact monitoring using log-based and host-based system monitoring, IDS, cyber-physical simulation, and attacks modeling.

4.2.1 Log-based and Host-based System Monitoring

One of our modules performs host-based system monitoring, which involves malicious URLs, masks, and botnet Control & Command (C&C) URLs. This module scans malicious and botnet URLs whenever communicates (send or receive) over the HTTP. This module also scans MD5/SHA1 hashes of the malicious object database and computes a hash of each object before accessing it. One of the malwares used in the Ukraine power system attack in December 2015 was BlackEnergy [22]. BlackEnergy is a Trojan that sneaks into the computer with shared programs when users download or update programs from the Internet or via spam email attachments or hacked web sites. Some of the detected Trojans used by BlackEnergy include:

```
Backdoor.Win32.Blakken, Backdoor.Win64.Blakken
Backdoor.Win32.Fonten, Heur:Trojan.Win32.Generic
```

BlackEnergy also uses executables as malicious drivers contained in the configuration files and tries to extract a list of proxy servers locally used in corporate networks. We monitor the malware samples (Win. drivers) used in the Ukraine attack [16], some of them are:

```
amdide.sys (SHA1: 2D805BCA41AA0EB1FC7EC3BD944EFD7DBA686AE1)
aliide.sys (SHA1: C7E919622D6D8EA2491ED392A0F8457E4483EAE9)
acpipmi.sys (SHA1: 0B4BE96ADA3B54453BD37130087618EA90168D72)
aliide.sys (SHA1: C7E919622D6D8EA2491ED392A0F8457E4483EAE9)
adpu320.sys (MD5: 2D805BCA41AA0EB1FC7EC3BD944EFD7D)
acpipmi.sys (MD5: 0B4BE96ADA3B54453BD37130087618EA)
```

Another way of injecting a Trojan is to spam email the power system operator with malicious macro enabled MS Word or Excel document. This was the strategy utilized by the adversaries on the Ukraine power grid during which the adversaries were able to compromise three operators. Upon receiving the document, the operators curiously opened the document and clicked yes when it asked to enable a macro. As a result, the enabled macro injected a BlackEnergy Trojan into the computer system, which has the capability of hiding itself deep in the system and corrupting the anti-virus files to disable scanning activity. This Trojan also drops a KillDisk virus that corrupts the master boot sector on the disk. As a result, the compromised system cannot reboot. In order to protect the systems against macro-enabled BlackEnergy Trojans in MS Word or Excel documents, we use a technique to verify whether a document has enabled macros and to extract its content. To extract the macros from a document without running Excel or Word, we use a tool called oledump (object linking and embedding tool) [7].

4.2.2 Intrusion Detection System (IDS)

The IDS deployed (mirror image) at each substation scans every DNP3 packet sent and received by the substation RTU. The IDS also notifies the operator about each control command it receives and requests verification. Suricata [28] can be used for the IDS implementation, which is an open source implementation and provides rich functionality for a customized IDS system. Suricata evaluates functions on network messages and performs DNP3 deep packet inspection. The rules of the IDS are developed using Domain Specific Language (DSL), which are binary valued functions. The IDS functionality (such as verifying read and write DNP3 commands) is modeled using Java Script Object Notation (JSON). JSON provides specific classes, groups, and identifiers to represent the rules. The IDS scans the received DNP3 packet from the Distributed State Estimator (DSE) [15], triggers the specific rule based on filters applied to the packet, and passes it to the control center, if the packet is not malicious. If the packet is suspected to be malicious, the IDS sends a notification (an alarm) to the control center. The IDS combines signature and behavioral analysis to protect the system against known, unknown, and advanced threats. Detecting suspicious behavior involves several factors, such as measurement data threshold, protocol modifications, and tracking IP addresses and port numbers. We also perform a traffic analysis on received packets using Wireshark with the jpcap/WinPcap tool.

We also examine the communication patterns over several nodes (RTUs, control center ports, and routers). The process is carried out over an extended period of several days as opposed to micro-examination, since the IDS alerts on specific protocol patterns tend to generate many false positives. We also impose strong policies for role-based and attribute-based access control, and encryption for securing last mile communications [25].

4.2.3 Cyber-Physical Simulation

This co-simulator tool assesses the overall security of the entire system, and allows management of the communication links (by controlling the baud rate, propagation delay, and Maximum Transmission Unit (MTU)) and the substations topology (connection of nodes and routers). In the co-simulator, all communication nodes interact with each other using a message passing protocol. We use a star communication topology to connect RTUs with a router (Router-1). This router is connected to another router (Router-2), which is connected to the control center. We also developed a predictive global state estimator that supports fast modeling and simulation. The co-simulator and distributed state estimator allow the development of more advanced security measures including: estimation of future vulnerable states, identification of suspicious system behavior, and measurement of the effects of different attacks attempted through the communication network on the power system. The co-simulator is built using Java-based GridSim and Java Agent DEvelopment Framework (JADE) in conjunction

with MATLAB and PowerWorld. The co-simulator allows the centralized monitoring of link latency and bandwidth values as the power system and control network state evolves. The co-simulator is capable of detecting anomalies and misbehavior in the combined power and cyber layers of the SG system. This tool will be directly utilized by operators of interconnected power grids for detection of cyber-attacks and provide cyber security and decision-making capabilities. This co-simulator simulates the communication network with realistic parameters: data rate, propagation delay, number of packets, size of each packet, number of devices including RTUs and routers and network topology. The simulator also got functionality to develop and run power system algorithms: power flow, observability analysis, state estimation and N-1 contingency analysis, where N is the number of power components in the system. We simulated a communication network with 24 substation RTUs and performed a cyber-physical security assessment on a 42-bus power system. The simulation is expensive, which requires a specific scenario with dynamic topology to simulate and also has a latency requirement of generating each output file in 4-5 sec. Therefore, it is not recommended to simulate every action, but only the suspicious commands identified by the IDS and selected by the operator.

4.2.4 *Attack Modeling*

We model the malicious command injection attack and monitor the impact of command execution on the power system using our co-simulator. An adversary can send a malicious command encapsulated in a DNP3 packet from the control center (as an insider attacker) or from any other location (with a different IP address or spoofed IP and pretends to be a legitimate IP address of the control center) to the substation RTU, which has a specific IP address and a port number. Once the operator receives the malicious command attack information, it uses the co-simulator to model the malicious command injection attack scenario.

4.3 Designing Malicious Command Countermeasure

In this subsection, we design the countermeasure against malicious command injection attacks.

Pre-conditions: The IDS notifies the operator about a malicious command based on its rule formation and command pattern matching. We simulate the system to predict and generate future states of the power system for the next 40 seconds based on the current power system state. The simulation lasts for 40 seconds with 8 timesteps where each timestep represents a 5 seconds interval, as one cycle of cyber-physical simulation with 8 timesteps takes 40 seconds to generate the output files and security metrics. Generating a single output file takes 5 seconds, which is fast enough for making an appropriate decision. An attack can be targeted at a specific timestep.

Main Process: We use our co-simulator for assessing the effect of a command over the communication network.
1) The co-simulator models a communication scenario, which maps the real communication network parameters. These parameters are as follows: the baud rate = 1572864 bits/sec, propagation delay = 300 ms, command = "CC → RTU: Send Measurement Values-", packet buffer size at the CC = 180 bytes and packet buffer size at the RTU = 1500 bytes. The propagation delay is estimated based on the number of bits transmitted in a packet over the network with a specific speed. We considered network speed as 8.51 Mbps with a packet transmitting 2553K bits needs to set a propagation delay of 300 ms.
2) We model and perform a single attack as malicious command injection operation, and the command type as "Change Generator Status" to open a generator breaker is sent at timestep 5 of 8 iterations.
3) The IDS suspects the command is not a "legitimate command" based on its rules filtration and pattern matching. Thereafter, the IDS sends an alert message to the CC as shown in Figure 2.
4) The operator at the CC views the command sent log information and finds that the command was not initiated by him/her. The operator decides to simulate the command and observe its effect on the power system. The role of IDS is critical here that notifies the operator about a cyber incident, which is not a normal power routine operation.
5) The operator sets up the communication parameters as shown in Figure 3.

Expected Result: The adversary is able to inject a malicious command at a specific time. The simulation is initiated and at timestep 5, a malicious command is suspected. The IDS sends an alert message through the IDS-operation notification interface. This alert message prompts the operator for the next action - simulate or reject the command as shown in Figure 2. The operator decides to simulate the effect of the malicious command, generates the attack output file, and finally allows or rejects the command execution on the real power system as shown in Figure 4.

Post-conditions: A malicious command is successfully injected and simulated, and the power system state is evaluated. Based on load forecast information (which has a very small error of approximately 2%) derived from historical data, we simulate the expected normal operational behavior of the power system (under no attack) for 8 iterations. The result of this simulation is stored in files and is adopted as the baseline case. Simulations of different attack scenarios are be compared with the baseline case to characterize the systems deviations from the normal operations. Then, these forecasted data files are compared to the files generated in real-time. An attack is identified if the real results differ significantly from the projected results. These characterizations are then used in developing metrics that are used for evaluating the cyber-physical security of the system. In this scenario, at timestep 5, the real results are compared against the projected normal operational results at timestep 5. Then, a decision to reject or allow the execution of said command

Fig. 2: An alert message sent from the RTU to the CC.

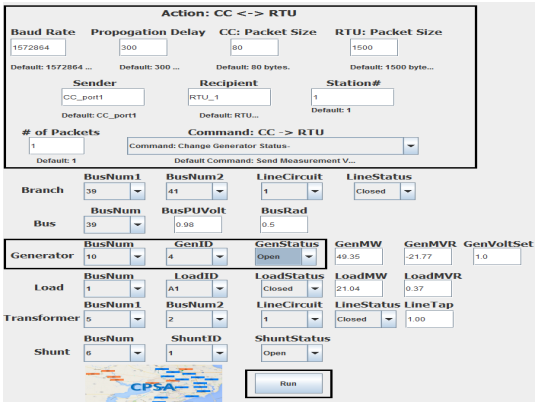


Fig. 3: A command simulation GUI at the CC.

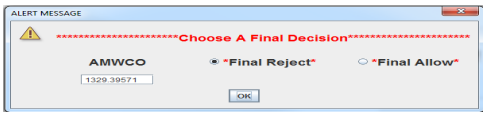


Fig. 4: Final decision to accept or reject the command.

on the power system is made by the operator, and the RTU is notified with the appropriate action.

4.4 Cyber-Physical Control Impact Evaluation

We observe the cyber-physical impact of different attacks on the power system with different setting preferences in the Wide Area Communication Network (WACN). The parameters to vary are the baud rate, propagation delay, number of transmitted packets and MTU of each packet.

4.4.1 Pre-Attacks Power System Security Evaluation

In order to clearly present our evaluation of the power system health, we study different power components deployed over the 24-substations. The polling requests (a read command) from the CC to different substations' RTUs are initiated every 5 seconds. Upon receiving the request, each RTU acknowledges the request and starts the process of gathering field measurements. Then each RTU prepares to send the measurement value packets over the wide area network. Similarly, once the CC receives these packets from the RTU, the CC sends an acknowledgment to each respective RTU. The sent power system measurements include active and reactive line power (LineMW, LineMVR), bus voltage and angle (BusPUVolt, BusRad), generator active and reactive power (GenMW, GenMVR) and voltage (GenVolt), load active and reactive power (LoadMW, LoadMVR), and transformer tap ratio (LineTap). In addition, the operator performs control actions in order to balance the demand-supply of power. These actions include changing the status (open/close) of circuit breakers connected to various power system components, such as transmission lines (LineStatus), generators (GenStatus), loads (LoadStatus), transformers (modeled as LineStatus) and shunt capacitors (SSStatus).

4.4.2 Post-Attacks Power System Security Evaluation

In this scenario, we monitor the behavior of the power system as discussed in the previous subsection under a malicious command injection attack. Detailed analysis of our approach provides a quantitative basis for standardized security metrics. Closely observing and utilizing these metrics improve our ability to understand, control, and better defend against cyber-attacks. Multiple metrics from different perspectives are usually needed in order to detect and identify the real threats. We formulate the following cyber-physical security metrics using our co-simulator [14]:

1. System Susceptibility Metric: This system construction metric reflects a way to minimize the number of access points to system critical functions and components. This metric is a direct consequence of identification and verification of suspicious activities (data and command transmission) on the power system components, including the critical components.

2. Access Points Metric: The goal of utilizing this metric is to minimize the amount of I/O and system process visibility to an attacker. This metric is a direct consequence of detecting malicious activities on different access points throughout the integrated system.

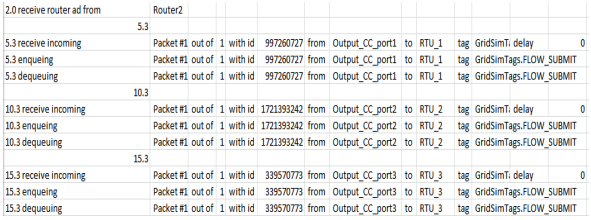
3. Threat Capability Metric: Minimize useful insight into system operations in the sense that data observed at one time by the attacker may or may not be similar or consistent with data observed at another time. This dynamic metric helps to protect the system against targeted attacks.

5 Discussion

In this section, we discuss the security and performance analysis of our approach along with its limitations.

5.1 Security Analysis

The security analysis of the integrated cyber-physical system involves a discussion on the communication network as well as the power system security, which ultimately concludes whether the current state of the power system is secure or not. The proposed approach is capable of preventing and detecting the malicious commands that target different power components at the substation. The adversary can either send a malicious command to the substation's RTU or alter a legitimate command that was sent by the control center over the insecure network. The cyber-physical security metrics, discussed in the previous section, are able to identify and detect the malicious activities performed by the adversaries. We consider a 24-substation power system with 42 buses, 62 lines, 8 generators, 27 loads, 6 transformers, and 9 shunt capacitor banks. Tables 2, 3, and 4 represent the system susceptibility metric, access points metric and threat capability metric, respectively, for our power system case study. The system susceptibility metric provides an attack probability (Low, Moderate, High, and Critical) on different power components: buses, generators, loads, transformers and shunt capacitors. The access points metric records the severity level (Low, Moderate, High, and Critical) of each access point across the communication network and the power system including the substation RTU, control center port and routers. Numbers mentioned in Table 2 and 3 represent the identity number of the component in the considered topology of the communication network and the power system case with 24 substations. The threat capability metric



2.0 receive router ad from	Router2											
5.3												
5.3 receive incoming	Packet #1	out of	1	with id	997260727	from	Output_CC_port1	to	RTU_1	tag	GridSimTa	delay 0
5.3 enqueing	Packet #1	out of	1	with id	997260727	from	Output_CC_port1	to	RTU_1	tag	GridSimTags.FLOW_SUBMIT	
5.3 dequeuing	Packet #1	out of	1	with id	997260727	from	Output_CC_port1	to	RTU_1	tag	GridSimTags.FLOW_SUBMIT	
10.3												
10.3 receive incoming	Packet #1	out of	1	with id	1721393242	from	Output_CC_port2	to	RTU_2	tag	GridSimTa	delay 0
10.3 enqueing	Packet #1	out of	1	with id	1721393242	from	Output_CC_port2	to	RTU_2	tag	GridSimTags.FLOW_SUBMIT	
10.3 dequeuing	Packet #1	out of	1	with id	1721393242	from	Output_CC_port2	to	RTU_2	tag	GridSimTags.FLOW_SUBMIT	
15.3												
15.3 receive incoming	Packet #1	out of	1	with id	339570773	from	Output_CC_port3	to	RTU_3	tag	GridSimTa	delay 0
15.3 enqueing	Packet #1	out of	1	with id	339570773	from	Output_CC_port3	to	RTU_3	tag	GridSimTags.FLOW_SUBMIT	
15.3 dequeuing	Packet #1	out of	1	with id	339570773	from	Output_CC_port3	to	RTU_3	tag	GridSimTags.FLOW_SUBMIT	

Fig. 5: Event logs maintained at the intermediate routers.

keeps the details of suspicious threats, such as malicious source or destination IP, and altered data or commands. Table 4 represents only the suspected records filtered by the IDS or the operator, which helps to make and add new rules to the IDS for strengthening the detection of such events or actions in the future. There were one data threat suspect on control center port 10, and 3 commands threat suspect on RTU 6, 16 and 24, respectively.

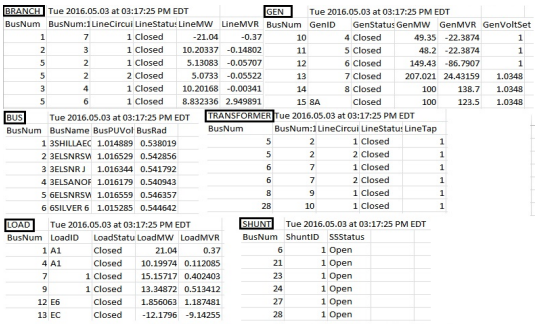
Our approach also maintains event logs of the activities performed at the intermediate routers, substation RTUs and the control center. A sample event log at an intermediate router is shown in Figure 5. Also, whenever an adversary injects a malicious command into the communication network, the IDS deployed at the substation sends an alert to the control center. Synthetic meta-data for different parameters of the power system components is shown in Figure 6, which consists of lines (bus number to and from, line circuit, line status, line MW and line MVR), buses (nus number, bus name, bus per unit voltage and bus angle in radius), generators (bus number, generator ID, generator status, generator MW, generator MVR and generator voltage set), loads (bus number, load ID, load status, load MW and load MVR), transformers (bus number to and from, line circuit, line status and line tap) and shunt capacitors (bus number, shunt ID and shunt status). An operator responsible for coordinating and controlling the power system can simulate the command and observe the real-time impact of the command. An example is shown in Figure 7 where a malicious command targets the opening of a generator breaker. When the command is injected into the power system, the breaker status changes from "closed" to "open". This unexpected and undesirable operation may result in

TABLE 2: System Susceptibility Metric

Components	Low	Moderate	High	Critical
Bus	1-12, 18, 35	17, 13-16, 37-42	20-23, 25-34	19, 24, 36
Generator	2-4	5	7-8	1, 6
Load	3-10, 26	1-2, 22-24	11-20	21, 25, 27
Transformer	2-5	1	-	6
Shunt	1-3	5-9	-	4

TABLE 3: Access Points Metric

Components	Low	Moderate	High	Critical
Substation RTU	1-4	5, 7-14	16-23	6, 15, 24
CC Port	1-9, 11-18	19-24	10	-
Router	1	-	2	-



BRANCH Tue 2016.05.03 at 03:17:25 PM EDT

BusNum	BusNum:1	LineCircui	LineStatu	LineMW	LineMVR
1	7	1	Closed	-21.04	-0.37
2	3	1	Closed	10.20337	-0.14802
5	2	1	Closed	5.13083	-0.05707
5	2	2	Closed	5.0733	-0.05522
3	4	1	Closed	10.20168	-0.00341
5	6	1	Closed	8.832336	2.949891

GEN Tue 2016.05.03 at 03:17:25 PM EDT

BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
10	4	Closed	49.35	-22.3874	1
11	5	Closed	48.2	-22.3874	1
12	6	Closed	149.43	-86.7907	1
13	7	Closed	207.021	24.43159	1.0348
14	8	Closed	100	138.7	1.0348
15	8A	Closed	100	123.5	1.0348

BUS Tue 2016.05.03 at 03:17:25 PM EDT

BusNum	BusName	BusPUVol	BusRad
1	3SHILLAEC	1.014889	0.538019
2	3ELSNRSW	1.016529	0.542856
3	3ELSNR J	1.016344	0.541792
4	3ELSANOF	1.016179	0.540943
5	6ELSNRSW	1.016559	0.546357
6	6SILVER 6	1.015285	0.544642

TRANSFORMER Tue 2016.05.03 at 03:17:25 PM EDT

BusNum	BusNum:1	LineCircui	LineStatu	LineTap
5	2	1	Closed	1
5	2	2	Closed	1
6	7	1	Closed	1
6	7	2	Closed	1
8	9	1	Closed	1
28	10	1	Closed	1

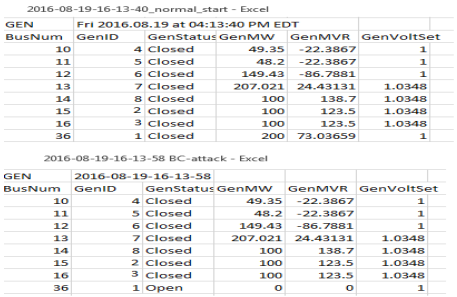
LOAD Tue 2016.05.03 at 03:17:25 PM EDT

BusNum	LoadID	LoadStatu	LoadMW	LoadMVR
1	A1	Closed	21.04	0.37
4	A1	Closed	10.19974	0.112085
7	1	Closed	15.15717	0.402403
9	1	Closed	13.34872	0.513412
12	E6	Closed	1.856063	1.187481
13	EC	Closed	-12.1796	-9.14255

SHUNT Tue 2016.05.03 at 03:17:25 PM EDT

BusNum	ShuntID	SSStatus
6	1	Open
21	1	Open
23	1	Open
24	1	Open
27	1	Open
28	1	Open

Fig. 6: A sample meta-data for different parameters of the power system components.



2016-08-19-16-13-40_normal_start - Excel

GEN Fri 2016.08.19 at 04:13:40 PM EDT

BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
10	4	Closed	49.35	-22.3867	1
11	5	Closed	48.2	-22.3867	1
12	6	Closed	149.43	-86.7881	1
13	7	Closed	207.021	24.43131	1.0348
14	8	Closed	100	138.7	1.0348
15	2	Closed	100	123.5	1.0348
16	3	Closed	100	123.5	1.0348
36	1	Closed	200	73.03659	1

2016-08-19-16-13-58 BC-attack - Excel

GEN 2016-08-19-16-13-58

BusNum	GenID	GenStatus	GenMW	GenMVR	GenVoltSet
10	4	Closed	49.35	-22.3867	1
11	5	Closed	48.2	-22.3867	1
12	6	Closed	149.43	-86.7881	1
13	7	Closed	207.021	24.43131	1.0348
14	8	Closed	100	138.7	1.0348
15	2	Closed	100	123.5	1.0348
16	3	Closed	100	123.5	1.0348
36	1	Open	0	0	1

Fig. 7: Legitimate vs. malicious command to open a generator breaker (Bus number 36, generator ID 1).

the shedding of electrical load since other generators in the system may not be able to respond to sudden loss in time.

5.2 Performance Analysis

We developed an experimental setup with a co-simulator [24]. The co-simulator uses JDK1.7 with JADE, MATLAB and PowerWorld to simulate scenarios between the control center and the substation RTUs. Table 5 describes the selected ranges of communication parameters for our simulation. The co-simulator inherits the functionalities of Java-based GridSim [4], which is a toolkit for resource modeling that provides a rich functionalities for implementing the communication network with a specific topology between the nodes, and supports C37.118 protocol for packets with message passing. Figure 8 shows the simulation in real-time, where communication traffic generated by each substation to the control center has its own data rate. If there is a delay in sending a command by the control center to a substation, the communication traffic (blue dots) becomes slow as compared to other substations. Similarly, if executing a command results in opening a breaker at a substation, the co-simulator can easily detect which breaker was recently opened and the operator can check whether it was a legitimate operation.

5.2.1 *Overhead*

The overhead generated by the proposed approach includes packet scans by the IDS and command simulation by the operator if the IDS flags the command as malicious.

5.2.2 *Scalability*

The proposed approach can detect single as well as multiple malicious commands targeting power system components.

TABLE 4: Threat Capability Metric

Threat Suspect	Source IP	Destination IP	Timestamp	Data Type	Packet Size (Octets)
CC Port-10	192.168.0. 3	192.168.0.7	23-Oct-16, 10:15:27	substation data	255
RTU-6	192.168.0.7	192.168.0.13	31-Oct-16, 21:32:11	command "open Gen 6"	125
RTU-16	192.168.0.7	192.168.0.23	5-Nov-16, 11:45:37	command "open Load 21"	127
RTU-24	192.168.0.7	192.168.0.31	10-Nov-16, 18:10:23	command "open Trans 6"	122

TABLE 5: Parameters for Simulation Setup

Parameters	Range Value	Unit
Baud Rate	100-9600	bits/s
Propagation Delay	10-500	ms
MTU/Packet Size	50-500/150-800	bytes
Number of packets	1-5	–

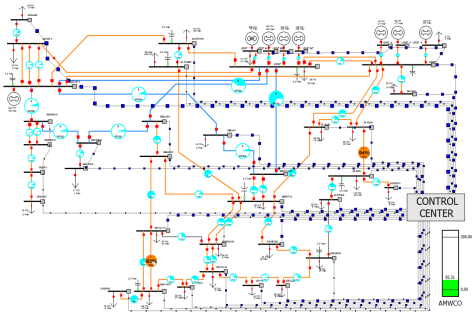


Fig. 8: Power system visualization by co-simulator integrated with communication network.

This work specifically tested in a real power system environment, which was having 24 substations involving 42 buses. This is the reason why we modeled and simulated the idea with 42-bus system. However, the simulator can easily adopt and support several hundred buses based system considering the fact that PowerWorld simulation supports more than 10,000 buses [24].

5.2.3 Accuracy

The accuracy of the proposed scheme depends on the ability of the IDS to detect suspicious commands based on their behavior, target, action and timing. In general, the proposed approach supports high accuracy because the effect of each suspicious command is first analyzed using a co-simulator. Then the output is presented to the operator who makes an executive decision to accept or reject the command based on that information. The power system analysis output includes a plot of the total system electric load over time and the calculated System Aggregate Megawatt Contingency Overload (SysAMWCO) for each timestep. The SysAMWCO is a system-level power system security metric. A transmission line AMWCO is equal to the sum of megawatts of overload under a given set of contingencies. If a line is never overloaded under a postulated set of contingencies, the AMWCO is zero. The SysAMWCO corresponds to the sum of the AMWCOs for all the transmission lines in the system:

$$SysAMWCO = \sum_{\forall line} AMWCO_{line},$$

where the AMWCO for each line is defined as the product of the aggregate percentage contingency overload (APCO) and the MVA thermal rating of the line:

$$AMWCO_{line} = APCO_{line} \times MVA\ Rating_{line}.$$

In turn, the APCO for each line is calculated by summing the percent overload for all contingencies that overload a specific branch:

$$APCO_{line} = \sum_{contingencies} (\%\ overload - 100).$$

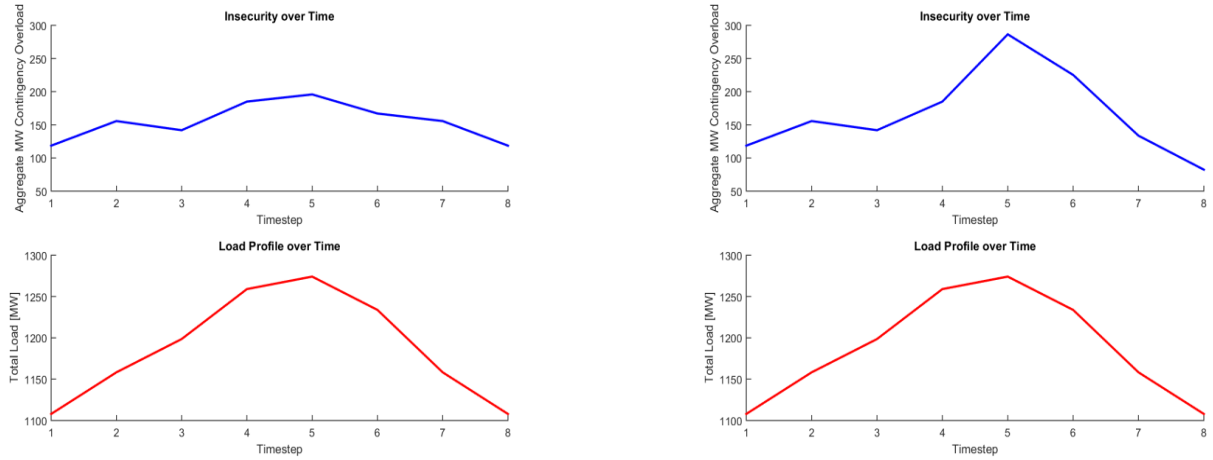
The co-simulator is highly accurate in its ability to determine the attack status (attack versus no attack) of the grid because the SysAMWCO is an efficient and reliable metric that always indicates the presence of the attack. Note that the SysAMWCO can also increase if there was an outage in the power system for other reasons, for example a major storm that damages power lines, or if there is a blackout. Therefore, it is important to also rely on information from the IDS in order to know if it's due to a cyber-attack or any normal power system reasons. Figure 9 compares the actual SysAMWCO against the forecasted SysAMWCO over a period of 40 seconds as the total system load initially increases and then decreases. Using the current-day forecasted load, we simulate the system behavior assuming no cyber-attack. This forecasted SysAMWCO fluctuates with the load but is relatively stable. In real-time operations, a malicious command attack occurs at timestep 5 (transition 4 to 5 in Figure 9). Suddenly, the SysAMWCO jumps to nearly 300. This large deviation from the forecasted SysAMWCO signals the presence of a malicious command attack.

5.2.4 Robustness

The proposed approach is robust, which maintains the accuracy of the power system even with erroneous input, such as malicious commands. In the general case, the malicious command is flagged as suspicious by the IDS. Even if the IDS does not detect the malicious command and the command is executed on the real system, our approach can detect the power system disturbance and report the effect to the operator, who can take appropriate actions (such as sending other control commands) to diminish the impact of the previously executed malicious command.

5.2.5 Execution and Response Time

Our co-simulator simulates normal operations for 8 timesteps using the current-day next 40 seconds load forecast. Each timestep represents a 5 seconds interval, and the generated output for each iteration is stored in a file. The co-simulator runs faster than real-time in the sense that during real-time operation, the system compares the actual



(a) Normal operation.

(b) Malicious command injection operation.

Fig. 9: Detecting malicious operation at timestep 5 by comparing the SysAMWCO of the malicious operation against the SysAMWCO of forecasted normal operation.

output against the simulated output parameters (AMWCO and other system metrics of measurements). Using our co-simulator, each output file is generated in less than 3 seconds, which is important in ensuring the fast response time of the power system operator.

5.3 Limitations

The limitation of the proposed approach is that it has only been tested using single and sequential malicious attacks. The proposed approach will extend its support in the future against coordinated attacks. Testing multiple attacks is not straightforward, as it involves coordinated attacks targeted infrastructures. This work assesses the impact of malicious command attacks on the power system, which itself involves a large piece of work: modeling malicious command attacks, generating new IDS rules, and building and implementing a new cyber-physical co-simulator using Java, JADE, MATLAB and PowerWorld. Here, the idea is to model the behavior of cyber-attacks into the power system behavior so that the operator sitting at the control center can understand that something is malicious and trace back the malicious activities even when the IDS does not detect completely. This probably is very difficult in the case of coordinated attacks, as the IDS, deployed at substations, will not be able to catch if something is malicious at operator's end, say a phishing activity or a botnet (which are generally a part of coordinated attacks). A coordinated attack comprises of comprising operator's system, stealing devices' and VPN login credential, targeting DDoS attack on communication devices, such as mobile, landline, or communication node, i.e., router, updating firmware, and sending malicious commands and perform other actions.

6 Conclusions and Future Directions

The paper presents an approach using a unique and novel co-simulator to understand the potential impact of malicious command-based cyber-attacks on the power system. The generated output files, metrics and graphs help the operator to understand changes in power system behavior in the presence of cyber-attacks. The detection of a malicious command takes place in real-time, and the operator can quickly respond to protect the system from malicious events in order to prevent cascading failures and eventually blackouts. In the future, we will test this co-simulator on significantly larger power system with a large number of communication network nodes. The work will also extend the proposed approach to understand the impact of coordinated attacks on the power system.

References

[1] A. Abur and A. G. Exposito. In *Power System State Estimation: Theory and Implementation*, vol. 24, CRC Press, 2010.

[2] Comprehensive analysis report on ukraine power system attacks, 2016. Anity Labs, http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks.

[3] A. Ashok, A. Hahn, and M. Govindarasu. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of Advanced Research*, 5(4):481–489, 2014.

[4] R. Buyya and M. Murshed. GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing. *Concurrency and Computation: Practice and Experience*, 14(13):1175–1220, 2002.

[5] CEN-CENELEC-ETSI smart grid coordination group, smart grid information security. http://www.energynetworks.org/assets/files/electricity/engineering/Standards/SGCG%20Reports%20071014/SGCG_WGSGIS_Sec0078_INF_ReportforComments.pdf.

[6] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen. Smart attacks in smart grid communication networks. *IEEE Communications Magazine*, 63(1):3–18, 2014.

[7] Oledump.py, 2015. https://blog.didierstevens.com/programs/oledump-py.

[8] ENISA, smart grid security, annex ii. security aspects of the smart grid, 2012. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf.

[9] S. Etigowni, D. Tian, G. Hernandez, S. Zonouz, and K. Butler. CPAC: securing critical infrastructure with cyber-physical access control. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ACSAC '16, pages 139–152, Los Angeles, California, 2016.

[10] Cyber security of the smart grids, expert group on the security and resilience of communication networks and information systems for smart grids, european commission. http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=1761&usg= AFQjCNFj5NxVMnOeyjXWVa0nWR4ZV_aUpA.

[11] T. Godfrey, S. Mullen, R. C. Dugan, C. Rodine, D. W. Griffith, and N. Golmie. Modeling smart grid applications with co-simulation. In *Proceedings of the IEEE International Conference on Smart Grid Communications*, SmartGridComm, pages 291–296, Gaithersburg, USA, 2010.

[12] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu. Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*, 4(2):847–855, 2013.

[13] A. Hahn and M. Govindarasu. Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, 2(4):835–843, 2011.

[14] J. Hughesa and G. Cybenkob. Three tenets for secure cyber-physical system design and assessment. In *Proceedings of the SPIE Defense and Security*, pages 1–5, Baltimore, USA, 2014. SPIE.

[15] Interoperability and cyber security plan, NRECA CRN smart grid regional demonstration, grant DE-OE-0000222. https://www.smartgrid.gov/files/Interoperability_Cyber_Security_ Plan_NRECA_CRN_Smart_Grid_Re_201001.pdf.

[16] Killdisk and blackenergy are not just energy sector threats, 2016. https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats.

[17] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry. Towards a framework for cyber attack impact analysis of the electric smart grid. In *IEEE International Conference on Smart Grid Communications*, SmartGridComm, pages 244–248, Gaithersburg, USA, 2010.

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

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

[20] NIST framework and roadmap for smart grid interoperability standards, office of the national coordinator for smart grid interoperability, nist special publication 1108. https://www.nist.gov/sites/default/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf.

[21] Introduction to NISTIR 7628 guidelines for smart grid cyber security, cyber security working group, sep. 2010. https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf.

[22] Black energy: The committed destructors strike again, 2016. https://business.kaspersky.com/black-energy/5091.

[23] The role of dsos in a smart grid environment, european commission, dg ener, amsterdam/rotterdam, 23 april 2014. https://ec.europa.eu/energy/sites/ener/files/documents/20140423_dso_smartgrid.pdf.

[24] N. Saxena, V. Chukwuka, L. Xiong, and S. Grijalva. CPSA: a cyber-physical security assessment tool for situational awareness in smart grid. In *Proceedings of the ACM CCS workshop CPS-SPC*, pages 69–79, Dallas, USA, 2017.

[25] N. Saxena and S. Grijalva. Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication. *IEEE Transactions on Industrial Informatics*, 13(3):1482–1491, 2017.

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

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

[28] Suricata - open source network threat detection engine. https://suricata-ids.org.

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

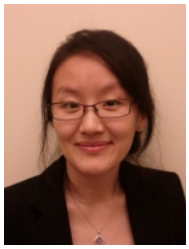
[30] J. Wei and D. Kundur. A flocking-based model for dos-resilient communication routing in smart grid. In *Proceedings of the Global Communications Conference (GLOBECOM)*, pages 3519–3524, Anaheim, USA, 2012. IEEE.

[31] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, 14(4):998–1010, 2012.

[32] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, Eul G. Im, Z. Q. Yao, B. Pranggono, and H. F. Wang. 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)*, pages 1–8, Hangzhou, China, 2012. IEEE.

[33] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li. A denial of service attack in advanced metering infrastructure network. In *Proceedings of the IEEE International Conference on Communications*, pages 1029–1034, Sydney, Australia, 2014. IEEE.

Netesh Saxena is currently an Assistant Professor in the Department of Computing and Informatics at Bournemouth University, United Kingdom. Prior to this, he was with the Georgia Institute of Technology, USA and the State University of New York (SUNY) Korea, South Korea as a Post-Doctoral Researcher, and a Visiting Scholar at Stony Brook University, USA. He earned his PhD from IIT Indore, India. He was also a DAAD Scholar (Germany) and TCS Scholar (India). He is an IEEE senior member and a member of the ACM.



Leilei Xiong received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, IL, USA, in 2007 and 2009, respectively. She is currently working toward the Ph.D. degree at the Georgia Institute of Technology, Atlanta, GA, USA. From 2009 to 2011, she was a Project Engineer with GE Energy. Her research interests include power system operation and visualization.

Victor Chukwuka is a PhD student in the School of Electrical and Computer Engineering at Georgia Institute of Technology. His areas of research interest include communication system, MIMO, cyber-physical system, and power system dynamics.

Santiago Grijalva is the Georgia Power Distinguished Professor of Electrical and Computer Engineering, and Director of the ACES Laboratory at the Georgia Institute of Technology. Prior to joining Georgia Tech in 2009, he spent 10 years in the power industry, developing of commercial grade algorithms for real-time power system control, optimization, and visualization. He graduated with his M.Sc. and PhD degrees from the University of Illinois at Urbana-Champaign in 1999 and 2002, respectively.