SENSOR VERIFICATION FOR CYBER-PHYSICAL MODELS OF POWER SYSTEMS

An Undergraduate Research Scholars Thesis

by

MEGAN CULLER

Submitted to the Undergraduate Research Scholars program at
Texas A&M University
in partial fulfillment of the requirements for the designation as an

UNDERGRADUATE RESEARCH SCHOLAR

Approved by Research Advisor: Dr. Katherine Davis

May 2018

Major: Electrical Engineering

TABLE OF CONTENTS

Page

ABSTRACT 1

DEDICATION 2

ACKNOWLEDGMENTS 3

NOMENCLATURE 4

CHAPTER

I. INTRODUCTION 5

Background 5
Purpose 7
Literature Review 8

II. METHODS 12

Case Study: 8-Substation Model 13
Simulation Tools 14
False Data Injection Attacks 17
Project Development 18

III. RESULTS 22

Topology Results with CyPSA 23
Real Time Probing Results 24
Sensor Trustworthiness Scores 34

IV. CONCLUSION 37

Scoring Technique 37
Impact 38
Future Work 39

REFERENCES 40

APPENDIX 42

ABSTRACT

Sensor Verification for Cyber-Physical Models of Power Systems

Megan Culler
Department of Electrical Engineering
Texas A&M University

Research Advisor: Dr. Katherine Davis
Department of Electrical Engineering
Texas A&M University

This project explores the ways that data from sensors in power systems can be authenticated by enhancing the security of power systems from a cyber-physical point of view. This is a continuation of the work for the NSF project "CPS: Synergy: Collaborative Research: Distributed Just-Ahead-Of-Time Verification of Cyber-Physical Critical Infrastructure**.**" Adversaries who gain access to a cyber-physical system can cause significant physical damage and financial loss by injecting false data into a sensor node. Identifying adversarial action in a system can mitigate unsafe actions made based off of bad data. The technique presented in this work combines topology analysis with real-time probing to create a measure of trustworthiness of sensors in a system. A previously developed tool called Cyber Physical Security Assessment (CyPSA) gives each node a topology vulnerability score based on the cyber accessibility and potential physical impact should it be compromised. We develop a real-time vulnerability score by simulating attack and non-attack scenarios with PowerWorld. The data from these simulations is processed in MATLAB. Results show improved attack detection over current methods. The measure of trustworthiness developed will improve attack detection in power systems, and it may be used to help prevent a system from entering an unstable state.

DEDICATION

I would like to dedicate this work to my mother, Teresa Jordan-Culler. She has been an inspiration to me and to many others in the STEM field, and I am grateful for her love, encouragement, and passion. She is retiring this year after 37 years of service, and it seems fitting that as her career is ending, mine is just beginning. Thank you for everything you have taught me. I could not have done it without you.

ACKNOWLEDGEMENTS

I would like to thank my research advisor, Dr. Kate Davis, for her support, mentoring, and encouragement throughout the course of this project.

My research group has also been invaluable in helping me learn new software, get a good introduction to relevant background information, and encouragement to pursue conference and publication opportunities.

The work was fulfilled with the help of funding from National Science Foundation under Award #1446471.

NOMENCLATURE

CyPSA	Cyber Physical Security Assessment
HAN	Home Area Network
PLC	Programmable Logic Controller
RAS	Remedial Action Scheme
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
WSN	Wireless Sensor Network

CHAPTER I

INTRODUCTION

Cyber threats are one of the largest threats to the power grid and to utility companies today. While parts of the grid continue to use old equipment that is difficult and expensive to replace or upgrade, we continue to add more connectivity to grid systems for enhanced performance and for meeting government regulations. Cyber-attacks on power systems have the potential to cause widespread damage, and have the additional threat of the ability to be launched from anywhere in the world [1]. The Department of Homeland Security reported that from 2009 to 2014, about 40% of total critical infrastructure cyber incidents occurred in the energy sector [2]. While network security is increasing, the attack surface is also increasing with the development of smart grid technology and devices. It is clear from discussions with real electric utilities that they currently have poor visibility into these problems.

Background

Previous Attacks

One example of the effects that these cyber-attacks can have is the attack on the Ukraine power grid in December 2015. Over 80,000 customers lost power, and manual overrides had to be used for several weeks while traces of the malware remained in the system. The damage could have been much worse but for the quick response of operators to switch to manual mode despite efforts of the attackers to cloak the attack by blinding dispatchers and flooding phone lines to call centers to prevent customers from reporting the blackout [2]. The attacks used a worm called BlackEnergy to take over the system [3].

Attackers gained access to the system by infiltrating the external security perimeter, at which point they were able to damage the Supervisory Control and Data Acquisition (SCADA) system. Having more internal security measures, such as verifying sensor data internally, could help prevent attacks like these even if external perimeters were breached. Attacks can breach either the consumer side, as in false data saying that customers are using more power than they are, which causes a load increase for the utility company and strains their resources, or directly to the power generation side, when malware causes too many switches to be open and overloads critical infrastructure and causes physical damage to a plant or substation.

Another type of attack that should be considered is an insider threat. In 2001, in Australia, a power system controlling a waste treatment plant was attacked through a remote attack by an employee of the company that installed the system [4-6]. The attacker made dozens of attempts before successfully spilling the waste by activating and deactivating valves [6]. The attack caused millions of liters of raw sewage to flow into public areas and local rivers. This example shows directly how attacks on cyber-physical systems can cause destruction and expensive repair.

One final noteworthy attack on a cyber-physical system is that of the StuxNet virus. This attack also targeted the SCADA system by uploading malicious code to Programmable Logic Controllers (PLCs). This action caused physical damage to 20% of Iranian PLC-controlled centrifuges [3]. In this case, although the data from the sensors was accurate, the control units responsible for adjusting parameters in the system was compromised, which caused the system to take unsafe actions.

Current State-of-the-Art

As of now, state-of-the-art cyber-physical verification research has developed coupled infrastructure models that are utilized in the recent framework and toolset for electric power utilities called Cyber-Physical Security Assessment (CyPSA) [7] as well as theoretical ways of verifying that the power system controllers can never take any unsafe action [8]. These solutions have largely focused on the controllers (actuators). Part of this framework that needs more development is how to ensure the trustworthiness of sensor data and how to use sensor data corroboration (from both power and cyber side sensors) to construct a trustworthy view of the cyber-physical state of the system, provide situation awareness, and determine and detect various cyber-attack signatures. Assurance of sensor data quality is critical as this data is ultimately used to construct or enhance models, where those models are further coupled with measurements and used for analyses determine the state of the grid. Thus, understanding both how to account for errors in sensor data and how to use the sensor data itself to detect events is foundational for rigorously analyzing power systems as a cyber-physical system.

Purpose

There are many weaknesses in power systems that could be improved. This project focuses on the way that sensors interact with the whole cyber-physical system in order to improve the security of these utility systems. Sensor data is used to apply and develop techniques that will detect and inform operational decisions in power systems related to predicting hazards, with a focus on cyber-attacks.

The goal of this research project is to understand what can be done with sensor data in a power system environment to help electric power utilities better prepare for, detect, and defend against cyber-attack. Various sensors may offer different methods to improve the security of power system operations. Algorithms developed for this project will determine how reliable data from sensors in different parts of a system are. The power and cybersecurity field will benefit from improved understanding and the development of new techniques of sensor-level defenses against cyber adversaries, which will enhance the current state-of-the-art in power systems. In addition, it will contribute to power system cyber-physical modeling and analysis by helping to develop a more complete view of sensor threat profile and providing insight into how to incorporate the results from this research into existing frameworks for power system cybersecurity risk analysis (i.e., CyPSA).

One of the challenges facing grid security is that power and utility companies are hesitant to reveal details about attacks they have faced, or even reveal when they are attacked. This underemphasizes the significance and prevalence of attacks, leading many to believe that the threats are not severe. In addition, they may not want to reveal how attacks occurred in order to avoid publicizing weaknesses in their system, which hinders companies with similar equipment from protecting against similar attacks. Finally, companies may not want to reveal the existence or severity of attacks in order avoid destroying the confidence of their customers or stakeholders. The compartmentalization of information only compounds the effect of the increasing complexity and dynamic nature of power grids, and the unpredictability of malicious actors [1]. Research that can be conducted on synthetic grids is intended to close the gap between technology and current security practices. We hope that this research will inform the industry of potential vulnerabilities and possible detection and mitigation methods.

Literature Review

In the past, cybersecurity of power systems has largely focused on keeping intruders out of the system entirely. In recent years, there have been advances in prevention, detection, and remediation of attacks. The focus here will be on methods involving sensors and false-data injection attacks.

Most power grids, particularly on the user end, are moving towards system monitoring using wireless sensor networks (WSNs) to aid with smart device technology. Each sensor in and WSN has relatively limited capability and range, but the large network of sensors can provide more detailed information for a lower cost. Many small sensor nodes are desirable due to the lack of wiring needed, cost and power efficiency, redundancy in data, high fault tolerance, and simple installation and maintenance [9, 10]. WSNs are vulnerable to simple attacks such as spoofing, replaying, man-in-the-middle, and eavesdropping in addition to more sophisticated attacks [10]. In addition to the ability to disrupt the larger power system, these attacks make customers vulnerable to the collection of their power-use habits, which can be used for targeted burglary or other crime. WSN topologies include Star, Ring, and Mesh configurations, which are shown in Figure 1.

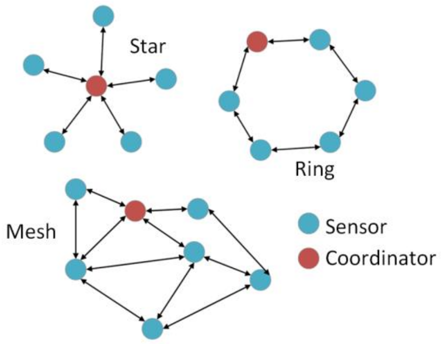


Figure 1. WSN topologies.

In a Star topology, each sensor communicates directly with the base station. In a Ring topology, nodes can only communicate through a specified path. If any link along this path breaks, the whole communication chain breaks down. Finally, Mesh topology allows many nodes to talk with one another, creating multiple communication paths. This method is strongly resistant to communication breakdown due to its redundancies, but these same redundancies make this topology more costly [9]. While this method may be preferred for its stability, the increased number of links provides more opportunities for an adversary to find a path into control nodes of the system. Privacy leakage attacks are a particular threat for WSNs as they are most widely used in Home Area Networks (HANs). Cryptography techniques to protect WSNs are discussed in [10], and state estimation and protection against data injection attacks is discussed in [11].

Continued reliable operation under an attack is important for a cyber-physical system in order to mitigate damage, identify the source of attack, and return the system to safe operation. It is not possible to guarantee the safe operation of a system if we do not know what the current state of the system is. State estimation is a technique which allows operators to construct a full model of the current state of the system from a limited number of sensors. State estimation from sensors spread throughout the system is a complicated problem, and both [12] and [13] develop methods to improve accuracy of state estimation for increased observability of a system. Secure state estimation for power systems under attack is discussed in [6, 11, 14]. Secure and trustworthy state estimation is not possible under all circumstances, including those described in [6]. Defense mechanisms for both stealthy and non-stealthy attacks are shown in [11] through advanced signal processing techniques. Additional intrusion tolerance specific for general cyber-physical systems is developed in [15]. Besides continued operation under attack, it is necessary to take action to return the system to a safe and trustworthy state. Improved remedial action schemes (RAS) are developed in [16] which can increase the speed corrective action taken to maintain system reliability.

There are a variety of novel approaches to identifying which components have been compromised during an attack. This research intends to contribute to the attack detection field, building on some of the work discussed below. [17] discusses device fingerprinting by identifying small differences in operation times for different actions due to physical variations in construction which would be impossible to spoof. Significant changes in the fingerprint of a device could also suggest that the physical component has been infected with malware. Probing techniques which identify compromised components through their response to intentional small disturbances in the system are developed in [18, 19]. Various types of side channel attacks are explored in [20]. Side channel attacks aim to exploit data leakage through measureable responses to the code being run on devices such as bit flipping through the RowHammer attack, device execution time, power dissipation, and electromagnetic emissions. The significance of electromagnetic signal leakage is further developed in [21] as a means to identify the physical location of devices in a power system, and in [3] as a method to confirm the trustworthy operation of PLCs.

These methods and others have made progress in ensuring the resiliency of cyber-physical systems. This research intends to fill some holes in the current research, as well as combine developing techniques to create more robust intrusion detection schemes.

CHAPTER II

METHODS

This research studies sensor data from the perspective of cyber-physical systems security enhancement. Cyber-physical assessment refers to the context of studying the interactions between physical components in the real world and the communications channels through which information, data, and control signals flow. With the rising trend of integrating technology into all parts of our lives, more and more systems can be viewed from a cyber-physical perspective due to their cyber components controlling physical parts of our lives. This can be seen with smart home technology, such as using voice activated controls to turn lights on and off, adjust temperatures, or remotely monitor locks and video feeds.

In this research, we view large scale power grids as cyber-physical systems. The generation plants, solar arrays, wind farms, transmission lines, distribution networks, and load devices represent the physical components. The control units (i.e. PLCs and Remote Terminal Units (RTUs), data transmission networks (wired or wireless), and operator stations make up the cyber components. Sensors form a bridge between the cyber and the physical by measuring physical values and passing this information into the cyber domain via a SCADA system. Figure 2 shows how these elements are connected on a large scale.

It is intended that the work on this project will focus on developing and enhancing data analysis and data processing techniques in a cyber-physical framework to achieve the goal of securing electric power grids from cyber-attacks. In order to make good decisions about the operation of a power grid, analysts need to trust the data on which they are basing their decisions. If this data cannot be verified, poor economic decisions, or even decisions that endanger the stability of the grid, can occur. In the event of a fault, operators need trustworthy data to ensure the resiliency of the power grid to single or multiple contingencies. The view of sensors as bridges between the physical and cyber space makes them crucial components of the system, and motivates our exploration of methods to secure the system through data verification.

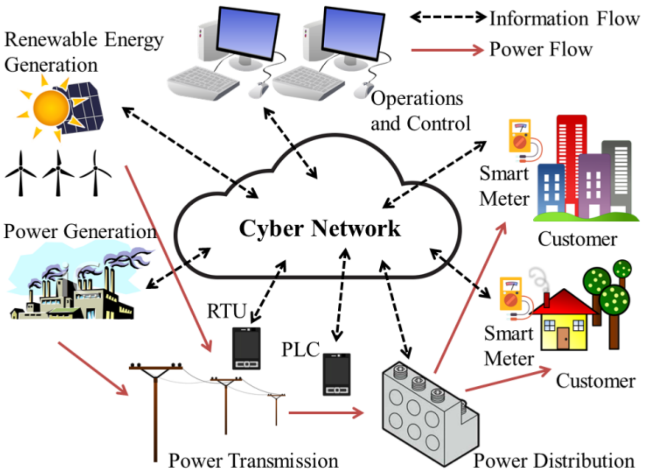


Figure 2. Power grid as a cyber-physical system.

Case Study: 8-Substation Model

Although real power systems can have dozens to hundreds of substations, this simple 8-substation model that we use is a good tool for proof-of-concept research. This model contains eight substations, five of which have generator units. All buses are connected to at least one other bus, and up to five other buses. Six of the buses feed consumer loads. Although there are only eight actual substations, this model provides extended detail at the substation level. Internal substation lines, relays, breakers, firewalls, and routers are all modeled. There are a total of 52 buses in the system, each with their own voltage, angle, real power, and reactive power measurements.

This model was created as a test case for live data feeds connected to SCADA systems. It is not build for state estimation, but it is a full topology case. The relays and breakers represented within the substation are is necessary for accurate cyber-physical modeling, because the relays detect when a fault has occurred based on sensor measurements and trip breakers to prevent physical damage to the system. Protective relays and a control network were later added by an expert in the area based on real utility setups. These protection schemes were based on Schweitzer Engineering Laboratories published best practices [22]. As one of the older PowerWorld test cases, relay models were written externally in JSON files, although PowerWorld now has the capability to import these automatically.

Simulation Tools

PowerWorld

PowerWorld is a simulation tool to visualize, solve, and analyze power system models. Its capabilities include real time simulation, transient stability analysis, and a variety of data processing tools. For this research, PowerWorld is used as a visualization tool for the 8-substation case that was analyzed. In addition, this case was initially set up and solved in PowerWorld in order to find the initial parameters for the real-time probe algorithm development in MATLAB. The variables that were needed from PowerWorld were the Ybus admittance matrix, which defines the impedances on the lines connecting the buses, and the list of slack buses, which helps solve the power flow equations. The power flow equations make sure the load is balanced with the generation, and optimization equations can be used in conjunction with the power flow equations to dispatch power and maximize profit. Data from PowerWorld is used to verify which buses correspond to which substations, and this allows us to set up the attack scenarios correctly. Finally, this software was also used to verify cyber components and connections for CyPSA analysis.

PowerWorld uses oneline diagrams to visualize power systems. Generation and consumption levels are shown, as is the line flow on all transmission lines. Arrows indicate the direction of real and reactive power flow. The oneline for the 8-substation study used in this research is shown in Figure 3, where boxes indicate the different substations.

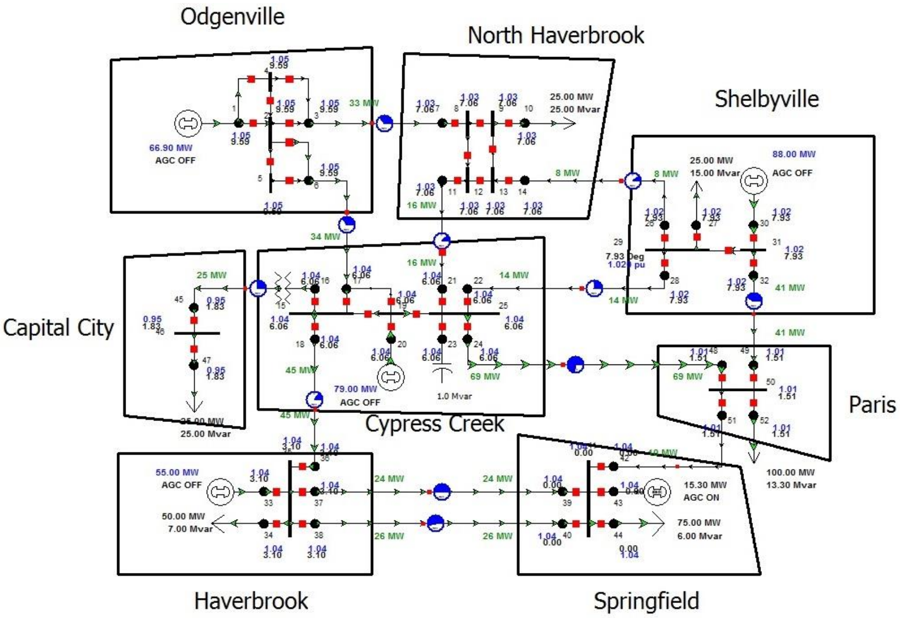


Figure 3. 8-substation model.

MATLAB

MATLAB is a data processing and visualization tool. PowerWorld is capable of solving power flow equations, and it is possible to set up cases in MATLAB that can be sent through SimAuto to PowerWorld to be solved. This method was investigated, but ultimately rejected because it was not necessary to tap into the extensive resources offered by PowerWorld. Rather, MATLAB code previously developed by this research team was used to solve for the necessary power and voltage measurements given the initial parameters about the setup of the system. MATLAB is a tool that specializes in matrix math, which is useful for solving power flow equations, and has special toolboxes that are useful for many electrical engineering applications. In addition to the regular power flow solution code, a “special” power flow solver was developed that allows the simulation of a system under attack by designating “unprotected buses,” which correspond to the substation that the attacker controls. Additional algorithms set up the attack, send the probe through the attacked and un-attacked simulations, and analyze and display the results.

CyPSA (Cyber-Physical Security Assessment)

CyPSA is a multi-platform tool that is used to analyze the vulnerability of different nodes in a power system based solely on the cyber and physical topologies. It is a prime example of the cyber-physical viewpoint discussed earlier. CyPSA’s basic functionality is providing two sets of scores to the user, which are then combined into a single security index for each cyber component in the system. This security index indicates how vulnerable each bus is in the system.

The security index (SI) is the ratio of the performance index (PI) to the cyber cost (CI), as seen in equation 1, where the PI is the severity of an attack and the CI is the difficulty for an attacker to reach a critical asset along path p(i).

$$SI(p(i)) \ = \frac{PI(p(i))}{CC(p(i))} \tag{1}$$

A higher CyPSA score indicates a more damaging, less costly attack path, therefore higher scores indicate more vulnerable assets. CyPSA performs its analysis by calculating the cyber cost based on a certain entry point. The cyber costs for different components can change based on where the point of attack is, so we need to know the cyber entry node when using the CyPSA tool. In a real world situation, the operator would not know what substation might be under attack, so they may choose to perform a CyPSA analysis from many cyber entry nodes with the goal of learning the risk from different attacks. While knowing how vulnerable a component is cannot inform an operator if that component has been compromised, it can be used in conjunction with other methods to determine how likely it is that a system is under attack.

False Data Injection Attacks

There are many types of cyber-attacks that can be perpetrated against a power grid. The one we use for this experiment is an unobservable false data injection attack. In this scenario, an adversary who gains access to a bus in the system will tamper with the data sent to the command center in some way. They may add some sort of fixed or variable offset to the current data being measured. They may replay data from a different day. Or, they may overwrite the data entirely with a simulated data set of their own design. In each of these cases, false data in injected into the system.

The unobservable part of this attack comes into play as follows. If the data injected into the system still allows the power flow equations to be solved, the attack is said to be unobservable, because it still appears that the load and the generation are balanced. Power flow equations are nonlinear, so there may be many solutions for a particular set of parameters, and it will not be obvious to an operator that the solution did not stem from real data.

Attacks like these are dangerous, because they are much harder to detect than observable false data injection attacks. An adversary who attempts this kind of attack may be trying to hide the real state of the system, which they may be manipulating by other means, from the operator, who will then take action (or not take action) based off of the current stable state they believe the system is in. In the meantime, the adversary may be causing real damage to the system. Alternately, their goal may be as simple as making the operator use resources inefficiently. They could manipulate components such that delivering the correct amount of power is much more expensive than it needs to be by introducing more losses into the system. On a more critical level, the false data injection may be indicating to the operator that some action needs to be taken, for example that the generation needs to increase, when in reality the system is already operating close to capacity. In this situation, the adversary makes the operator take unsafe actions because the operator cannot see the true state of the system.

Project Development

The goal of this experiment was to combine a topology analysis with real time probe analysis to determine if sensors in the power grid system were compromised. The topology analysis was performed with the online platform of CyPSA. The real time analysis was performed with MATLAB, using initial variables from PowerWorld. Different probing methods of attack detection were used. All methods were essentially simple residual difference analyses, but various probe parameters and measurement samples were tested to determine the best way to find a compromised substation. The topology scores and real time scores were then tested in a simple weighted multiplicative relationship. In this way, if the CyPSA analysis revealed that a certain substation was very secure, the probing results at that substation are considered less significant than probing results at more vulnerable buses.

The first step performed was to set up sample cases on existing tools. CyPSA was installed and run using the 8-substation model. We picked one substation as the substation under attack, and began the cyber analysis from a node in that substation chosen at random. Cyber connections in the system had to be verified manually before running the CyPSA analysis. We collected data for the cyber cost, performance index, and security index for each bus in the expanded 8-substation case. Buses that were deemed “unreachable” from the cyber entry node do not appear on CyPSA’s list of security indices, so their security index can be considered zero. This is justified because if there is no way to reach an internet-connected relay from a given cyber entry node it is not a security threat.

For the real time probing half of the project, the initial variables from PowerWorld were used to set up two sets of power flow equations to be solved in different ways. The first was set up to run under normal operations. The second was setup so that data from the generator at the attacked substation, as well as the voltage level at another bus within the substation, were both programmed to be significantly lower than normal operation when the system was solved. The first represented the normal operation base case. Since we are interested in how the system behaves under attack, the base case is only used to compute the observed results when the probing occurs. The second simulated a system under attack, meaning some buses were not “protected” from changes in the system, or in other words, the attacker was allowed to control how these buses respond. Under this type of false data injection attack, an operator who views this data may choose to increase generation, which creates the potential of overloading lines.

To see how the system responds to the probe, we use the attacked case to find what the operator expects to see, and the unattacked case to see how the system actually responds to the probe at the uncompromised substations. Finding the expected results from the probe is straightforward. We add the probe signal to the compromised system, and run a normal power flow analysis. This effectively represents what the operator expects to see because they assume the compromised system shows the real values and that they system is responding normally. Calculating the observed results is slightly more complicated for this simulation. First, we assume that the adversary cannot respond in real time to the probing signal, even if they can detect that it was sent. More likely, the probe would not appear to be very different from the normal operation of the system, and the adversary would not know it was anything special. They would not take special action in response to the probe, and they would not change the modifications at the compromised substation. To model this, we can resolve the attacked case again without the probe, and take the values from the compromised substation. However, since the attacker does only controls one substation, the values at the other substations would react normally to the probe sent by the operator. To model this, we add the probe signal to the original unattacked case and resolve the normal power flow equations. The final observed set of measurements is taken as the probed results from the unattacked case at the unattacked -substations, and the non-probed results from the attacked case at the attacked substation. A summary of the real-time probing algorithm can be seen in Figure 4.

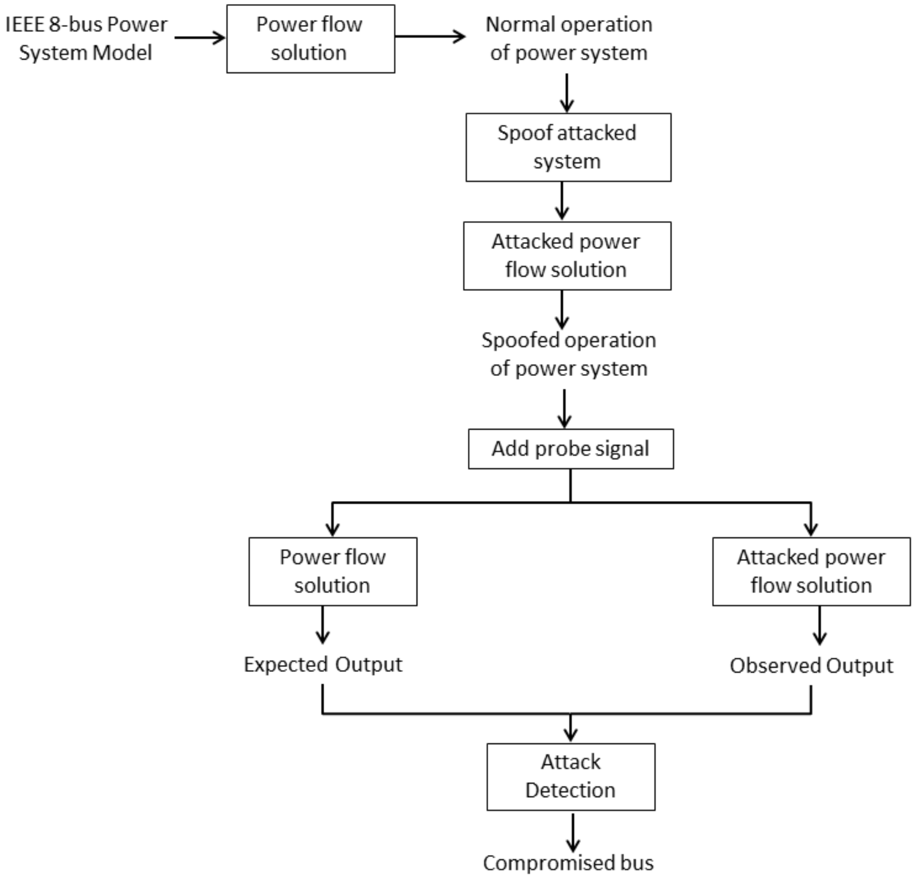

IEEE 8-bus Power System Model
Power flow solution
Normal operation of power system
Spoof attacked system
Attacked power flow solution
Spoofed operation of power system
Add probe signal
Power flow solution
Attacked power flow solution
Expected Output
Observed Output
Attack Detection
Compromised bus

Figure 4. Flowchart depicting real-time probe attack detection.

In summary, we are able to analyze what happens when the system experiences a false data injection attack. We assume the system is under attack and start from the initial “attacked” state. We then send the probe through the system, and reanalyze the system with a non-attacked power flow solution to get the expected values, and with an attacked power flow solution to get the observed values. We then compare the attacked and observed values and look for a threshold difference in the various types of measurements taken between these two as an indication that certain sensor nodes have been compromised.

Finally, the real-time probing and state topology results can be used to create an overall measure of trustworthiness for each sensor in the system. Using information about the cyber-physical layout as well as the real-time results creates a fuller picture of the real security state of the system. In equation 2, we combine the results into the trustworthiness score, V(i), for each node, i, by letting the CyPSA security index, S(i), be a weight by which to emphasize the results from the real-time probing analysis, R(i).

$$V(i) = S(i) * R(i) \tag{2}$$

If a cyber component is not accessible from the attacker’s cyber point of entry, than we do not care what the real-time probe results are at that node because we know the attacker has not compromised that node. If the attacker is in the system, we would expect to see major differences at the compromised substation, and perhaps smaller differences elsewhere. The CyPSA scores allow us to prioritize the nodes that are deemed more accessible and higher value targets.

CHAPTER III

RESULTS

Although the model used represents 8 substations, as described above, there is more detailed modeling of the substations. We can take measurements at multiple buses within the substation for the real time probing, but we need to know which buses represent which substation so the attacks and probes can be properly set up. Table 1 the correspondence of buses to substations, which is data obtained from data tables in PowerWorld.

Table 1. Correspondence of nodes to substations.

Substation Number	Buses
1 (Odgenville)	1-6
2 (North Haverbrook)	7-14
3 (Cypress Creek)	15-25
4 (Shelbyville)	26-32
5 (Haverbrook)	33-38
6 (Springfield)	39-44
7 (Capital City)	45-47
8 (Paris)	48-52

Topology Results with CyPSA

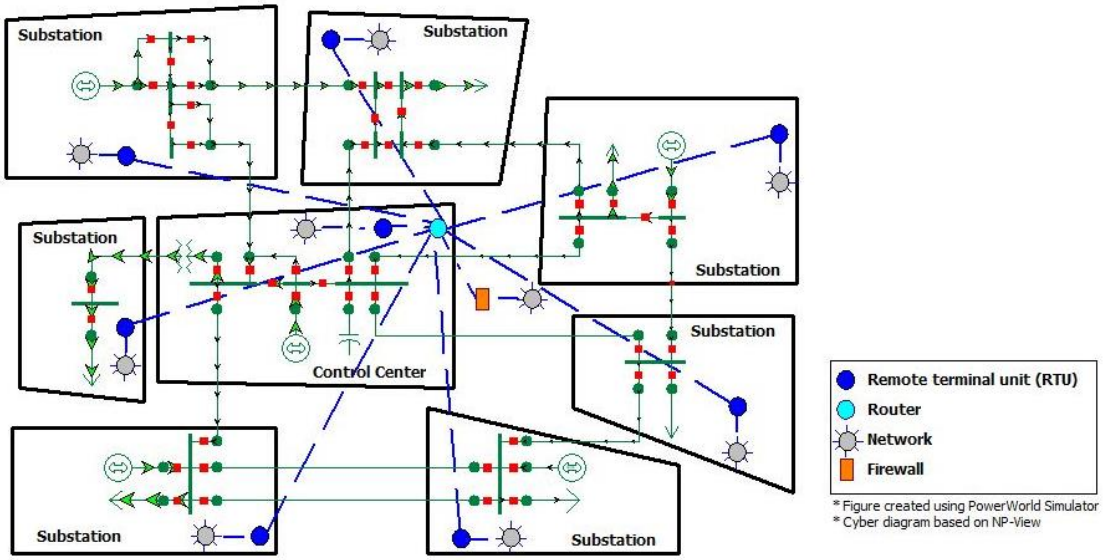
The following data in Table 2 shows the cyber accessibility, physical impact, and overall vulnerability scores for each cyber component accessible from the cyber entry point in the Cypress Creek substation. There is no direct correspondence between cyber components, namely relays and switches, and buses. However, the substation that each part belongs to is known, and we can use that information to correlate the results from CyPSA and the real-time probes.

Table 2. CyPSA scores for 8-substation model for cyber entry at 10.31.1.201.

IP Address	**Performance Index**	**Cyber Cost**	**Security Index**
10.31.1.101	1.38	8.95	0.15
10.31.1.102	2.23	8.95	0.25
10.31.1.103	3.89	8.95	0.43
10.31.1.104	1.38	8.95	0.15
10.31.1.104	1.57	8.95	0.18
10.31.1.201	10.45	44.76	1.17

There are only six communication hardware components that appear to have CyPSA scores. This means that all other components have a cyber cost of infinity, or in other words, they are not accessible from our cyber entry point, which we have chosen to be at the same substation as the compromised station of the real-time probing tests. The performance index for each node is independent of the cyber entry point, and the performance index for all 70 communication devices can be found in Table 3 in the appendix. As expected, the cyber entry node has the highest security index. The other relays that it is connected to are each connected to one or more breakers, which means they can have a bigger impact on the system. There are other cyber devices at the Cypress Creek substation, however, they are not connected to any breakers or to each other, so they cannot have a physical impact on the system if they are compromised.

Since the same data can be visualized in many ways, we created a new oneline diagram for the 8-substation model to show both the cyber and physical connections in PowerWorld. The gray network nodes in Figure 5 represent the relays and switches that are analyzed by CyPSA. These communications components are all IP connected.



* Figure created using PowerWorld Simulator
* Cyber diagram based on NP-View

Figure 5. Oneline diagram with cyber connections shown.

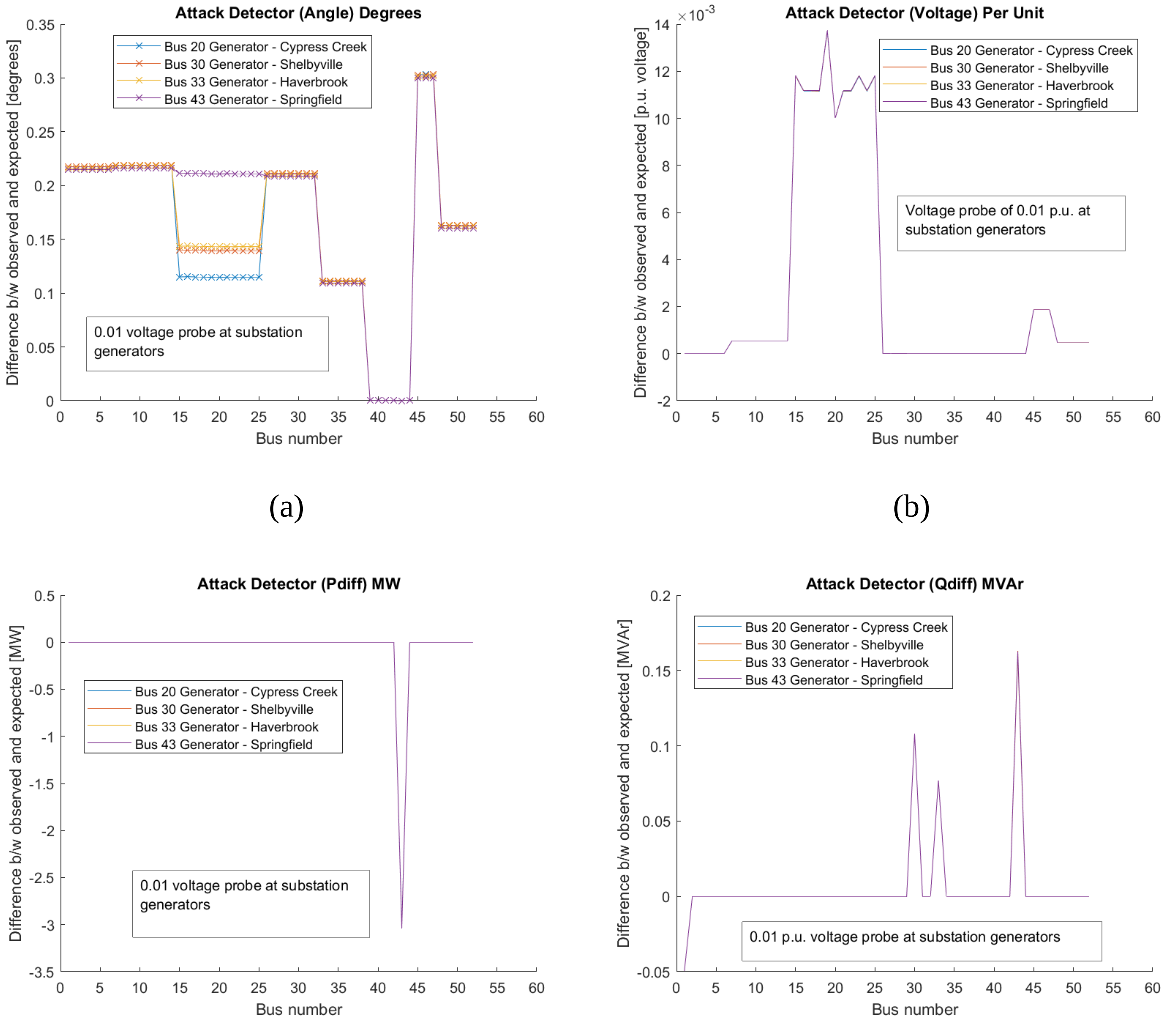
Real Time Probing Results

As described in the methods, the 8-substation case was loaded into MATLAB and solved with a non-transient AC analysis. We set up a simulated attack scenario and solved the power flow to get voltage and power measurements at each bus. The scenario was set up as follows. We set up generator 20 to have a constant 50 MVAr less reactive power than what was actually flowing in the system. Another internal bus was set up to show a voltage of only 80% of the true value in the system. Normally, acceptable limits for bus voltages are set to be between 0.95 and 0.10 p.u. All buses at the same substation as bus 20, Cypress Creek, were assumed to be compromised by the adversary in the attacked simulation, meaning the attacker could control the output at these nodes. The Cypress Creek substation includes buses 15-25. In this attack scenario, an operator would likely increase the generation at Cypress Creek to try to fix the low voltage. Depending on what the state of the rest of the system was, increasing generation could cause transmission line overloads or other faults.

Basic Voltage Probe

The first type of probe tested was a voltage probe. This probe is valid only at pv buses, which means power and voltage levels at the bus are known, and other values are calculated. Generators represent pv buses in systems, because operators control the voltage level and real power output of generators. Because voltage is a known value, we can add the probe signal and solve for the other values. There were five generators in the original case, but one of these was the slack bus for the system, so in order to correctly compute values for the system, we could not probe the slack bus. For each trial, the same probe magnitude was added to each generator individually so that results would show the overall response of the system to a probe rather than relying on a specific relationship between the attacked substation and any other substation. The probes were added one at a time. Some results stayed the same for all probe source locations, while others had different magnitudes of results, though relatively similar shapes.

The first probe tested had a magnitude of 0.01 p.u., which is a low enough value not to make any large instabilities in the system. In general, voltage levels are carefully monitored throughout the system since changes can have a large impact on the power flow. The results, which show the difference between expected and observed measurements of voltage magnitude, voltage angle, real power injected, and reactive power injected at each bus, is seen in Figure 6.

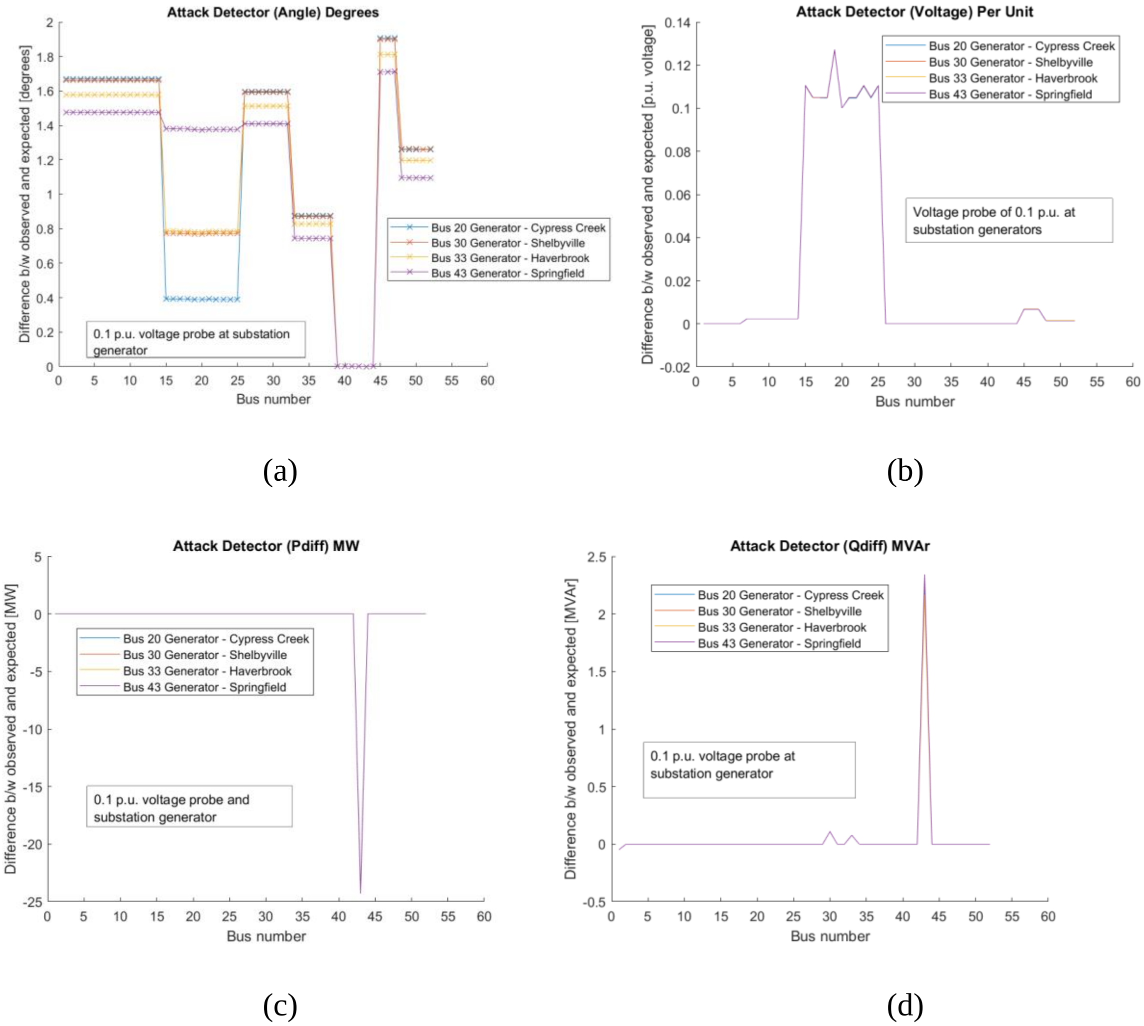


(a) (b)

(c) (d)

Figure 6. Results of voltage probe of 0.01 p.u. for (a) voltage angle, (b) voltage magnitude, (c) real power injected, and (d) reactive power injected at each bus.

These initial results are not very promising. The angle results do not clearly identify the compromised substation. The voltage magnitude results are largest at the compromised substation, but too small to likely be detected in a real systemThe power results indicate something at bus 43, but they are very small compared to the base value of power in the system, and they do not identify the compromised substation either. Differences of less than 1 MVA will be lost in the noise of the system as the load dynamically changes. In order to better analyze the system, we send a slightly larger voltage probe of 0.1 p.u.



(a)

(b)

(c)

(d)

Figure 7. Results of voltage probe of 0.1 p.u. for (a) voltage angle, (b) voltage magnitude, (c) real power injected, and (d) reactive power injected at each bus.

The results in Figure 7 indicate an abnormality at bus 43, which is seen in the results for Figure 7(c), and (d). Figure 7(a) shows the same shape of results for any probe start location, but different magnitudes. There are significant changes at the compromised substation, but there are also significant changes at other substations. It’s possible that the voltage results from Figure 7(b) would reveal the compromised substation correctly, but the magnitude of these results depends highly on the magnitude of the probe, which should be as small as possible. It would not be good practice to test a voltage probe larger than 0.1 p.u., because acceptable voltage limits for each bus are typically set between 0.95 and 1.1 p.u. A probe large than 0.1 p.u. would make the probe source bus immediately jump beyond its acceptable limits. Because the results from the voltage probe could not strongly identify the compromised substation, and because changing voltage levels can be risky, voltage probes are not the best way to identify bad data in the system.

Real Power Probe

A real power probe is an acceptable and reasonable form of probing at a pv bus because generator power output levels are adjusted all the time. As long as the generator that is probed is not already operating at capacity, a small real power probe will not be dangerous to the system. In addition, although load and generation must always be balanced, and we assume a constant load in this model, very small changes for short periods of time will not make the system unstable. In a real system, the load is constantly changing, and although loads can be forecasted with reasonable accuracy, there will almost always be small mismatches in the system. The probe signal, which is sent only for a very short period of time, will not impact the stability of the system. The first real power probe that is tested on the model has a magnitude of 1 MW. As seen in Figure 8, this probe is tested at all generators except the slack bus.

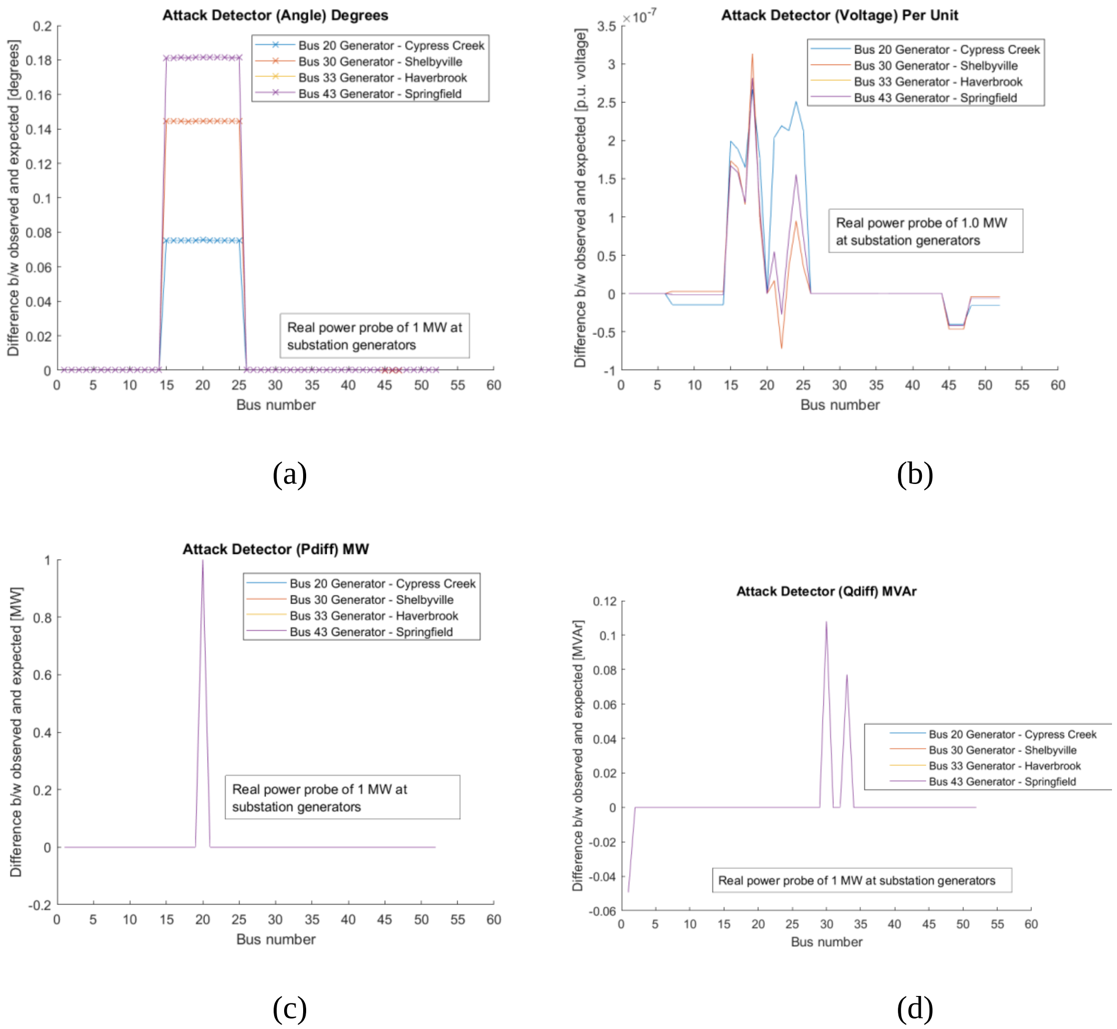
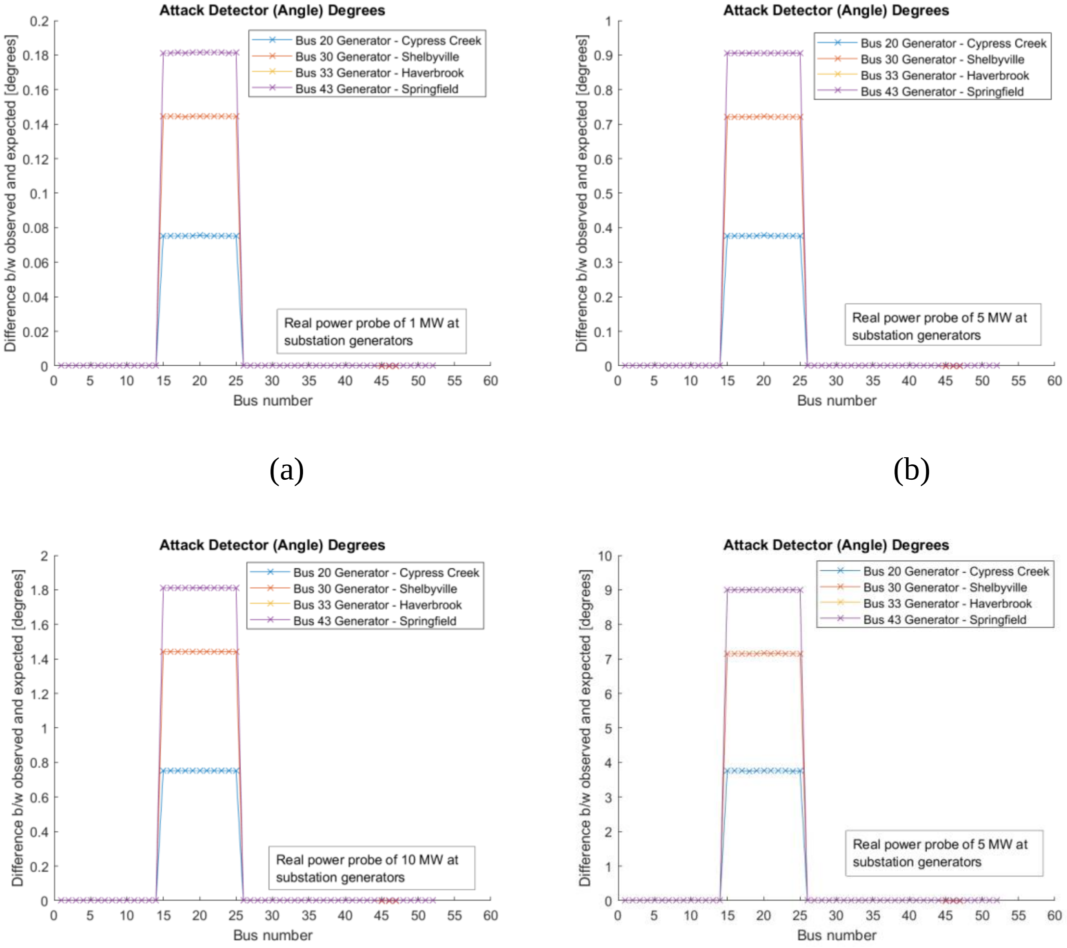


Figure 8. Results of real power probe of 1.0 MW for (a) voltage angle, (b) voltage magnitude, (c) real power injected, and (d) reactive power injected at each bus.

Like the voltage probe, the results for reactive power at each bus are negligible compared to system noise and base values, as are the results for voltage magnitude. However, we can see that our real power probe appeared in the real power results at bus 20, which is one of the compromised buses. These results were the same no matter where the probe was launched from. Finally, in Figure 8(a), we can see that the difference in voltage angle very clearly identifies the compromised substation. The only place where there is a difference between the expected and observed results is at the compromised substation. Although the magnitudes of the angle results are small, the voltage angle is a very tightly controlled value, so this would be an observable difference in a real system. We can look at the results with different sizes of real power probes in Figure 9.



(a)

(b)

(c)

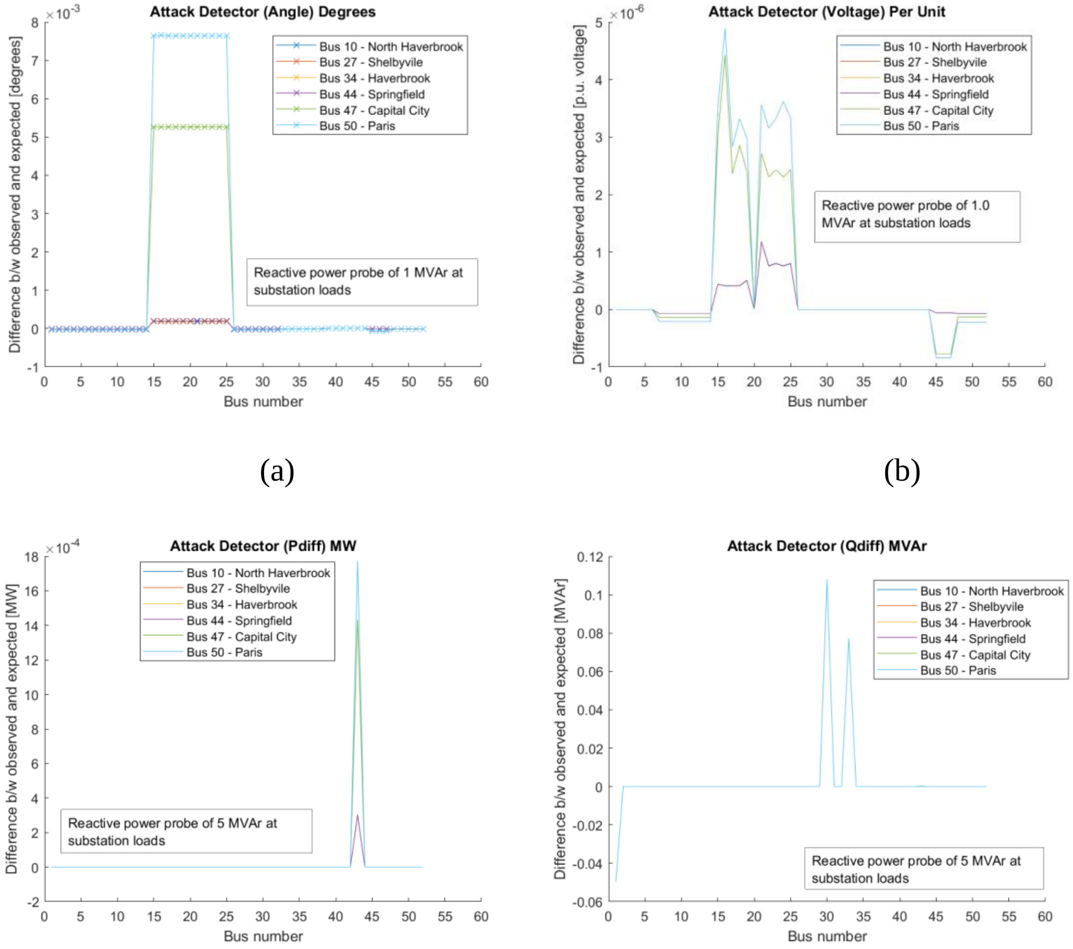
(d)

Figure 9. Voltage angle results of real power probe of (a) 1.0 MW, (b) 5.0 MW, (c) 10.0 MW, and (d) 50.0 MW.

The shape of the results curve looks the same for all magnitudes of the probe, but the magnitude of the results changes proportionally to the probe. The larger probes create clearer evidence that the substation is compromised without producing more noise at other substations, but care should be taken not to inject too much real power. Large differences between generation and load can make the system unstable. The acceptable size of a probe depends on the size of the system and the total amount of generation and load, as well as how fast the load is fluctuating.

Reactive Power Probe

The final set of probes that may give insightful results is reactive power probes at pq buses. Specifically, we model the probe as an increase in reactive power at a load bus. This is reasonable for a real system because we can turn capacitor banks on or off at the load, which will change the reactive power absorbed at that bus. Unlike generator buses, pq buses can control how much reactive power is being absorbed, but the voltage levels must be solved for. This type of probe corresponds to the load changing at a substation. In a real system, the load is constantly changing, so it may seem that this is something the attacker would account for. However, in this test, we assume that the load is constant and that the amount of time we are looking at the system is short. During this time, the small, short-lived probe is sent. If it were an actual change in load, it is unlikely that it would turn on and off so quickly. We can be reasonably confident that this is a realistic type of probe, and that a real system would behave similarly to the model that we have simulated. Like the previous cases, the probe is iteratively sent from different locations. However, in this case, rather than sweeping through the different generators, we sweep through the different loads. There are six substations with loads in this case, and there is no load at the compromised substation. To start, we analyze all measurements for a reactive power probe values of 1.0 MVAr in Figure 10.



(a)

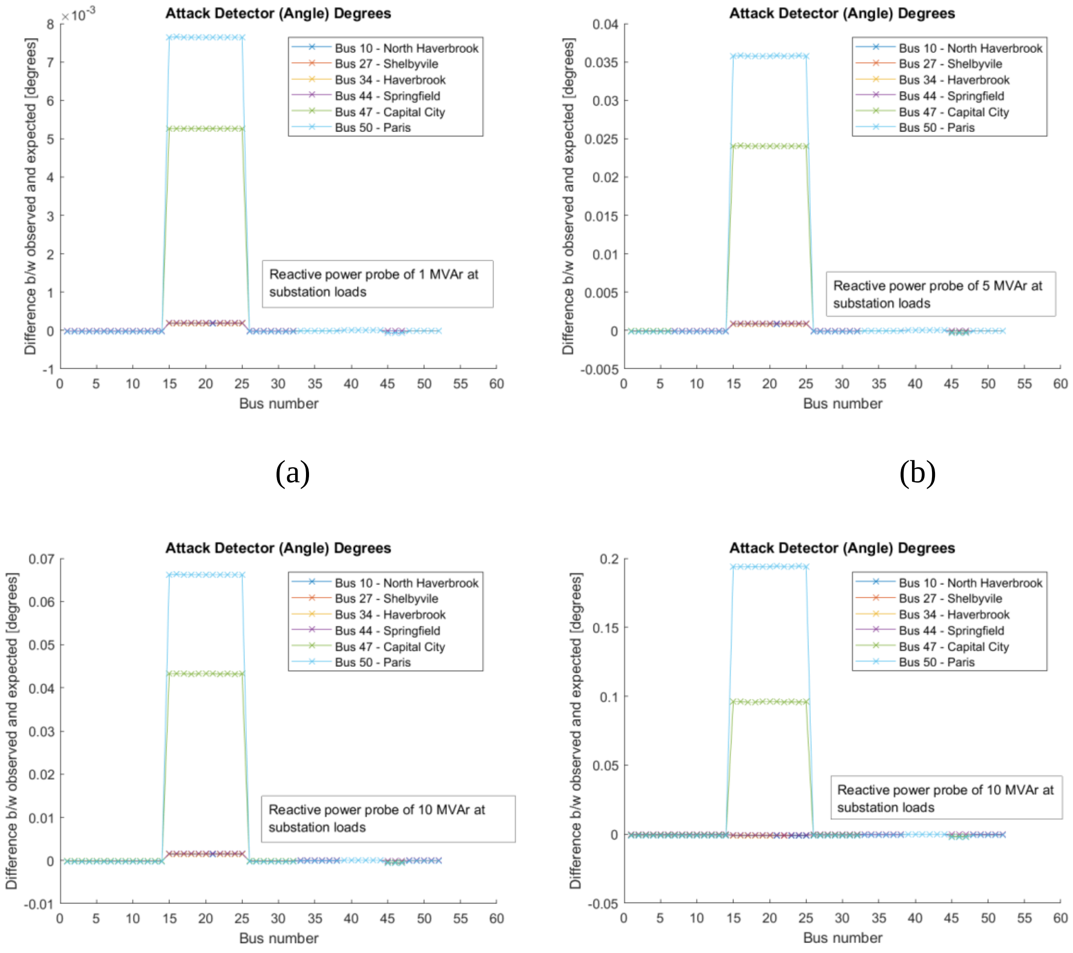
(b)

(c)

(d)

Figure 10. Results of reactive power probe of 5.0 MVAr for (a) voltage angle, (b) voltage magnitude, (c) real power injected, and (d) reactive power injected at each bus.

There are similar reactive power results between this probe and the real power probe. In both cases, the only difference between expected and observed measurements of reactive power is around buses 30 and 35. This difference is not dependent on probe source or size. The magnitude of the difference is small, and probably would not be noticed in a real system, but it is interesting that these results overlap. The magnitudes of the other results indicate that these results are negligible, so we try with different probe sizes for the most likely useful results, the angle difference. These results can be seen Figure 11.



(a)

(b)

(c)

(d)

Figure 11. Voltage angle results of reactive power probe of (a) 1.0 MW, (b) 5.0 MW, (c) 10.0 MW, and (d) 50.0 MW.

While the magnitude of the results is observable for some of the buses, this was not true for all probe source locations. Because the operator would not know a priori where the attacked substation was, all probe sources should be tested. In addition, there is only so much capacitance available, so we must make sure that the size of the probe is reasonable for the system.

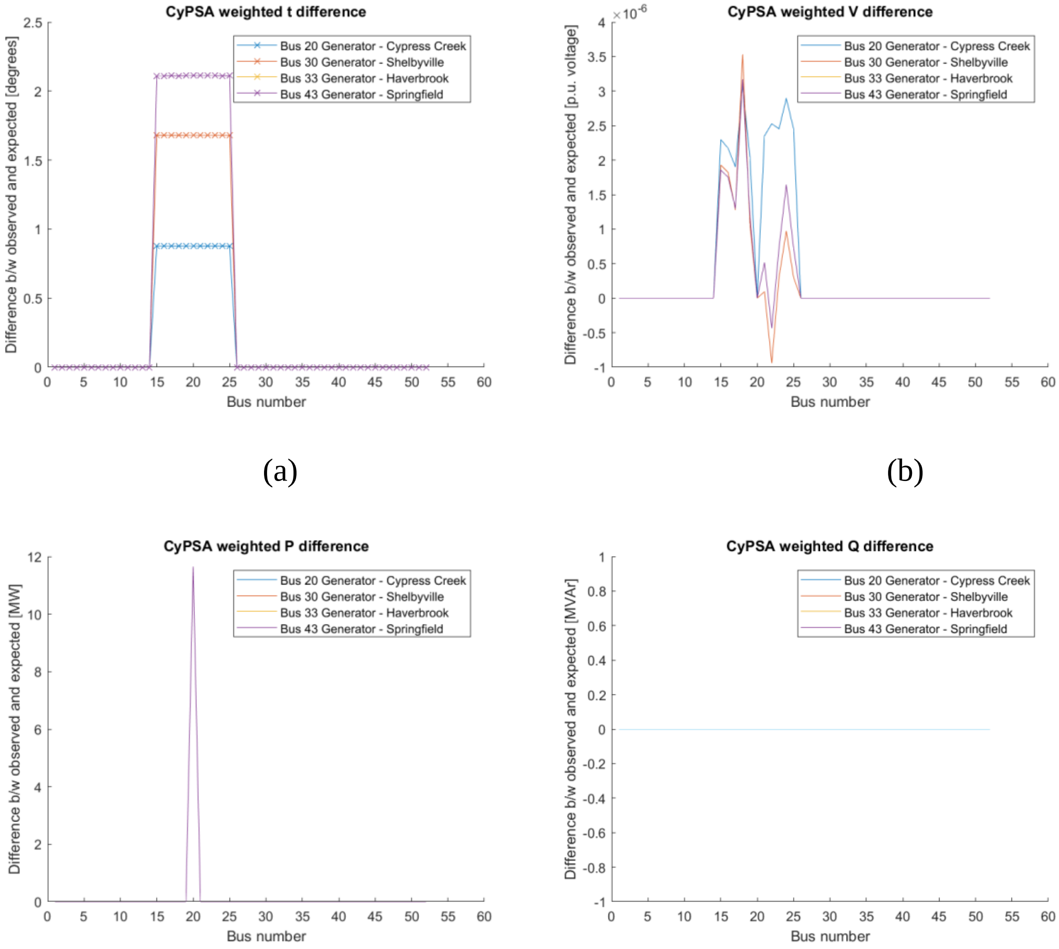
Sensor Trustworthiness Scores

The final step was to combine the topology analysis and real-time probing results. The purpose of combining these is to understand if the results from the real-time probing make sense in the context of the system topology. If it is not possible to reach a communications component, which might give an adversary access to measurements at certain buses, then any differences between expected and observed values in the real-time probe analysis should be discarded because we already know the attacker is not at this substation

The unexpected challenge that arose was that the number of communications devices and the number of buses did not match. It is not possible to see which communications devices are at each bus, only what substation they are at. To account for this, we assume that having a single communications device that is accessible from the cyber entry node makes the entire substation vulnerable. In other words, if any communications device at a substation is accessible by a cyber path, then we will consider the real time probing results at that substation.

In this particular test case, the only cyber components that were accessible from the compromised substation were at that substation, Cypress Creek. This is partially because there were firewalls in place, but future work should consider more inter-substation connections. In order to account for the multiple cyber components within a substation, we add the security indices of each substation together, and provide that same "security sum" to all buses at the substation. Again, this method is only used because there is not a direct connection between buses and cyber devices. Since this case only has one compromised substation, most buses will have a zero "security sum," but the Cypress Creek substation will have a security sum of 2.33.

The CyPSA combination can be performed for any of the results shown above. However, only one case is shown in Figure 12 for demonstrative purposes. The probe with the best results, real power probe, was chosen to test the CyPSA weighting. The 5.0 MW probe was chosen for its good ratio of small probe size to observable result magnitudes.



(a)

(b)

(c)

(d)

Figure 12. Results of real power probe of 5.0 MW weighted by CyPSA score for (a) voltage angle, (b) voltage magnitude, (c) real power injected, and (d) reactive power injected at each bus.

The angle results are measureable with the CyPSA weighted results, and they indicate very clearly that Cypress Creek is the compromised substation. Even the lowest measurements of 1 degree would be detectable. The voltage results are too small, and would be lost in the system noise. The real power results show a measureable difference at bus 20, which is in the compromised substation. These results would support the conclusion from the angle results that the Cypress Creek substation has been compromised. Finally, the CyPSA weighting has removed the only measureable reactive power results, so these results are not useful.

CHAPTER IV

CONCLUSION

Scoring

The results from the CyPSA analysis was helpful for identifying which substations were accessible from a given cyber access point, but the model we used did not have enough connections simulated to create a full image of the system. One of the reasons there were not as many inter-substation connections simulated is that the model was intended to have barriers between the substations as a security measure. While this models a good practice of security, real systems today have many more connections and there are more cyber communication channels between substations. Another part of the challenge with the CyPSA analysis was that the software used was outdated and no longer worked very well. The user interface did not update with values, and multiple versions of the software did not update the cyber access point.

The most promising results from the probing tests were from the real power probes. In this test, the difference between measured and expected values of the angle measurements was only observable at the compromised substation. Although the magnitude of the difference changed based on where the probe was sent from, the results were observable for all source generator locations. The real power measurements had observable differences at the compromised substation. The latter two did not have any dependence on the source of the probe. All of these results were visible with a small probe of just 1MW, but they increased proportionally with larger probes. In contrast, the reactive power measurements did not indicate any change at the compromised substation, but did have small differences between observed and expected values at other buses. However, the magnitude of these results did not change with changes in the magnitude of the probe, which suggests that these results are not related to the probe. Another advantage of this probe is that it is very easy to adjust the power output of generators in order to create this probe. This is less likely to cause unbalances in the system like a voltage probe might do, and can be more precisely controlled than turning on capacitor banks for the reactive power probe. The clarity of the results and the applicability of the probe both made real power probe the most desirable.

Combining the real-time probing and CyPSA topology analysis expands the range of probes that give successful results. All types of probes tested showed some sort of difference at the compromised substation, but not all clearly stood out from the uncompromised substations. Using the CyPSA scores to weight the probing results limits the possible range of attacked substations. However, in a real situation, we would not know a priori where the attack originated from. In order to make these results useful, we would have to run a CyPSA analysis from a variety of cyber entry nodes, and see if this collection of results together identifies one substation as most likely compromised.

Impact

Results strongly indicated that a combination of real-time probing and system topology analysis could be used to identify when an attack was occurring, and more specifically, what substation was compromised. This work can be used to build tools that allow operators to check the status of the trustworthiness of sensors in a system, and to identify previously hidden unobservable false data injection attacks. Utility companies have been slow to adopt new cybersecurity measures beyond firewalls and other measures that aim to keep adversaries out. While keeping adversaries out is desirable, there need to be protection schemes in place if an adversary does compromise the external barriers. This research provides a low cost method that can help utilities determine if adversaries have compromised sensor measurements, and we hope the adoption of these methods can improve the internal security for local utilities, power transmission, power distribution, and power generation companies.

Future Work

This project provided a good foundation for future work about topology and real-time probing attack detection methods for cyber-physical systems. The 8-substation case used is an unrealistic representation of real systems, which can be hundreds or thousands of buses large. We intend to expand this work to more realistic models, including the IEEE 300-bus case and the 3000-bus Texas Synthetic Grid case. Future work should attempt to implement the dynamic power flow analysis for this detection, which provides a more detailed and accurate view of the system and allows users to see how the probe propagates through the system. Preliminary tests of different types of probes were conducted, but future work should include a more thorough analysis of the type of probe used. This may include looking at using different waveforms for the probe, or a combination of probe types.

Another question we would like to consider is how the attacker responds to this probe. In this study, we assumed the adversary did not modify attack parameters in response to the probe, but an adversary hacking the system in real time may be able to modify their attack to respond to the probe.

As mentioned previously, there are some challenges associated with using the current version of the CyPSA tool. Our research group intends to consolidate and rewrite the CyPSA tool onto a single platform, enhance the visualization and user interface, and improve the functionality of this tool. We hope to create an platform that makes it easy to upload a case, run the topology analysis, and interactively adjust controls to fix threats and vulnerabilities.

REFERENCES

[1] W. F. Boyer and S. A. McBride, "Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues," Idaho National Laboratory, Idaho Falls, Idaho2009.

[2] J. Wirfs-Brock, "The Realities Of Cybersecurity At A Rural Utility," *Inside Energy*, September 23, 2015. Accessed on: Sept. 23 2017Newsletter. Available: https://grid.insideenergy.org/cybersecurity/

[3] Y. Han, S. Etigowni, H. Li, S. Zonouz, and A. Petropulu, "Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations," *CCS '17*, October 30-November 3, 2017 2017.

[4] M. Farooq-i-Azam and M. N. Ayyaz, J. A. Zubairi and A. Mahboob, Eds. *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*. IGI Global, p. 17, 2016.

[5] T. Smith, "Hacker jailed for revenge sewage attacks," *The Register*, 31 October 2001.

[6] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454 - 1467, 2014.

[7] M. J. Assante, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," in *SANS Industrial Control Systems Security Blog* vol. 207, ed: SANS Institute, 2016.

[8] K. R. Davis, R. Berthier, S. Zonouz, G. Weaver, R. B. Bobba, E. Rogers, P. W. Sauer, D. M. Nicol, "Cyber-Physical Security Assessment for Electric Power Systems," *IEEE HKN- The Bridge*, 2016.

[9] P. Sharma and G. Pandove, "A Review Article on Wireless Sensor Network in Smart Grid," *International Journal of Advanced Research in Computer Science*, Review Article vol. 8, no. 5, pp. 1903-1908, 2017.

[10] D. He, S. Chan, and M. Guizani, "Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring," *IEEE Wireless Communications*, vol. PP, no. 99, pp. 2-7, 04 April 2017 2017.

[11] J. Jiang and Y. Qian, "Defense Mechanisms against Data Injection Attacks in Smart Grid Networks," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 76 - 82, 2017.

[12] S. Hossain-McKenzie, S. Etigowni, K. Davis, and S. Zonouz, "Augmented DC Power Flow Method with RealTime Measurements," presented at the Power Systems Computation Conference, Genoa, 20-24 June 2016, 2016. Available: http://ieeexplore.ieee.org/abstract/document/7540973/

[13] J. Johnson, S. Hossain-McKenzie, U. Bui, S. Etigowni, K. Davis, and S. Zonouz, "Improving Power System Neural Network Construction Using Modal Analysis," *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*, pp. 17-20 Sept. 2017 2017.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *CCS '09 Proceedings of the 16th ACM conference on Computer and communications security*, pp. 21-32, 2009.

[15] S. Hossain, S. Etigowni, K. Davis, and S. Zonouz, "Towards Cyber-Physical Intrusion Tolerance," presented at the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, 2-5 Nov. 2015, 2015. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7436290&isnumber=7436263

[16] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic Corrective Control Selection for Online Remedial Action Scheme Design in a Cyber Adversarial Environment," *IET Cyber-Physical Systems: Theory & Applications*, Available: http://digital-library.theiet.org/content/journals/10.1049/iet-cps.2017.0014

[17] D. Formby, P. Srinivasan, A. Leonard, J. Rogers, and R. Beyah, "Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems," *Network and Distributed System Security Symposium*, 2016.

[18] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology Perturbation for Detecting Malicious Data Injection," presented at the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, 2012. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6149267&isnumber=6148595

[19] K. R. Davis, K. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," presented at the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 2012. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6486007&isnumber=6485945

[20] A. P. Fournaris, L. P. Fraile, and O. Koufopavlou, "Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: a Survey of Potent Microarchitectural Attacks," *Electronics*, vol. 6, no. 3, p. 52, 13 July 2017 2017.

[21] R. Garg, A. Hajj-Ahmad, and M. Wu, "Geo-location estimation from Electrical Network Frequency signals," *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 26-31 May 2013 2013.

[22] G. A. Weaver *et al.*, "Cyber-Physical Models For Power Grid Security Analysis: 8-Substation Case," *2016 IEEE International Conference On Smart Grid Communications (Smartgridcomm)*, 2016.

APPENDIX

Table 3. Cyber-Physical Assessment: Physical Indices.

Cyber Node Number	IP Address	PI
1	192.168.7.200	1.37963033
2	10.37.1.201	2.03302169
3	10.37.1.101	2.03302169
4	10.37.1.102	2.03302169
5	192.168.1.200	1.37963033
6	10.31.1.201	1.37963033
7	10.31.1.202	1.37963033
8	10.31.1.203	1.37963033
9	10.31.1.204	1.37963033
10	10.31.1.205	1.37963033
11	10.31.1.206	1.37963033
12	10.31.1.207	1.37963033
13	10.31.1.101	1.37898254
14	10.31.1.102	2.23180151
15	10.31.1.103	3.88744092
16	10.31.1.104	1.37963033
17	10.31.1.105	1.57131398
18	192.168.2.200	1.37963033

Table 3. Cont.

Cyber Node Number	**IP Address**	**PI**
19	192.168.3.200	1.37963033
20	10.33.1.201	1.99316859
21	10.33.1.202	1.44495595
22	10.33.1.203	1.55922353
23	10.33.1.101	1.99316859
24	10.33.1.102	2.25283337
25	10.33.1.103	1.37963033
26	10.33.1.104	1.37963033
27	10.33.1.105	1.37963033
28	10.33.1.106	1.44495595
29	10.32.1.201	1.38041353
30	haverbrook-network:DistanceRelay_2	1.37963033
31	haverbrook-network:DistanceRelay_3	1.37963033
32	haverbrook-network:ReversePowerRelay_1	1.37963033
33	haverbrook-network:OvercurrentRelay_1	1.37963033
34	haverbrook-network:OvercurrentRelay_2	1.37963033
35	haverbrook-network:OvercurrentRelay_3	1.37963033

Table 3. Cont.

Cyber Node Number	**IP Address**	**PI**
36	haverbrook-network:OvercurrentRelay_4	1.37963033
37	haverbrook-network:OvercurrentRelay_5	1.37963033
38	10.33.1.107	1.55922353
39	192.168.4.200	1.37963033
40	10.34.1.201	1.37963033
41	10.34.1.202	1.37963033
42	10.34.1.101	1.86783731
42	10.34.1.102	1.87627852
43	10.34.1.103	1.75332034
44	192.168.5.200	1.37963033
45	10.35.1.201	1.37963033
46	10.35.1.202	1.37963033
47	10.35.1.203	1.37963033
48	10.35.1.101	1.37963033
49	10.35.1.102	1.38664079
50	10.35.1.103	1.37898111
51	10.35.1.104	1.38538003
52	10.36.1.203	1.37963033
53	10.36.1.201	1.37963033

Table 3. Cont.

Cyber Node Number	IP Address	PI
54	10.36.1.202	1.37963033
55	10.36.1.101	1.44520104
56	10.36.1.102	1.38491452
57	10.36.1.103	1.38651896
58	10.36.1.104	2.55639505
59	10.36.1.105	2.06386328
60	10.36.1.106	3.94312406
61	192.168.8.200	1.37963033
62	10.38.1.201	1.38033605
63	10.38.1.202	1.38537943
64	10.38.1.203	1.38041425
65	springfield-network:ReversePowerRelay_1	1.37963033
66	10.38.1.102	1.38537943
67	10.38.1.103	
68	10.38.1.104	1.37963033
69	10.38.1.105	1.38041425
70	10.38.1.101	1.38033605