2017

Attack-resilient state estimation and testbed-based evaluation of cyber security for wide-area protection and control

Aditya Ashok
Iowa State University

Attack-resilient state estimation and testbed-based evaluation of cyber security for wide-area protection and control

by

Aditya Ashok

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering

Program of Study Committee:
Manimaran Govindarasu, Co-major Professor
Venkataramana Ajjarapu, Co-major Professor
Ian Dobson
Umesh Vaidya
Doug Jacobson

Iowa State University

Ames, Iowa

2017

DEDICATION

என் அம்மா, அப்பா, மற்றும்
அண்ணாவிற்கு சமர்ப்பிக்கிறேன்.

To my Amma, Appa, and Anna.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to acknowledge several people who have supported, guided, and inspired me throughout the several years I have been in graduate school at Iowa State University.

First and foremost, I would like to convey my heartfelt and sincere thanks to my major professor *Dr. Manimaran Govindarasu* for guiding me through my PhD over several years. His constant motivation and guidance has been critical in pushing myself to new areas in research and has been instrumental in the formation of my own research outlook. I'm also eternally grateful for the broad exposure outside core research that he provided me in terms of developing competitive research proposals, teaching opportunities, and external professional networking.

Second, I would like to thank my co-major professor *Dr. Venkataramana Ajjarapu* for his support and guidance throughout my PhD. Especially, his inputs were very critical in defining the direction of my PhD research during my initial years. I would also like to thank the other members of my graduate program of study committee for providing me valuable feedback at various points during my PhD that helped steer my research in the right direction.

Third, I would like to thank all those I have worked and collaborated with as part of the PowerCyber research group under *Dr. Manimaran Govindarasu*. Specifically, I would like to thank *Dr. Adam Hahn* for helping me with the basics of cybersecurity tools and experimentation in the lab during my initial years as a graduate student.

Last, but not least, I would like to thank my family and friends for their unconditional love and support throughout my PhD. Especially, I would like to acknowledge my close group of friends at Iowa State University, the *Madras Machis*, for supporting me through the ups and downs of my PhD and for making me feel at home in Ames. Particularly, I would like to thank my dear friend and mentor, *Dr. Siddharth Sridhar* for always being there, both personally and professionally.

ABSTRACT

Critical infrastructures such as the power grid have been increasingly targeted by advanced and persistent cyber threats making cyber security one of the nation's top research priorities. Traditional information technology (IT)-based cybersecurity measures are no longer adequate to address such threats, and there is a compelling need to develop a multi-layered defense strategy that utilizes a combination of infrastructure and application layer security measures. This dissertation specifically addresses attack-resilient application layer security approaches for critical wide-area monitoring, protection, and control (WAMPAC) applications. The first component, *Attack-Resilient State Estimation*, addresses the vulnerability of state estimation to stealthy cyber attacks, and discusses two complementary approaches to enhance its resilience. A topology-based attack vector that bypasses bad data detection methods and causes loss of system observability is identified. To mitigate the stealthy attacks on measurements and topology, an offline attack-resilient measurement design methodology is presented. Further, an online attack-resilient anomaly detection method that utilized load forecasts, generation schedules, and synchrophasor data to detect measurement anomalies is described. The second component, *Testbed-Based Experimentation and Performance Evaluation*, addresses the need to architect, develop, and leverage cyber-physical system (CPS) security testbed environments specifically for performing realistic attack-defense experimentation for WAMPAC use cases. An overview of testbed design objectives and design tradeoffs are discussed for different types of testbeds. A three-layered WAMPAC specific testbed architecture to address critical research challenges is presented. Finally, three experimental case studies that involved realistic coordinated cyber attacks on critical WAMPAC applications such as Automatic Generation Control (AGC) and Remedial Action Schemes (RAS) are described in detail. Further, the hypothesis that timing of attack actions also plays a critical role in the attack impact severity is experimentally validated using the PowerCyber testbed.

CHAPTER 1. INTRODUCTION

The electric power grid is one of the most complex engineering machines ever built by man. It is a highly interdependent cyber-physical system where the dynamics of one system is tightly coupled to the other. The power grid, as we know of today, is undergoing a massive transformation in all its constituent segments like generation, transmission and distribution. This transformation of the grid is driven by the US Department of Energy's Smart Grid vision[1]. Under this vision, the electric grid is envisaged to leverage advances in technology in several areas namely, renewable generation, advanced measurement devices like Phasor Measurement Units (PMU), Plug-in Hybrid Electric Vehicles (PHEV), Advanced Metering Infrastructure (AMI), and high-speed communication networks to enhance the security, and resiliency of the grid, at the same time reducing its dependence on non-renewable sources of generation and reducing energy production costs.

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control the operations of the power grid. Traditionally, SCADA systems were not designed keeping security as one of the important design criteria. Unfortunately, the exposure of SCADA network infrastructure to cyber threats has increased enormously due to increased interconnectivity of SCADA and public network infrastructures. In the last decade, the power grid's SCADA and several other critical infrastructures (CI) such as banking, water distribution, oil and natural gas, etc., are increasingly being targeted by advanced, sophisticated adversaries as they are critical to national security and societal well-being [2, 3, 4, 5, 6, 7, 8, 9].

National-level cybersecurity policies, standards and guidelines - Several government reports have highlighted the various deficiencies in cyber security for the electric sector that could result in major impacts due to emerging Advanced Persistent Threats (APTs), and also the urgent need to take measures to protect them [6, 10, 11]. The Department of Energy's

(DOE) Office of Electricity Delivery and Energy Reliability (OE) was setup especially to oversee activities that enhance the reliability and resilience of the nation's energy infrastructure. Recognizing the importance of the cyber security of the Energy Delivery Systems(EDS), the DOE OE released a roadmap in September 2011 to address the issues and concerns relevant to energy sector cybersecurity[12]. Also, OE created the Cybersecurity for Energy Delivery Systems (CEDS) program to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused R&D effort[13].

DOE, in coordination with the National Institute for Standards and Technology (NIST), and the North American Electric Reliability Corporation (NERC) developed a cybersecurity Risk Management Process (RMP) for the electric sector that will enable organizations to proactively manage cybersecurity risk[14]. Additionally, several efforts like NERC Critical Infrastructure Protection (CIP) [15], NIST Interagency Report (NISTIR) 7628[16] have been, and are being made at the national level to ensure that the appropriate standards and safeguards are put in place to prevent the electric power grid from potential cyber vulnerabilities and threats.

Beyond Infrastructure Security - The recent cyber attacks in Ukraine [9] on a distribution utility's power grid control network showed the inadequacy of relying on just infrastructure-based traditional cybersecurity measures when dealing with a resourceful and sophisticated adversary. The adversary was able to steal valid credentials through social engineering to get into the control network and perform reconnaissance and planning for several months. These types of incidents, similar in nature to insider threats, highlight the need to go beyond a single layer of security in order to detect and quickly recover from a sophisticated cyber attack. This need to develop intelligent countermeasures in multiple layers to secure SCADA infrastructure elements and the fundamental applications they support has been recognized in [17]. Also, the CEDS program has adopted a strategic and hierarchical approach to fund several R&D projects that specifically target multiple domains to develop novel solutions that go beyond traditional Information Technology (IT) infrastructure-based security to leverage the physical properties of the grid as part of application layer security.

One of the key motivations of the research presented in this disseration is to go beyond traditional infrastructure security solutions to develop attack-resilient application layer security approaches for critical monitoring, protection and control applications, which leverage both cyber and physical aspects of the grid. Together with developing new cyber-physical attack-resilient approaches for fundamental applications such as state estimation (SE), the dissertation also addresses the need to architect, develop, and leverage cyber-physical security testbed environments for performing realistic attack-defense experimentation to move the research closer to industry adoption.

1.1 Chapter Organization

The rest of this dissertation is organized as follows. Chapter 2 introduces wide-area monitoring, protection and control (WAMPAC), and then describes the different types of cyber attacks that could potentially impact WAMPAC. Also, it presents a detailed review of related work in the context of cyber security of WAMPAC. Chapter 3 and Chapter 4 describe how coordinated cyber attacks impact state estimation and their mitigation measures in detail. Chapter 5 discusses in detail CPS security testbed design, architecture, tradeoffs and experimental case studies specifically focusing on WAMPAC applications. Chapter 6 summarizes the main contributions of the current work and provides potential research directions for future work.

CHAPTER 2. WIDE-AREA MONITORING, PROTECTION, AND CONTROL (WAMPAC)

2.1 Introduction to WAMPAC

WAMPAC systems leverage Phasor Measurements Units (PMUs) and existing SCADA measurements to gain real-time awareness of current grid operations and also provide real-time protection and control functions such as RAS, SE, and AGC, besides other emerging applications such as oscillation detection, transient stability predictions, etc. While communication is the key to a smarter grid, developing and securing the appropriate cyber infrastructures and their communication protocols is crucial. WAMPAC can be subdivided further into its constituent components namely, Wide-Area Monitoring (WAM), Wide-Area Protection (WAP), and Wide-Area Control (WAC).

SE provides the operators with situational awareness of the entire system's current operating conditions and are one of the main deployments of WAM systems. The output of SE is used by several applications in the operations and planning of the power grid, like contingency analysis (CA), security constrained optimal power flow (SCOPF), markets, etc., to name a few. Figure 3.1 provides a high-level overview of the utility of power system SE and how SE is performed from the several thousands of SCADA analog and status points gathered every few seconds. Emerging WAM applications mainly utilize high sampling rates and accurate GPS-based timing from PMUs to provide very accurate, synchronized voltage and current measurements. While PMUs provide increasingly accurate situational awareness capabilities, their full potential will not be realized unless these measurement data can be shared among other utilities and regulators. The North-American Synchrophasor Initiative network (NASPInet), is a separate network for PMU data transmission and data sharing including real-time control,

quality of service and cybersecurity requirements, and is an example of the latest WAM system deployments to support emerging PMU applications of the future [18].

WAP involves the use of system wide information collected over a wide geographic area to perform fast decision-making and switching actions in order to counteract the propagation of large disturbances [19]. The advent of PMUs has transformed protection from a local concept into a system level wide-area concept to handle disturbances. Several protection applications fall under the umbrella of WAP, but the most common one among them is Special Protection Schemes (SPS). NERC defines SPS as an automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than, or in addition, to the isolation of faulted components to maintain system reliability [20]. Such action may include changes in demand, generation (MW and MVAR), or system configuration to maintain system stability, acceptable voltage, or power flows. Some of the most common SPS applications are: generator rejection, load rejection, under frequency load shedding, under voltage load shedding, out-of step relaying, VAR compensation, discrete excitation control, and HVDC controls.

Until the advent of PMUs, the only major WAC mechanism in the power grid was AGC. The AGC functions with the help of tie-line flow measurements, frequency and generation data obtained from SCADA infrastructure. The purpose of the AGC in a power system is to correct system generation in accordance with load changes in order to maintain grid frequency at 60 Hz. Currently, the concept of real-time WAC using PMU data is still in its infancy and there are no standardized applications that are widely deployed on a system wide scale, though there are several pilot projects in that area [21]. Some of the potential WAC applications are secondary voltage control using PMU data, Static VAR Compensator (SVC) control using PMUs, and inter-area oscillation damping.

2.2 WAMPAC - A Generic Architecture

Figure 2.1 shows a generic WAMPAC architecture with the various components involved [22]. The system conditions are measured using measurement devices (relays and PMUs), these measurements are communicated to a WAMPAC controller to determine appropriate control

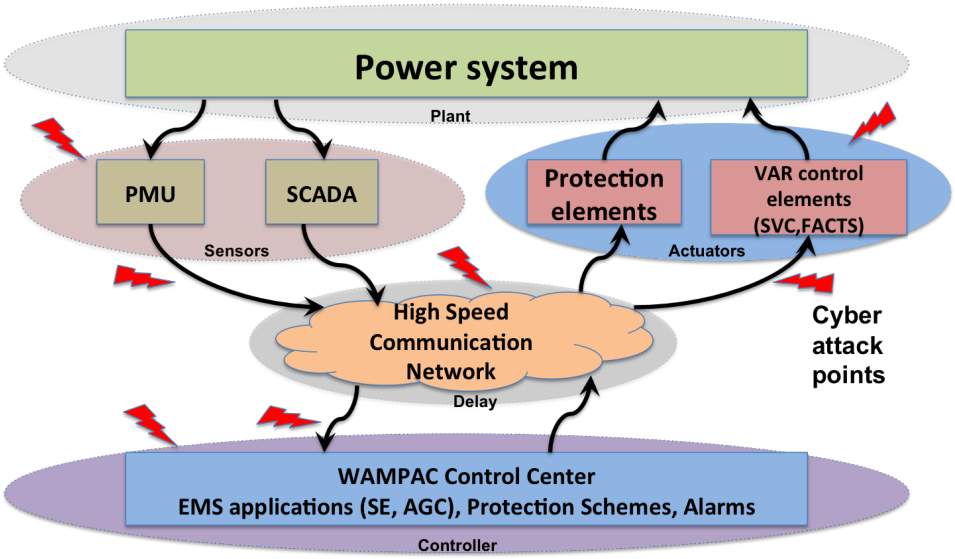

Figure 2.1 Generic WAMPAC architecture

actions for economic operations or in some cases for contingencies. Then, the appropriate control actions are initiated, usually through high-speed communication links. The inherent wide-area nature of these schemes presents several vulnerabilities in terms of possible cyber intrusions to hinder or alter the normal functioning of these schemes.

Even though the WAMPAC applications like SE,AGC or SPS are designed to cause minimal or no impact to the power system under failures, they are not designed to handle failures due to malicious events like cyber attacks. Also, as more and more applications are added in the power system, it introduces unexpected dependencies in the operation of the various schemes and this increases the risk of increased impacts like system wide collapse, due to a cyber attack. It therefore becomes critical to reexamine the design of the WAMPAC applications with a specific focus on cyber-physical system security.

Figure 2.1 also presents a control systems view of the power system and the WAMPAC applications at the control center. The power system is the plant under control, where the parameters like currents and voltages at different places are measured using sensors (PMUs) and sent through the high-speed communication network to the WAMPAC controller for appropriate decision-making. The controller decides based on the system conditions and sends

corresponding commands to the actuators which are the generators, protection elements and VAR control elements like SVC and FACTS. There are different places where a cyber attack can take place in this control system model. The cyber attack could affect the delays experienced in the forward or the feedback path or it could directly affect the data corresponding to sensors, the actuators or the controller. Figure 2.1 also indicates the attack points on this control system model through the lightning bolts.

2.2.1 Cyber Attack Classification

Conceptually, we identify three classes of attacks on this control system model for WAMPAC. They are timing-based attacks, integrity attacks and replay attacks.

Timing attacks: Timing is a crucial component in any dynamic system (e.g. protection scheme) and typically the control actions should be executed on the order of milli-seconds after the disturbance. Therefore, WAMPAC applications cannot tolerate any type of delay in communications and therefore are vulnerable to timing-based attacks. Timing attacks tend to flood the communication network with packets and this slows the network down in several cases and also shuts them down in some cases, both of which are not acceptable. These types of attacks are commonly known as DoS attacks.

Data Integrity Attacks: Data integrity attacks are attacks where the data is corrupted in the forward or the reverse path in the control flow. This means that there could be an attack which directly corrupts the sensor data (measurement data), or the control data (commands given to the generators, protection elements or the VAR control elements). This translates to actions like blocking of the trip signals in scenarios where the controller actually sent a trip command to the protection elements or the controller commanded to increase VAR injection while the attack caused the injection to decrease or vice versa.

Replay Attacks: Replay attacks are similar to data integrity attacks, where the attacker manipulates the measurements or the control messages by hijacking the packets in transit between the measurement device and the control center. Several of the modern communication protocols have replay protection features that make it extremely hard to execute a successful replay attack. However, in some cases where legacy protocols are used, a replay attack could

be possible even under encrypted communication as the replayed packets are valid packets with the messages data integrity being intact except for the timestamp information.

2.2.2 Coordinated Attacks on WAMPAC

Coordinated attacks are cases where several different attack actions can be coordinated in space and/or time. For example, elements that do not share electrical or physical relationships can be forced to fail simultaneously, or in a staggered manner at appropriate time intervals depending on the system response, which could result in unanticipated consequences. Intelligent coordinated attacks can significantly affect a power system's security and adequacy by negating the effect of system redundancy and other existing defense mechanisms after an initial attack. NERC has instituted the Cyber Attack Task Force (CATF) to gauge system risk from such attacks and develop feasible, and cost-effective mitigation techniques. NERC CATF identifies intelligent coordinated cyber attacks as a category of events that are classified as High-Impact Low-Frequency (HILF), which cause significant impacts to power system reliability beyond acceptable margins [11]. Therefore, the traditional approach to determining system reliability with (N-1) contingencies and a restricted set of multiple contingencies is no longer sufficient and new approaches have to be developed to deal with plausible (N-k) contingencies.

Figure 2.2 presents several sample coordinated attack scenarios on several important WAMPAC applications like SE, AGC, RAS respectively, and their impacts. A coordinated data integrity attack on a key monitoring application like SE could be achieved by compromising the various meters that measure or transfer the power flow measurements to the control center. This spatial coordinated attack results in a poor situational awareness of the power system and also could lead to incorrect system dispatch leading to line overloads and market impacts in terms of uneconomical generation [23]. Similarly, a coordinated data integrity attack on AGC would cause an imbalance in system generation and load resulting in frequency imbalance and reliability impacts [24]. Finally, we can consider the case of a coordinated attack on RAS, which are part of WAP. The attack scenario is a combination of data integrity and DoS attacks on the protection relays and substation communications happening in different locations, staggered in

time. Such an attack impacts reliability and could cause cascading outages depending on the system loading [25].

Attack Type	*Attack vectors*	*Attack Target*	*Impacted Application*	*Coordination*	*Impacts*
Data Integrity	Via SCADA network, Remote Terminal Unit (RTU), Relay access	SCADA status and analog measurements	State Estimation (**Wide – Area Monitoring**)	Space, same time	Poor situational awareness, Line overloads, Market Impacts
Data Integrity, DoS, Combination	Via SCADA network RTU access	Frequency, Tie-line power flow measurements	Automatic Generation Control (**Wide – Area Control**)	Space, same time	Frequency Imbalance, Operational reliability, Market Impacts
Data Integrity and DoS Combination	Via Substation LAN remote access	IEC 61850 GOOSE messages	Remedial Action Schemes (**Wide – Area Protection**)	Space, staggered time	Operational reliability, Potential to cascading outages

Figure 2.2 Sample coordinated attack scenarios in WAMPAC

2.3 Literature Review

This section identifies the related work in the context of cyber security of WAMPAC, especially pertaining to cyber attacks on SE and is grouped based on the specific focus of the work.The importance of SE in providing situational awareness and its dependence on wide-area measurements has been a major driving factor for the study of how cyber attacks impact SE. Existing literature in this area addresses one or more main themes, identifying attack vectors, characterizing impacts and proposing mitigation methods.

2.3.1 Cyber Security Issues in WAMPAC

The transition towards a smarter electric grid has spurred a lot of interest in cybersecurity research for the power infrastructure. Several papers have been published studying the applicability of cyber security for power system operations like AGC, voltage control, SE, dis-

tribution applications like AMI and infrastructure elements like Phasor Data Concentrators (PDC). In [24], the authors study the impact of data integrity attacks on the AGC system operation and quantify the attack impacts in terms of load-generation imbalance and frequency violations. Similarly, in [26], the authors extend the data integrity attack model described in [24] to the voltage control loop and study how data integrity attacks on voltage control devices like FACTS, SVC, etc. can cause abnormal voltages, violating NERC reliability standards. The various cyber security issues related to confidentiality, integrity, availability, etc. for AMI have been discussed in [27]. Paper [28] discusses security issues for Phasor Data Concentrators and also presents a scenario of compromising the database which stores PMU data through a SQL-injection attack.

2.3.2 Cyber Attacks on SE

State Estimators rely on wide-area measurement data from SCADA networks to construct a real-time network topology based on the breaker and switch statuses, and also validate the analog measurements from the Remote Terminal Units (RTU) to provide accurate state estimates. The dependence on wide-area measurements creates an inherent vulnerability to data denial or manipulation through malicious cyber attacks either at the measurement source or in transit. The attacks could target either the integrity of the topology measurements or the analog measurements in the SCADA data, or it could also target the availability of the data at the control center. Integrity-based attacks require much more information than the actual attack, such as attack locations and attack values to remain undetected, whereas DoS attacks do not require too much information other than the target of the attacks.

2.3.2.1 False Data Injection Attacks

The paper by Liu et al. was one of the first works to look at the vulnerability of state estimation to cyber attacks is [23], where the attacker is assumed to possess knowledge about measurement configuration to create undetectable attacks. The paper characterizes attacks into two major types: random and targeted attacks, where targeted attacks aim to inject specific errors into selected state variables. The paper also identifies the potential attack vectors given

a particular attacker's resource limitation and the characterizes the impacts in terms of injected error in the state variables. Bobba et al. proposes a method to detect such attacks by protecting a set of selected measurements and independently verifying certain state variables [29].

Kosut et al. developed a heuristic in [30] to find the attacks that impact bad data detection the most, given a set of compromised meters under a particular attacker. This paper also presents a new bad data detector which outperforms the traditional bad data detector. The work done by Kim et al. in [31] looks at protection of a subset of measurements from data injection attacks, given the attacker model as proposed in [23], under an optimization framework and also proposes an algorithm to aid in PMU placement on strategic buses in the network.

Le et al. present a false data injection attack, against the state estimation in deregulated electricity markets in [32]. They show that such a class of attacks bypass the bad data measurement detection, and can lead to profitable financial misconduct by affecting the locational marginal prices (LMP). The paper also presents a heuristic to find out the most profitable attack in terms of an optimization problem.

Giani et al. proposes an algorithm to determine the presence of attacks that involve minimal compromise of meters given a measurement configuration and also proposes a measurement placement algorithm to tolerate such attacks [33]. Dan et al. consider the attack template as proposed by [23], define a security metric that quantifies the cost to perform a stealthy attack and also an algorithm to compute the attack vectors [34]. The paper also proposes two approaches to place encryption devices to maximize security. Teixerira et al. considers a scenario where the attacker possess only a perturbed model of the system and proposes a method to find stealthy deception attacks [35]. The paper also identifies the limits of the attack vector for commonly used bad data detection methods in state estimators.

The papers mentioned previously [23, 29, 30, 33, 32], use the DC power flow model in their analysis of the false data injection attack on the state estimator. Hug et al. uses AC power flow analysis to distinguish their analysis and present a graph-based algorithm to find stealthy data injection attacks [36]. The paper also provides a comparative analysis of the errors introduced when using DC vs. AC power flow model and identifies that it is very difficult to create a truly undetectable attack due to the non-linearity of the power flow equations.

2.3.2.2 Topology-based attacks

Integrity-based attacks, commonly known as false data injection attacks, require knowledge about the measurement configuration in order to remain undetected as bad measurements due to measurement errors are inherently filtered out by Bad Data Detection(BDD) in SE. All of the existing literature discussed previously use the attack model as defined in [23]. However, all these papers make certain assumptions. The pertinent ones are

1. Network topology is valid and error free.
2. Measurement redundancy is adequate.
3. Only analog measurements (injection and flow) have errors.

Though these assumptions are reasonable to study some aspects of this problem, some of these assumptions do not hold considering the exposure of the SCADA network to cyber-based threats. Especially, the assumptions concerning valid network topology and errors only in analog measurements. Therefore, it becomes really critical to study the effects of how topology errors created by cyber attacks impact the SE and power system operations.

As part of the dissertation, we identified another type of attacks that are aimed at creating topology errors by virtue of knowledge of measurement configuration while remaining undetected [37]. This paper addresses the problem of how topology errors, in particular, the branch status errors, can be created by malicious adversaries through intelligent cyber attacks. We have shown how an unobservable topology error can be created by manipulating the field devices corresponding to the critical measurements or critical branches in the SCADA measurement set configuration. Also, we have shown how the impacts of such an attack can be analyzed through system operating limit (SOL) violations on the altered network topology. More details about the work is presented in Section 3.2.

2.3.2.3 DoS attacks

One could also identify another type of attack vector where the attacker just denies carefully chosen measurements from reaching the control center forcing the state estimator to lose total

system observability. SE normally handles loss of observability (critical measurements) by using pseudo-measurements, which are obtained generally from short-term forecasts or from historical and recent data. Pseudo-measurements are less accurate than regular measurements, and this directly contributes to a loss of accuracy in state estimates if done improperly [38]. Loss of SE accuracy when the system is operating under heavy system loads could impact operator decisions adversely. Though these type of attacks have not been not studied separately, the mitigation methods for these types of attacks are similar to the ones employed for topology-based attacks.

2.3.3 Measurement Design

We briefly introduce the measurement design problem before reviewing the existing literature in this area. Typically, the objective of measurement design problem is to minimize the cost and the number of new measurements added to the measurement configuration such that it satisfies two main constraints. One is to maintain total system observability under all credible contingencies. The other is to satisfy accuracy requirements of the state estimates. Another byproduct of these two is the bad data detection capability of the estimator. An observable system with a reasonable accuracy of estimates ensures good bad data detection capability. It is to be noted here that the under the context of measurement design, contingencies could be actual contingencies that involve a change in the actual topology of the system, or situations where there is a loss of measurement availability at the control center.

The problem of measurement design has been very well researched and there is an excellent wealth of literature on this topic. Sarma et al. proposed a measurement design process that included multiple phases: (1) satisfying acceptable redundancy, (2) satisfying basic observability, (3) elimination of critical measurements, and (4) measurement placement to handle measurement loss of single RTU failure [39]. Celik and Liu proposed an incremental measurement placement algorithm that created a ranking of buses with low accuracy and identified candidate measurements which are not leverage points to add to the measurement set until a desired accuracy is obtained [40].

Baran et al. proposed a meter placement method that addressed multiple aspects in the measurement design whilst also minimizing the cost of meter deployments [41]. The basic measurement placement addresses accuracy constraints in the form of a system accuracy index. The subsequent stages address meter placement for reliability using a marginal cost approach and meter placement for bad data detection eliminating critical measurements. More recently, Magnago and Abur presented a measurement placement approach that handled loss of any single branch measurement or single contingency without loosing network observability [42]. The approach identifies candidates for all situations where observability is lost and minimizes the cost of candidate measurements by formulating a binary integer linear optimization problem.

In the last few years, the papers on measurement design have focussed on optimal placement of PMUs for state estimation. Gou presented a generalized integer linear programming formulation for optimal PMU placement that included cases for redundant placement, complete and incomplete observability [43]. The paper introduced the concept of depth of one and depth of two unobservability, where the neighboring buses of any unobservable buses are rendered observable by PMU placement. Abbasy et al. also proposed a binary integer linear programming formulation for optimal PMU placement which also considers conventional measurement placements and loss of multiple PMUs [44]. Chakrabarti et al. proposed a binary search-based algorithm for determining the minimal number of PMUs to ensure full observability including single branch outage cases [45]. All the above papers on PMU placement assume that a PMU installation at a bus would enable measurement of all branch currents in the bus, whereas Emami et al. propose an optimal PMU placement method for branch PMUs that enable voltage and current measurement only on one branch [46]. The method also addresses reliability aspects by considering loss of PMUs or branch outages into placement constraints, ensuring complete observabiliity.

Most of the literature mentioned previously, do not address the issue of loss of multiple measurements, except one or two of the earlier papers that addressed loss of RTU's as part of the problem formulation. Most of the papers considered the loss of a single branch or measurement to be sufficient for measurement design. However, we strongly believe that measurement design

also needs to consider loss of multiple critical measurements, or even loss of measurements from multiple RTU's due to targeted cyber attacks.

If we consider the possibility of the loss of multiple measurements or loss of multiple RTU's simultaneously, we would encounter situations where there is incomplete observability and in order to handle such cases we typically resort to the use of pseudo-measurements. It is well known that pseudo-measurements are often generated with the help of forecast-based predictions or historical data, and depending on the load level and the quality of past measurements, pseudo-measurement quality also varies. This in turn influences how much variance is added in the state estimates. It has been shown that if pseudo-measurements are not used properly, their errors can impact the estimates of other state variables also [38]. We believe that this is another reason to rethink traditional measurement design process as not all cases of unobservability should be handled with pseudo-measurements. With more and more push for utilizing transmission lines to their maximum capacity, errors in estimation of line flows impact operational decisions to a greater extent. Therefore, we believe that an attack-resilient measurement design process should include a careful consideration of the type of contingencies that could occur, loss of multiple critical measurements, and the use of pseudo-measurements to address situations with incomplete observability.

2.3.4 Mitigation of Cyber Attacks on SE

While there are enough papers in the area of identifying possible attack vectors and impacts on the state estimates, markets and operations, not enough work has been done to address the problem of detecting and mitigating stealthy cyber attacks on state estimators.

Irrespective of the type of cyber attacks, the more there are measurements in the measurement configuration, the more resilient state estimator becomes, and the harder it gets for the adversary to execute a stealthy attack. The proposed solutions by existing literature fundamentally address two aspects: adding more measurements into the estimation process, indirectly protecting certain essential measurements from being corrupted, so that the adversary has to manipulate even more measurements to remain stealthy against the bad data detectors. Another way is by ensuring the security of enough number of essential measurements in the

measurement configuration by performing additional infrastructure security mechanisms such as encryption, authentication of the data. This problem of making the estimator robust to measurement corruption (natural and malicious) and measurement loss is known as the 'measurement design' problem. A well-designed measurement configuration in state estimation will make the possibility of creating a stealthy cyber attack very slim.

The existing category of solutions are mostly reliant on an efficient measurement design, which is an offline problem to increase the redundancy, accuracy and bad data detection capabilities of the state estimators. Section 3.3 proposes an attack-resilient measurement design methodology for SE to increase robustness against data injection and DoS attacks.

A well-designed measurement system increases the degree of difficulty of an attack, but cannot completely rule out the possibility of a highly skilled attack. In contrast to the former solution type, which is an offline process, the key in the second solution type is to use information that is independent of the SCADA data to validate the state estimates. We believe that to the best of our knowledge there is no prior work on an online anomaly detection method to detect cyber attacks and validate the state estimates and detect anomalies. Chapter 4 proposes an online anomaly detection method to leverage the information obtained from load forecasts, generation schedules, and real-time synchrophasor data to provide a coarse real-time validation for the state estimates produced from untrusted SCADA measurements, thereby enabling the detection of false data injection attacks.

2.3.5 Cyber-Physical System Security Testbeds

The development of CPS security testbeds and cybersecurity experimentation leveraging CPS testbeds has been an active research topic over the last few years. Several educational institutions and research laboratories are setting up individual CPS security testbeds for validating their research and are also exploring possibilities for CPS testbed federation to perform large-scale, high fidelity, hardware-in-the-loop cyber attack/defense experiments.

The National SCADA Testbed (NSTB) at Idaho National Laboratory, is one of the earliest collaborative testbed efforts across several U.S national laboratories where actual power system resources (generation and transmission lines), and the associated cyber system compo-

nents were used to perform vulnerability assessments and impact analysis studies [47]. Sandia National Laboratory houses the Virtual Control System Environment (VCSE), which is a cyber-physical testbed with a hybrid mix of simulated, emulated and physical system components for attack-defense experimentation [48]. The powerNET testbed at Pacific Northwest National Laboratory (PNNL) leverages a combination of cloud-based computing platform for virtualization, real-time power system simulators, and a variety of field equipment such as multi-function protection relays and PMUs from multiple vendors to provide a highly customizable and configurable environment for cyber-physical security experimentation [49]. The University of Illinois at Urbana-Champaign hosts the Virtual Power System Testbed (VPST), consisting of a mix of simulated, emulated and physical components to perform cyber security research across a wide range of topics including vulnerability assessments, communication protocol and security product testing and research validation [50].

The PowerCyber CPS security testbed at Iowa State University consists of a hybrid mix of industry grade SCADA hardware and software, emulators for wide-area network routing and real-time power system simulators, which enable a high-fidelity, hardware-in-the-loop, cyber-physical testbed environment for cyber-physical security research and experimental validation studies [25]. The SCADA testbed at the University College, Dublin is used to perform experiments on intrusion detection and anomaly detection related to power grid cyber security [51]. Mississippi State University consists of a SCADA security testbed, which is used to perform intrusion detection and security testing of PMUs and PDCs [52].

The University of Southern California‘s Information Sciences Institute hosts the DETER cyber security testbed, which is a large-scale testbed for cyber security experimentation, but it does not contain physical system resources, like relays and phasor measurement units, which some of the earlier testbeds mentioned have for hardware-in-the-loop experimentation [53]. The Smart Grid testbed at Washington State University consists of several hardware resources like PMUs and PDCs interfaced with a real-time power system simulator, but is primarily focused on developing new power system monitoring and control algorithms [54]. Other notable research efforts that leverage CPS security testbeds for experimentation on telecommunication, networking, and intrusion detection includes the European CRUTIAL project [55], TASSCS

testbed at the University of Arizona [56], SCADASim testbed at the Royal Melbourne Institute of Technology [57].

2.4 Dissertation Contributions

The dissertation is based on two main research components: *1. Attack-resilient State Estimation, 2. Testbed-based experimentation and performance evaluation of cyber attack-defense on WAMPAC applications.* The following section details the various research components and the associated contributions.

- **Attack-Resilient State Estimation** In this component, a topology-based attack vector that bypasses bad data detection methods and causes loss of system observability is identified. Two complementary mitigation measures are proposed to mitigate stealthy cyber attacks and improve resiliency of state estimators. First, an offline attack-resilient measurement design methodology is presented that increases robustness of state estimators against false data injection and DoS attacks. Second, an online attack-resilient anomaly detection method is presented that utilizes load forecasts, generation schedules, and synchrophasor data to coarsely validate state estimates and detect false data injection attacks.

  The specific and expected contributions from this research component are given below:

  1. **Topology-based stealthy attacks and impact evaluation**
     - Identification of attack vector to create topology-based attack.
     - Development of a methodology to analyze attack impacts in terms of SOLs.
     - Case study on IEEE 14 bus system
  2. **Offline mitigation strategy for stealthy cyber attacks**
     - Development of attack-resilient measurement design methodology including SE redundancy, accuracy, bad data detection.
     - Minimum cost optimization formulation for placement of new measurements.
     - Case study on IEEE 14 bus system

3. **Online mitigation strategy for stealthy cyber attacks**
   - Development of attack-resilient anomaly detection methodology leveraging load forecasts, and synchrophasor data.
   - Sensitivity analysis of proposed method considering variation in load forecasts, measurement configurations, SE measurement accuracies and PMU data for different attack magnitudes.
   - Analysis of false positives, and false negatives for a range of attack detection thresholds and attack magnitudes.
   - Development of an empirical methodology to determine minimum attack detection magnitudes and detection thresholds for target false positive rate (FPR) and true positive rate (TPR) specification.
   - Case study on IEEE 14 bus system

- **CPS Testbed - objectives, design methodology, architecture and performance evaluation of coordinated attacks on WAMPAC applications**

  In this component, we describe several aspects pertaining to CPS testbed design, development and experimentation. We also showcase results from testbed-based experimentation and performance evaluation of cyber attack-defense on critical WAMPAC applications. Overall, this component is expected to have the following contributions:

  1. **CPS security testbed - objectives, design methodology, architecture, and challenges**
     - An overview of the basic testbed design objectives and design tradeoffs for various types of testbeds.
     - A top-down methodology for the engineering of the CPS security testbed based on specific WAMPAC use cases.
     - Three layered testbed architecture abstraction and its application to create an architecture for WAMPAC specific cyber attack-defense experimentation that addresses research challenges identified.

- Qualitative analysis of testbed federation looking at research challenges, federation architectures, and WAMPAC specific use cases that could benefit from federation.

2. **Attack-defense experimentation and performance evaluation on WAP and WAC applications**
   - Identification of novel coordinated attack vector for RAS that involved a combination of spatial and temporal coordination and its quantitative impact assessment experimentally using the testbed.
   - Experimental case studies that show how CPS security testbeds enable realistic attack-defense experimentation on critical WAMPAC applications such as AGC, RAS that could not be performed on ordinary simulation-based environments.

CHAPTER 3. ATTACK-RESILIENT MEASUREMENT DESIGN FOR STATE ESTIMATION

This chapter describes about the cyber-physical security of state estimators against stealthy cyber attacks. The remainder of this section is organized as follows. Section 3.1 provides a general context to cyber attacks on SE by describing the attack models, attack scope and the need for application level security beyond traditional infrastructure security. Section 3.2 introduces a topology -based stealthy attack and describes a methodology to study its impacts on the power grid. Section 3.3 describes an offline attack-resilient measurement design methodology that increases robustness of state estimators against false data injection and DoS attacks.

3.1 Cyber Attacks on Power System State Estimation

This section provides a brief overview of the two main attack vectors that have been mentioned previously in the context of state estimators. Also, it explains the scope of the attacks in the context of the current security mechanisms in SCADA networks.

3.1.1 Cyber Attack Models

We consider the following types of cyber attacks on state estimators:

- Data integrity-based attacks - Attacks that target the integrity of analog or status measurements from the remote terminal units to the control center.
- DoS attacks - Attacks that target the availability of analog or status measurements from the remote terminal units to the control center.

The impact of DoS attacks on state estimators have not been studied in detail so far. However, the potential impacts of such an attack are likely to reduce the available redundancy in

SCADA telemetry to very dangerous levels that could cause a significant deterioration in the quality of the produced state estimates and/or lack of total system observability translating into inadequate operator situational awareness. These type of attacks can cause other secondary and tertiary impacts as they affect the performance of the SCADA networks used in system operations and also need to be systematically studied. In contrast, the two main types of integrity attacks, the ones where analog measurements are impacted (false data injection attacks) and the ones where status measurements are impacted (topology-based attacks) are more stealthy and therefore considered more harmful.

3.1.1.1 False Data Injection Attacks

The basic attack vector for a stealthy false data injection attack as mentioned in [23] is to find an attack vector a that satisfies the following equation:

$$z + a = Hx + e, \ where \ a = Hc \ is \ the \ attack \ injection. \tag{3.1}$$

This ensures that the attack is undetected in the largest normalized residual test which the most commonly used BDD method in state estimators.

3.1.1.2 Topology-based attacks

The basic attack vector for a topology-based attack as mentioned in [37] is to find the critical measurements in a particular system measurement configuration and create a topology change that reduces the observability of the system.

If H is the system measurement matrix, then the critical branches in the system can be obtained through the procedure shown in Section 3.2.5.2. A topology change in any one of these measurements causes no change in the measurement residuals and therefore cannot be detected by the BDD in state estimators.

3.1.2 Cyber Attack Scope

The SCADA network is used to obtain telemetry from the RTUs that are located at the substations once every 2-10 seconds. The RTUs collect measurements from the Intelligent

Electronic Devices (IED), Merging Units, various types of measurement devices through a local communication protocol or through hard wired configurations. The communication from the RTU to the control center goes over the wide-area network and is typically one of the following protocols namely Distributed Network Protocol (DNP) 3, Modbus, Profibus, etc. The entire SCADA infrastructure is made up of a variety of these legacy devices and communication protocols. Therefore, the scope for cyber attacks on these devices are numerous despite several infrastructure protection mechanisms such as firewalls, VPNs and security standards such as NERC CIP [58]. Most of the devices like RTUs are still embedded devices which do not possess enough computation power to perform encryption and authentication mechanisms. Hence the chances of snooping clear text communications and manipulating control commands or measurements in the communication protocols is a real concern. Therefore, it becomes very necessary to provide tools and methods that analyze the possibility of cyber attacks and enhance application level security with the help of diverse information sources. Designing a secure system should ideally involve a defense-in-depth approach combining infrastructure and application level security mechanisms effectively.

3.1.3 Need for Application Security beyond Infrastructure Security

We briefly look at the need to secure cyber infrastructure involved, and about the relevant standards in place. Equally important to infrastructure security is application security, as state estimation depends heavily on both the SCADA infrastructure and its data. Here, we look at the need to have application specific security analysis beyond traditional IT and infrastructure security.

Lack of adequate security measures at the electronic perimeters for critical infrastructures could lead to attacks in the form of unauthorized access to confidential and critical data, control of cyber infrastructure elements, injection of malicious software, exploitation of security vulnerabilities in poorly patched software, etc. NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system. They not only identify the critical cyber assets in the bulk electric system, but also the vulnerabilities to which they are exposed

to, which could be exploited to create cyber attacks. The following list provides a brief overview of some relevant CIP standards which help reinforce the cyber security of the power grid.

- CIP-002-4 - Requires the identification and documentation of the critical cyber assets which support the reliable operation of the bulk electric power system.
- CIP-003-4 - Talks about minimum security management controls to be put in place so as to protect critical cyber assets from unauthorized access, data and information breaches.
- CIP-005-4 - Requires the identification and protection of the Electronic Security Perimeters (ESPs) inside which all critical cyber assets reside, as well as all access points on the perimeter.
- CIP-007-4 - Mandates the creation of methods, processes, and procedures for securing critical cyber assets within the ESP, which includes an annual cyber vulnerability assessment by responsible entities.

Even though the NERC CIP standards have identified and recommended several best practices for cyber security, the possibility of cyber attacks happening is still high due to several factors. A poor implementation of the standards or security measures, or partial CIP compliance could still present several vulnerabilities which could be exploited to create attacks. Also, the partial or incremental deployment of security measures is another issue which could potentially lead to security holes. It could also be difficult to incorporate modern security mechanisms like encryption, authentication and intrusion detection algorithms, given the moderate capabilities available to several legacy SCADA field devices. Even in the case of complete deployment of security measures as identified by CIP standards, there are possibilities of cyber attacks through insider threats, where the attacker has a very thorough understanding of the systems and the security processes involved [59]. Another interesting possibility is that data integrity attacks could still be possible under a secure infrastructure in the form of a replay attack, where the same set of command packets could be replayed at a later point in time, bypassing the security mechanisms by virtue of eavesdropping. Therefore, it is essential for us

to develop adequate security measures at the application level also, in addition to securing the infrastructure elements, creating a layered defense mechanism against cyber attacks.

3.2 Topology-Based Cyber Attacks

This section explains how the topology of the system can be altered through cyber attacks without being detected by Bad Data Detection (BDD) in SE. The remainder of this section is organized as follows. Section 3.2.1 explains how topology processing, topology error processing, BDD fit in within the overall SE process as described in Figure 3.1. Also, it presents the cyber attack model in detail. Section 3.2.5 explains the method used in creating unobservable topology errors due to cyber attacks and studying their impact in terms of SOL violations. Section 3.2.6 shows how the methodology can be applied to an example power system model to find attack locations and also analyzes attack impacts.

3.2.1 Topology Processing

The Energy Management Systems (EMS) at the control center contain a network model which contains the power system topology information in terms of physical breakers and switches, commonly referred as a breaker-switch model. However, all the traditional power system analysis functions are performed on a bus-branch network model. The bus-branch network model is derived from the breaker-switch model by consolidating the status of breakers and switches obtained from telemetry and obtaining a reduced equivalent network topology[60]. This translation which involves the process of building a network topology is performed by the topology builder or the topology processor.

The topology processor is one of the key components of a state estimator. A wrong network topology can not only result in a significant error in the estimates of the system states, but also sometimes could result in the state estimator solution not converging [61]. This can result in several problems if left unattended for a long time. Operating the power system without a converged SE solution is like flying blind, in other words, the operators will have no situational awareness of the power system operating conditions. There are several procedures in place in the Independent System Operators (ISO)s to specifically handle the occurrence of SE solutions

not converging over a set of consecutive execution runs, as the ISO's are required to maintain a high, valid SE solution availability.

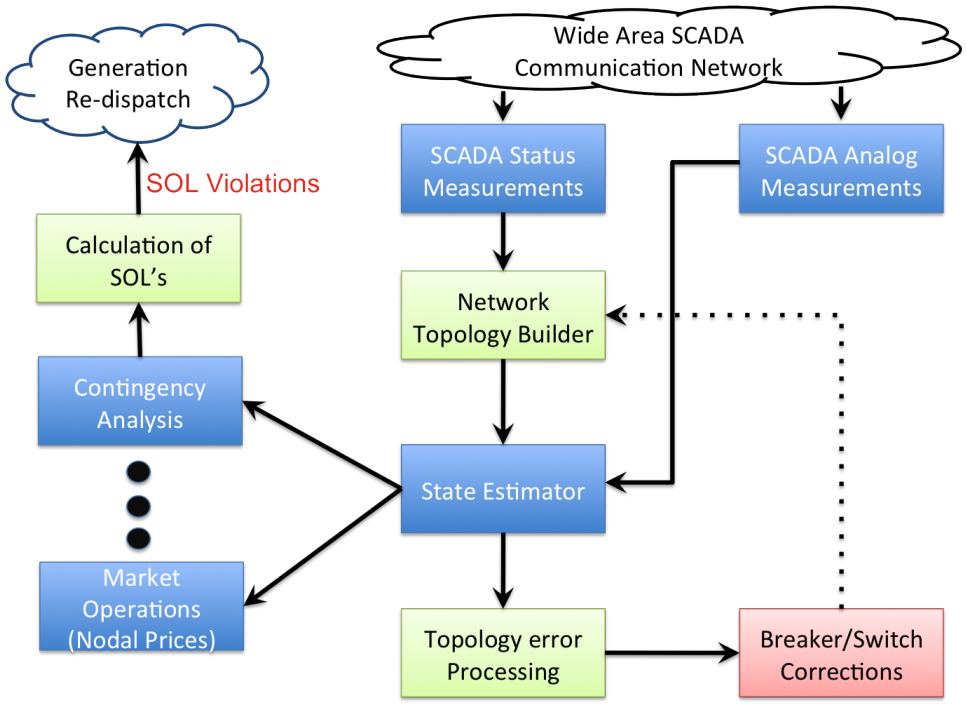

Figure 3.1 Overview of SE in power system operations

3.2.2 Topology Error Processing

Since the process of network topology construction depends on telemetered status measurements from the field devices, it is bound to contain several sources of errors. There are several factors which can contribute to a wrong network topology:

1. Unavailability of status points due to network failure.
2. Faulty field devices.
3. Manual status update of certain devices during maintenance.
4. Outdated status in case of non-telemetered devices.
5. Malicious data manipulation of device status through cyber attacks.

Therefore, every state estimator has a component which validates the network topology identified by the topology processor, and this is known as the topology error processor. There are two broad methods by which this topology error processing can be performed [61],[62]. The first set of methods are a *priori* methods, and are based on simple consistency checks correlating the analog measurements to validate the network topology. Other methods are based on *posteriori* processing, which rely on a converged SE solution to validate the network topology. It is to be noted here that a *prioiri* methods are based on fast and approximate techniques, and are applied usually at the substation level. Therefore, they may fail to identify several topology errors. *Posteriori* methods rely on results of a converged SE, which may not exist in the presence of some topology errors.

3.2.3 Bad Data Detection

One of the main functions of SE is to validate the measurements obtained from SCADA, as they are known to contain measurements with various types of errors. Therefore, detecting and identifying bad data in SE is very important, which is done by comparing the telemetered measurements with the estimated values of the states. It is worth mentioning that bad data detection and identification is dependent on the configuration of the entire measurement set of a system. Bad data in the measurements could be categorized as single or multiple, and interacting or non-interacting. Bad data can be detected using the $Chi-squares$ test or using *normalized residuals*. Identification of bad data, i.e, to find out which measurements actually contain bad data, can be done using *largest normalized residual test* and *hypothesis testing identification* method. One caveat is that bad data can be detected, only if removal of the measurement does not render the system unobservable. This means that bad data in critical measurements cannot be detected.

3.2.4 Cyber Attack Scope and Attack Model

The SCADA analog and status measurements are polled once every 2 to 4 seconds (typically) from RTU in every substation. The RTU collects this information at a much faster rate from IEDs like relays and circuit breakers. These measurements from the RTU travel through a

wide-area communication network to the control center. The communication network could be encrypted and/or authenticated using the protocol specific encryption or end-to-end solutions like Virtual Private Network (VPN) and firewalls.

Timing attacks based on delaying of the data are relevant when there is some sort of control mechanism involved, which requires a strict timing constraint. With respect to SE, since the data is expected to be unavailable occasionally, they do not pose any real threats. Replay attacks are similar in nature to data integrity attacks, where the attacker manipulates the status and analog measurements of the data that the RTU is sending by hijacking the packets in transit from the RTU to the control center. False data injection attacks, which several researchers have discussed with respect to state estimation, and the topology related attacks, which this work identifies, fall under this category. DoS attacks are those where the attacker can flood the communication network with arbitrary traffic to deny service to either the RTU or the control center. This can be achieved by either grabbing the packets sent by the RTU, or by bombarding the RTU, which acts as a server (data source) with too many data requests, causing it to crash.

In this work, the attacker's objective is to create a topology error in the network model which the SE software uses, by intelligently finding appropriate locations inside the model, and attacking the relevant field devices in the SCADA network. The attack model can be characterized by the following set of assumptions:

1. The attacker has access to the SCADA measurement set configuration.
2. The measurement configuration does not have very high redundancy always.
3. Data integrity attacks are possible in cases where internal SCADA network traffic uses a clear text format and the network is protected using some sort of VPN or firewalls.
4. Replay attacks are possible even under encrypted data communications in the SCADA network.

The above stated assumptions are considered to be realistic, considering the current SCADA network environment, which is characterized by legacy devices, protocols and network security

measures. Also, the complexity of cyber attacks executed in the recent past on SCADA networks like Stuxnet [8], strengthen the validity of our assumptions.

3.2.5 Method to Create an Unobservable Cyber Attack through Topology Errors

It is obvious that a topology error can be created by manipulating any single field device through an arbitrary cyber attack. However, this type of naive attack can be easily detected as SE contains a bad data detection component, which identifies the topology error appropriately. An intelligent adversary would go well beyond the naive attack described above to remain undetected. There are certain elements in the SCADA measurement configuration which when manipulated can slip unnoticed by traditional bad data detection methods.

This section will describe the steps which are involved in creating such an attack by identifying what measurements are to be manipulated and thereby identify the attack target also (i.e. the corresponding breaker or field device). Also, this section will explain the steps to quantify attack impact in terms of SOL violations, which are monitored by operators constantly in everyday operations. There are NERC standards which stipulate that the power system is always operated under SOL for all the line flows, voltage limits, etc., and any SOL violation needs to be addressed to within a period of 30 minutes through a generation re-dispatch [63],[64],[65]. The adversary's aim is to create this unnecessary re-dispatch by causing some SOL violations, leading to potentially unhealthy system conditions, while also causing economic impacts.

The following subsections will explain in detail the method of creating an unobservable cyber attack by manipulating the network topology selectively at carefully defined locations. Figure 3.2 presents an overview of the method described below.

3.2.5.1 Identifying Critical Measurements

There are certain measurements in a SCADA measurement configuration called 'critical measurements,' which when removed makes some portion of the system unobservable. The approach to identify the critical measurements in a measurement configuration described below has been adopted from [61]. In this analysis, we use the linear Weighted Least Squares (WLS) formulation for our SE model. The problem of interest to us lies in the observability analysis

of the system and this is independent of the branch parameters or the operating state of the system. Hence, for simplicity we assume all bus voltages to be 1.0 $p.u.$ Our problem now is to estimate the phase angles at all the buses in the system except the slack bus. Let $n,\ m$ be the total number of states and measurements in the sytem($m \geq n$).The measurement vector z is related to the state vector x according to the following equation:

$$z = Hx + e \tag{3.2}$$

where,

z is a $m \times 1$ vector which contains m injection and flow measurements in total, x is a $n \times 1$ vector of the system states, e is a $m \times 1$ vector of the measurement errors.

H is a $m \times n$ matrix which is the Jacobian matrix of the measurement matrix $h(x)$.

By definition, "critical measurements" are those whose removal leads to an unobservable network [61]. There are different methods by which one can obtain the critical measurements in the measurement configuration. One of them is given below:

Choose a set of n measurements out of the available m measurements to be the "essential measurements". It is to be noted here that this set is not unique in general, but will contain all of the critical measurements, as without those the system would be unobservable. Ordering the essential measurements first, we can write the measurement equations as

$$\begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \cdot [x] = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \tag{3.3}$$

where H_1, H_2 correspond to the essential and non-essential measurements z_1, z_2 respectively. Applying the Peters-Wilkinson decomposition[66] method,

$$\begin{bmatrix} H_1 \\ H_2 \end{bmatrix} = \begin{bmatrix} L_1 \\ M_2 \end{bmatrix} \cdot \begin{bmatrix} U \end{bmatrix} \tag{3.4}$$

where L_1 is a $n \times n$ lower triangular matrix,

M_2 is a $(m-n) \times n$ rectangular matrix,

U is a $n \times n$ upper triangular matrix,

Based on matrix algebra we can write,

$$z_1 = L_1.U.x \tag{3.5}$$

$$z_2 = M_2.U.x \tag{3.6}$$

$$z_2 = M_2.L_1^{-1}.z_1 \tag{3.7}$$

$$z_2 = T.z_1 \tag{3.8}$$

Here we can see that the non-essential measurements z_2 are dependent linearly on essential measurements z_1. Therefore, an element of z_1 is critical if the corresponding column of T is null. If the critical measurement identified by the null column of T is removed from the measurement set, the system cannot be said to be fully observable any more.

3.2.5.2 Identifying Critical Branches

The method in the previous subsection identifies the critical measurements in a given measurement set. Similar to these, we can identify the critical branches in a measurement configuration. Critical branches are those branches of a measured, observable network, whose removal renders the system unobservable. The critical branches in a measurement set can be found using the following method[61].

The effect of topology errors in the Jacobian matrix H can be modeled as

$$H = H_e + E \tag{3.9}$$

where,

H_e represents the erroneous Jacobian matrix

E represents the Jacobian matrix error

The measurement residuals denoted by r, can be written as

$$r = z - H\hat{x} = T_{cb}.\Delta f \tag{3.10}$$

where, Δf is a vector of branch flow errors. From [61], matrix T_{cb} can be shown to be equal to

$$T_{cb} = (I - K)M\Delta f \tag{3.11}$$

$$K = H_e(H_e^T.R^{-1}.H_e)^{-1}H_e^T R^{-1} \tag{3.12}$$

where,

I is the identity matrix

R is the diagonal co-variance matrix

M is the measurement topology matrix

A null column in T_{cb} would make a zero entry in the residual matrix no matter what the branch flow error is, thereby evading bad data detection.

Based on the proofs in [67], we can say that a branch is not single topology error detectable, if it is a critical branch, or incident only to critical measurements. Hence, after we obtain the critical measurements or critical branches, we can identify the locations of the field devices which are prone to topology manipulations through cyber attacks.

3.2.5.3 Analysis of Impacts: Computation of SOL for Transmission Lines

Once a particular attack to create an unobservable topology error can be identified, the next step is to study the impact it causes on the power system operations. As defined earlier, the output of SE is used in CA, Market analysis tools like SCOPF, etc. We choose to show the impact in terms of violations of SOL, which are the most constraining operating limits on line flows, system voltages etc., for the system under a set of credible contingencies. Computation of SOL for a particular line requires information about the line flow ratings denoted by f_l^{max}, the linear Generation Shift Factors (GSF) denoted by a_{li} and the Line Outage Distribution Factors (LODF) denoted by $d_{l,k}$.

$$a_{li} = \frac{\Delta f_l}{\Delta P_i} \tag{3.13}$$

where, the GSF identifies the change in flow on a given line l for a change in power injection at bus i.

$$d_{(l,k)} = \frac{\Delta f_l}{f_k^0} \tag{3.14}$$

where, the LODF identifies the change in flow on a line l for an outage on line k, for a pre-outage flow of f_k^0 on line k. The SOL for a given line for a particular contingency is given

by

$$f_l^{sol} = f_l^0 + \frac{(a_{li} - a_{lj})(f_l^{max} - f_l^0 - d_{l,k}.f_k^0)}{a_{li} - a_{lj} + d_{l,k}(a_{ki} - a_{kj})} \tag{3.15}$$

where, f_l^{SOL} provides the SOL under one particular contingency and a defined stress direction for power transfer. However, in practice the Equation 3.15 should be computed for every contingency on a screened contingency list and the lowest value among those gives the SOL for every line flow [68].

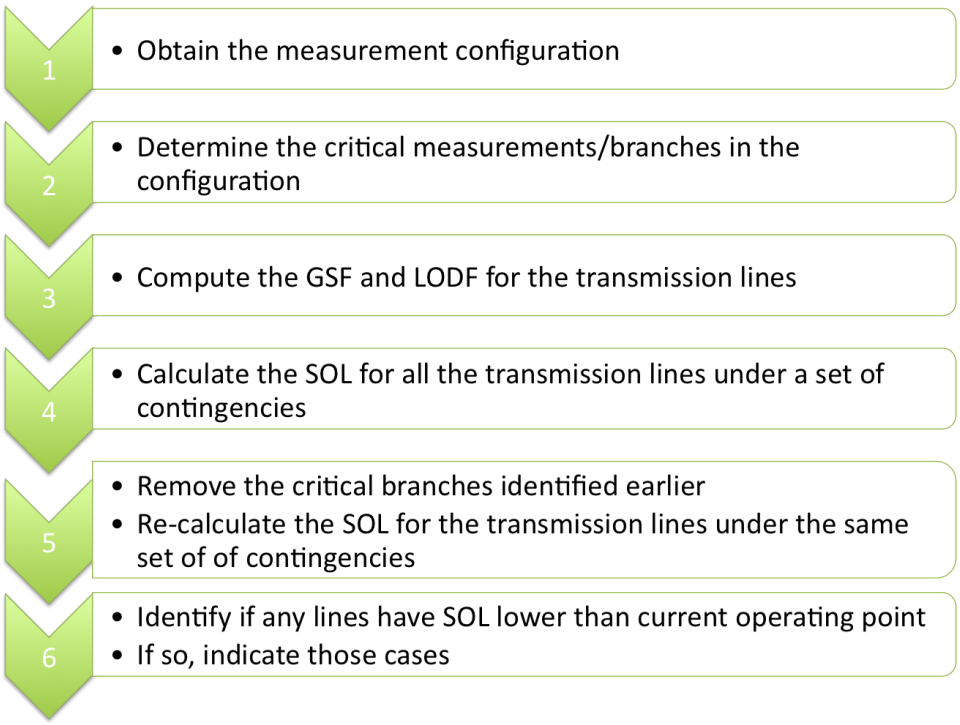

Figure 3.2 Method for creating an unobservable attack and studying its impacts

3.2.6 Case Study

The method described in Section 3.2.5 has been applied to the IEEE 14-bus power system model to identify the critical measurements and branches and also to show the impacts of the topology-based cyber attack. Figure 3.3 shows the IEEE 14-bus system model. The impedances of the transmission lines and its ratings are shown in Table 3.1. The line flow measurements and power injection measurements are shown in Figure 3.3 with rectangular boxes and arrow heads

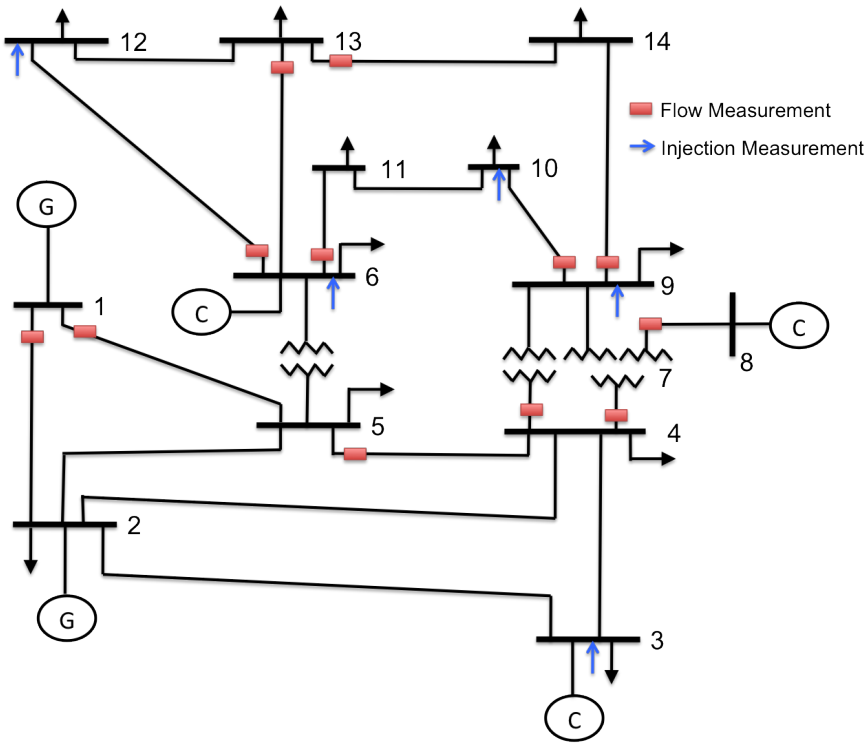

Figure 3.3 IEEE 14-bus power system with measurement configuration

respectively. The measurement configuration has 17 measurements in total for estimating 13 states (phase angles) in the system.

3.2.6.1 Finding the Critical Measurements/Branches

The measurement matrix z is given as

$$z = \begin{bmatrix} P_{1-2} \\ P_3 \\ P_{5-4} \\ P_{4-7} \\ P_6 \\ P_9 \\ P_{7-8} \\ P_{9-10} \\ P_{1-5} \\ P_{10} \\ P_{12} \\ P_{13-6} \\ P_{9-14} \\ P_{6-11} \\ P_{4-9} \\ P_{6-12} \\ P_{13-14} \end{bmatrix} \tag{3.16}$$

where,

P_i is the power injection measurement at any bus i.

P_{j-k} is the power flow measurement on line between bus j and bus k.

The measurement Jacobian matrix H is of the order 17×13. Based on the procedure mentioned in Section 3.2.5.1 for obtaining the critical measurements, the T matrix (4×13) has been computed. The null columns found in T are columns 1, 2 and 7, which correspond to the critical measurements being P_{1-2}, P_3, P_{7-8}.

Table 3.1 IEEE 14-bus system parameters

Line number	**Reactance(p.u)**	**Line rating(p.u)**
$1-2$	0.05917	2
$1-5$	0.22304	2
$2-3$	0.19797	2
$2-4$	0.17632	2
$2-5$	0.17388	2
$3-4$	0.17103	2
$4-5$	0.04211	1.5
$4-7$	0.20912	1.5
$4-9$	0.55618	2
$5-6$	0.25202	1.5
$6-11$	0.19890	2
$6-12$	0.25581	2
$6-13$	0.13027	1.5
$7-8$	0.17615	2
$7-9$	0.11001	2
$9-10$	0.08450	2
$9-14$	0.27038	2
$10-11$	0.19207	1.5
$12-13$	0.19988	2
$13-14$	0.34802	1.5

Similarly, using the procedure mentioned in Section 3.2.5.2 for obtaining the critical branches, the T_{cb} matrix (17×20) has been computed and columns 1, 2, 3, 4, 5, 6 and 14 contain all zeros. These correspond to the following branches in the 14-bus system, namely 1-2, 1-5, 2-3, 2-4, 2-5, 3-4, 7-8. Out of these, branches between buses 1-5, 2-3, 2-4, 2-5 and 3-4 do not contain any measurements and are therefore irrelevant measurements. The branches 1-2, 7-8 are the critical branches.

3.2.6.2 Cyber Attack Impact Analysis

The base case power flow conditions are given in Table 3.2.

Table 3.2 Base case power flow conditions

Bus number	**Generation(p.u)**	**Load(p.u)**
1	2.81	0
2	1.0	0.217
3	0	0.942
4	0	0.7
5	0	0.2
6	0	0.112
7	0	0
8	0	0
9	0	0.25
10	0	0.29
11	0	0.2
12	0	0.25
13	0	0.35
14	0	0.3

The GSF's for this network model are of the order 20×14 and are therefore omitted for the sake of space. Every column in the GSF matrix represents the a bus at which the injection change takes place and every row represents the particular transmission line on which the change in flow is to be computed.

The LODF's are of the order 20×20 and are also omitted for the same reason as above. Every column in the LODF matrix represents the contingency where a particular transmission

line is outaged, and every row represents the line at which the change in post-contingency flow is to be measured.

Table 3.3 SOL and pre-contingency line flows before the attack

Line	**SOL before attack(p.u)**	**Line flows before attack(p.u)**
$1-2$	1.8834	1.7574
$1-5$	1.3907	1.0536
$2-3$	1.4650	0.8732
$2-4$	1.2172	0.9137
$2-5$	1.1731	0.7535
$3-4$	-2.0	-0.0688
$4-5$	-1.5	-0.7145
$4-7$	0.7517	0.5427
$4-9$	0.6594	0.3167
$5-6$	0.9782	0.8926
$6-11$	0.4921	0.1492
$6-12$	0.5708	0.2256
$6-13$	0.61	0.4057
$7-8$	2	0
$7-9$	0.8498	0.5427
$9-10$	0.6865	0.3408
$9-14$	0.6217	0.2686
$10-11$	0.3553	0.0508
$12-13$	-2.0	-0.0244
$13-14$	0.3061	0.0314

Of the critical branches identified earlier, branch 7-8 is a branch where a transformer is connected to a synchronous condenser. Since we are using a DC power flow model, it will not carry any power on it and therefore would yield a trivial result. Let us remove the critical branch 1-2 to model an unobservable topology error caused by a cyber attack. On removal of this branch, the H matrix will now become a 16×13 matrix. In the new H matrix, even though there are 16 measurements available to estimate the 13 system states, the system is not totally observable. This can be identified by the rank of the new H matrix, which reduces to 12 due to the removal of the critical branch.

Since the attack has changed the network topology, we need to re-evaluate the GSF's and LODF's again. The new GSF matrix is of the order 19×14 and the new LODF matrix is of

Table 3.4 SOL and pre-contingency line flows after the attack

Line	**SOL after attack(p.u)**	**Line flows after attack(p.u)**
$1-2$	NA	NA
$1-5$	**2.0**	**2.8110**
$2-3$	1.1846	0.5765
$2-4$	0.8843	0.2927
$2-5$	-2.0	-0.0862
$3-4$	-2.0	-0.3655
$4-5$	$\mathbf{-1.5}$	$\mathbf{-1.5815}$
$4-7$	**0.3706**	**0.5107**
$4-9$	0.6126	0.2980
$5-6$	**0.6571**	**0.9433**
$6-11$	0.4395	0.1798
$6-12$	0.5209	0.2301
$6-13$	0.5790	0.4214
$7-8$	2.0	0
$7-9$	0.8097	0.5107
$9-10$	0.6407	0.3102
$9-14$	0.5736	0.2485
$10-11$	0.3154	0.0202
$12-13$	-2.0	-0.0199
$13-14$	0.2645	0.0515

the order 19×19. The SOL and the pre-contingency line flows in the transmission lines before and after the attack are given in Table 3.3 and Table 3.4 respectively.

3.2.7 Discussion

By definition, SOL specifies the maximum pre-contingency line flows on a given transmission line for a particular network topology. We can see that the pre-contingency line flows before the attack are less than the SOL's from Table 3.3. The perceived line flows according to the new network topology after the attack are much closer to their limits in several of the lines, as though a contingency(outage of line 1-2) has already occurred. We can see from the **bold** entries of Table 3.4 that the corresponding lines 1-5, 4-5, 4-7 and 5-6 have SOL violations after the cyber attack.

This has provided an illusion that these lines have SOL that is lower than the current line flows. This change in SOL is not accompanied by any alarms from SE as the cyber attack has been created to introduce a topology error unobservable in bad data detection. The operator would thereby re-dispatch the generation so as to alter the line flows to be within the limits as per the NERC operational guidelines. This re-dispatch may result in a dangerous scenario if there are any real contingencies which occur during that time, which would not have otherwise occurred if the attack was detected. This re-dispatch also has an impact in the markets as it causes the LMPs to change unnecessarily causing potential losses to customers.

3.2.8 Conclusions

This work addresses the problem of how topology errors, in particular, the branch status errors, can be created by malicious adversaries through intelligent cyber attacks. We have shown how an unobservable topology error can be created by manipulating the field devices corresponding to the critical measurements or critical branches in the SCADA measurement set configuration. Also, we have shown how the impacts of such an attack can be analyzed through SOL violations on the altered network topology.

3.3 Offline Mitigation: Attack-resilient Measurement Design

Section 2.3.3 explained the attributes of good measurement design and reviewed relevant literature in this area. In this section, we describe in detail an attack-resilient measurement design methodology that extends traditional measurement design with consideration for the loss of multiple measurements including loss of entire substation data, and also the ability to detect bad data in the presence of malicious data manipulations due to a cyber attack by ensuring adequate redundancy, and bad data detection capabilities of the resultant measurement configuration [69].

3.3.1 Attack-Resilient Measurement Design Methodology

Figure 3.4 presents the proposed methodology for attack-resilient measurement design. We consider the existing measurement set configuration as a baseline. For the existing measurement set, we generate the list of possible scenarios to be included for our analysis of the measurement design. We include the loss of any two measurements and branch outages involving two components also in our preliminary analysis to eliminate the presence of critical measurements in the measurement set. When the measurement set has no critical measurements, we then consider the list of scenarios that involve loss of one and two RTUs. In order to simulate the case of RTU failure, we remove all the measurements that are associated with a particular bus.

In general, the method checks the observability of the measurement set for each scenario, and if the contingency (either loss of measurement or branch outage) does not involve any loss of observabiility we ignore that case and skip to the next scenario. In cases where there is a loss of observability, we identify possible pseudo-measurements that need to be added to the measurement set to restore observability. Mostly, the pseudo-measurements used are injection measurements that are obtained from forecasts at the respective buses. We obtain pseudo-measurements by adding the appropriate errors to the actual measurements based on the statistical model of the pseudo-measurements. After we insert the pseudo-measurements to the measurement set, we consider a load scenario, and perform state estimation using a power flow model. Based on the power flow and a measurement model we perform state estimation

along with the pseudo-measurements and identify the deviation of the line flows with and without pseudo-measurements. We choose line flow violations as one of the metrics because incorrect line flows could mislead the operators into believing that there are SOL violations for line flows. According to NERC operational standards, all SOL violations for all the line flows need to be addressed using generation redispatch within 30 minutes [63],[64],[65]. As the accuracy of pseudo-measurements could vary depending on the forecast accuracy, we assumed accuracy parameters to generate the pseudo-measurements for the purpose of this analysis.

We can also check for accuracy metrics specific to state estimators as defined in [70]. If the chosen metrics are under threshold, we move to the next scenario as this scenario provides acceptable performance with available pseudo-measurements. If the inclusion of pseudo-measurements does not provide acceptable performance, we add the scenario to the list of scenarios for addition of new measurements in a measurement design or PMU placement problem. After we identify all possible such scenarios that need new candidate measurements to provide acceptable performance, we can obtain optimal placement of measurements using one of the methods mentioned in [43, 45, 44, 46, 42].

We choose to adopt a similar optimization formulation as mentioned in [42]. The measurement placement is formulated as a binary integer linear optimization problem. The decision variables are whether a given candidate measurement is chosen to be part of the new measurement placement or not. The objective of the problem is to minimize the cost of new measurements subject to the constraints that the resulting measurement set is always observable under the different scenarios. Mathematically, the problem can be stated as:

$$\min C^T \cdot X$$

$$subject\ to\ A \cdot X \geq b$$

$$A_{ij} = \begin{cases} 1 & \text{if measurement } j \text{ is selected} \\ & \text{as a candidate for scenario } i \\ 0 & \text{otherwise} \end{cases}$$

$$X(i) = \begin{cases} 1 & \text{if measurement } i \text{ is selected} \\ 0 & \text{otherwise} \end{cases}$$

$$b^T = [2\ 2\ ..\ 1\ ...\ 2..]$$

where, C is the cost vector for new candidate measurements. X is the candidate measurement selection vector, which determines whether candidate measurement i is chosen or not. A matrix represents the suitability of a particular candidate measurement j for a scenario i considered. The overall dimension of the A matrix depends on the number of scenarios considered and the number of candidate measurements used. b is a vector of 1 or 2's depending on whether scenario i results in rank reduction of one or two in the measurement Jacobian matrix. The optimization problem requires a set of candidate measurements as inputs, but is independent of the method used to choose them for a particular scenario.

The attack-resilient measurement design approach greatly improves the redundancy, reliability, bad data detection capabilities of the measurement configuration for state estimation and it not only addresses the cyber attacks that target availability of multiple measurements or RTUs, but also eliminates a large possibility of low-sparsity stealthy cyber attacks as discussed in [23, 35]. In other words, we can say that due to the increased measurements in the measurement configuration, the minimum amount of effort that is needed to influence a single state variable without being detected in bad data detection is increased. We also believe that complementing this approach with some of the existing PMU placement methods that provide

complete observability, we can even further improve the resiliency and robustness of the state estimators against various forms of cyber attacks.

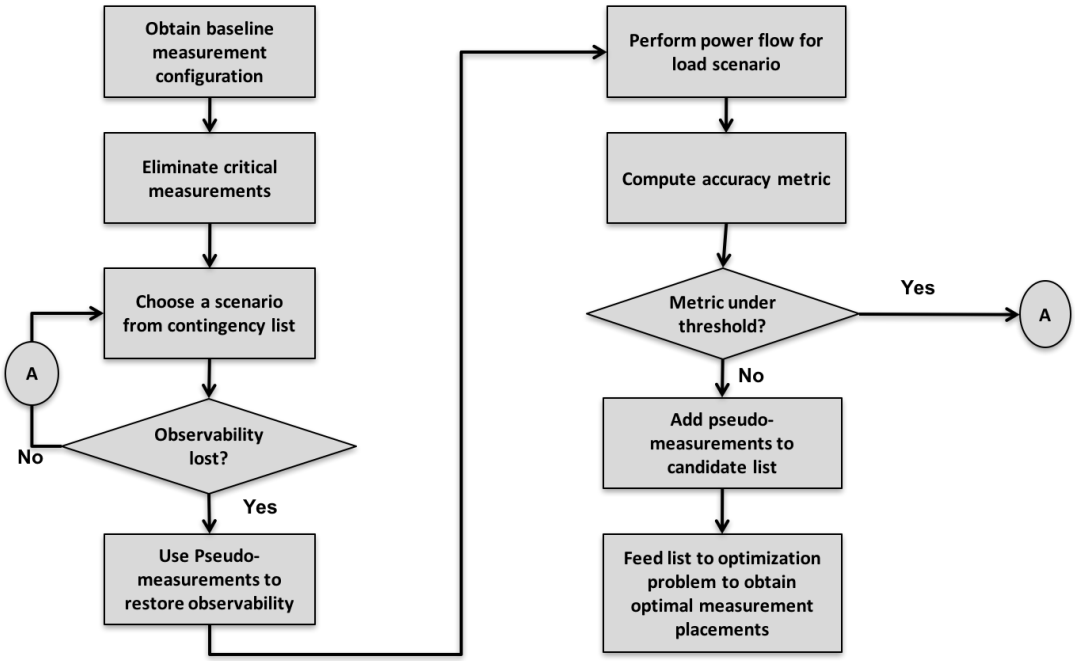

Figure 3.4 Flowchart of attack-resilient measurement design

3.3.2 Case Study on IEEE 14-Bus System

In this section, we present a case study for the proposed attack-resilient measurement design approach using the IEEE 14-bus system. Figure 3.3 shows the IEEE 14 -bus system with the baseline measurement configuration. We consider only the estimation of phase angles in this case study for simplicity. This configuration has 17 measurements to estimate 13 states (phase angles). The measurements that are included in the baseline measurement set are shown in Table 3.6. P_i is the power injection measurement at any bus i, and P_{j-k} is the power flow measurement on the line between bus j and bus k.

In this measurement configuration we have four critical measurements P_{1-2}, P_{1-5}, P_3, P_{7-8}. In our preliminary analysis, we found that for the list of scenarios that involve loss of two measurements, there were 60 occurrences where complete observability was lost. Out of 60

scenarios, most of the scenarios involved the loss of one of the four critical measurements and another redundant measurement. There were also 2 critical pairs of measurements identified. There were 6 scenarios where two critical measurements were lost. The critical measurement pairs are $P_{5-4},\ P_6$ and $P_{4-7},\ P_9$.

We augmented this baseline measurement set with additional measurements to eliminate all critical measurements, before further analyzing them for loss of multiple measurements failing at substation level (i.e) RTU failures. The additional measurements that were added are $P_1,\ P_{3-4},\ P_7,\ P_{2-3}$. We then considered the loss of all possible scenarios where any two RTUs would fail simultaneously to perform our analysis. In order to model the measurement loss at RTU level, we remove all the measurements corresponding to a particular bus from the measurement set and then test for observability. If the resulting measurement matrix is not of full rank, we use pseudo measurements to restore observability and then perform state estimation using a load scenario and a DC power flow model. We add random normal distribution errors to the DC power flow solutions to generate actual state estimation measurements. We consider the relative confidence of regular measurements to be 0.01 and accuracy of pseudo measurements to be 0.1 in our case study.

Table 3.5 Base case load scenario

Bus number	**Generation (p.u)**	**Load (p.u)**
1	2.81	0
2	1.0	0.217
3	0	0.942
4	0	0.7
5	0	0.2
6	0	0.112
7	0	0
8	0	0
9	0	0.25
10	0	0.29
11	0	0.2
12	0	0.25
13	0	0.35
14	0	0.3

The load scenario that we used in our case study is shown in Table 3.5. We considered our accuracy metric to be a difference of 0.1 p.u in the estimated line flows after the use of pseudo-measurements. If the use of pseudo-measurements violated the metric, we identify those scenarios as those where we need new measurements instead of using pseudo-measurements.

In the IEEE 14-bus system, for our measurement configuration, there were 91 possible scenarios with loss of two RTUs. Out of that, 23 of the scenarios violated the flow deviation metric for the load scenario and one specific realization of pseudo-measurements considered. We note here that the number of scenarios that exactly violate the metric depends on these two factors and a more accurate analysis can be performed by repeating simulation runs and choosing parameters based on actual worst case values.

Once we obtain the scenarios that need measurements added to ensure acceptable state estimator performance, we select candidate measurements and feed them as inputs to the binary integer optimization problem as explained previously. In this case study, we use branch flow measurements only as the candidate measurements, although this method also works equally well with injection measurements included. The cost vector C is assumed to be all 1's in our case although this also could be varied if more data was available about specific substation level meter deployment costs. Depending on the selection of candidate measurements, we can populate the A matrix for all scenarios. The b matrix is also populated with 1's or 2's depending on the particular scenarios considered, and the corresponding rank reduction in the measurement Jacobian matrix. Table 3.7 presents the candidate measurements selected in integer optimization problem for the IEEE 14-bus system for addition into the existing measurement set to tolerate loss of upto any 2 RTUs simultaneously.

Table 3.6 IEEE 14-bus system baseline measurements

Baseline measurement set
$P_{1-2}, P_3, P_{5-4}, P_{4-7}, P_6, P_9, P_{7-8}, P_{9-10}, P_{1-5},$ $P_{10}, P_{12}, P_{13-6}, P_{9-14}, P_{6-11}, P_{4-9}, P_{6-12}, P_{13-14}$

Table 3.7 Results of measurement placement

Selected new flow measurements
$P_{2-1}, P_{3-2}, P_{4-3}, P_{5-1}, P_{6-12}, P_{7-8}, P_{8-7},$ $P_{9-10}, P_{10-9}, P_{11-6}, P_{12-6}, P_{14-9}$

3.3.3 Practical Challenges

One of the main challenges in designing a measurement set with all possible scenarios for the loss of any two RTUs is the size of the problem. If we were to consider all possible cases in the analysis, the number of scenarios would quickly become intractable, even for moderately sized systems due to its combinatorial nature. However, we can eliminate a lot of scenarios from the analysis with the help of knowledge about practical implementations of existing measurement configuration. We can rule out cases where possibilities of two RTUs that do not share common network routes or eliminate certain RTUs that have adequate backup, etc. Existing cyber security measures at substations would also help in further reducing the size of the problem.

3.3.4 Conclusions

In this work, essentially, scenarios of multiple measurement loss where pseudo-measurements cause unacceptable deviations in state estimates or related accuracy metrics was identified. Then, the list of scenarios was fed into an optimization problem to obtain a least cost measurement set that ensures system observability and acceptable estimator performance. Also, the obtained measurement set would provide increased resiliency against stealthy data injection attacks by increasing the minimum effort needed by the adversary.

CHAPTER 4. ATTACK-RESILIENT ANOMALY DETECTION

In this chapter, we describe an online attack-resilient anomaly detection method that utilizes load forecasts, generation schedules, and synchrophasor data to coarsely validate state estimates and detect anomalies [71]. While Section 3.3 presented an offline approach to make the state estimation more resilient to cyber attacks, Section 4.1 introduces the proposed online anomaly detection method to detect stealthy cyber attacks. Section 4.2 presents the case study and performance analysis of the proposed method on IEEE 14-bus test system. Section 4.3 summarizes the chapter contributions and briefly discusses future work.

4.1 Proposed Online Anomaly Detection Methodology

The proposed online methodology for detecting stealthy false data injection attacks on state estimators by leveraging information that is separate from SCADA measurements to detect measurement anomalies. As mentioned earlier, the proposed methodology differs from existing offline solution approaches that either rely on infrastructure security mechanisms, or adding new measurements. The proposed anomaly detection algorithm would serve as a complementary tool to SE by detecting malicious measurement manipulations due to stealthy attacks, which could otherwise go undetected.

4.1.1 Proposed Detection Methodology

The proposed detection methodology, shown in Figure 4.1, makes use of the existing SCADA measurements, and in addition, uses load forecasts, generation schedule information, and existing synchrophasor data to detect measurement anomalies in state estimators. Existing SCADA measurements contain *status measurements*, which are used to perform topology processing, and *analog measurements*, which are used along with the output of topology processing to

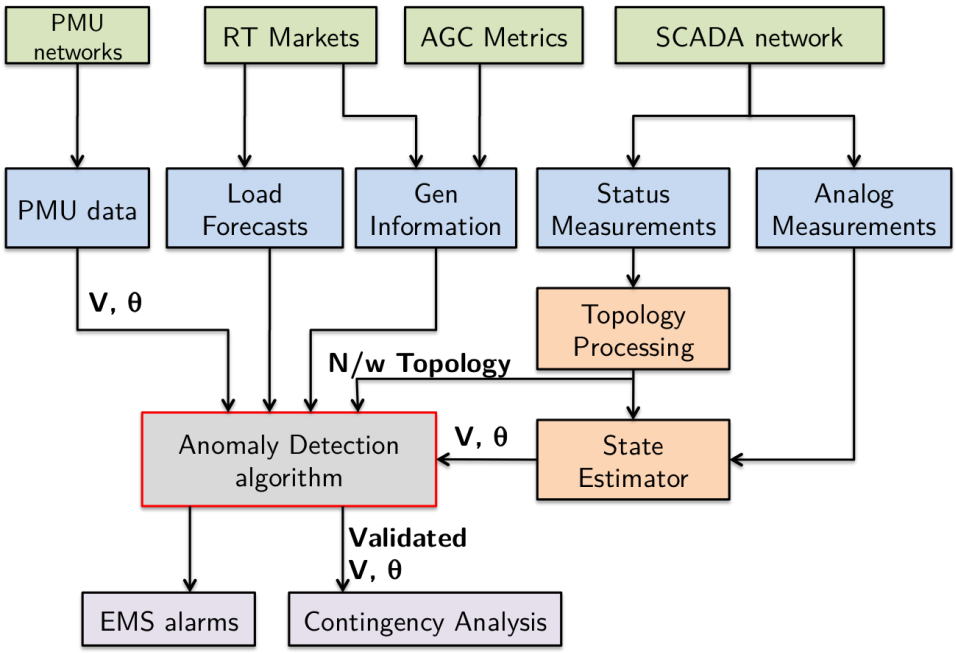

Figure 4.1 Overview of proposed anomaly detection methodology

perform conventional SE. The proposed approach uses the output of the topology processor to update its current network model and system parameters for the anomaly detection algorithm. Real-time short-term load forecast information (at the individual bus level), and generation schedule information, which are available as part of the real-time energy markets are also fed as inputs to the algorithm. In addition, the proposed approach utilizes real-time data from existing PMU deployments, which are obtained from a separate communication network. Typically, the SCADA measurement data gets updated once every 4-8 seconds and typical ISO intervals between successive SE is between 1.5 to 5 minutes. Real-time short term load forecasts are updated once every 5 minutes and generation schedules are updated once every hour in real-time energy markets.

Since the proposed algorithm depends on the update frequency of load forecasts, it would be executed once every 5 minutes, where the appropriate forecast-based estimates and the corresponding state estimator outputs would be compared. Because the detection methodology relies on load forecasts there could be false positives, i.e. large deviations from forecast-based

predictions, which could limit the minimum attack that can be detected. While this could be captured to some extent through statistical characterization using historical data, the balance between false alarm probability and detection probability could be adjusted favorably with better forecasts and the availability of more secure PMU measurements. In addition, real-time operational metrics from the AGC algorithm could be used to further narrow down the false positives due to forecast/real-time operational abnormalities and improve the performance of the anomaly detection algorithm.

The use of load forecasts for pseudo-measurements in state estimators has been known for a long time [61, 62]. Typically, pseudo-measurements are included only when there is a loss of system observability. It is also well known that the use of pseudo-measurements will adversely affect the quality of state estimates produced if used incorrectly [38]. However, the integration of pseudo-measurements directly into state estimator would not be a suitable solution to the problem of detecting stealthy false data injection attacks, because we would not know what measurements have been corrupted (the attack would cause no change in normalized measurement residuals). Therefore, we would not be able to identify where pseudo-measurements need to be inserted.

Recently, the integration of PMU measurements in SE has been a research topic of interest to increase redundancy and bad data detection [72, 73]. However, solutions that integrate additional measurements like PMUs into the SE measurement configuration are part of offline solution approaches and are outside the scope of the paper. Also, as mentioned previously, the offline solutions would be inadequate if attacker resources are increased.

In this work, our main emphasis is not to make any changes directly in SE by adding forecast-based estimates or PMU data into the measurement set to improve bad data detection capabilities, rather it is to develop an anomaly detection algorithm that can detect gross measurement anomalies due to stealthy cyber attacks by predicting states independently and comparing them with state estimator outputs using information that is independent from the untrusted SCADA measurements.

4.1.2 Anomaly Detection Algorithm

Figure 4.2 shows a detailed flowchart of the analysis that is performed by the proposed anomaly detection algorithm. The key steps that are performed as part of the proposed anomaly detection algorithm are described in detail below.

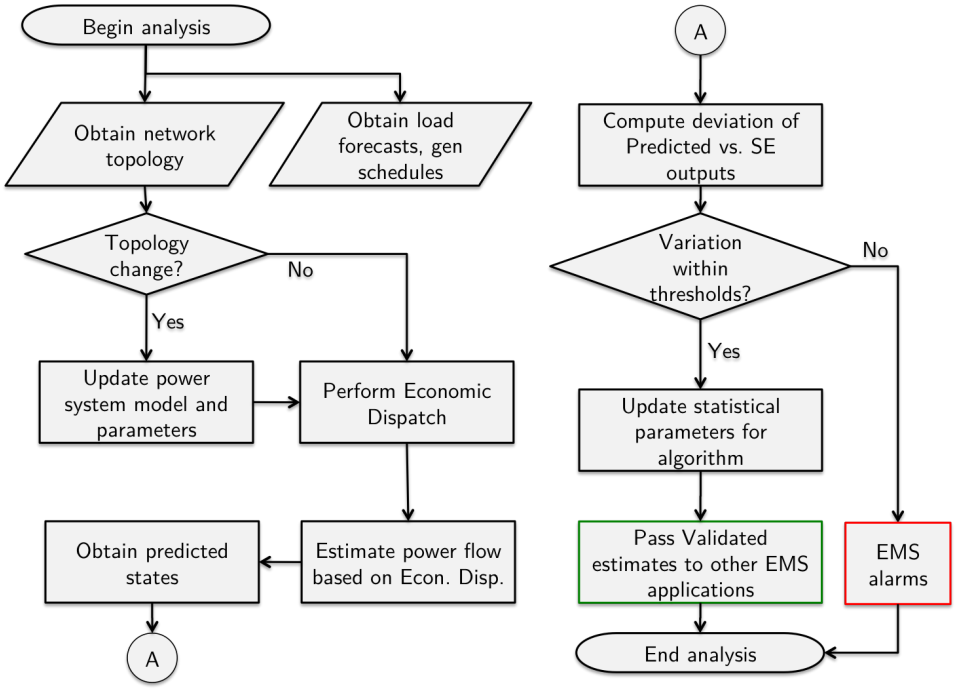

Figure 4.2 Anomaly detection algorithm flowchart

Step 1: Update Power System Model

The output of the topology processor is used to obtain the latest network topology from SCADA status measurements. Based on the current topology, the power system model and its corresponding parameters are updated in the algorithm. Simultaneously, for each 5 minute interval, real-time generation schedules and forecast information are obtained from the real-time markets.

Step 2: Perform Economic Dispatch

The data obtained is fed as an input to the economic dispatch algorithm. Eq. 4.1-4.4 describe the standard economic dispatch formulation to obtain the optimal generation set points that could exist for the next interval. c_i represents the generator cost curves of each of the m generators, P_{gen_i} represents the generator output which is to be obtained, $P_{loss}(P_{gen})$ represents the transmission line losses as a function of generator outputs, P_{load_total} represents the total system load obtained from load forecasts. $P_{gen_i}^{min}$ and $P_{gen_i}^{max}$ represent each generator's limits.

$$\min \sum_{i=1}^{m} c_i(P_{gen_i}) \tag{4.1}$$

$$\sum_{i=1}^{m} P_{gen_i} - P_{loss}(P_{gen}) - P_{load\_total} = 0 \tag{4.2}$$

$$P_{gen_i}^{min} \leq P_{gen_i} \leq P_{gen_i}^{max}, \ \forall i = 1, ...m \tag{4.3}$$

$$P_{gen_i} \geq 0, \ \forall i = 1, ...m \tag{4.4}$$

Step 3: Calculate Power Flow Based on Economic Dispatch

Based on the estimated generation set points from the economic dispatch, a power flow algorithm is run to obtain the line flows and voltages at different buses in the system model. Eq. 4.5-4.8 describe the power flow problem, where the unknowns are the $N-1$ phase angles and the $N-N_G$ voltages in the system (N, and N_G represents the total number of buses and generators respectively). There are a total of $2N-N_G-1$ unknowns. Typically, the power flow problem is solved using an iterative method such as the Newton-Raphson method, where the update formula for the $(i+1)^{th}$ iteration is given by Eq. 4.6. J represents the system's Jacobian matrix. P_k and Q_k represent the real and reactive power injections at each bus except the slack bus, which is obtained from a difference of the real, reactive power outputs P_{gen}, Q_{gen} and the real, reactive loads P_{load}, Q_{load} respectively as shown in Eq. 4.7 and Eq. 4.8. Eq. 4.9 shows $f(x)$ expressed as the vector of real and reactive power mismatches between the iteratively calculated power injections and the actual power injections at a bus.

$$f(\underline{x}) = 0,\ \underline{x} = \begin{bmatrix} \underline{\theta} \\ \underline{V} \end{bmatrix} \tag{4.5}$$

$$\underline{x}^{(i+1)} = \underline{x}^{(i)} - J^{-1}\underline{f}(\underline{x}^{(i)}) \tag{4.6}$$

$$P_k = P_{gen_k} - P_{load_k}, \forall k = 2, ..., N \tag{4.7}$$

$$Q_k = Q_{gen_k} - Q_{load_k}, \forall k = N_{G+1}, ..., N \tag{4.8}$$

$$f(\underline{x}) = \begin{bmatrix} P_2(\underline{x}) - P_2 \\ . \\ P_N(\underline{x}) - P_N \\ Q_{N_G+1}(\underline{x}) - Q_{N_G+1} \\ . \\ Q_{2N-N_G-1}(\underline{x}) - Q_{2N-N_G-1} \end{bmatrix} = \begin{bmatrix} 0 \\ . \\ 0 \\ 0 \\ . \\ 0 \end{bmatrix} \tag{4.9}$$

Equivalently, steps 2 and 3 could be combined into an Optimal Power Flow (OPF) formulation, which combines power flow constraints with economic dispatch. In that formulation, in addition to P_{gen_i}, all the branch flows (P_B), and phase angles (θ) would also be part of the solution vector. Correspondingly, power flow equations and limits would have been added to the existing constraints to ensure power flow feasibility.

Step 4: Update Predicted State Variables and Compute Deviations

The power flow solution gives the predicted state variables based on load forecasts, namely, voltage magnitudes and phase angles. As mentioned before, the proposed approach will leverage available PMU data at selected buses to directly obtain the values of state variables (voltages, phase angles). These values would be used in place of the predicted state variables based on load forecasts as their accuracies are better and would lead to tighter detection thresholds. Therefore, the deviations are computed from the difference of the state estimator outputs (based on SCADA measurements) and either the forecast-based predicted state estimates or PMU data depending on the measurement configuration. This can be expressed as:

$$x_{dev} = x_{pred/pmu} - x_{act} \tag{4.10}$$

where, x_{act} represents the state estimator outputs, $x_{pred/pmu}$ represents either predicted state variables based on load forecasts or PMU data, and x_{dev} represents the deviation between these two quantities. All these are $n \times 1$ vectors corresponding to the n state estimates being compared.

Step 5: Compare Deviations Against Threshold

The real-time deviations between the predicted/pmu measurements and state estimator outputs are compared with an existing statistical model of the deviation obtained from historical data analysis. The historical data of load forecasts and SE outputs can be processed to obtain a characterization of the variation to a reasonable accuracy of these load forecasts. In order to keep the approach simple, mean and standard deviation are the statistical parameters currently chosen for characterizing the deviation between the predicted and actual state estimates. Extending the previous definitions, each element i in the x_{dev} vector $(n \times 1)$ essentially consists of a mean μ_dev_i and σ_dev_i. Depending on the measurement set, forecast accuracy, and the availability of synchrophasor data each element in the μ_dev and σ_dev vector would vary. The deviation of state estimates from the predicted values or PMU data for each state variable is compared against a detection threshold. The proposed algorithm detects an anomaly in the data if, for any state variable i,

$$|x_{dev_i}| > \tau\_dev_i \tag{4.11}$$

where, τ_dev_i represents the detection threshold corresponding to each state variable i. If this deviation does not fall within existing thresholds, the anomaly detection algorithm raises alarms to indicate the possibility of data manipulation. An analysis of individual state variables' variations could provide detailed information on the possible source of manipulations. In order to mitigate the attack impacts, the mitigation should ensure that the state estimates are not corrupted and the bad measurements are identified and removed. This could be achieved

by triggering an on-demand run of the SE that includes additional detail by looking at a more detailed (node-breaker level) network model to be used around the locations of the suspect measurements [61, 62] identified in the anomaly detection. This essentially changes the measurement configuration matrix (H) and includes redundant measurements, which enable better bad data detection to identify and remove malicious measurements.

Computational Performance

There are two aspects to the proposed algorithm: *offline characterization of the minimum attack magnitudes and detection thresholds using historical data, online comparison of state estimator solutions to detect anomalies.* Specifically, the offline characterization process involves iterating over all the steps (1-5) for multiple days of archived state estimator solutions to obtain the minimum attack magnitudes and detection thresholds. Because this is an offline step, there is no real constraint on the time it takes for these runs. With respect to the online comparison process, the algorithm needs to execute once concurrently with each state estimator run. In our case, we assume this to be once every 5 minutes. Considering a real deployment with utility scale systems, the proposed algorithm would leverage existing tools in the EMS that solve linear optimization formulations and power flows in a computationally efficient manner under this time constraint easily. Therefore, we do not expect any computational performance bottlenecks.

Illustrative Example for the Proposed Algorithm

Figure 4.3 shows an illustrative example that walks through the algorithm for one of the state variables θ_2 in the IEEE 14-bus model (Figure 4.5), for a single execution of SE. In this example, we use an arbitrary detection threshold ($= 1.25\sigma$) for the purposes of illustration. However, we describe later how this threshold can be obtained systematically for each state variable such that the false positives and false negatives are under specification. As shown in Figure 4.3, the same process is repeated for all the other variables.

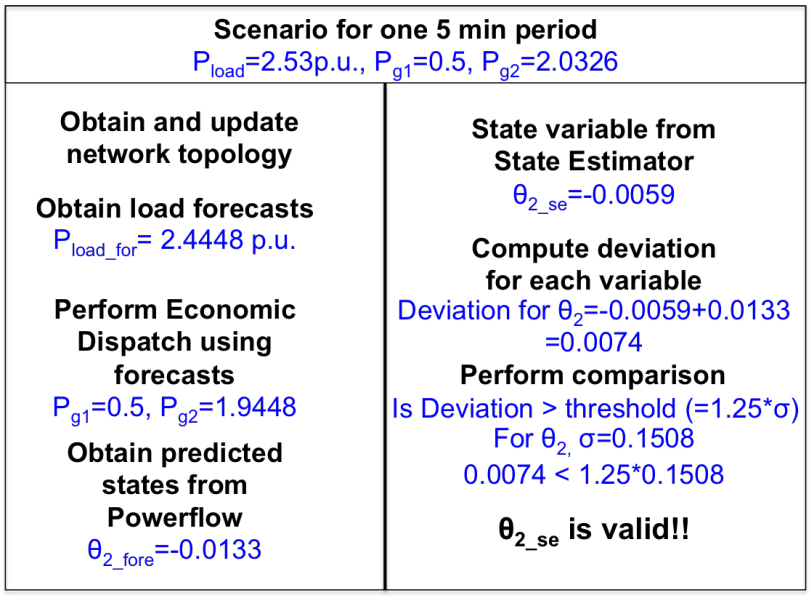

Figure 4.3 Illustrative example for the proposed anomaly detection algorithm

4.1.3 Factors Affecting Performance

The proposed detection approach is based on a comparison of the predicted state estimates that are generated based on load forecasts with the actual state estimator outputs. Therefore, the following factors influence the performance of the anomaly detection method.

- Accuracy of the load forecasts (mean, standard deviation).
- Accuracy of measurements (traditional SCADA, PMU).
- Threshold for comparison with estimated states.

The performance of the proposed approach relies heavily on the availability of accurate real-time, short-term load forecasts. Based on a review of current short term-load forecasting methods in ISO's, it has been observed that the accuracy of the forecasts are typically much lower than SCADA measurements [74]. However, the accuracy of load forecasts, combined with availability of synchrophasor data provides a coarse validation to detect large measurement anomalies. Based on a recent study, it has been observed that the use of PMU measurements can improve the accuracy of state estimates [75]. Therefore, this aspect contributes to an im-

provement in the minimum measurement anomaly that can be reliably detected (with low false positive and false negative rates). The minimum attack magnitude, and the detection thresholds of the anomaly detection algorithm need to be obtained appropriately so as to ensure a balance between false positive and false negatives. Another factor that influences that performance of the proposed approach is the method that is used to compare the deviation against a threshold. When the algorithm uses single values, its performance is often affected by spikes in the load forecasts resulting in unnecessary false positives. In order to partially eliminate this, we employ the concept of weighted moving average, where the algorithm constantly updates a window of current and past values that are averaged to be used for comparison against the threshold.

False Positives and False Negatives

Intuitively, the attack magnitude that can be detected depends on the typical range of deviations that are considered acceptable. A very accurate forecast combined with PMU data at available buses will help to significantly narrow the typical range and consequently provide detection of smaller attack magnitudes. Another important factor in distinguishing attacks vs. temporary abnormalities is the setting of detection threshold values for each state variable such that the false positives and false negatives are acceptable. As is the case with any anomaly detection approach, proper analysis and tuning of false positives and false negatives is extremely critical.

By definition, false positives are the cases where the anomaly detection algorithm detects an attack when there is none and false negatives represent the cases where the algorithm fails to detect an attack. Similarly, we can define true positives and true negatives as cases where the algorithm correctly detects an attack and no attack respectively. Based on standard definitions [76], false positive rate (FPR) is defined as the ratio of false positives to the total negatives (true negatives and false positives) in the dataset (Eq. 4.12). Similarly, false negative rate (FNR) is defined as the ratio of false negatives to the total positives (true positives and false negatives) in the dataset (Eq. 4.13). A complementary measure of false negative rate is the true positive rate (TPR) or detection rate, which is defined as the ratio of true positives to the total

positives in the dataset (Eq. 4.14). TPR and FNR are complementary measures and could be used interchangeably. Ideally, we would strive to have a FNR close to 0, which translates to a TPR close to 1. In the rest of our analysis, we would use FPR and TPR to identify the balance between false positives and false negatives.

$$FPR = FP/(TN + FP) \tag{4.12}$$

$$FNR = FN/(TP + FN) \tag{4.13}$$

$$TPR = 1 - FNR = TP/(TP + FN) \tag{4.14}$$

The FPR depends on the detection threshold for the deviations between predicted states vs. state estimator outputs. A high threshold limits the false positives, but it also decreases the TPR as the algorithm fails to detect certain attacks. On the contrary, a low threshold causes several false positives, which are caused due to genuine random forecast fluctuations.

4.1.4 Empirical Method to Obtain Minimum Attack Magnitudes and Detection Thresholds

In this section, we outline an empirical method that could be applied to obtain the design parameters of the proposed anomaly detection algorithm. This involves identifying the optimal balance point between the design parameters to meet the desired FPR and TPR. For a specified measurement configuration, forecast accuracy, and a specified acceptable FPR and TPR cutoffs, we can obtain the minimum attack magnitude and detection thresholds for each state variable that would be used in the proposed anomaly detection algorithm.

Figure 4.4 shows the method that could be applied to obtain the minimum attack magnitudes and detection thresholds. Step 1 is to define the system input parameters such as measurement configuration, SCADA measurement accuracy, locations of PMU measurements and their accuracies (optional), load forecast accuracy, load curves, etc., and target performance measures such as FPR of less than 1% i.e 0.01 and TPR of greater than 95% or 0.95. Step 2 is to generate load forecasts based on the input load profile. In our experiments we used the load profile of an entire day coupled with several iterations of load forecasts as the nature of load forecasts is random. Step 3 involves increasing the detection threshold from the base value

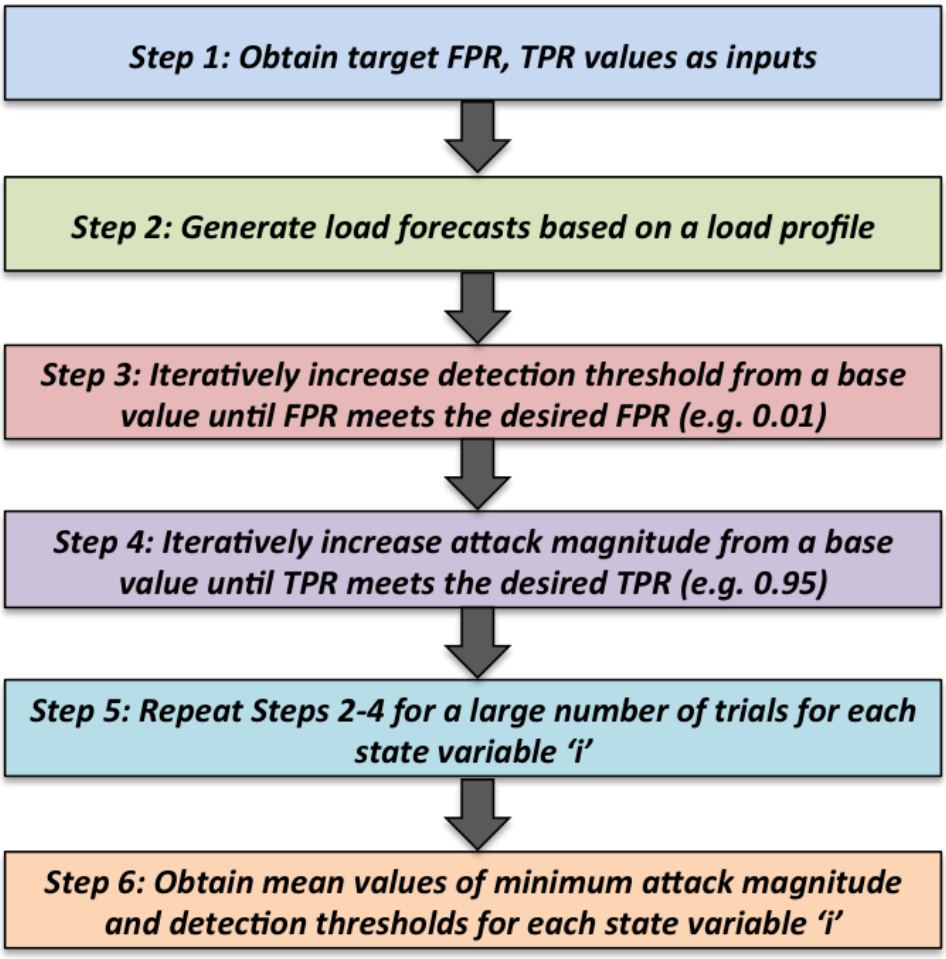

Figure 4.4 Empirical method to obtain minimum attack magnitudes & detection thresholds

until the FPR is under the desired FPR. This step is done to fine tune the detection thresholds for a low FPR. Step 4 is to start from a base attack magnitude (i.e. injection of δ to a phase angle) for each state variable. This attack magnitude would result in a particular TPR for that state variable for the given load profile. Using the detection threshold identified in Step 3, iteratively increase the attack magnitude from the base value until it meets the desired TPR. This process finds the minimum attack magnitude that falls just outside the detection band for a particular forecast accuracy. At the end of Step 4, we have a set of detection thresholds and minimum attack magnitudes for each state variable that meet the desired FPR and TPR respectively. Step 5 involves the performing the above process (Steps 2-4) for a large number of trials due to the random nature of generating measurements, and load forecasts. In each trial, we generate a fresh set of load forecasts (Step 2) and then proceed to Steps 3 and 4. Step 6 is to obtain the mean values of the minimum attack magnitude and detection thresholds for each state variable that meets the desired FPR and TPR.

4.2 Case Study on IEEE 14-bus System

This section presents a detailed case study and performance analysis of the proposed anomaly detection algorithm described in Section 4.1.2. The key motivation is to provide an insight into the various factors that affect the performance of the proposed method, thereby providing a better intuition about its capabilities and limitations. Figure 4.5 shows the IEEE 14-bus system model with a base case measurement configuration that is used in the performance analysis. The load forecast accuracy information (mean and standard deviation) used in the analysis is based on the information obtained from [74]. For simplifying our analysis, the basic economic dispatch formulation without losses and also a DC power flow model is used in our case study. This does not in any way reflect the limitation of the proposed algorithm as can it be readily extended to complex economic dispatch formulation and the power flow formulation, or equivalently an optimal power flow formulation that is used in the real-time power system markets and operations. In the 14-bus power system model, under the DC power flow model assumption, all voltage magnitudes are considered to be 1 p.u. Therefore, there are 13 state variables (phase angles) in the analysis, where one of the 14 phase angles is considered as

a reference. The parameters (mean μ, and standard deviation σ) that are used to generate the load forecasts, SCADA measurements and PMU measurements in the case study are provided in Table 4.1.

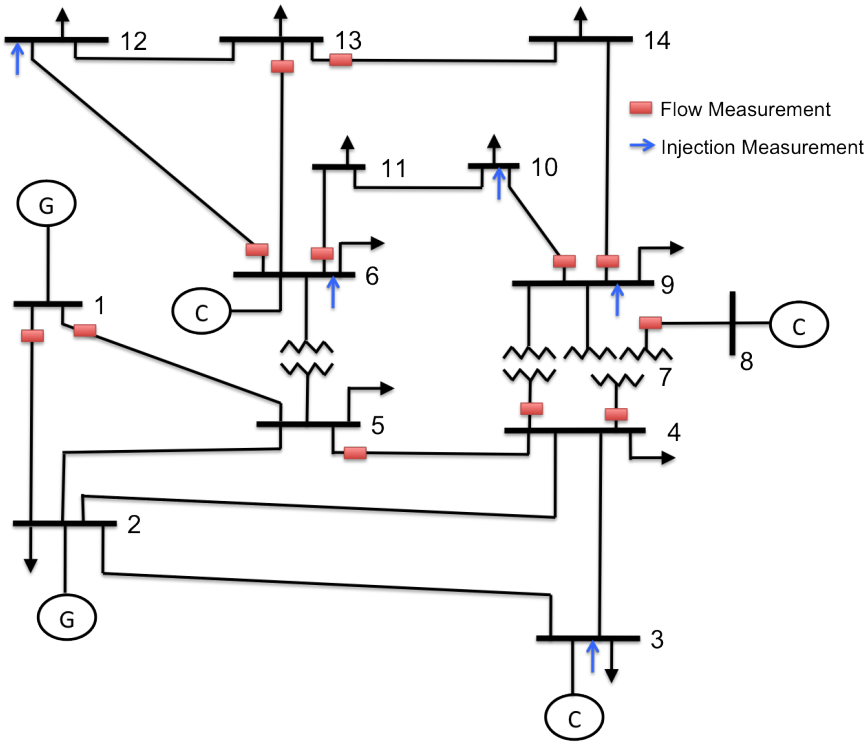

Figure 4.5 IEEE 14-bus power system with measurement configuration

4.2.1 Experimental setup

In order to analyze the impact of the various factors over the performance of the proposed anomaly detection algorithm, we consider the following scenarios in our analysis.

- Attack magnitude – 5 different attack magnitudes.
- Measurement configuration – Low (option 1), High redundancy (option 2).
- Forecast accuracy – Low (option 1), High forecast accuracy (option 2).

Table 4.1 Experimental parameters for case study

Parameter	**Option 1**	**Option 2**
Load Forecasts Accuracy	$\mu = 0.00427$, $\sigma = 0.051194$	$\mu = 0.001$, $\sigma = 0.01$
SE Measurements	17 (*low*)	22 (*high*)
SE measurements Accuracy	$\mu = 0.0$, $\sigma = 0.001$	$\mu = 0.0$, $\sigma = 0.001$
PMU measurements Accuracy	$\mu = 0.0$, $\sigma = 0.0001$	$\mu = 0.0$, $\sigma = 0.0001$

Therefore, the total set of scenarios include a combination of 5 attack scenarios, 2 measurement configurations, 2 forecast accuracies. Each of the scenarios mentioned above will be evaluated for a typical stealthy false data injection attack as described in [77]. In each of the scenarios, the following performance measures will be monitored: *maximum deviation of predicted states vs. state estimates, false positives, false negatives*. The first performance measure is related to quantifying the variation of the difference in the comparison. A high variation indicates that the detection band for the particular state variable is very broad, consequently more attacks can go unnoticed. Conversely, a tighter variation indicates that a narrow detection band can be used. In the context of the proposed anomaly detection approach, *false positives* are the cases where the anomaly detection algorithm detects an attack where there is none. Similarly, *false negatives* are cases where the anomaly detection algorithm fails to detect an attack.

The experiment was carried out by analyzing the variation of the state estimates obtained from traditional SCADA measurements and then comparing them with predicted states obtained from load forecasts for a single day. The real-time 5 minute load information provided by New-England ISO was used a data source in order to get a realistic load curve for the purpose of our experimental study [78]. This load profile data was normalized and converted to per unit in order to be used for our IEEE 14-bus system. The load forecasts were generated based on the statistical characteristics mentioned in Table 4.1, which was obtained from a CAISO study report [74]. A typical load profile over a day is shown in Figure 4.6.

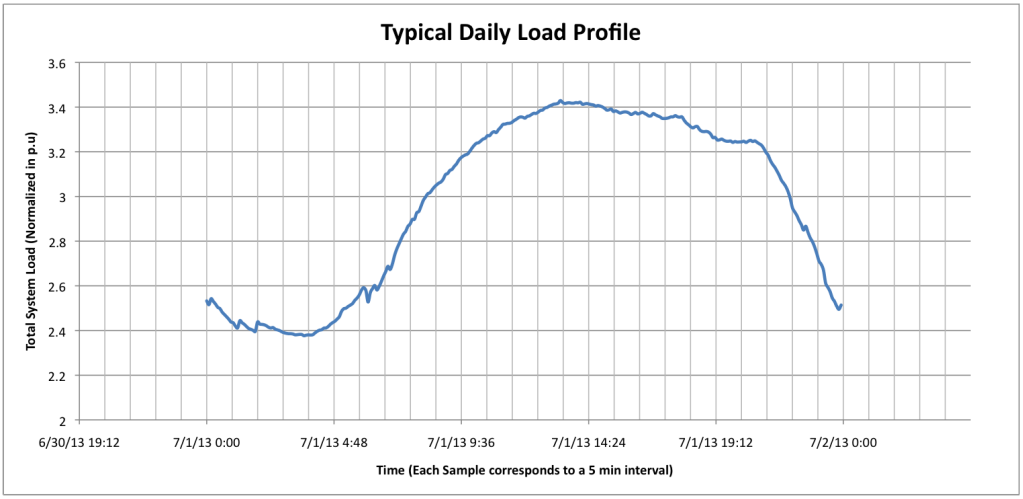

Figure 4.6 Typical daily load profile of sample data

The SCADA measurements used for SE were generated by adding measurement noise to computed power flow solutions for each 5 minute load based on the accuracy parameters as listed in Table 4.1. In certain experimental scenarios, we assumed that buses 2, 6, 8, and 9 (this configuration provides complete observability with minimum PMUs) had PMU data, which were generated by adding noise to the phase angles at these buses directly. The accuracy of the PMU data generated were based on parameters as listed in Table 4.1. In our experimental scenario, we assumed that the frequency of execution of state estimator is the same as the frequency of real-time load forecasts, which is 5 minutes. Therefore, each experiment consisted of running the economic dispatch and the SE for 288 intervals (24 hours * 12 5-minute intervals per hour) throughout the day. For obtaining historical characterization of variation between state estimates and predicted states, prior load profile information over a week was used from [78].

The attack vector that has been used is the one specified in [77]. Specifically, for this case study, the measurement meters that were corrupted by false data injections correspond to state variables $\theta_2, \theta_4, \theta_{13}$. Over the course of one day, the measurements that corresponded to these particular state variables were manipulated only between 4 AM and 4:40 PM on the day. This was done to distinguish the performance of the method during normal and attack phases.

4.2.2 Performance results

Figure 4.7 shows the deviation of the state estimates and load forecast-based predicted states over the course of a day. The plot on the top shows the deviation of state estimates from the predicted states during an attack and the bottom subplot shows the deviation during normal condition. The y-axis indicates the difference of the state estimates and the predicted states (in degrees). The blue line in the plot indicates the mean of the variation between the state estimates and predicted states for a state variable, (θ_{13} in this case). Similarly, we can obtain similar plots for each of the state variables. The green and red lines indicate 1 and 1.25 standard deviations for the variations. Analysis of the deviations for each state variables would provide an insight about the detection thresholds, which could be used to clearly distinguish an attack from an abnormal condition. In Figure 4.7, the variation in the lower plot mostly falls

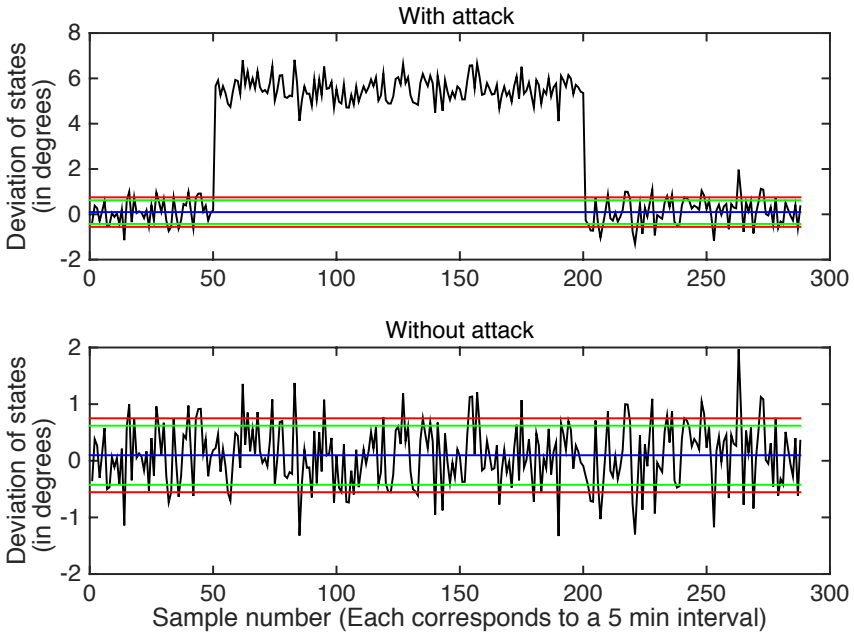

Figure 4.7 Deviation of predicted and actual state estimates over a day (θ_{13})

in the acceptable zone except for a few spikes which are due to forecast inaccuracies. Whereas, in the top plot, we can see that the variation is outside the acceptable threshold throughout the attack period in a particular day. This indicates that there is a potential case of data

manipulation or anomaly in the data that has gone unnoticed in bad data detection. In our case, this is the indication that state variable θ_{13} has been injected with an arbitrary error. We can see that by observing these deviations it is possible to detect stealthy data injection attacks, which cannot be observed by the traditional Bad Data Detection method that is based on normalized measurement residuals.

4.2.2.1 Sensitivity Analysis

In order to identify the sensitivity of the proposed anomaly detection method to the various factors mentioned previously, a systematic study was performed by varying individual parameters while keeping the others constant. For example, in order to study the sensitivity of the anomaly detection method to forecasts, we fix a particular measurement configuration and associated SE accuracy, fix the attack magnitude and perform the analysis over two possible forecast accuracies. Also, the attack is performed only on a subset of the total 288 5-minute intervals over the course of a day.

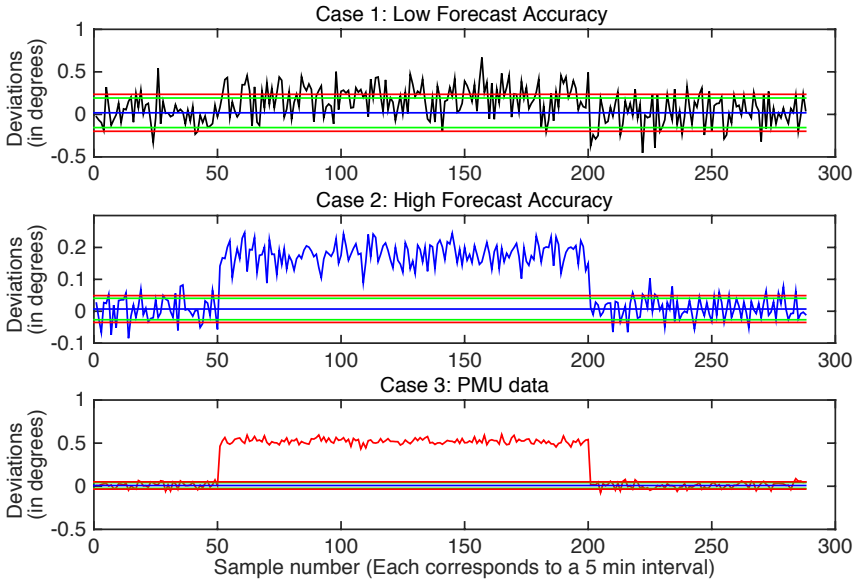

Figure 4.8 Sensitivity to forecasts and synchrophasor data for θ_2

Figure 4.8 shows how the proposed anomaly detection method performs for two different forecast accuracies (Cases 1 and 2). Also, it shows the performance when PMU measurements are used instead of forecasts for a fixed attack magnitude (Case 3). For this scenario, the experiments were performed keeping the measurement configuration corresponding to Option 2 as mentioned in Table 4.1. All the sub plots indicate the deviations of predicted states vs. actual state estimates for θ_2, which is a state variable whose corresponding power flow measurements are under attack. The 3 subplots correspond to 3 cases, which are as follows:

- Case 1: Low forecast accuracy.
- Case 2: High forecast accuracy.
- Case 3: PMU data used instead of forecasts.

In Case 1, a very negligible portion of the deviation falls outside the typical range. In this case, the anomaly detection method fails to detect the attack (false negatives) and the deviations look similar to the case without attack. Whereas, for Case 2, with the same attack magnitude and a higher forecast accuracy, the attack period can be clearly identified as the the band of acceptable deviations is much tighter for this case.

4.2.2.2 Impact of PMU Data in Attack Detection

Case 3 shows how the proposed anomaly detection method performs in the presence of PMU data for selected bus (bus 2) for the same attack scenario. The accuracy of the PMUs are as defined in Table 4.1 and are based on observations from [75]. For case 3, we can clearly detect the attacks when using PMU data instead of less accurate load forecasts as they are much more accurate than forecast-based estimates. We can clearly see that the detection band gets tighter and tighter with the use of more accurate predictions based on either better load forecasts or PMU data. While this behavior is expected intuitively, the key is to understand how the false positives and false negatives are influenced by these parameters. Therefore, the key takeaway from Figure 4.8 is that the accuracy of the load forecasts or availability of secure PMU data plays an important role in determining the minimum attack magnitude and the corresponding detection thresholds for the proposed anomaly detection algorithm.

Similar to the study with forecast accuracies, a comparison was made to see how the proposed anomaly detection method performs for two different measurement configurations in the SE. The corresponding accuracies of the measurements are as mentioned in Table 4.1. Based on our observations, we found that for a given attack magnitude, there is no significant difference in the detection capability as the accuracy of state estimates is very close in both cases. As forecasts are typically an order of magnitude less accurate than SCADA measurements, any improvement in forecast accuracy, improves the performance significantly, whereas the performance improvement is very minimal for an increase in measurement redundancy.

4.2.2.3 Analysis of False Positive and False Negatives

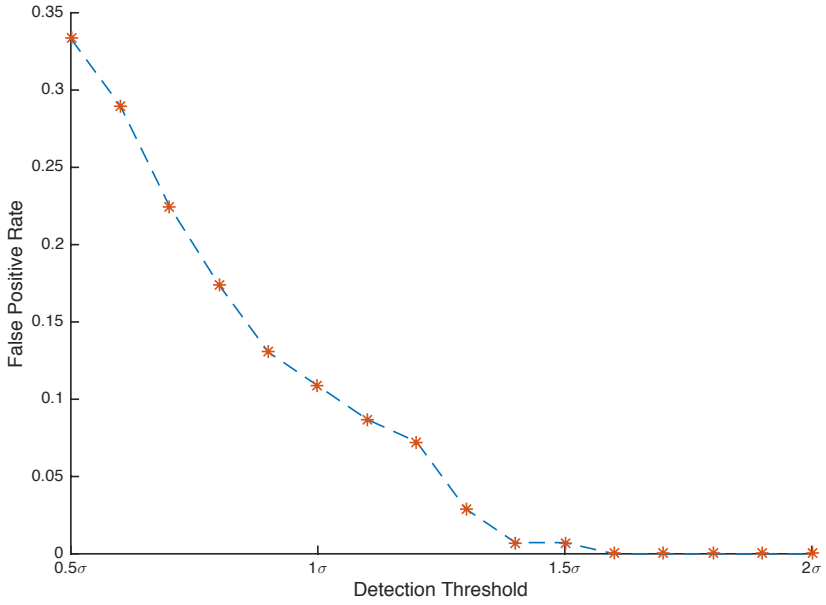

Figure 4.9 Variation of FPR with threshold for state variable θ_2

Figure 4.9 shows the variation of false positive rate for the state variable θ_2 as a function of detection threshold that is used for declaring the deviation between predicted vs. actual state estimator outputs as anomalous. The detection threshold for each state variable was varied from 0.5σ to 2σ and the corresponding FPR was observed. In order to avoid confusion, only

the variation for θ_2 has been plotted. As described earlier, the false positive rate decreases sharply with increase in detection threshold. We observed a similar trend in the variation of FPR vs. the threshold for all the other state variables as well. From Figure 4.9, we can see that for threshold larger than 1.5σ, FPR of state variable θ_2 becomes negligible (i.e. under 1%). The distinction of forecast abnormalities from real attacks is a very important aspect for the acceptable performance of the proposed method. This is determined by how well the historical data that is used to obtain the base statistical parameters for the detection thresholds captures this aspect. Another key factor is the determination of the right values for the detection threshold that balances false positive rate and the false negative rate.

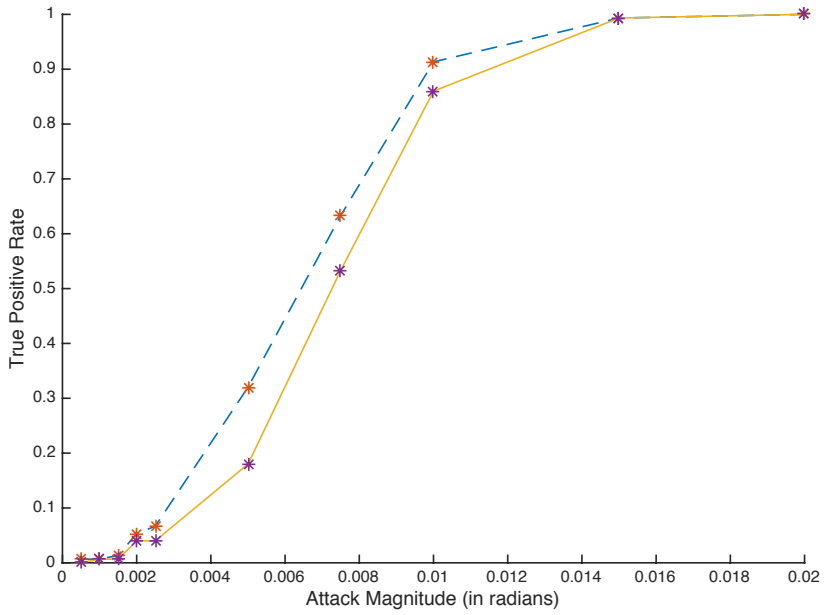

Figure 4.10 Variation of TPR with attack magnitudes for two detection thresholds: 1.4σ (dotted curve) and 1.6σ (solid curve) for state variable θ_2

Figure 4.10 shows the variation of true positive rate for state variable θ_2 for a set of attack magnitudes from very low to very high magnitudes under 2 different thresholds: 1.4σ (dotted curve) and 1.6σ (solid curve). These two detection thresholds that are shown have reasonably low FPR for θ_2. Intuitively, the TPR or the detection rate depends on attack magnitude. If

we have attacks that are less than the minimum attack magnitude that can be detected by the algorithm for a given set of load forecasts, then FNR tends to be high and the TPR tends to be low and vice versa. We can see that around lower attack magnitudes for θ_2 (0.005 - 0.01 radians), the variation of TPR with detection thresholds is noticable. As the attack magnitude increases, TPR quickly approaches 1, and the variation of TPR due to detection thresholds reduces. This figure along with Figure 4.9 helps to show the interplay between FPR and TPR, wherein a high detection threshold is good for FPR, it is not optimal for TPR. Therefore, in order to achieve optimal performance, we need to obtain the right balance between two design parameters, i.e. the minimum attack magnitude that can be detected for a state variable and its detection threshold.

4.2.3 Receiver Operating Characteristics (ROC)

ROC plots serve as a useful tool to analyze the performance of anomaly detection algorithms and identify tradeoffs between true positive rates and false positive rates for various decision classifiers [76]. Since our anomaly detection algorithm produces only a 'yes' or 'no' classification, it belongs to the category of discrete classifiers. Therefore, it produces only a single data point in the ROC space for each dataset. Figure 4.11 shows the various data points in the ROC space for 2 different attack scenarios: low (asterisk), and high (diamond) attack magnitudes over a range of detection thresholds used for anomaly detection for state variable θ_2. The magnitude of the low and high attack scenarios are $0.5*m\_att\_mag$ and m_att_mag respectively, where m_att_mag represents the minimum attack magnitude corresponding to state variable θ_2. The minimum attack magnitudes for each state variable can be obtained by applying the methodology described in Section 4.1.4. Please refer to Table 4.2 for specific results. For each of the two attack scenarios considered in Figure 4.11, there are 16 points in the ROC space, and each point corresponds to a particular detection threshold, which was varied from 0.5σ to 2.0σ.

In general, the farther north-west of the diagonal line a classifier is in the ROC space, the better the performance of the algorithm. From Figure 4.11 we can clearly observe that the proposed anomaly detection algorithm performs very well for the attack scenario with high

magnitude as it has low FPR and high TPR for a range of thresholds. For attack magnitudes that are lower than the minimum attack magnitude as is the case with the low attack magnitude scenario, the FPR and TPR performance of the algorithm is highly sensitive to thresholds. From Figure 4.11, we can see that even for the low magnitude attack case with $0.5 * min\_attack\_mag$ for θ_2, the proposed algorithm was able to detect attacks with about 80% TPR and 10% FPR for a certain detection threshold.

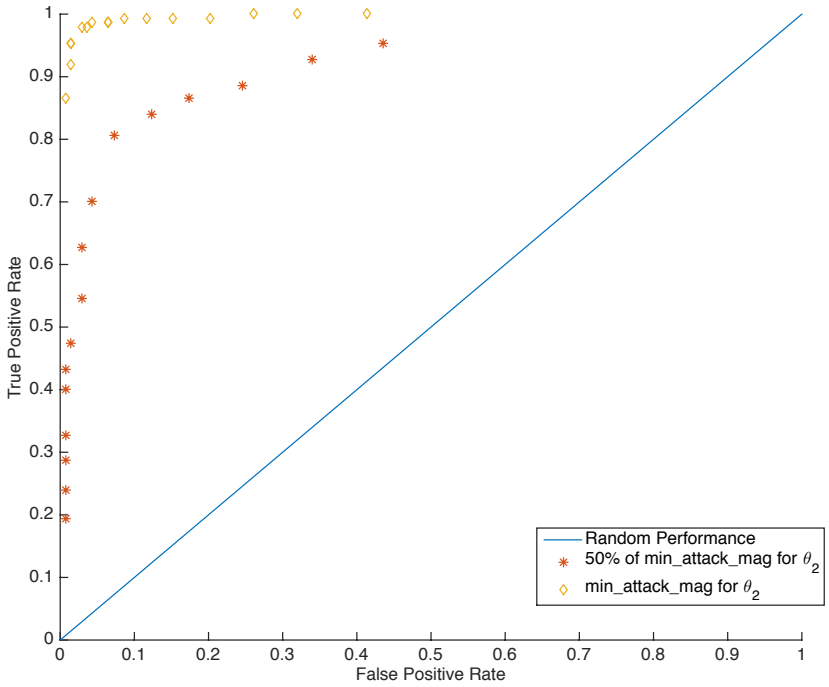

Figure 4.11 Points in ROC space for low (asterisk) and high (diamond) attack magnitudes with multiple detection thresholds for state variable θ_2

4.2.4 Minimum Attack Magnitudes and Detection Thresholds

Based on the earlier results, we can infer that FPR is dependent on the detection threshold that is used for declaring deviations as anomalous or normal. Also, we can see that if we use a very high threshold for eliminating false positives, that adversely impacts FNR or TPR, which impacts the minimum attack magnitude that can be reliably detected by the algorithm.

We used the empirical method shown in Figure 4.4 and obtained the minimum attack magnitudes and detection thresholds for all the 13 state variables in the IEEE 14-bus system. The target FPR and TPR were chosen to be 1% and 95% respectively, for forecast and measurement accuracies as mentioned in option 1 of Table 4.1. Table 4.2 shows the mean minimum attack magnitude and detection thresholds for all state variables that were obtained based on our simulation runs using the empirical method proposed earlier in Section 4.1.4.

Table 4.2 Minimum attack magnitudes and detection thresholds for IEEE 14-bus system

State variable	**Minimum attack magnitude (radians)**	**Detection threshold**
θ_2	0.012	1.66 σ
θ_3	0.014	1.58 σ
θ_4	0.013	1.6 σ
θ_5	0.012	1.61 σ
θ_6	0.023	1.54 σ
θ_7	0.018	1.55 σ
θ_8	0.018	1.59 σ
θ_9	0.021	1.55 σ
θ_{10}	0.023	1.55 σ
θ_{11}	0.024	1.54 σ
θ_{12}	0.028	1.52 σ
θ_{13}	0.024	1.56 σ
θ_{14}	0.022	1.57 σ

Based on information provided in [79], the maximum acceptable deviation in line flows based on state estimator solutions is 10% of the line rating, which is equivalent to 0.1 p.u. In order for the proposed anomaly detection algorithm to be relevant for practical application, the minimum attack magnitude that can be detected should be comparable to this range. In our experiments, for state variable θ_9, 0.021 radians was the minimum attack magnitude that met the specified FPR and TPR constraints of 0.01 and 0.95. This attack magnitude could be translated to an equivalent change in line flow of about 0.095 - 0.098 p.u depending on the operating conditions. Therefore, even though the algorithm cannot detect any attacks under this limit for the given forecast accuracies, the low magnitude attacks would not cause a significant impact in real-time operations and markets. However, the proposed algorithm is

effective against detecting measurement anomalies that could cause significant operational or market impacts. Also, its performance can be further enhanced with a hybrid combination of more accurate forecasts and increased PMU deployments.

4.3 Conclusions

In this work, we proposed a model-based anomaly detection approach that utilizes information that is essentially independent of traditional SCADA measurements to detect measurement anomalies due to stealthy cyber attacks. We described a detection methodology that leverages load forecast information, generation schedules, and synchrophasor data to obtain a statistical characterization of the variation between SCADA-based state estimates and forecast-based predictions to detect anomalies. We provided key insights about various factors that impact the performance of the proposed algorithm. We also outlined an empirical method to obtain the minimum attack magnitude and detection thresholds for each state variable such that it satisfied a target FPR and TPR specification for the proposed algorithm.

We presented a detailed case study of the proposed algorithm on the IEEE 14-bus system where we evaluated its performance under different experimental scenarios. We observed that the performance of our proposed approach depends primarily on forecast accuracy and the addition of PMU data improves its performance further. We also observed that the false positive rate is dependent on the threshold for deviations of predicted vs. actual state estimates. We identified that the true positive rate or the detection rate increases with increasing attack magnitudes, but decreases with increasing detection thresholds. We also obtained the minimum attack magnitudes and detection thresholds for each state variable in the IEEE 14-bus system for meeting target FPR and TPR through simulation studies.

CHAPTER 5. TESTBED-BASED EXPERIMENTATION AND EVALUATION FOR WAMPAC

Cyber security of critical infrastructures (CI) like the power grid is becoming extremely important and is currently one of the top R&D priorities globally. It is quite obvious that existing operational systems cannot be used to perform various types of cyber security experiments to discover vulnerabilities and fix them. CPS security testbeds serve as test environments, which can be used to perform various types of cyber attack and defense experimentation using a hybrid combination of real, simulated and emulated components that represent the real world as closely as possible. The real utility of testbeds over traditional standalone simulation tools is the ability to model complex cyber-physical interdependencies and their relevant interactions across multiple domains such as computation, communication and physical systems in a single coherent environment. One of the distinguishing features of CPS testbeds is the ability to map real hardware devices seamlessly into the experimental framework to perform real-time, hardware-in-the-loop experiments, which allow the ability to observe computation, communication and physical system dynamics together, some of which otherwise would have been abstracted away due to shortcomings in the modeling platform.

5.1 Motivation for Testbed-Based Experimentation for WAMPAC

The need for CPS security testbeds is driven by the fundamental limitation that traditional simulation-based tools cannot capture the dynamics of control, communication and physical systems in a single environment. Testbeds provide this capability by having a combination of real hardware devices, automation software, and communication protocols, combined with emulated devices and simulated systems such that the essential behaviors and cyber-physical in-

teractions are captured accurately. Testbeds serve as a validation platform for a broad spectrum of research areas like vulnerability assessment, impact analysis, risk assessment, risk mitigation, and other real-time defense algorithms against various forms of cyber attacks such as data integrity attacks, timing and replay attacks, and denial of service attacks. In addition, testbeds provide a platform to accelerate development of countermeasures (secure architectures and algorithms) and evaluate/validate their effectiveness/adequateness. Testbeds not only serve as a validation platform for research and engineering development, but also serves as a powerful training and educational environment, which could be leveraged to provide classroom and laboratory-based coursework. Also, CPS security testbeds can be used a training ground for active, grid-wide, national cybersecurity exercises like NERC GridEx [80, 81] to improve cyber security preparedness and response capabilities in defending the critical infrastructures against various cyber threats.

5.2 Testbed Design Objectives and Tradeoffs

5.2.1 Design Objectives

The key design objectives [82] for a CPS security testbed include:

- Modularity - being composed of different functional units, which do not affect each other's functionalities and could be abstracted depending on experimental needs.
- Scalability - the ability to be able to increase/decrease the size of the system to be modeled without loosing out on the ability to integrate real hardware.
- Repeatability - the ability of the testbed platform to be able to consistently reproduce identical results for repeated trials of an experimental scenario.
- Re-configurability - the testbed should be able to support multiple configurations that allow a variety of experimental scenarios using the same hardware or tools.
- Interoperability - components in the testbed should be replaceable seamlessly provided they have similar functionalities and interfaces such as communication protocols and services.

While CPS testbeds provide modeling of computation, communication and physical system dynamics in a single environment, there are several design challenges because of the necessity to have real and emulated devices interacting with simulated components. Some of the key challenges in designing a CPS security testbed are: accuracy, scalability, realism, and cost. The modeling accuracy is driven by the interdependencies that are to be modeled. Realism is closely associated with modeling accuracy and is based on how close the simulation models capture real-world behaviors. The scalability of the system is limited by the amount of physical hardware that is available to be mapped into the experiment and also mostly by the capability of the real-time simulation tools that model the physical system. It is straightforward to understand how these two factors interact with cost: a system with all real hardware would be extremely expensive, but would have a high modeling accuracy; whereas, a system with all simulated components would be cheap, but would loose out on the modeling accuracy.

5.2.2 Testbed Design Tradeoffs

One of the main challenges in developing a large-scale, high-fidelity CPS security testbed is the cost of the various systems and devices. Testbed design is a challenging task, which involves finding the optimal balance between scalability, accuracy, realism, and cost.

Optimal CPS testbed design involves the identification of the right level of balance between these competing factors using a hybrid combination of simulated components, emulated components and real physical components. The design of the CPS testbed should carefully consider the type of experimental use case scenarios that would be implemented on it. Figure 5.1 shows the various types of testbeds across a broad spectrum and their design tradeoffs.

For example, a testbed that is built to test/prototype a new protection device would require a real-time power system simulator with the capability to interface real devices through its analog and digital I/O's along with the associated communication protocols. Similarly, a testbed that is expected to test market algorithms would require a network of multiple market agents that are deployed on computing nodes distributed realistically over an emulated wide-area communication network.

Each type of testbed has a specific set of use cases that could be supported as one or more

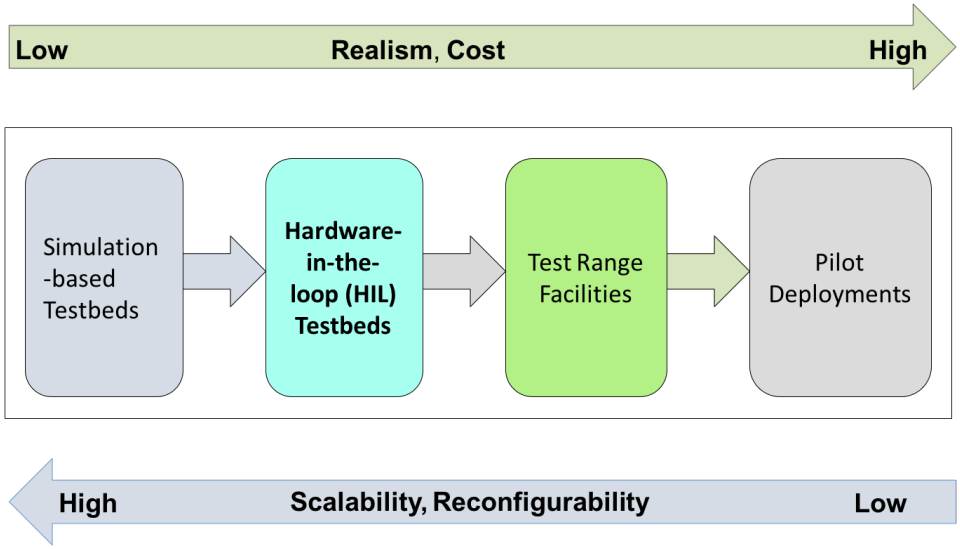

Figure 5.1 Types of testbeds

design tradeoffs are made. Figure 5.2 shows the relative ordering of these factors for the various testbeds. In the figure, these factors are arranged in concentric diamonds ranging from low to high representing scores from 1 to 3 respectively. A score of 1 for cost indicates low cost vs. a score of 3 indicates high cost. Similarly, for scalability, realism and accuracy, a score of 1 represents poor and so on. Based on this qualitative ranking of low to high for various factors, we can intuitively get a feel for how various testbed types tradeoff the design factors.

While test ranges and pilot deployments score high on realism and accuracy, they lack scalability and are extremely expensive options for WAMPAC cyber security experimentation. Also, the availability and configurability of such testbed types is very limited for different types of experimental scenarios.

Simulation-based testbeds, commonly used to refer to 'non-real-time' power system simulation tools, score highly on model scalability and cost very less money. However, they score very low on realism and accuracy as they cannot support integration of real hardware devices and often are incapable of modeling communication network behaviors and anomalies during cyber attacks accurately.

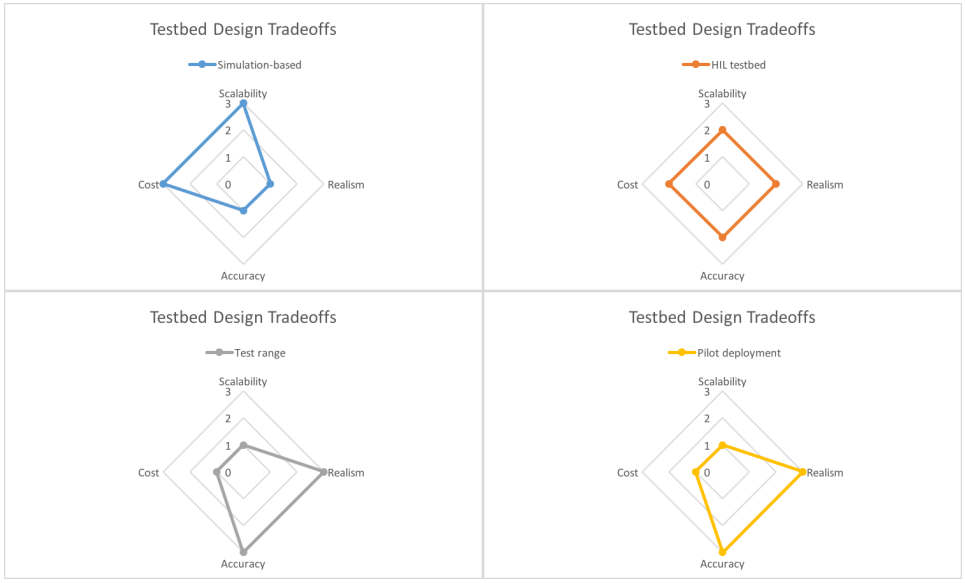

Figure 5.2 Design tradeoffs for different types of Testbeds

Hardware-in-the-loop (HIL) testbeds, commonly used to refer to testbeds that consist of 'real-time' power system simulators in combination with physical hardware and real network emulators, serve as ideal middle grounds in the spectrum of testbeds that not only capture communication layer aspects accurately, but also allows researchers to uncover anomalous behaviors involving real hardware and communication protocols under realistic attack conditions that cannot be modeled on pure simulation-based approaches statically. The next section will provide a detailed walkthrough of the uniqueness of HIL testbeds for cyber security for common WAMPAC use cases.

5.3 Uniqueness of HIL Testbeds for Supporting WAMPAC Cybersecurity Use Cases

In this section, we would like to discuss the uniqueness of HIL testbeds to support WAMPAC cyber security use cases that regular non-real-time simulation-based tools cannot provide. Figure 5.3 shows a comparison between HIL real-time testbeds and non-real-time simulation-based power system simulation tools for supporting cyber security use cases with common WAMPAC

applications. It is to be noted here that because specialized testbeds such as test ranges and pilot deployments, though very realistic and accurate, are extremely expensive and not flexible for varied experimentation. Hence, they have not been included in the comparison.

WAMPAC application	HIL testbeds	Simulation-based testbeds
Wide-area Protection • RAS (ms)	• Accurate modeling of relay behaviors and interactions • Ability to study effect of communication delay on performance of RAS	• Approximate modeling of protection behavior • Cannot reproduce probabilistic nature of GOOSE communication in RAS • Communication abstracted and attack effects not captured fully and accurately
Wide-area Monitoring • PMU- based oscillation monitoring (ms)	• Analog interfacing produces accurate PMU data stream • Effect of timing, packet drops, data integrity could be studied	• PMU data is produced and consumed within simulator • Network impairments cannot be modeled accurately • Real-time network characteristics such as congestion are hard to model
Wide-area Control • AGC (s)	• Modeling of AGC outside simulator captures realistic scenario • Allows realistic data integrity attacks, DoS on both measurements and control	• Internal modeling of AGC abstracts communication • Limited scope for studying realistic attack vectors

Figure 5.3 Comparison of HIL and simulation-based testbeds

One of the common disadvantages that we could observe against simulation-based testbeds for supporting WAMPAC use cases is the shortcoming that because these testbeds rely on 'non-real-time' power system simulators, they cannot interact with other network simulators and/or real hardware. This places hard constraints on the modeling of the attacks within the power system simulators and therefore the attack actions are abstracted. This restricts the attack implementation and evaluation to be separate and within the network simulation or emulation tools. The combined analysis of network-based cyber events with the WAMPAC application in the power system simulation cannot be performed together.

5.3.1 Timing is Critical

One of the unique capabilities offered by HIL testbeds due to the combined modeling of control, network and physical systems in a common environment is the ability to model timing related impairments and observe its effect on not only the WAMPAC application use case being

considered, but also on the overall power system reliability and stability. Specifically, as an example, the PowerCyber testbed was used to validate the hypothesis that timing is a critical parameter that could be favorably exploited by the attacker in executing coordinated attacks in addition to spatially coordinated attack actions. In Section 5.8.1 shows how the PowerCyber HIL testbed was used to study the impact of varying the timing between two attack actions (data integrity and DoS) on a RAS.

5.3.2 Network Behaviors During Attacks

HIL testbeds consist of a mix of emulated and actual hardware to enable the realistic modeling of network characteristics such as latency, jitter variations during experiments involving DoS attacks and provide variable delays in communication. Referring to the RAS example cited earlier, the case study in Section 5.8.1 presents results on how the coordinated attack resulted in a failure of RAS under range of DoS attack thresholds based on whether the network was attacked or the relay. Such type of effects cannot be captured on simulation-based testbeds as 'non-real-time' simulation tools cannot interact with real or emulated hardware properly.

5.3.3 Modeling Communication Protocols

HIL testbeds capture the probabilistic behavior of communication protocols on realistic networks that may not be modeled accurately with simulation-based tools. Considering the example of the coordinated attack on RAS again (Section 5.8.1), one of the unique aspects that was observed during the experimentation was that even under heavy DoS attack magnitudes, valid traffic would sneak through to enable successful execution of RAS. Such behavior resulted in the attack success being probabilistic rather than being deterministic due to the nature of the GOOSE protocol. Even though certain network simulation tools can model some of these behaviors they cannot be used in combination with power system simulation due to the non-real-time nature.

We discussed several unique features offered by HIL testbeds especially for supporting WAMPAC use cases. A lot of realism and accuracy is lost when these use cases are executed on non-real-time simulation-based tools when compared to HIL testbeds. While scalability is

often the bottleneck to HIL testbeds, federation approaches try to improve scalability of HIL testbeds without compromising too much on realism and model fidelity.

5.4 Testbed Engineering Methodology - From Use Cases to Requirements and Architecture Elements

Overall, the engineering methodology for a testbed should be firmly driven top-down starting from the use cases that need to be supported. This begins by defining critical requirements that need to be satisfied by the testbed for supporting the use cases. Based on the requirements, the use cases would then be realized by executing strategic testbed engineering tasks. These research tasks should synergistically leverage existing testbed resources to provide a platform for the development of innovative approaches for WAMPAC cyber-physical security. Figure 5.4 shows the mapping of WAMPAC experimental use cases into testbed requirements, then shows how these requirements could be satisfied by the testbed engineering tasks that leverage underlying testbed infrastructure resources.

5.4.1 Testbed Use Cases for WAMPAC Cyber Attack-Defense Experimentation

The design and engineering of CPS security testbeds for WAMPAC cyber-physical security should cover a set of topics typically spanning the entire spectrum of research. The use cases could be broadly categorized into:

- Vulnerability assessment - This covers the use cases that target a systematic assessment of systems (WAMPAC applications, software), devices (hardware), and communication protocols. One example of a vulnerability assessment specific to WAP application such as a RAS would be the identification of a coordinated attack vector that involved a combination of data integrity and DoS attacks to prevent proper operation of RAS controller.

- Impact assessment - This covers use cases that focus on the quantification of the impact of a particular type of cyber attack (data integrity, DoS, coordinated attacks) on the power system and the specific WAMPAC application. One example would be the impact

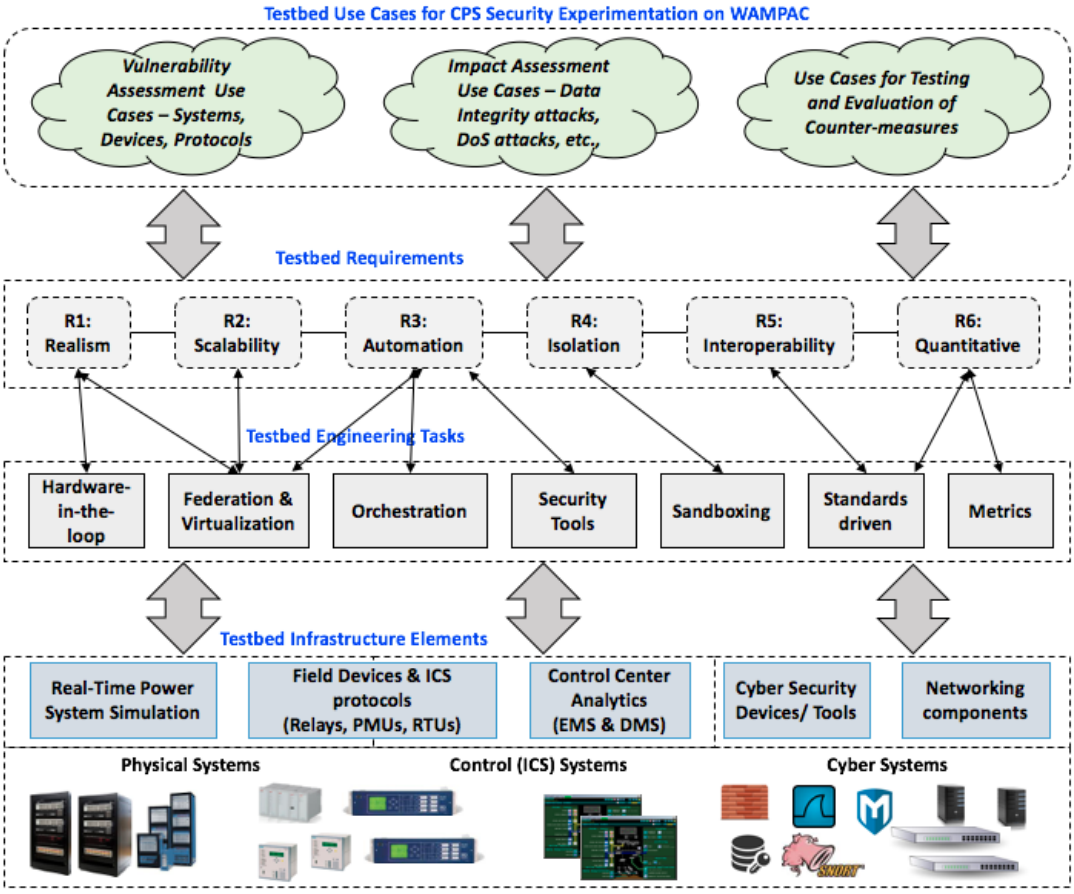

Figure 5.4 Testbed engineering methodology

assessment of stealthy cyber attacks that impacted AGC measurements to cause undesired frequency conditions, eventually leading to under-frequency load shedding (UFLS).

- Implementation and performance evaluation of CPS-based counter measures - This covers the use cases where the effectiveness of a particular counter measure is evaluated against known attack vectors to validate them. One example would be evaluation of CPS model-based attack-resilient control algorithm [83] for stealthy measurement attacks on AGC.

5.4.2 Testbed Requirements

In order to support the use cases identified, we carefully synthesized six critical requirements that need to be supported as part of engineering the testbed. The essential testbed requirements that need to be supported are:

- (R1) Realism - The capability to mirror real-world as close as possible. This typically involves emulation of hardware devices and support for hardware in the loop experimentation.
- (R2) Scalability - The ability to increase the size of the power system simulation without trading off real-time execution, model accuracy and hardware in the loop integration capabilities.
- (R3) Automation - The capability to perform automated actions that could be scripted to enable setup and teardown of several types of real and emulated devices, virtual machines and real-time simulators for complex experimental use cases.
- (R4) Isolation - The ability to isolate multiple experiments such that there is support for running experiments in parallel leveraging exclusive subset of computational resources on the real-time simulator and physical/emulated devices.
- (R5) Interoperability - The capability to support integration of diverse vendor agnostic hardware with similar functionality based on common standards.

- (R6) Quantitative - The capability to support measurement of various experimental parameters and states across control, communication and physical layers, and also the ability to produce repeatable experimental results.

5.4.3 Testbed Engineering Tasks

These testbed requirements that have been identified serve as a concrete basis for the development of testbeds to support WAMPAC specific cyber-physical attack defense experimentation. The testbed engineering tasks that are needed to support the requirements are listed below:

- HIL - Providing support to enable interfacing of real-hardware components in conjunction with real-time power system simulators.
- Federation & virtualization - Leveraging testbed resources through interconnection of network layers, addressing experimental scalability through virtualization and emulation of ICS devices.
- Orchestration - Providing flexibility, and automated experimentation capabilities to test multiple scenarios in an automated manner.
- Security tools - Developing and providing standard tools to perform vulnerability assessments, and test known attack scenarios by performing orchestrated attack actions automatically.
- Sandboxing - Supporting isolation of experiments through virtualization of computing resources and also through network segmentation.
- Standards-driven - Allowing for interoperability by integrating hardware and software components that comply with common industry standards for modeling and communication.
- Metrics - Developing quantitative metrics to measure experimental results and perform validation.

5.4.4 Testbed Infrastructure Resources

Each of these eight strategic testbed engineering tasks would leverage the testbed infrastructure resources such as physical systems, industrial control systems and cyber systems. These include a broad spectrum of various hardware and associated software pertaining to the cyber, control, physical and communication systems, such as real-time power system simulators, SCADA devices such as RTUs, protection relays, and PMUs along with their associated communication protocols, SCADA systems at the control center needed for various analytics such as EMS, Distribution Management Systems (DMS), networking components such as routers, switches, firewalls, VPNs, etc., and standard cybersecurity toolsets.

5.5 Testbed Conceptual Architecture for WAMPAC Experimentation

A typical CPS testbed conceptual architecture can be explained with the help of a layered abstraction approach, based on each layer's functionality [82]. This method of functionally organizing the testbed helps to vary models that are used for different use case scenarios and abstract the unnecessary details appropriately.

5.5.1 Generic Layered Architecture

Figure 5.5 shows the conceptual testbed architecture with the three different layers, namely, information/control layer, communication layer, and physical layer.

5.5.1.1 Information/Control Layer

This layer consists of devices/ software components that act on the various analog and status measurements coming from the substations to perform monitoring and control of the physical system components. Specifically, this layer consists of the SCADA EMS, that perform various analytics at the control center like SE, AGC, CA, etc., substation automation system (SAS) hardware and software including RTUs that collect data from the different IEDs deployed in the field like protective relays and PMUs.

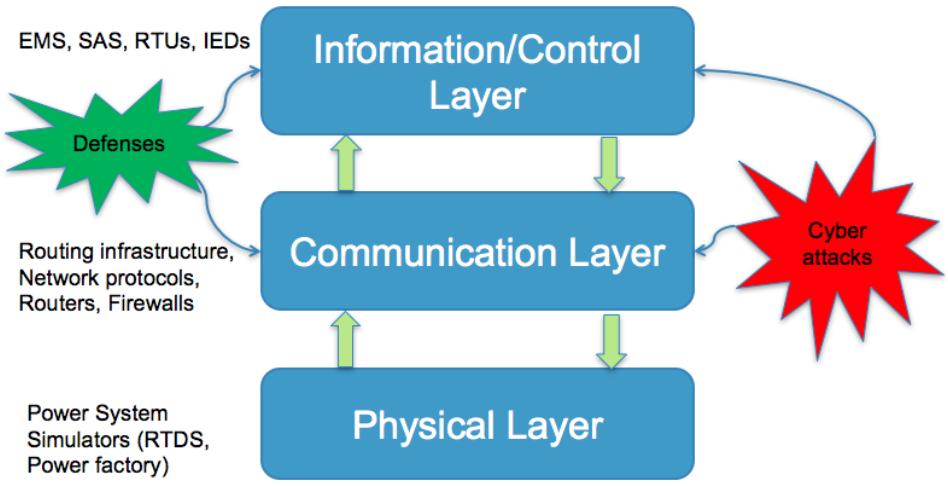

Figure 5.5 Layered Testbed Architecture

5.5.1.2 Communication Layer

This layer consists of the network infrastructure that interfaces the control layer with the physical layer. Specifically, this layer consists of the network infrastructure that emulates wide-area network routing, network routers and switches, security devices like firewalls, intrusion detection systems, and the communication protocols that are used to enable intra and inter-substation communications (e.g. distributed network protocol (DNP) version 3, IEC 61850 manufacturing message specification (MMS), IEC 61850 generic object oriented events (GOOSE), IEC 61850 sampled values (SV)), and wide-area communications with the control center (e.g. DNP3, Modbus).

5.5.1.3 Physical Layer

This layer consists of the components/devices that model the physical system. Typically, this layer consists of real-time power system simulators with the ability to interface real devices to perform hardware-in-the-loop experiments. The capability to interface with real devices with real communication protocols allows a realistic testing of the various attack/defense scenarios. Also, this helps to study the impacts of malicious events in the SCADA control layer (say the

opening or closing of a breaker) on the physical layer (in the power grid) and the communication layer (in the wide-area network) in real time and vice-versa.

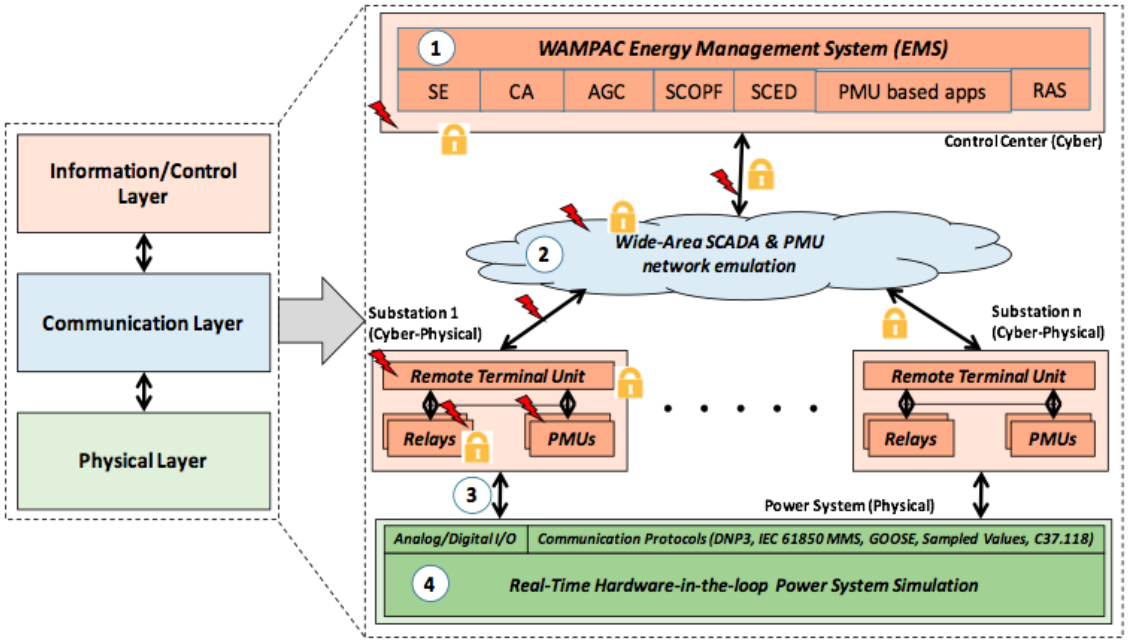

Figure 5.6 WAMPAC-specific testbed conceptual architecture

5.5.2 Addressing WAMPAC Cybersecurity Research Challenges

Based on the three-layered abstraction shown, Figure 5.6 shows a CPS testbed architecture specifically for WAMPAC cyber security use cases that address the following research challenges specific to cyber attack-defense experimentation:

1. **Modeling of information/control layer** - Explicitly modeling the WAMPAC applications' functionality without abstracting away communication aspects like simulation-based environments using real/emulated components. This enables the study of network conditions such as packet drops, retransmissions and congestion on the power system impacts with/without the presence of attacks.

2. **Modeling network layer** - Modeling realistic network communication through real/emulated network environments that enable deployment of a mix of real/emulated devices using

real-world SCADA communication protocols, and supporting the study of network-based cyber impairments on WAMPAC applications such as latencies, delay jitter, etc.,

3. **HIL experimentation** - Providing multiple types of interfacing capabilities such as direct analog interfacing with and without amplifiers, digital interfacing to allow exchange of status and control bits, and real-time network-based interfacing using SCADA communication protocols to also support fast time-scale WAMPAC (synchrophasor and protection) applications.

4. **Modeling physical layer** - Enabling real-time simulation that models the power system components with high-fidelity to allow cyber-physical coupling allowing HIL for conducting realistic experiments to study grid impacts due to cyber attacks. In order to drive physical hardware, the power system simulation model needs to execute in real-time and capture electro-magnetic transient phenomenon to provide high fidelity.

5.6 Challenges for CPS Testbed Federation to Conduct Large-Scale WAMPAC Cyber Attack-Defense Experimentation

We believe that some of the reasons for existing testbed federation efforts not achieving widespread success and adoption are due to a lack of systematic analysis into the various barriers to federate testbeds taking into account the technology constraints and application use cases holistically. However, as part of this work, we would like to underscore the importance of: (i) understanding the technology constraints to interconnect simulators, (ii) identifying the specific use cases that can be modeled with federated testbeds at the different layers, while still providing benefits of scalability and realism. Therefore, the remainder of this section will identify major barriers to testbed federation and potential ways to overcome them to leverage testbed federation wherever possible.

5.6.1 Power System Simulation vs. Network Latencies

High-fidelity, large-scale, real-time power system simulation is one of the main factors that motivates federation of testbeds as existing power system simulator resources at the major

CPS testbeds in the country cannot scale to large-scale systems. Yet, ironically, high-fidelity, real-time power system simulation presents the biggest technology barrier to federate testbeds at the physical layer. Existing high-fidelity, real-time power system simulators typically run at a time-step of 50 μs for performing an electromagnetic transients-based (EMT) simulation, while the average network latency to interconnect remote testbed sites across a few thousand miles typically is around 30-60 ms. Because wide-area network latencies are orders of magnitude slower, interconnection of real-time simulators with physical hardware in the loop across remote sites is nearly impossible at high simulation fidelities. Therefore, existing attempts at testbed federation have relied on centralized power system simulation at one site while choosing to federate the cyber layer across testbed sites or on loosely coupled/independent power system simulation across remote testbed sites [84, 85].

Alternatively, the idea of multi-fidelity, real-time power system simulation seems to slowly gain traction. This would enable the simulation of a large-scale system model with a medium level fidelity, with specific areas of the system modeled in greater detail at high fidelity. Also, such an approach would enable federation of real-time, power system simulators across domains such as transmission and distribution co-simulation, where one testbed site simulates the large-scale transmission system model, and the other sites simulate the distribution system models that plug into the transmission system model. There has been some recent proof-of-concept work done to interconnect power system simulators over a wide-area network for T&D co-simulation demonstrating the feasibility of testbed federation at the physical layer [86].

Adopting a similar approach for performing testbed federation across T&D domains would enable wide-area distributed co-simulation-based use cases, as distribution system simulation time-scales are typically slower (order of ms to s) than transmission system for real-time simulation. Another approach to enable testbed federation across at the physical layer would involve potentially leveraging some existing research on hybrid simulation models that merge extremely high-fidelity electro-magnetic transient simulation models with transient stability phasor-based simulation models as described in [87, 88]. Under such an approach, specific parts of the system under study could be modeled in greater detail, while the interface between two simulators

could be performed at the transient stability simulation time scales to minimize degradation of model fidelity due to network latencies.

5.6.2 Centralized vs. Decentralized Architecture

Centralized architecture – Figure 5.7 presents a centralized architecture that enables federation of testbeds at the control layer level, similar to how real control areas in the power grid share information and resources. In this case, the level of federation is limited to exchange of information at the system level and not a direct resource sharing at the individual device level, where individual devices can be controlled and/or monitored by multiple testbeds. This type of federation allows for limited control and because the interaction is at the higher level, this approach is mainly suited for system level applications.

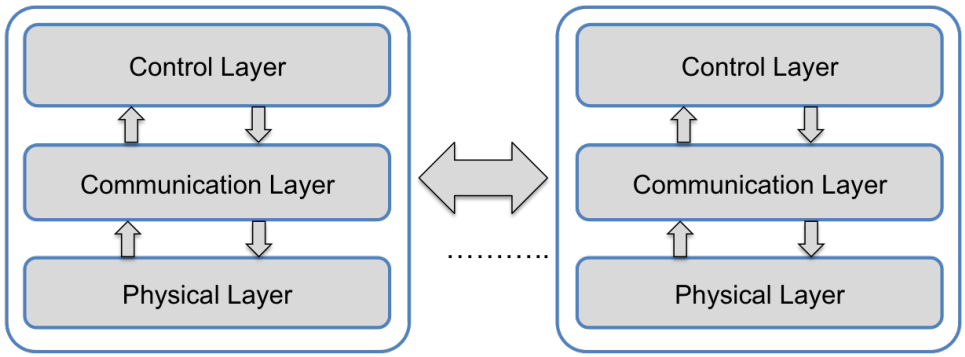

Figure 5.7 Centralized testbed federation architecture

Decentralized architecture – Figure 5.8 presents a distributed architecture for testbed federation that involves a modular approach, where multiple testbeds can be combined at the communication layer, and each of the testbeds either contain the control layer components (like EMS, RTUs, SAS), or physical layer components (like real-time power system simulators, field devices like relays, etc.), or a combination of all three. This type of flexible integration provides a much more fine-grained sharing of resources across locations in a single experiment. Though this approach is reasonably scalable for realistic experimentation, there could be some challenges for supporting applications of fast time scales.

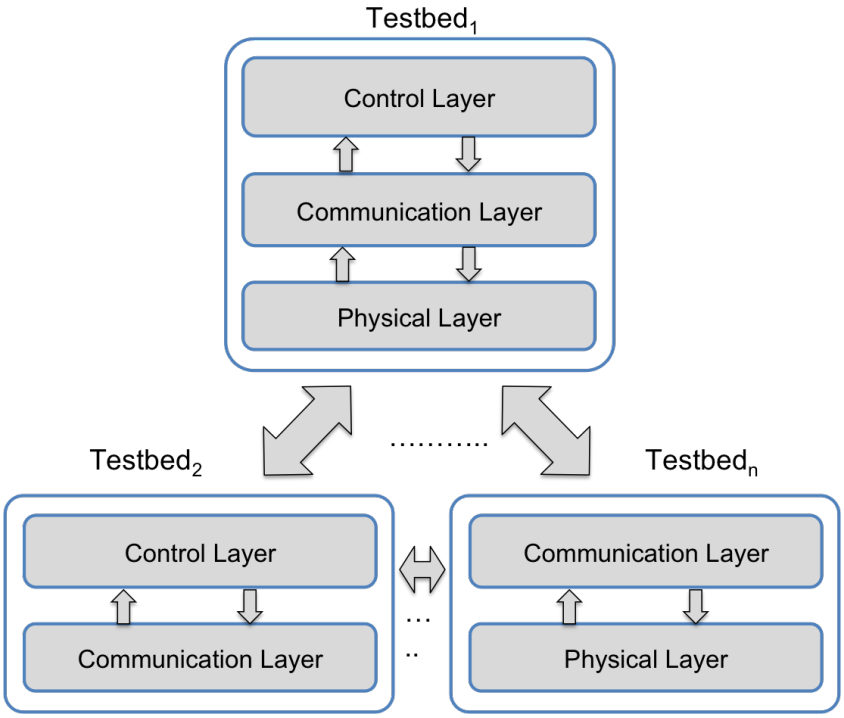

Figure 5.8 Decentralized testbed federation architecture

When deciding on the federation architecture that is required, it is essential to study and characterize the different CPS security research applications based on the timescales and the coordination required so that the appropriate strategy can be identified.

Recently, there have been advancements in the domain of real-time power system simulation that enable a large-scale, phasor-based simulation to run at timesteps of around 1-10 ms [89]. Phasor-based simulations are based on certain approximations of system component models such as machines (generators/motors), transmission lines, and loads. Therefore, they are not as detailed and accurate as EMT-based simulations. However, depending on the specific use case and the application being modeled, the loss in modeling accuracy might be traded off for scalability, enabling large-scale, centralized power system simulations. This would relax the tough constraints on exchanging messages between remote power system simulators frequently to prevent a loss in modeling fidelity. A centralized power system simulation in a federated experiment will result in only the cyber layer resources being distributed across testbed sites and such interconnections are often not constrained by network latencies. Detailed performance evaluations on the appropriate type of power system simulation approach that is needed for specific use cases and applications has still not been performed and documented extensively. There is no general consensus on this and it remains an open issue that merits further interest and exploration by the research community.

5.6.3 Interoperability & Standardization

While the availability of standardized hardware resources and power system simulators would be ideal to federate testbeds at remote sites across cyber and physical layers, such a scenario is not practical. One of the barriers that needs to be overcome is the interoperability of various types of hardware resources across the different federated testbed sites such as the IEDs or protection relays, PMUs, RTUs, and programmable logic controllers (PLC). While the notion of interoperability enables devices with similar functionalities to communicate with each other seamlessly over standard interfaces and communication protocols (Modbus, DNP3, IEC 61850, C37.118, ICCP), oftentimes there still are various differences in implementations that make interoperability difficult.

5.6.4 Experiment Orchestration & Troubleshooting

One of the major challenges in large-scale, federated cyber-physical security experimentation is the ability to automate the various configuration/setup actions, the attack actions and the defense measures, and reverting back to baseline configurations through a well-designed orchestration framework. While the DETER testbed environment provides a web-based orchestration framework [53], there are additional complexities involved in automating the configuration/setup of SCADA/ICS devices such as RTUs, relays, PMUs and PLCs. Some of the software used to set the devices are GUI-based and require additional effort to automate and orchestrate as part of the framework.

Extending the discussion on experiment orchestration, troubleshooting and reverting to a known baseline configuration for the hardware devices and software is extremely critical.Especially with cyber security experiments, there could be possibilities of devices becoming unresponsive or software crashing leading to the need to perform power reboots and/or reconfigurations. It is extremely important to have skilled personnel at each site for technical support and maintenance of testbed infrastructure and issues during experimentation, especially a federated experiment involving multiple sites.

While it is extremely difficult to completely automate all tasks as part of a federated testbed experiment through an orchestration framework, it is extremely critical to have some core features as part of the orchestration framework at individual testbed sites to allow for provisioning of cyber resources such as virtual machines, and network configurations that are more amenable to automated configuration, deployment and management.

5.7 PowerCyber Testbed Implementation Architecture

Figure 5.9 shows the current implementation architecture of the PowerCyber testbed. The SCADA portion of the testbed is composed of industry-grade hardware/software from Siemens that include substation automation system (SICAM PAS), control center software (Power TG), SCADA and and multifunction protection relays (7SJ610, 7SJ82). Recently, the testbed has been integrated with three Schweitzer Engineering Laboratories (SEL) 421 PMUs and a syn-

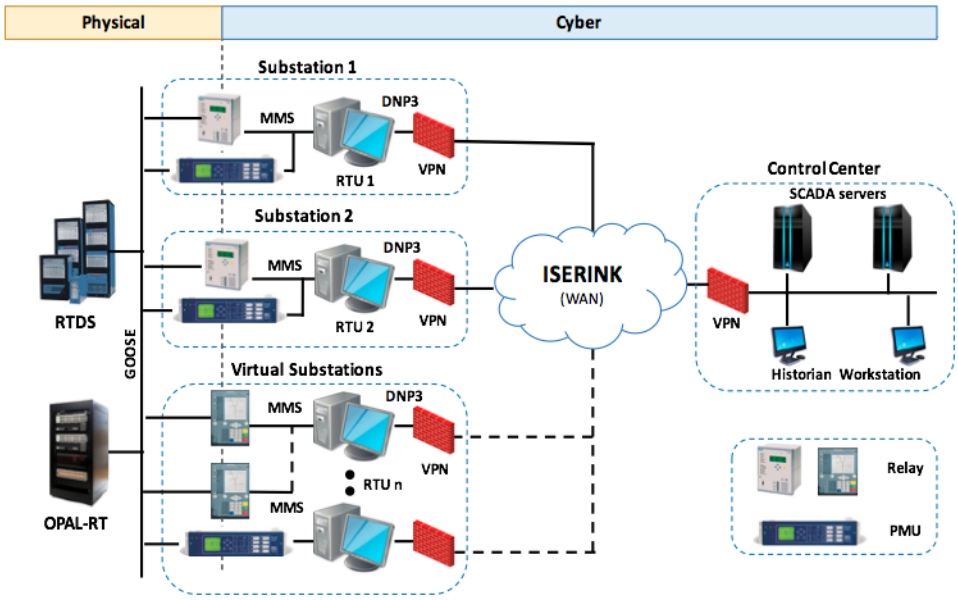

Figure 5.9 PowerCyber testbed architecture

chrophasor vector processor. The EMS software runs on two workstations in a primary-backup, hot standby configuration. There are two software RTUs running the SICAM PAS substation automation systems, which represent two substations, and each of them are connected to a Siemens SIPROTEC Multi-function relay and a SEL 421 PMU. Apart from these two RTUs, the testbed leverages virtualization technology to spin up several RTU virtual machines on a virtualization server (VMware ESXi), depending on the experimental requirements. These virtual RTUs can also be interfaced to appropriate physical relays or to the power system simulators directly to receive/send SCADA measurements/control. The physical relays in the testbed communicate with the RTUs through IEC 61850 MMS protocol and the RTUs communicate with the control center EMS using the DNP3 protocol.

In the testbed, we have two real-time power system simulators, one from Real Time Digital Simulator (RTDS) and another from OPAL-RT. Both of these real-time simulators are used based on appropriate experimental needs and both provide an accurate, high-fidelity, real-time power system simulation enabling hardware-in-the-loop experimentation. The simulators are directly interfaced to the Siemens relays using the IEC 61850 GOOSE protocol, while the

SEL PMUs are interfaced to the simulators through analog interfacing as well as through the GOOSE protocol. This allows the study of the impact of switching events in the SCADA control layer (say the opening or closing of a breaker) on the physical layer (in the power grid) in real time and vice-versa.

The communication between RTUs and control center takes place over an Ethernet-based Wide-Area Network provided by the ISERINK platform. ISERink is a virtual environment for cyber defense competitions, and attack-defense evaluations [90] and creates a dynamic network infrastructure similar to real SCADA network through the emulation of routers. In order to encrypt the traffic between the control center and the substations, the testbed uses SCALANCE network security devices from Siemens, and traditional linux-based firewall and VPN software. Vulnerability assessment capapbilities are based on a set of free and open-soure software tools such as NMap, Nessus, Wireshark, Metasploit and many others that are part of the Kali Linux distribution.

5.8 Experimental Case Studies on WAMPAC Applications

5.8.1 Coordinated Attack-Defense Experimentation on Wide-Area Protection

This section describes a case study that involves coordinated attacks on a WAP scheme and is described in detail in [25]. In this particular case study, we show how the PowerCyber testbed was used to replicate the conditions of a RAS and study the impact of coordinated cyber attacks on the power system. The WECC 9-bus system, shown in Figure 5.10 was chosen as the power system for our case study. The particular RAS that was adapted for this case study was taken from the WSCC RAS list [91] and is explained below.

The RAS scheme is designed to trip one of the generation units at bus 2, (modeled by a reduction in the generation), if there is a fault on one of the transmission lines connected to it. In our case there are two transmission lines, namely, $7-8$ and $7-5$. The RAS scheme would be armed only if generation at bus 2 exceeds a particular value. This generation would have to be reduced to prevent the thermal overloading of one of the transmission lines in case of a fault on the other line and also to maintain the stability of the generation units.

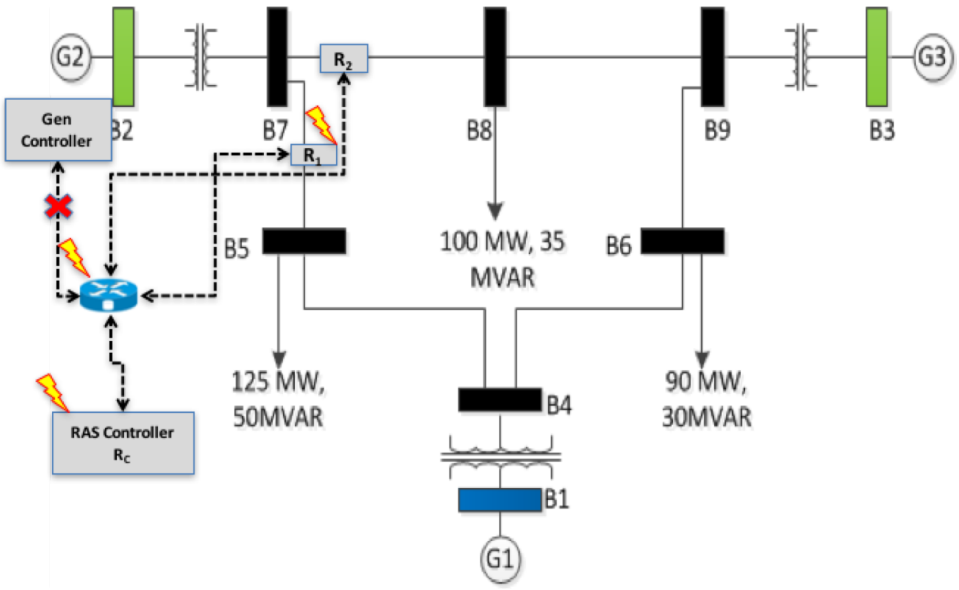

Figure 5.10 IEEE 9-bus system with RAS mapping

Typically, for every RAS, there is a RAS controller, which determines when the scheme is to be armed and also sends appropriate commands to the corresponding relays that are part of the scheme. In our case, the controller sends a trip command to one of the generation units at bus 2 when it receives a fault indication from one of the relays on the transmission lines $7-8$ or $7-5$. In our experimental scenario, the RAS controller is mapped to one of our two physical relays (Relay 1) interfaced to the RTDS. The RAS is triggered by tripping the relay (Relay 2) protecting line $7-5$. This causes Relay 2 to send a GOOSE message to the RAS controller indicating that it has tripped. Based on whether the RAS was armed or not, the RAS controller responds back with a IEC GOOSE message to the relay (modeled inside RTDS) which controls the breaker commands for the tripping of one of the generation units connected at bus 2 to reduce generation and thereby prevent thermal overload of line $7-8$.

5.8.1.1 Coordinated Attack Template

The case study involves the execution of a coordinated attack to prevent the RAS from operating and reducing the loading on the transmission line 7-8. This causes a thermal overload

on that line and leads to its tripping. If we assume that the RAS is already armed, i.e generation at bus 2 greater is than a specified threshold, the coordinated attack actions are:

- Creating a data integrity attack to trip Relay 2 which protects line 7-5 to activate the RAS.
- Creating a DoS attack to prevent the GOOSE trip command to the generation unit at bus 2 to result in a thermal overload on line 7-8 and cause it to trip out.

By looking at Figure 5.10, we can explain how the RAS operates by walking through the sequence of events and IEC 61850 messages being exchanged between the devices associated with this protection scheme. Generally, the control center operator can manually arm/disarm the RAS through an IEC 61850 message to the RAS controller directly outside the typical flow of events that are listed below.

1. The Generating station at bus 2 exceeds a threshold, communicates this to the RAS controller (Relay 1) to arm the RAS.
2. Relay 2 associated with the protected line 7-5 sends a message to the RAS controller to indicate a fault.
3. RAS controller performs the necessary validation checks and issues a trip command to the unit at generating station in bus 2 to reduce generation immediately.
4. Because of the successful cyber attack, generation at bus 2 is not reduced, and Relay 3 protecting line 7-8 detects thermal overload.
5. Relay 3 reaches maximum time for withstanding the thermal overload and trips, isolating the generation station at bus 2.

5.8.1.2 Results - Cyber Impact

We evaluated impacts of two types of DoS attacks that could disrupt the RAS communication, (1) flooding the switch that carries RAS traffic, (2) flooding the RAS controller directly.

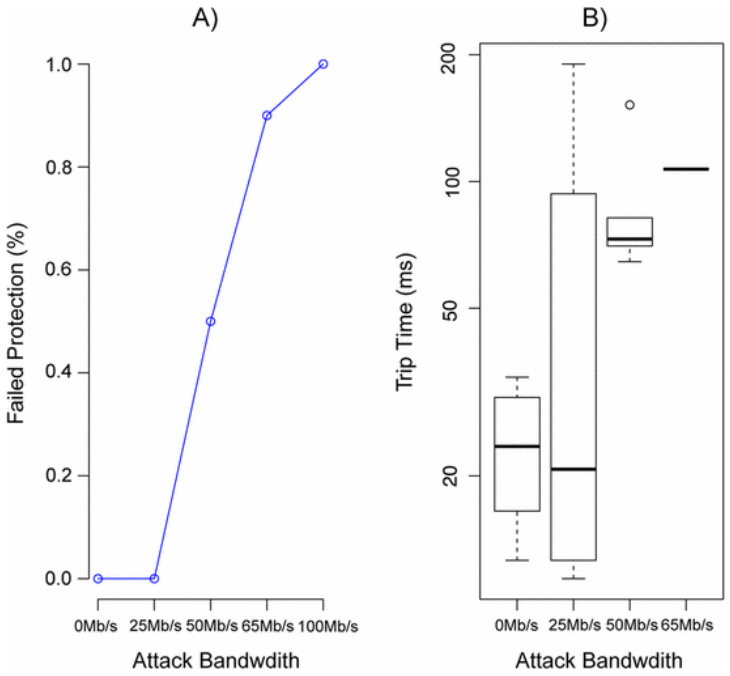

Figure 5.11 DoS protection scheme impact (switch flooding)

We performed several runs with various traffic rates to determine the amount of DoS traffic required to disrupt the RAS for both the scenarios. We were able to observe that the RAS scheme could be disrupted through both methods, although targeting the RAS controller requires significantly less bandwidth compared to flooding the switch.

Figure 5.11 shows the impact of the DoS attack by flooding the Ethernet switch. Figure 5.11(a) displays that the percentage of times that RAS failed based on various DoS attack rates. It is to be noted that as traffic hits 50 Mbps the RAS fails 50% of the time, while at greater attack rates the RAS fails consistently. Figure 5.11(b) displays averaged time for the RAS communication to travel from the relay to the RAS controller and back (note: these results only include successful RAS operations even though they were very delayed, as in several other cases the RAS communication never completes due to the flooding). Although the RAS only fails after not receiving the communication within 1 second, our results show that either the communication occurred within 200 ms or the RAS failed. This type of behavior is likely explained by Ethernet's collision detection exponential back-off and eventual collision timeout.

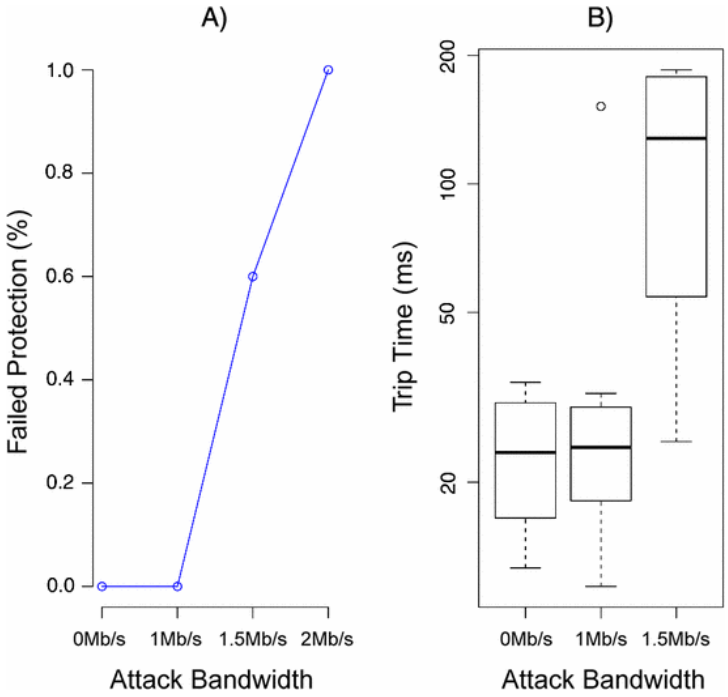

Figure 5.12 DoS protection scheme impact (relay flooding)

Figure 5.12 shows the results for the case where the RAS controller is directly flooded. Figure 5.12 shows that the RAS could be disrupted with significantly less bandwidth by directly targeting the relay. Figure 5.12(a) shows that traffic around 1.5 Mbps is sufficient to disrupt the RAS 60% of the time, while as traffic reaches 2 Mbps the RAS continually fails. Figure 5.12(b) displays the average delay of the RAS during successful runs.

5.8.1.3 Results - Physical system impact

Figure 5.13 and Figure 5.14 show the impacts of the coordinated attack on the power system. Specifically, Figure 5.13 shows how the system voltages are impacted and Figure 5.14 shows how the line power flows and the generation are impacted as a result of the attack. Each of these figures have two ovals highlighting the two events which constituted the attack. The first event represents the tripping of line 7-5 due to an attack, and the second event represents the tripping of line 7-8 due to the DoS attack on RAS.

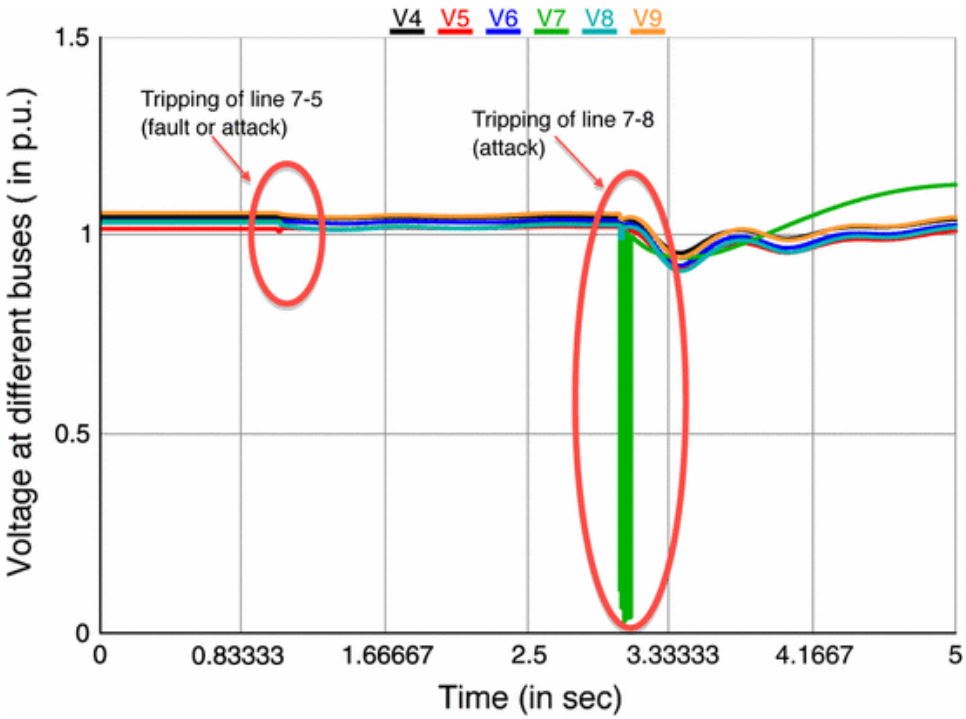

Figure 5.13 Impact of attack on system voltages

Figure 5.13 shows that the tripping of line 7-5 did not cause much impact on the system voltages and the voltages at all the buses stayed close to 1.0 p.u. Whereas, after the tripping of line 7-8, generator two was completely islanded from the grid and this impacted the voltages at several buses significantly.

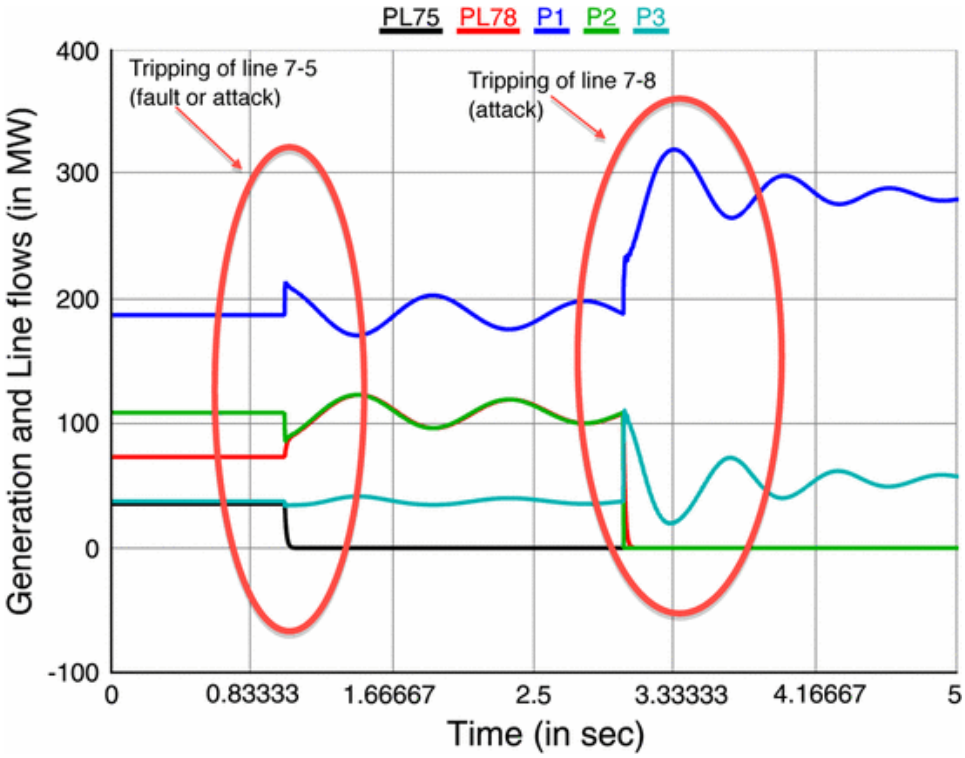

Figure 5.14 Impact of attack on generation and line flows

From Figure 5.14, we can observe that the tripping of line 7-5 changed the generation in all three generators by a small amount, but it overloaded the line 7-8 significantly. This prevented the generation reduction as per the RAS and eventually it led to the tripping of line 7-8. As mentioned before, it is to be noted here that the tripping of line 7-8 completely isolates generator 2 from the system. Therefore, it would result in a huge loss of generation which impacted the frequency profoundly. Such a scenario of generation loss in a real power system could potentially cause some frequency related problems and could potentially lead to under-frequency load shedding.

5.8.2 Coordinated Attack Experimentation on Wide-Area Protection and Control Applications - AGC and RAS

In this section, we present a detailed case study of a coordinated cyber attack performed on two WAMPAC applications, namely AGC, and a generator rejection RAS on the PowerCyber testbed [92]. Figure 5.15 shows the implementation architecture for the use case scenario in this case study.

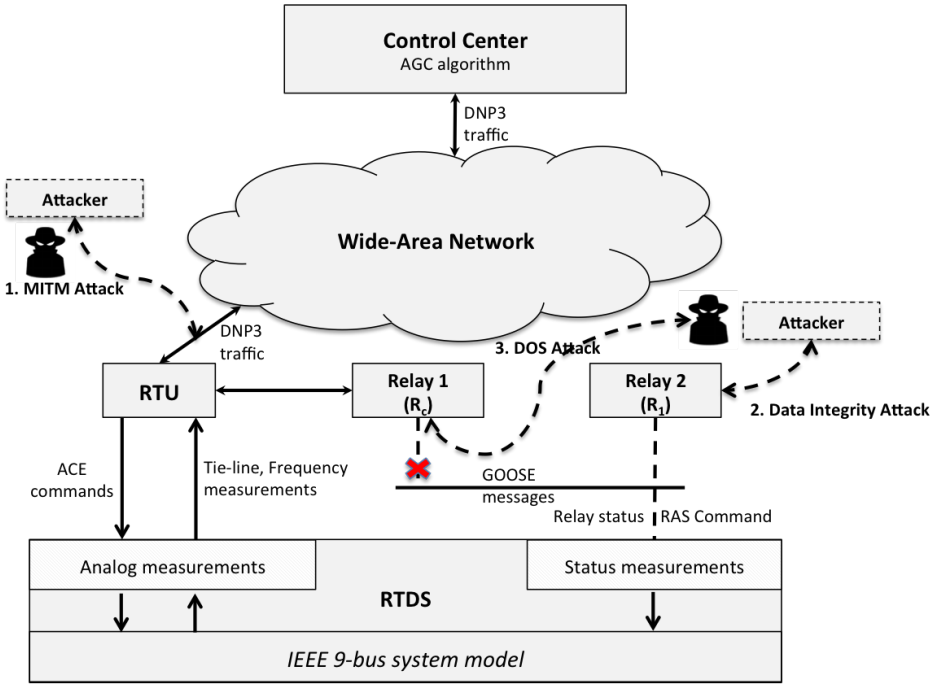

Figure 5.15 Implementation architecture of use case scenario on the PowerCyber testbed

The standard IEEE 9-bus power system model is implemented in the Real Time Digital Simulator (RTDS). The analog measurements and control signals corresponding to the AGC algorithm are communicated from/to the RTDS to/from the control center via the substation RTU over the DNP3 protocol. Figure 5.15 shows only one RTU for simplicity. Two physical relays Relay 1 and Relay 2 in the testbed are utilized for implementing the RAS scheme along with the RTDS. The relays and RTDS exchange GOOSE messages similar to real substation implementations to communicate the status signals when a relay trips or in order to send generation rejection commands to the generating stations in the RTDS model. The relays in

the testbed are mapped to control breakers in the RTDS power system model enabling real-time, hardware-in-the-loop experimentation. Therefore, actions such as data integrity attacks on the cyber layer, and/or DOS attacks on the communication layer can be observed in the power system model instantaneously.

Figure 5.16 shows the IEEE 9-bus model along with the control areas for AGC algorithm, and also the location of the generator rejection RAS that has been implemented. The relays on the testbed are mapped to Rc, and R1 in the power system model respectively. As part of the experimental scenario, we have also implemented line overload protection on the critical transmission lines, and under-frequency load shedding (UFLS) similar to real-world implementations. The relay R2 corresponding to overload protection in the power system model is modeled inside RTDS. We leveraged the communication modules in RTDS for exchanging the real-time simulation data using the DNP3 protocol (Tie-line power flow and frequency measurements), and GOOSE protocol (relay status, RAS generator rejection command) respectively. This enables a realistic implementation of AGC and RAS functions similar to real-world settings.

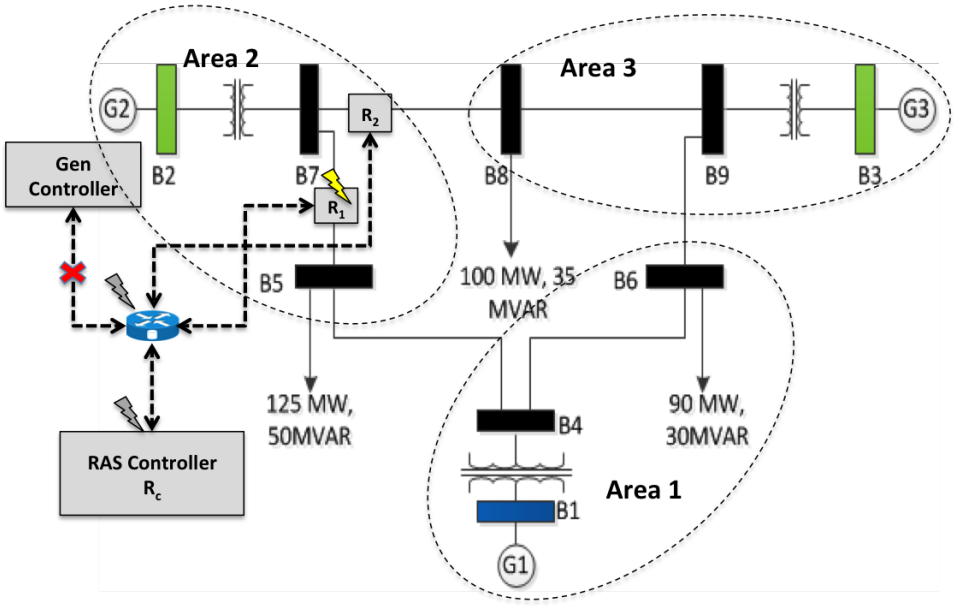

Figure 5.16 IEEE 9-bus model with AGC control areas and RAS location

In this case study, we only consider the AGC functioning with respect to Area 1 as shown in Figure 5.16 for simplicity. The associated tie-line flows for Area 1 are flows on transmission lines 4-5 and 6-9. According to AGC operation, any load change on Bus 6 would be addressed by correspondingly adjusting the mechanical turbine input power for generator G1 corresponding to the ACE value.

We have implemented the generator rejection RAS to decrease the generation level of G2 when either line 7-8 or line 7-5 is out of service and the power output from G2 is over a certain threshold. For example, if line 7-5 is tripped due to a natural or malicious event, the relay corresponding to line 7-5 (R1) will send out a status change alert to the RAS controller (Rc). On the condition that the RAS is currently armed (when G2 is over a pre-determined threshold), the RAS controller will send a command to G2 to ramp it down by a preset value. After the ramping down command is successfully carried out, the overload on line 7-8 due to the tripping of line 7-5 would be alleviated.

Table 5.1 IEEE 9-bus system base case

Line	**Power Flow (MW)**	**Generator**	**Output (MW)**	**Load**	**Value (MW)**
Line 7-8	42.34	Gen 1	150.3	Load 1	90
Line 7-5	37.71	Gen 2	80.1	Load 2	125
Line 4-5	87.65	Gen 3	85.4	Load 3	100
Line 4-6	62.61	-	-	-	-
Line 9-6	27.53	-	-	-	-
Line 9-8	57.84	-	-	-	-

As line overload protection is often armed for critical transmission lines, when the line flow goes beyond the secure level for a certain amount of time, the relay associated with line 7-8 (R2) will trip the line for self-protection. In this case study, overload protection is installed only for line 7-8 and line 7-5. As a last defense measure to prevent system frequency from causing system islanding, UFLS is configured as to shed 70 MW load from Bus 5 with 2 seconds delay when system frequency goes below 59.7 Hz and to further shed another 40 MW more immediately if the frequency is below 59.6 Hz. The base case of the IEEE 9-bus system is listed

in Table 5.1, and the configuration of line overload protection, RAS and UFLS in Table 5.2. The coordinated attack vector that was implemented for the case study has been described in the following paragraphs.

Table 5.2 RAS and UFLS configuration

Scheme	**Arming condition**	**Trigger condition**	**Action**
RAS for G2	P2 > 85 MW	Either line 7-8 or line 7-5 is out of service	Ramp down G2 by 40 MW.
UFLS in area 2	Always	Frequency < 59.7 Hz	Shed local load by 70 MW with 2s delay.
UFLS in area 2	Always	Frequency < 59.6 Hz	Shed local load by 40 MW with no delay.
Overload protection for line 7-8 or line 7-5	Always	Flow on the remaining single line > 70 MW for more than 20 s	Trip the overloaded line.

5.8.2.1 Coordinated Attack Vector

In practice, RAS are seldom used, as the condition to arm the RAS is satisfied only under heavy loading conditions such as peak summer loads. But when under peak load, RAS would be enabled to maximize transmission line utilization. In our case study, the generation level of G2 is very close the arming threshold in the base case. As shown in the Table 5.1, the generation level of G2 has only a 5 MW margin for the RAS to be armed. The coordinated attack vector consists of the following actions:

1. **Man-in-the-middle (MITM) attack** – The attacker compromises the tie-line flow and frequency measurements of Area 1 as they are in transit between the RTU and the control center. This MITM attack sends spoofed measurements to the control center resulting in Area Control Error (ACE) values that decrease the generation of Area 1, i.e., G1 will decrease its power output gradually. This causes the other generators to increase their output due to the governor actions to counteract the drop in system frequency. This increases generator G2s output above its threshold, effectively arming the RAS.

2. **Data integrity attack** – The attacker trips line 7-5 (R1) by sending a trip command to Relay 2 in the testbed after the RAS gets armed. This initiates the RAS sequence, where R1 sends a status update to the RAS controller Rc. Rc checks if the RAS is armed, and sends a generator rejection command to the generation controller for G2 (modeled inside RTDS). If this command does not reduce the generation within a certain amount of time, overload protection relay (R2) will trip line 7-8 and isolate generator G2 from the rest of the system.

3. **Denial of Service (DoS) attack** – The attacker blocks the RAS generation rejection command sent from the RAS controller Rc, which should ramp down G2. This is achieved by carrying out a DoS attack on the relay Rc. As G2 does not ramp down due to the DoS attack, overload protection relay R2 times out and trips the line 7-8.

The dotted arrows in Figure 5.15 show the implementation of the attack vector on the PowerCyber testbed.

5.8.2.2 Impact Analysis

Figure 5.17 and Figure 5.18 show the various impacts of the coordinated attack on AGC and RAS. The top subplot in Figure 5.17 shows the variation of system frequency with time and the bottom subplot shows the corresponding variation of critical tie-line power flows on lines 7-8, 7-5 and 4-5. Similarly, the top subplot in Figure 5.18 shows the variation of voltages at buses 4, 5, 7, and 8 respectively as they are involved in the attack vector. The bottom subplot in Figure 5.18 shows the output of the three generators and the load in area 2 during the entire scenario.

The timeline of all the major events in this attack vector are as explained below:

1. AGC measurement spoofing attack is carried out 8 s after simulation begins, and this causes G1's output to reduce slowly. Consequently, G2's output increases due to governor action and eventually crosses the threshold to arm the RAS for G2 at around 28 s.

2. R1 (Relay 2) is tripped by the attacker at around 28s almost instantaneously after the RAS is armed. At the same time, the attacker also floods the RAS controller Rc (Relay 1).

3. Due to the DoS attack, the generator G2 does not ramp down and therefore around 48 s, line 7-8 is tripped by overload protection (R2) and G2 is completely separated from the system.

4. System frequency decreases sharply due to a significant loss in generation, which triggers both the UFLS stages. After 110 MW load out of the total 125 MW being tripped, the system frequency finally recovers to 60 Hz.

All the subplots in Figure 5.17 and Figure 5.18 have been annotated with these four major phases as mentioned in the timeline to aid the readers understanding.

Frequency impacts: From the top sub-plot in Figure 5.17, we can see that the initial AGC attack (Phase 1) causes a steady decline in system frequency. The triggering of the RAS by tripping R1 (Phase 2) causes a minor disturbance, but the governor actions restore the frequency to a small extent. After the overload protection trips the line 7-8 (Phase 3), there is a sharp drop in frequency, as G2 is isolated, thereby, causing a huge deficit in generation. Finally, UFLS schemes kick in (Phase 4) to shed loads in two major chunks to restore the frequency back to normal.

Tie-line flow impacts: From the bottom sub-plot of Figure 5.17 we can see the impacts on the tie-line flows during the attack. As mentioned previously, the AGC attack (Phase 1) causes a reduction of generation in Area 1, which decreases the flow on line 4-5 steadily. After the line 7-5 is tripped (Phase 2), the power flow on line 4-5 increases again due to governor action to supply the load at bus 5. This is also accompanied by a loss in frequency. As a result of the DoS attack, the overload on line 7-8 (Phase 3) does not reduce until it is tripped out by thermal overload protection. Finally, the power flow on line 4-5 is reduced after the UFLS sheds the load (Phase 4).

Generation & Load impacts: The bottom subplot of Figure 5.18 shows the impact of the generation outputs and the load during the coordinated attack. The AGC attack clearly can

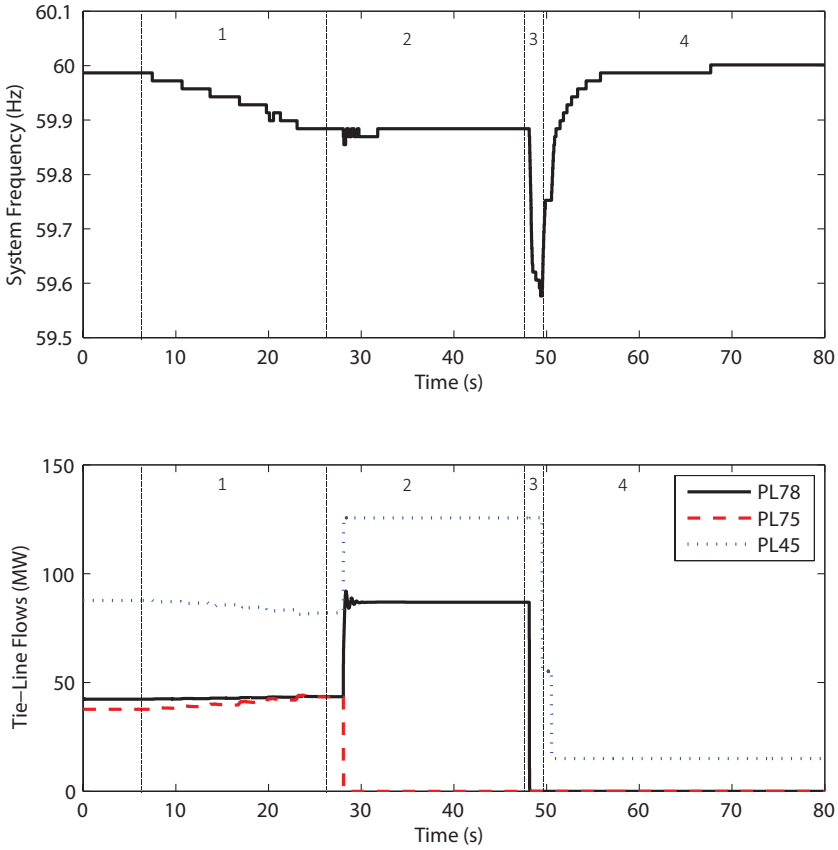

Figure 5.17 System frequency (Hz) and tie-line flows (MW) during the coordinated attack

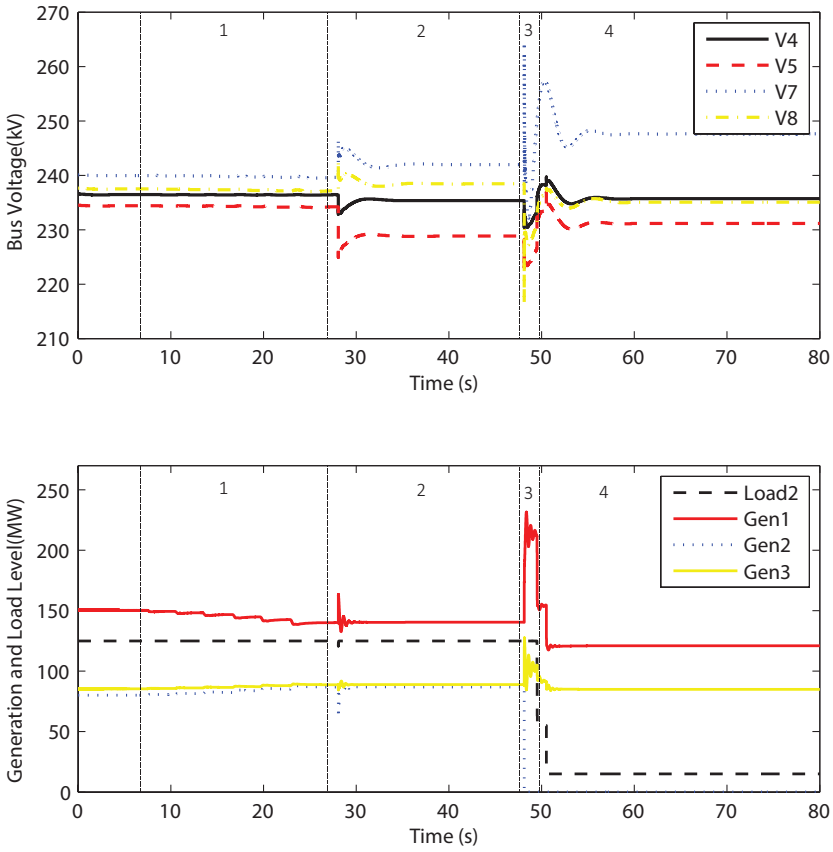

Figure 5.18 Bus voltages, generation and load levels during the coordinated attack

be observed as a steady decrease in the output of G1, corresponding to a steady increase in generators G2 and G3 due to the governor actions (Phase 1). All generators experience a minor fluctuation when the RAS is triggered (Phase 2). Due to the DoS attack, generation output of G2 does not decrease until it is isolated completely due to tripping of line 7-8 (Phase 3). UFLS kicks in to shed a bulk of the load at bus 5, which reduces the output of the generator G1 that was feeding the load (Phase 4). Overall, this coordinated attack isolated G2 from rest of the system, and caused a forced load shedding of 110 MW in Area 2.

Voltage impacts: From the top subplot of Figure 5.18, we can observe that the impacts on system voltages are much more severe than generation outputs. The line trip (Phase 2) creates a temporary voltage fluctuation, which damps out quickly. However, after the UFLS kicks in (Phase 4) there is a huge voltage fluctuation as the magnitude of load shedding is significant. In this case study, we have not modeled any voltage sensitive loads on the system. However, the evaluation of voltage impacts on voltage sensitive loads such as induction motors would reveal further insights into the stability of the system during such attacks. These would be explored as part of our future work.

5.8.3 Stealthy Cyber Attack-Defense Experimentation on Wide-Area Control Application

In this case study, we describe a testbed-based implementation and performance evaluation of Attack-Resilient Control (ARC), in an attempt to validate the results from an earlier simulation-based study [83]. This work leverages some of the implementation efforts done for a similar experimental case study documented in [93]. The experiment overview, implementation and results that are described below as part of this case study are published in [94].

The rest of this section is organized as follows. First, we provide a brief overview of AGC operation and stealthy attack templates on AGC that cause UFLS. Then, we provide a brief overview of ARC, which is described in detail in [83]. Next, we describe the implementation architecture of the experiment on the PowerCyber testbed. Finally, we present results from attack-impact and attack-defense studies.

5.8.3.1 Background on AGC Operation

The AGC algorithm is a wide-area control mechanism that maintains generation and load balance in each balancing area (BA) [95]. The AGC algorithm serves two critical functions - i) maintain system frequency at 60 Hz, and ii) maintain tie-line flows at scheduled values. In order to achieve this, the AGC calculates Area Control Error (ACE) every 2-8 seconds based on tie-line power flow and frequency measurements received from SCADA. The ACE, which is used to adjust generation set points, is calculated by the following equations.

$$ACE = \Delta P_{tie} + \beta \Delta f \tag{5.1}$$

$$\Delta P_{tie} = P_{act} - P_{sch} \tag{5.2}$$

$$\Delta f = f_{act} - f_{nom} = -\frac{\Delta P_{load}}{\Sigma(1/R + D)} \tag{5.3}$$

In the above, ΔP_{tie} represents the difference of scheduled tie-line power flows (P_{sch}) from actual tie-line power flows (P_{act}), Δf represents the deviation of the actual frequency (f_{act}) from nominal (f_{nom} = 60 Hz), β represents the balancing authority bias to help system frequency, ΔP_{load} represents the load change in the BA, R represents the droop constant of each generator in the system, D represents the frequency sensitivity of loads in the system [95].

A positive ACE indicates that the generators in the BA need to ramp down, and vice-versa. Depending on the ACE received, a subset of the generators in the BA regulate their outputs constantly meeting tie-line power flow and frequency constraints. The inherent dependence of both the measurement and the control data on wide-area SCADA communication make the AGC algorithm vulnerable to different types of cyber attacks that would potentially impact system frequency.

5.8.3.2 Data Integrity Attack Model

Earlier research efforts [96, 83] have shown how the tie-line and frequency measurements may be strategically modified by a knowledgeable attacker to cause system frequency to deviate from nominal value without being detected. In summary, this stealthy attack strategy involves modifying the frequency and tie-line measurements such that their change obeys the underlying

physics of the system. Such an attack could be executed by the attacker with some knowledge about the system parameters and constants [83]. For example, the attacker would send tie-line and frequency measurements that are higher than their actual values, causing the AGC to calculate an ACE that would reduce the generation below the actual load requirement. This would result in inadequate generation leading to a gradual decline in system frequency. Specifically, as part of the experimentation in this paper, we consider two attack models (scaling and ramp attacks) as defined in [83], and mathematically represented in Equations 5.4 to 5.7.

- **Scaling attack** – This attack vector involves scaling of the tie-line power flow measurements (P_{tie_act}) based on a scaling attack parameter $\lambda_{scaling}$, and then calculating the corresponding malicious frequency measurement. Such an attack would instantly cause system frequency to deviate from 60 Hz.

- **Ramp attack** – This attack vector involves adding a time-varying ramp signal to P_{tie_act} based on a ramp attack parameter λ_{ramp}, and calculating the corresponding malicious frequency measurement to cause a slow drift of the system frequency.

$$P_{tie\_scaling} = (1 + \lambda_{scaling}) * P_{tie\_act} \tag{5.4}$$

$$P_{tie\_ramp} = P_{tie\_act} + \lambda_{ramp} * t \tag{5.5}$$

$$\Delta P_{tie\_attack} = P_{tie\_scaling/ramp} - P_{tie\_act} \tag{5.6}$$

$$f_{attack} = f_{act} - \frac{\Delta P_{tie\_attack}}{\Sigma(1/R + D)} \tag{5.7}$$

5.8.3.3 Attack-Resilient Control Algorithm for AGC

Figure 5.19 shows a schematic of how ARC integrates with the AGC algorithm to detect and mitigate attacks through a combination of domain-specific, model-based anomaly detection and mitigation. The ARC algorithm validates the ACE received from AGC using anomaly detection and triggers model-based mitigation if an anomaly is detected.

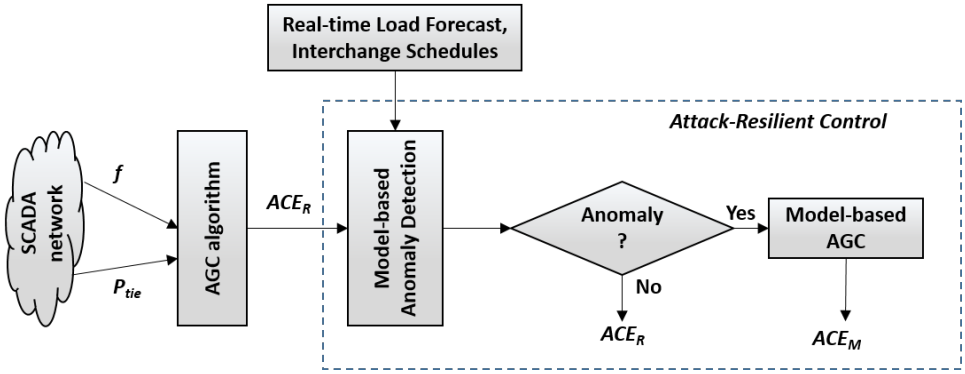

Figure 5.19 Attack-resilient control for AGC

Anomaly Detection

The anomaly detection component examines the real-time ACE (ACE_R) to identify corrupted data using two rules. Rule 1 is intended to identify attacks that attempt to trigger an instantaneous change, as in the case of a scaling attack. It compares ACE_R against a range of acceptable ACE values to flag anomalies. This range is determined using offline statistical analysis of model-generated ACE values based on real-time load forecast data [83]. The tightness of the bound for Rule 1 is driven by δ_1. The larger the value of δ_1, the wider is the range of acceptable real-time ACE (vice-versa). Rule 2 is intended to catch attacks such as the ramp attack, where small changes are injected in regular intervals to result in a significant change over a time period. Rule 2 compares the cumulative ACE from real-time operation (ΣACE_R) to the cumulative ACE from the ACE generated by offline AGC (ΣACE_M). If the value of ΣACE_R exceeds ΣACE_M by a factor of δ_2, an anomaly is flagged.

The tuning of anomaly detection algorithm involves selecting values for δ_1 and δ_2 that result in the least possible false positive and negative rates. From the system operator's perspective, the goal is to be able to detect scaling and ramp attacks with the least possible attack parameters - $\lambda_{S_{min}}$ and $\lambda_{R_{min}}$. This will enable ARC to detect the entire range of ramp and scaling attacks. Towards this end, the following steps are to be performed periodically.

1. Generate a measurement set that contains a mixture of true and corrupted values using the scaling and ramp attack models, with attack parameters $\lambda_{S_{min}}$ and $\lambda_{R_{min}}$.

2. Calculate FP and FN rates for a range of δ_1 and δ_2.

3. Select δ_1 and δ_2 for acceptable FP and FN rates.

Attack Mitigation

When ARC detects an anomaly, model-based attack mitigation is triggered. Attack mitigation essentially uses ACE_M instead of the ACE_R for AGC operation until trust in the SCADA measurements is regained. Thereby, model-based mitigation restores operating frequency close to nominal values limiting the attack impacts on the system loads.

5.8.3.4 Testbed Setup

Figure 5.20 shows the implementation architecture for our attack-defense experiment on the PowerCyber testbed. The IEEE 9-bus power system model is simulated on the RTDS. The measurements and control signals pertaining to the AGC algorithm are exchanged between the control center and the RTDS using DNP3 protocol. In our case, the RTDS serves as a DNP3 slave similar to a real substation, and the control center serves as the DNP3 master that initiates periodic polling of the substation to receive measurements and send control signals. The ARC algorithm runs at the control center in conjunction with the AGC to detect and mitigate stealthy attacks.

As shown in Figure 5.20, we implemented the stealthy attacks on AGC through a Man-in-the-Middle (MITM) attack. This MITM attack is performed by executing an ARP poisoning attack using the ScaPy tool [97]. ARP poisoning enables the attacker to access all DNP3 packets flowing between the simulator (substation) and the control center. By accessing the tie-line power flow and frequency measurements, the attacker is able to implement the scaling and ramp attacks.

Figure 5.21 shows the IEEE 9-bus system divided into 3 BAs. For our experiment, we considered attacks on the AGC algorithm in Area 1. Tie-lines L_{45} and L_{69} connect Area 1

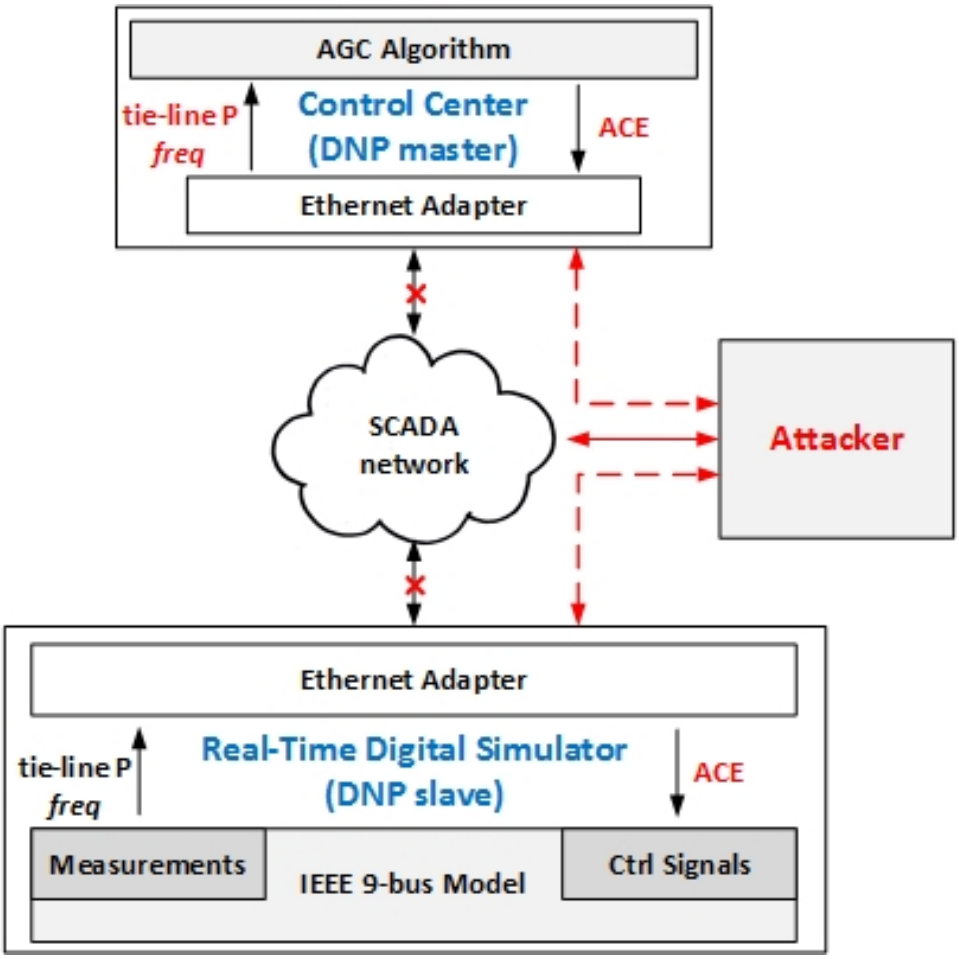

Figure 5.20 PowerCyber testbed configuration

with Areas 2 and 3, respectively. We assumed a constant value for scheduled tie-line flows for L_{45} and L_{69}. For simplicity, the generation and load level of Areas 2 and 3 were maintained as constant. For Area 1, the output of Gen 1 was dispatched every 5 minutes. Based on the load forecast, the real-time load in Area 1 (at Bus 6) was updated every second. In order to generate the real-time load, we added the forecasted load with a random forecast error, which follows a truncated normal distribution [74]. The AGC algorithm was executed once every 10 seconds to produce an ACE for Gen 1.

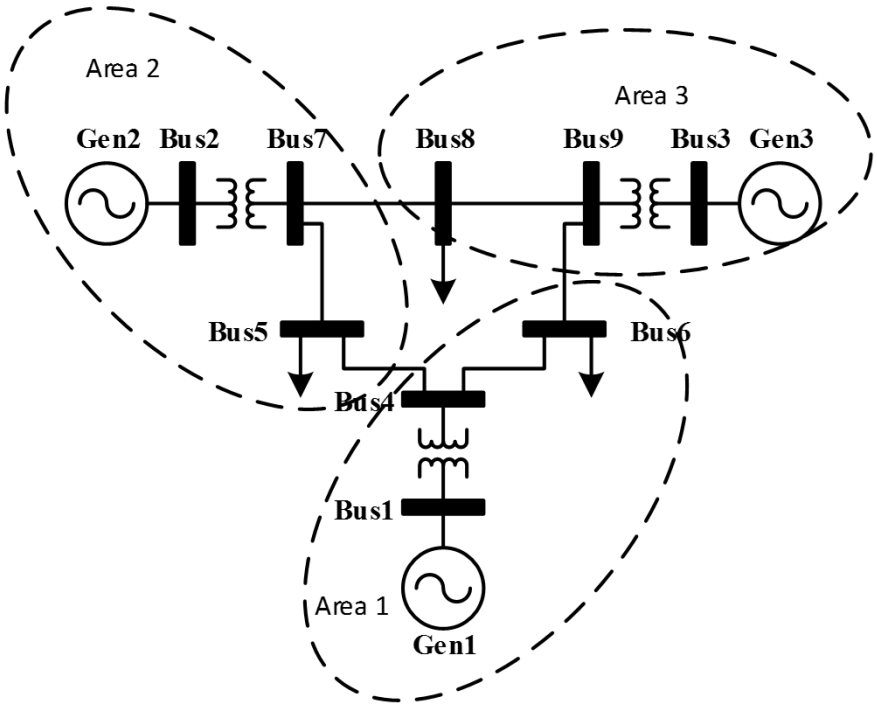

Figure 5.21 IEEE 9-bus system with 3 BAs

5.8.3.5 Experimental Results

Based on the methodology outlined in Section 5.8.3.2, the attack ranges presented in Table 5.3 were determined for ramp and scaling attacks. As the attacker would seek to cause maximum impact at the earliest, $\lambda_{S_{max}}$ (0.0570) and $\lambda_{R_{max}}$ (0.0245) were used for experimentation. On the contrary, from an operator's perspective, the attack detection algorithm was

tuned based on $\lambda_{S_{min}}$ (0.0253) and $\lambda_{R_{min}}$ (0.0180), as the goal would be to detect even the attack with the least impact. Based on these attack parameters, the values of δ_1 and δ_2 for rules 1 and 2 of the anomaly detection algorithm were tuned to achieve the lowest FP and FN rates and are shown in Table 5.4.

Table 5.3 Attack parameters for experimentation

Attack Type	$\lambda_{\mathbf{min}}$	$\lambda_{\mathbf{max}}$
Scaling	0.0253	0.0570
Ramp	0.0180	0.0245

Table 5.4 Anomaly detection bounds for rules 1 and 2

Rule	**Lower Bound**	**Upper Bound**
Rule 1	$-0.0328\ pu$	$0.0147\ pu$
Rule 2	$-0.0368\ pu$	$0.0368\ pu$

Based on the above parameters for attack and defense, we performed a detailed experiment on the PowerCyber testbed to evaluate the effectiveness of ARC algorithm. We first ran tests to demonstrate the disruption of ARC-less AGC operation using scaling and ramp attacks. Then, we re-executed the attack scenarios with ARC in place to capture its effectiveness. In each case, the system frequency and active system load were recorded. In all of the scenarios, we assumed that the AGC algorithm runs once every 10 seconds, with minor system load changes occurring every second. We also modeled an under-frequency load shedding (UFLS) scheme similar to real-world deployments, that sheds system load in two stages - one at 59.5 Hz and other at 59.4 Hz, respectively.

Figures 5.22 and 5.23 show the system frequency and load during the scaling and ramp attacks on AGC measurements corresponding to Area 1. In both figures, the initial conditions are such that the AGC is working with actual measurements, keeping system frequency close to 60 Hz. For the scaling attack (Figure 5.22), the attack starts at around 35 s, when the attacker scales P_{tie_act} and f measurements, causing the ACE to constantly push the system generation lower than actual requirement, thereby driving the frequency below 60 Hz.

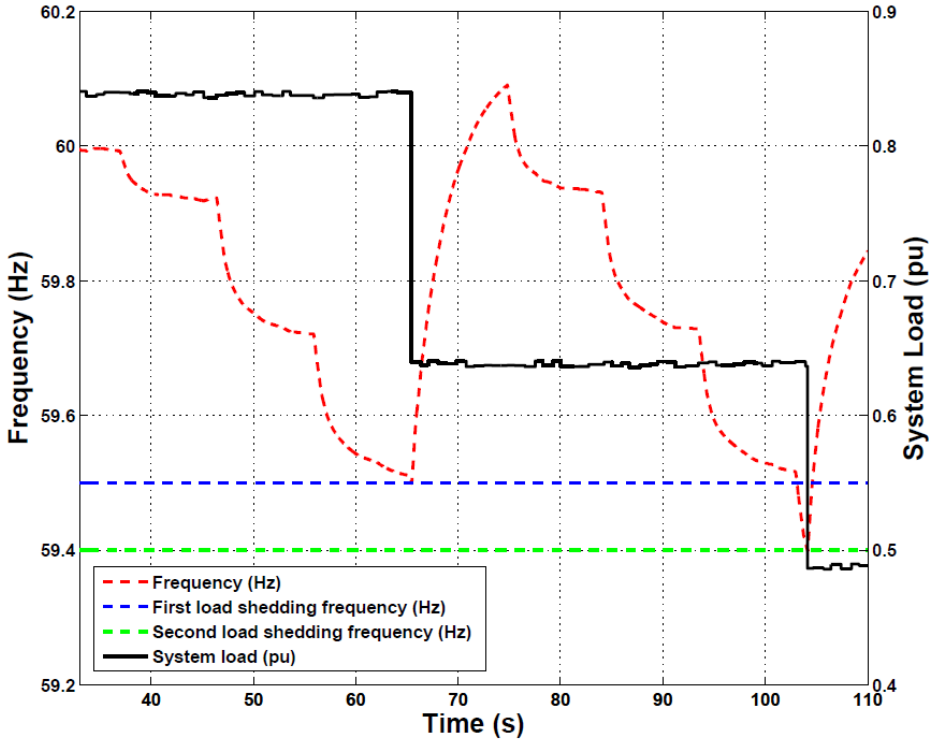

Figure 5.22 System frequency and load during scaling attack without ARC

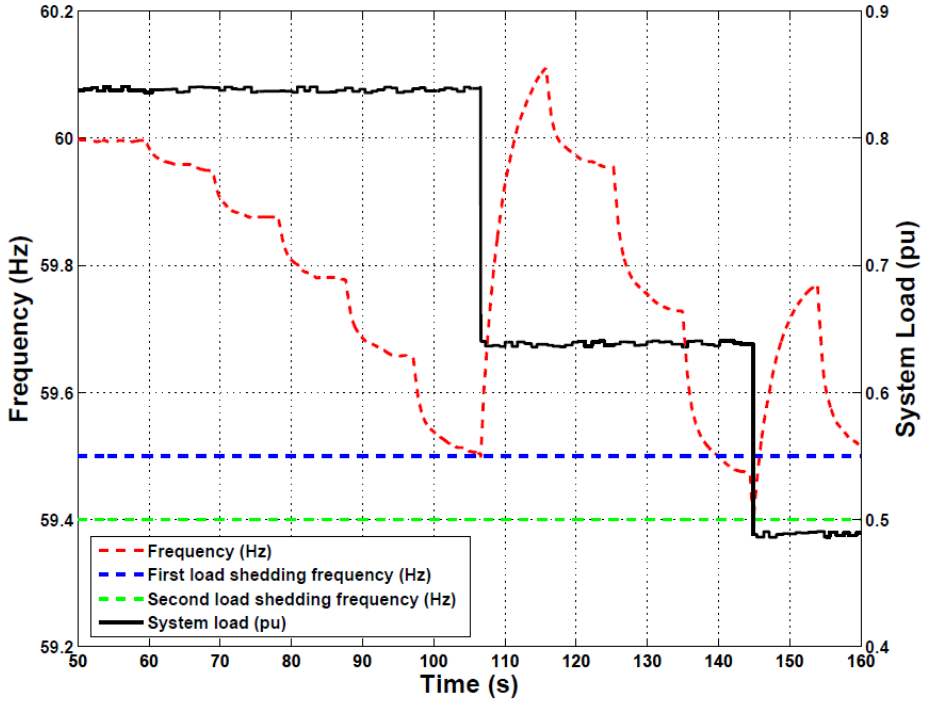

Figure 5.23 System frequency and load during ramp attack without ARC

At around 65 s, the system frequency hits 59.5 Hz to trigger the first stage of UFLS. After a chunk of load is shed, the system frequency improves briefly, but the attacker continues to drive the system frequency away from safe operating conditions. At around 105 s, the system frequency hits 59.4 Hz to trigger the second stage of UFLS to further shed a second chunk of load. At this point, a major portion of the system load is lost (about 40%) causing a significant impact.

The time line of events is similar for the ramp attack (Figure 5.23). At around 60 s the attacker modifies the AGC measurements by adding a time varying ramp to slowly push the system frequency away from 60 Hz. At around 105 s, the first stage of UFLS is activated, and similar to the previous case frequency improves briefly only to reduce further and also hit the second stages of UFLS at around 145 s. One of the key differences between the scaling and ramp attacks is the time it takes for the system frequency to hit UFLS frequency. As expected, the scaling attack affects the measurements instantaneously pushing the frequency down faster than the slowly varying ramp attack.

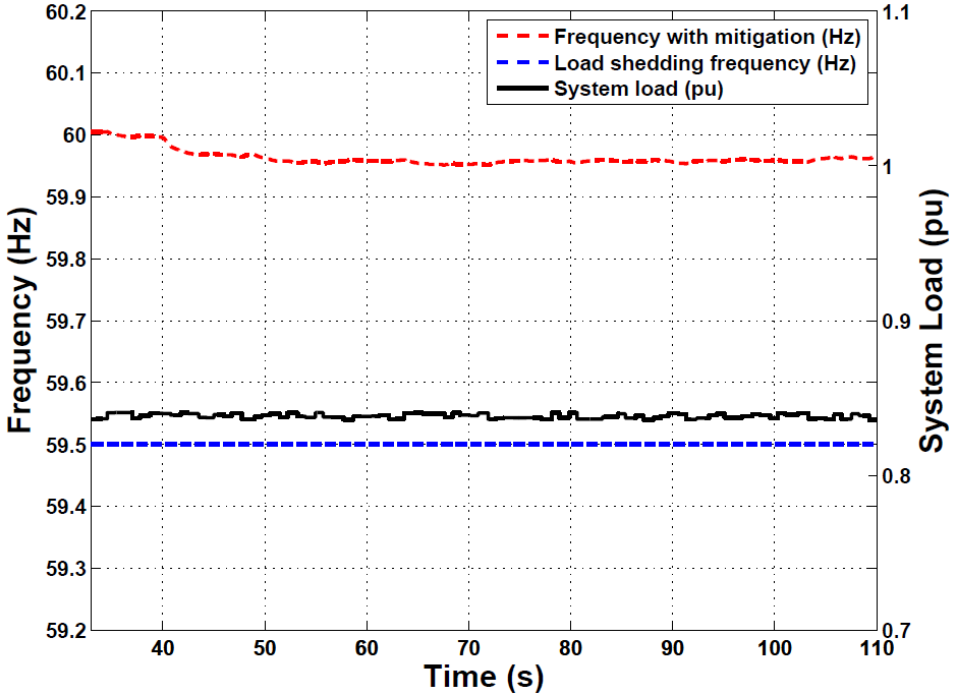

Figure 5.24 System frequency and load during scaling attack with ARC

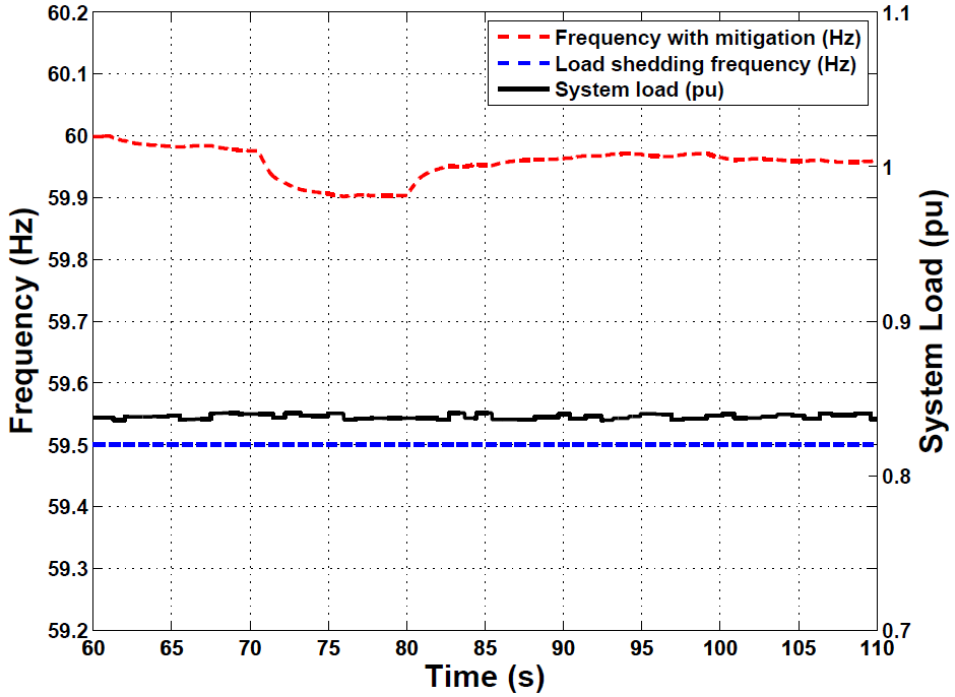

Figure 5.25 System frequency and load during ramp attack with ARC

Figure 5.24 and Figure 5.25 show the same attack scenarios with the ARC algorithm implemented at the control center. For the scaling attack (Figure 5.24), the attack begins at around 40 s. The frequency begins to drop a little initially, however, ARC detects the attack and switches to model-based AGC operation at around 50 s. This ensures that the system frequency does not decline further and performs better than the case without mitigation. Because load forecasts typically are less accurate, we have a non-zero frequency error with model-based AGC operation. For the ramp attack (Figure 5.25), the attack begins at around 61 s and ARC detects the attack at around 80 s, after which it switches to model-based AGC operation.

As expected, the ARC algorithm takes longer to detect a slowly varying ramp attack as its detection is based on a sequence of ACE control signals, as opposed to detection using a single ACE value for the scaling attack. The time that it takes to detect a ramp attack is closely related to the design parameter δ_2, which has been chosen to minimize FP and FN based on our experimental study.

In this section, we validated the ARC algorithm for AGC using the PowerCyber testbed. We implemented a realistic MITM attack on AGC measurements to impact system frequency and cause forced load shedding. We then validated the performance of ARC for scaling and ramp attacks. Our experiments showed that ARC was able to detect and mitigate attack impacts by ensuring that system frequency was maintained within acceptable bounds. Thereby, we were also able to corroborate the results obtained from a simulation-based implementation of the ARC algorithm [83].

5.8.4 Proof-of-Concept Testbed Federation

This section briefly describes the CPS testbed federation that was demonstrated at the Smart America Challenge Expo held in Washington D.C., on June 1, 2014 [84]. As part of this effort, the PowerCyber cyber-physical testbed at Iowa State University (ISU) was successfully federated with University of Southern California's DETER testbed to perform realistic, scalable and high-fidelity attack/defense studies on Wide-Area Protection. Figure 5.26 shows the implementation architecture of the testbed federation between ISU and DETER. The two

testbeds were interconnected using a VPN tunnel to establish seamless network connectivity between control center, substations and field devices that were distributed on the federated testbed.

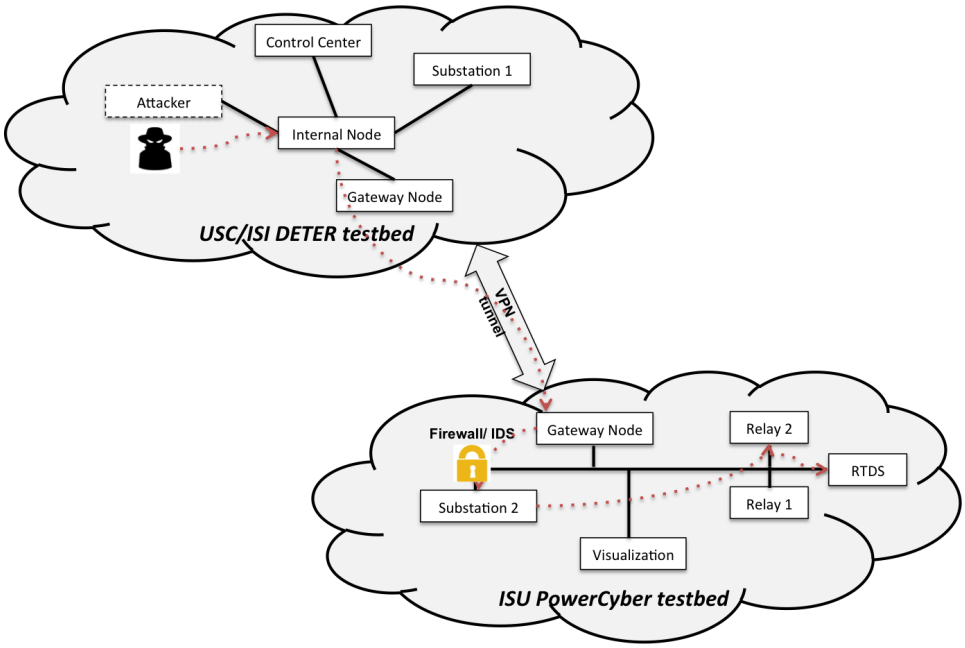

Figure 5.26 Proof-of-concept implementation architecture of CPS testbed federation

The control center and a few substations were implemented inside the DETER testbed. The DETER testbed environment allows the configurability of the topology of the cyber network and therefore, the connectivity between control center and the substations were setup corresponding to realistic configurations. Some of the substations were hosted inside the ISU PowerCyber testbed. Both the substations running inside DETER and the PowerCyber testbed shared the physical relays Relay 1 and Relay 2 located inside the PowerCyber testbed. The gateway nodes ensured that all network traffic was tunneled across the testbeds. The relays were interfaced to the RTDS at PowerCyber through the GOOSE protocol. The control center communications with the substations used the DNP3 protocol. The substation RTUs used the IEC 61850 MMS protocol for communicating with the relays. In the experimental scenarios, the attack originated from inside the DETER testbed and was tunneled into the PowerCyber testbed to target the relays as shown by the dotted arrows in Figure 5.26.

As part of the defense strategy, perimeter defense was employed and therefore each substation network had an Intrusion Detection System (IDS), which filtered malicious network traffic. The visualization node was running an OPC server, which talked to the substations to gather data about the status of the relays and fed it to a visualization engine. The visualization engine overlaid relay status information of various lines and attack/defense dynamically on a map as they occurred. As part of the experimentation, the latencies across the two end points on the VPN tunnel were measured and the use case was chosen appropriately. This work was a proof-of-concept to show the value of CPS security testbed federation. More involved experimentation on this federation architecture was performed to identify average, worst-case latencies and other constraints for federated experimentation [98]. As part of future work, additional use cases that demonstrate the value of testbed federation would be pursued.

5.9 Conclusion

This chapter motivated the need for CPS security testbeds, and briefly described the various testbed design objectives and design tradeoffs for various types of testbeds. Then, the uniqueness of HIL testbeds over non-real-time, simulation-based testbeds was articulated in the context of cyber security use cases for WAMPAC. Following that, a top-down methodology for CPS security testbed design based on specific WAMPAC use cases that included specific testbed requirements and engineering tasks. A three-layered testbed architecture abstraction and its application to create an architecture for WAMPAC specific cyber attack-defense experimentation that addresses targeted research challenges was identified. One of the major contributions that came out of testbed-based experimentation was the identification of a new coordinated attack vector for RAS that involved a combination of data integrity and DoS attacks. The chapter also discussed about testbed federation, looking at research challenges, federation architectures, and WAMPAC specific use cases that could benefit from federation. Finally, the chapter presented three experimental case studies that showed how CPS security testbeds enable realistic attack-defense experimentation on critical WAMPAC applications such as AGC, RAS that could not be performed on ordinary simulation-based environments.

Though the chapter did not describe the education and outreach aspects of testbeds, the case studies that were described were extensively leveraged for educational and outreach activities to promote workforce training and development in the critical area of CPS for the smart grid.

CHAPTER 6. CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

As the electric power grid continually evolves into a smarter, cleaner, reliable and resilient grid, the cyber and physical security of WAMPAC systems, including traditional SCADA and the recent deployments of PMUs, is more important than ever for the reliability and resiliency of the grid. The increasing dependence of WAMPAC on cutting-edge substation automation (hardware and software) and networking technologies has resulted in increased network connectivity. Consequently, it has also increased the potential attack surface. To address this, the need to go beyond traditional IT infrastructure-based security mechanisms to create a multi-layered defense approach that encompasses application layer security as well as infrastructure-based security has been highlighted and prioritized by government agencies such as the DOE, NERC and NIST. Also identified is the strong need to have cyber-physical security testbed environments that support realistic attack and defense experimentation to enable validation and performance evaluation of the novel security mechanisms that are developed.

As part of this dissertation, two major research components were described to address these research needs. The first component, *Attack-resilient State Estimation*, addressed the vulnerability of state estimation to stealthy cyber attacks along with two complementary approaches to mitigate the effect of attacks to enhance its resilience. Specifically, a topology-based attack vector that bypassed bad data detection methods and causes loss of system observability was identified. To mitigate the stealthy attacks on measurements and topology, an offline attack-resilient measurement design methodology was presented. This methodology increased the robustness of state estimators against false data injection, topology-based, and DoS attacks. In addition to the offline mitigation approach, an online attack-resilient anomaly detection

method was described that utilized load forecasts, generation schedules, and synchrophasor data to detect measurement anomalies that were created by stealthy attacks.

The second component, *Testbed-based Experimentation and Performance Evaluation*, addressed the need to architect, develop, and leverage cyber-physical security testbed environments specifically for performing realistic attack-defense experimentation for WAMPAC use cases along with three experimental case studies. As part of this component, an overview of testbed design objectives and design tradeoffs were discussed for different types of testbeds with a focus on how they could support realistic experimentation for WAMPAC use cases. Then, a methodology for CPS security testbed development based on specific WAMPAC use cases was detailed. A three-layered WAMPAC specific testbed architecture to address critical research challenges was presented. In order to address scalability limitations associated with HIL testbeds, a detailed qualitative analysis of testbed federation that covered research challenges, federation architectures, and WAMPAC specific use cases that could benefit from federation was discussed. Finally, three experimental case studies that involved realistic coordinated cyber attacks on critical WAMPAC applications such as AGC, RAS were described in detail. In one of the case studies, a novel coordinated attack vector for RAS was identified that involved a combination of data integrity and DoS attacks, leveraging both spatial and temporal coordination. As part of this contribution, the hypothesis that timing of attack actions also plays a critical role in the attack impact severity was experimentally validated using the PowerCyber testbed.

6.2 Future Work

The theoretical and applied research contributions as part of this dissertation address specific research gaps and milestones (under the roadmap thrust: "Developing new protective measures to reduce risk and managing incidents") that have been identified in the DOE roadmap for Energy Delivery Systems Cybersecurity [12]. As identified in the roadmap, more work needs to be done to address several key topics such as novel methods for risk assessment that capture cyber attack threat and impacts, attack detection and mitigation techniques that leverage cyber and physical properties of the grid without interfering with critical energy delivery functions

of the grid. There are several potential directions that could be pursued to extend the work discussed in this dissertation as part of future work.

6.2.1 Cyber-Physical Moving Target Defense (MTD)-based Approaches for Attack-Resilient State Estimation

In order to further enhance the attack-resilience of the state estimator to stealthy cyber attacks future work that looks at developing cyber-physical MTD-based approaches could be pursued. MTD-based approaches leverage redundancy and randomization to create a dynamic attack surface that increases the difficulty of the attack. One potential approach to apply MTD would be to leverage the redundancy in the measurement set used for SE to select randomized measurements for every execution interval. This variation in the measurement set would make the execution of a stealthy attack very difficult, in addition to the fact that the attacked measurements may be ignored as part of the measurement set. This randomization could be performed based on cyber alerts generated so as to choose the appropriate measurements to randomize.

Similarly, a line of future work that could be explored is to randomize the formulation of state estimator or the bad data detection method-based on cyber layer alerts. It is commonly known that different formulations of state estimators have differences in convergence, stability and robustness.

Another potential CPS MTD-based approach that could be pursued is to develop a strategy to adjust the weights of the measurements used in the estimation process based on cyber layer alerts dynamically. By adjusting the measurement weights appropriately, the impact of certain bad measurements could be minimized. However, this strategy should also take into account various practical issues such as convergence and leverage points to ensure the state estimates are not adversely affected.

6.2.2 Machine Learning Techniques for CPS Model-based Anomaly Detection

The online anomaly detection algorithm that was described as part of the dissertation described a statistical characterization approach that utilized load forecasts and available PMU

data to predict state estimates for comparison. As an extension of this approach, advanced machine learning techniques that fuse cyber layer alerts with physical measurement anomalies to perform cyber-physical model-based anomaly detection techniques for state estimation would be a potential line of future work.

6.2.3 Game-Theoretic Methods for Cyber-Physical Security of WAMPAC

In general, the application of game-theoretic tools for cyber-physical security of WAMPAC would not necessarily help in development of new attack detection or mitigation methods, but would help in performing quantitative risk assessment and operational planning based on attacker behaviors. Depending on the formulation of the strategic game, a game-theoretic approach can help identify the most likely attack scenarios by characterizing the impacts of different types of cyber attacks and also helps to identify mitigation measures, either in terms of security reinforcements or in terms of developing new planning approaches to reduce the impact, based on how the problem is formulated.

A potential line of future work that could be explored would be to apply game-theoretic tools to develop attack-aware operational planning approaches that are capable of handling (N-k) contingencies in the presence of coordinated attacks. Such an approach would result in obtaining *dynamic contingency sets* based on the solutions of the game formulations for a specified attacker behavior.

Another line of research using game-theoretic tools for cyber-physical security of WAMPAC would be to develop a mathematical framework for identifying attacker bounds based on the balance that exists between attack costs and their impact for various attack types on WAMPAC applications.

6.2.4 Cyber Security of PMU-based WAMPAC Applications

With more and more utilities deploying PMUs increasingly in their systems, the cyber security of PMU network infrastructure and the data they carry will become critical. As synchrophasor-based applications are still at nascent stages in terms of practical deployments, a lot of research focuses only on solving existing problems in cyber-physical security of WAMPAC

applications using new PMU data under the assumption that they are secure. Though there are several avenues along this direction such as the application of PMU data to develop anomaly detection methods, PMU-based linear state estimators, PMU placement problems considering multiple objectives such as security, bad data detection, observability, etc., there are several open research problems pertaining to the security of PMU data itself. Future research in this area includes the vulnerability assessment of PMU data and its impact analysis specifically pertaining to emerging WAMPAC applications such as oscillation monitoring, angle monitoring, etc.,

6.2.5 Modeling and Experimentation to Improve Testbed Federation

The proof-of-concept work on CPS testbed federation could be extended in the future to include realistic federated implementation of other WAMPAC specific use cases such as AGC, SE, and even other emerging PMU-based applications such as oscillation monitoring. Most of the federation use cases identified rely on a centralized power system simulation in real-time along with a distributed cyber layer across remote testbeds. In terms of new contributions toward modeling in federation, work could be done to identify novel methods to perform system equivalencing enabling the distributed implementation of power system models across real-time simulators such that highly scalable real-time HIL experiments could be performed without loosing too much on modeling fidelity.

BIBLIOGRAPHY

[1] Department Of Energy Office of Electricity Delivery and Energy Reliability, "The Modern Grid Vision," 2011. [Online]. Available: http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Whitepaper_The%20Modern%20Grid%20Vision_APPROVED_2009_06_18.pdf

[2] Gran N. Ericsson, "Cyber Security and Power System CommunicationEssential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, July 2010.

[3] *Sources: Staged cyber attack reveals vulnerability in power grid*, CNN U.S. Edition, Sep 2007. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

[4] J. D. McDonald, *Power Substations Engineering*, "June" 2003.

[5] *Supervisory control and data acquisition (SCADA) systems, Technical Information Bulletin 04-1*, National Communications System, October 2004. [Online]. Available: http://www.ncs.gov/library/techbulletins/2004/tib

[6] U.S. Government Accountability Office (GAO), "Critical Infrastructure Protection Report," May 2004. [Online]. Available: http://www.gao.gov/new.items/d04321.pdf

[7] S. Baker, S. Waterman, and G. Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, McAfee, 2009.

[8] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security Privacy, IEEE*, vol. 9, no. 3, pp. 49 –51, may-june 2011.

[9] SANS Institute, NERC Electricity - Information Sharing and Analysis Center (E-ISAC), "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," Mar. 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[10] *GAO-04-354: Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems*, U.S. Government Accountability Office (GAO), March 2004.

[11] *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy, Nov. 2009.

[12] *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, Energy Sector Control Systems Working Group, "September" 2011.

[13] Office of Electricity Delivery and Energy Reliability, "ENERGY DELIVERY SYSTEMS CYBERSECURITY," 2011. [Online]. Available: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity

[14] Department Of Energy Office of Electricity Delivery and Energy Reliability, "CYBERSECURITY RISK MANAGEMENT PROCESS (RMP)," 2011. [Online]. Available: http://energy.gov/oe/services/cybersecurity/cybersecurity-risk-management-process-rmp

[15] North American Electricity Reliability Council(NERC), "Criticial Infrastructure Protection (CIP) Reliability Standards," 2009.

[16] National Institute of Standards and Technology(NIST), "NISTIR 7628: Guidelines for smart grid cyber security– Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements," Aug. 2010.

[17] U.S Department Of Homeland Security - Control Systems Security Program), "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

[18] J. Dagle, "North american synchrophasor initiative - an update of progress," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, jan. 2009.

[19] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80–93, Jan 2011.

[20] V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, and A. Apostolov, "Ieee psrc report on global industry experiences with system integrity protection schemes (sips)," *IEEE Transactions on Power Delivery*, vol. 25, no. 4, pp. 2143–2155, Oct 2010.

[21] N. (NASPI), "Phasor Data Applications Table," dec 2009. [Online]. Available: https://www.naspi.org/File.aspx?fileID=537

[22] 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*, vol. 5, no. 4, pp. 481 – 489, 2014, cyber Security. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2090123213001495

[23] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM conference on Computer and communications security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653666

[24] Sridhar, S. and Govindarasu M., "Data integrity attacks and their impacts on SCADA control system," in *Power and Energy Society General Meeting, 2010 IEEE*, july 2010, pp. 1 –6.

[25] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 847–855, 2013.

[26] Sridhar, S. and Govindarasu M., "Data integrity attack and its impacts on voltage control loop in power grid," in *Power and Energy Society General Meeting, 2011 IEEE*, july 2011, pp. 1 –6.

[27] F. Cleveland, "Cyber security issues for advanced metering infrasttructure (ami)," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, july 2008, pp. 1 –5.

[28] S. D'Antonio, L. Coppolino, I. A. Elia, and V. Formicola, "Security issues of a phasor data concentrator for smart grid infrastructure," in *Proceedings of the 13th European Workshop on Dependable Computing*, ser. EWDC '11. New York, NY, USA: ACM, 2011, pp. 3–8. [Online]. Available: http://doi.acm.org/10.1145/1978582.1978584

[29] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, 2010.

[30] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 220 –225.

[31] T. Kim and H. Poor, "Strategic protection against data injection attacks on power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 326 –333, june 2011.

[32] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 226 –231.

[33] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, oct. 2011, pp. 232 –237.

[34] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct 2010, pp. 214–219.

[35] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Decision and Control (CDC), 2010 49th IEEE Conference on*, dec. 2010, pp. 5991 –5998.

[36] G. Hug and J. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1362 –1370, sept. 2012.

[37] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Power and Energy Society General Meeting, 2012 IEEE*, 2012, pp. 1–8.

[38] K. Clements, "The impact of pseudo-measurements on state estimator accuracy," in *Power and Energy Society General Meeting, 2011 IEEE*, 2011, pp. 1–4.

[39] N. D. R. Sarma, V. Veera Raju, and K. S. P. Rao, "Design of telemetering configuration for energy management systems," *Power Systems, IEEE Transactions on*, vol. 9, no. 1, pp. 381–387, 1994.

[40] M. Celik and W.-H. Liu, "An incremental measurement placement algorithm for state estimation," *Power Systems, IEEE Transactions on*, vol. 10, no. 3, pp. 1698–1703, 1995.

[41] M. Baran, J. Zhu, H. Zhu, and K. Garren, "A meter placement method for state estimation," *Power Systems, IEEE Transactions on*, vol. 10, no. 3, pp. 1704–1710, 1995.

[42] F. Magnago and A. Abur, "A unified approach to robust meter placement against loss of measurements and branch outages," *Power Systems, IEEE Transactions on*, vol. 15, no. 3, pp. 945–949, 2000.

[43] B. Gou, "Generalized integer linear programming formulation for optimal pmu placement," *Power Systems, IEEE Transactions on*, vol. 23, no. 3, pp. 1099–1104, 2008.

[44] N. Abbasy and H. Ismail, "A unified approach for the optimal pmu location for power system state estimation," *Power Systems, IEEE Transactions on*, vol. 24, no. 2, pp. 806–813, 2009.

[45] S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *Power Systems, IEEE Transactions on*, vol. 23, no. 3, pp. 1433–1440, 2008.

[46] R. Emami and A. Abur, "Robust measurement design by placing synchronized phasor measurements on network branches," *Power Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 38–43, 2010.

[47] *National SCADA Test Bed: Fact Sheet*, Idaho National Laboratory, 2009.

[48] Michael J. McDonald, Gregory N. Conrad, Travis C. Service, Regis H. Cassidy, *SAND2008-5954: Cyber Effects Analysis Using VCSE, Promoting Control System Reliability*, Sandia National Laboratories, September 2008.

[49] T. Edgar, D. Manz, and T. Carroll, "Towards an experimental testbed facility for cyber-physical security research," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, ser. CSIIRW '11, 2011.

[50] David C. Bergman, Dong Jin, David M. Nicol, Tim Yardley, "The Virtual Power System Testbed and Inter-Testbed Integration," *2nd Workshop on Cyber Security Experimentation and Test*, August 2009.

[51] J. Hong, S.-S. Wu, A. Stefano, A. Fshosha, C.-C. Liu, P. Gladyshev, and M. Govindarasu, "An intrusion and defense testbed in a cyber-power system environment," in *Power and Energy Society General Meeting, 2011 IEEE*, Jul. 2011.

[52] B. Reaves and T. Morris, "An open virtual testbed for industrial control system security research," *International Journal of Information Security*, vol. 11, no. 4, pp. 215–229, 2012.

[53] J. Mirkovic, T. Benzel, T. Faber, R. Braden, J. Wroclawski, and S. Schwab, "The DETER project: Advancing the science of cyber security experimentation and

test (https://www.isi.deterlab.net/index.php3)," in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, 2010, pp. 1–7.

[54] S. Biswas, F. Shariatzadeh, R. Beckstrom, and A. Srivastava, "Real time testing and validation of smart grid devices and algorithms," in *Power and Energy Society General Meeting (PES), 2013 IEEE*, July 2013, pp. 1–5.

[55] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi, "ICT resilience of power control systems: experimental results from the CRUTIAL testbeds," in *Dependable Systems Networks, 2009. DSN '09. IEEE/IFIP International Conference on*, 29 2009-july 2 2009, pp. 554 –559.

[56] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, Jan. 2011, pp. 1 –7.

[57] C. Queiroz, A. Mahmood, and Z. Tari, "Scadasim 2014;a framework for building scada simulations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec 2011.

[58] *NERC Criticial Infrastructure Protection (CIP) Reliability Standards*, North American Electric Reliability Corporation, 2009.

[59] F. Greitzer, A. Moore, D. Cappelli, D. Andrews, L. Carroll, and T. Hull, "Combating the insider cyber threat," *Security Privacy, IEEE*, vol. 6, no. 1, pp. 61 –64, jan.-feb. 2008.

[60] N. Vempati, C. Silva, O. Alsac, and B. Stott, "Topology estimation," in *Power Engineering Society General Meeting, 2005. IEEE*, june 2005, pp. 806 – 810 Vol. 1.

[61] Ali Abur and Antonio Gomez Exposito, *Power System State Estimation: Theory and Implementation*. CRC Press, 2004.

[62] A. Monticelli, *State Estimation In Electric Power Systems: A Generalized Approach*. Kluwer Academic Publishers, 1999.

[63] North American Electric Reliabillity Council(NERC), "TOP-007-0: Reporting System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations." [Online]. Available: http://www.nerc.com/files/TOP-007-0.pdf

[64] ——, "TOP-008-1: Response to Transmission Limit Violations." [Online]. Available: http://www.nerc.com/files/TOP-008-1.pdf

[65] ——, "TOP-007-WECC-1: System Operating Limits (WECC)." [Online]. Available: http://www.nerc.com/files/TOP-007-WECC-1.pdf

[66] G. Peters and J. H. Wilkinson, "The least squares problem and pseudo-inverses," *The Computer Journal*, vol. 13, no. 3, pp. 309–316, 1970. [Online]. Available: http://comjnl.oxfordjournals.org/content/13/3/309.abstract

[67] K. Clements and P. Davis, "Detection and identification of topology errors in electric power systems," *Power Systems, IEEE Transactions on*, vol. 3, no. 4, pp. 1748 –1753, nov 1988.

[68] A. K. Abou-Ardate, "On-line computation of system operating limits with respect to thermal constraints," Master's thesis, Iowa State University, 2006.

[69] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Attack-resilient measurement design methodology for state estimation to increase robustness against cyber attacks," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[70] M. Gol, A. Abur, and F. Galvan, "Metrics for success: Performance metrics for power system state estimators and measurement designs," *Power and Energy Magazine, IEEE*, vol. 10, no. 5, pp. 50–57, 2012.

[71] Ashok, A. and Govindarasu, M. and Ajjarapu, V., "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, To appear.

[72] G. Valverde, S. Chakrabarti, E. Kyriakides, and V. Terzija, "A constrained formulation for hybrid state estimation," *Power Systems, IEEE Transactions on*, vol. 26, no. 3, pp. 1102–1109, Aug 2011.

[73] R. Avila-Rosales, M. Rice, J. Giri, L. Beard, and F. Galvan, "Recent experience with a hybrid scada/pmu on-line state estimator," in *Power Energy Society General Meeting, 2009. PES '09. IEEE*, July 2009, pp. 1–8.

[74] California ISO, "Integration of Renewable Resources: Technical Appendices for California ISO Renewable Integration Studies," Oct 2010. [Online]. Available: http://www.caiso.com/Documents/DraftTechnicalAppendices_RenewableIntegrationStudies-OperationalRequirementsandGenerationFleetCapability.pdf

[75] KEMA, "Metrics for Determining the Impact of Phasor Measurements on Power System State Estimation- Eastern Interconnection Phasor Project," Jan 2006. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=E16B2AA774EE72DA716AA84B180ACED5?doi=10.1.1.134.1493&rep=rep1&type=pdf

[76] Tom Fawcett, "ROC Graphs: Notes and Practical Considerations for Data Mining Researchers," Intelligent Enterprise Technologies Laboratory, HP Labs, Jan 2003. [Online]. Available: http://www.hpl.hp.com/techreports/2003/HPL-2003-4.pdf

[77] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011. [Online]. Available: http://doi.acm.org/10.1145/1952982.1952995

[78] New England ISO, "New England ISO: Markets: 5-minute Data," Apr 2014. [Online]. Available: http://www.iso-ne.com/markets/5min_data/index.html

[79] Electric Reliability Council of Texas, "State Estimator Standards," June 2006. [Online]. Available: http://www.ercot.com/content/meetings/ndswg/keydocs/2006/0620/State_Estimator_Standards_ROS_.doc

[80] "2011 NERC Grid Security Exercise After-Action Report," North American Electric Reliability Corporation (NERC), March 2012. [Online]. Available: http://www.nerc.com/files/NERC_GridEx_AAR_16Mar2012_Final.pdf

[81] "Grid Security Exercise (GridEx II) After-Action Report," North American Electric Reliability Corporation (NERC), March 2014. [Online]. Available: http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf

[82] A. Ashok, A. Hahn, and M. Govindarasu, "A cyber-physical security testbed for smart grid: System architecture and studies," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, ser. CSIIRW, 2011.

[83] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *Smart Grid, IEEE Transactions on*, vol. 5, no. 2, pp. 580–591, March 2014.

[84] Govindarasu, M. and Benzel, T. and Hahn, A., "Smart Energy CPS - CPS Security Testbed Federation for Coordinated Cyber Attack/Defense Experimentation," June 2014. URL: http://smartamerica.org/news/iowa-state-researchers-to-demonstrate-cyber-physical-security-testbed-for-power-grid-at-smartamerica-challenge-expo/.

[85] Terry Benzel, David Manz, David Nicol, and Laura Tinnel, "DEFT Consortium," 2013. [Online]. Available: https://cps-vo.org/sites/default/files/webform/DEFT_Consortium_NSF_whitepaper_11-13.pdf

[86] R. Liu, M. Mohanpurkar, M. Panwar, R. Hovsapian, A. Srivastava, and S. Suryanarayanan, "Geographically distributed real-time digital simulations using linear prediction," *International Journal of Electrical Power & Energy Systems* , vol. 84, pp. 308 – 317, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0142061516308079

[87] V. Jalili-Marandi, F. J. Ayres, C. Dufour, and J. Belanger, "Real-time Electromagnetic and Transient Stability Simulations for Active Distribution Networks," in *International Conference on Power Systems Transients (IPST)*, Jul. 2013.

[88] Q. Huang and V. Vittal, "Application of electromagnetic transient-transient stability hybrid simulation to fidvr study," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 2634–2646, July 2016.

[89] OPAL-RT, "ePHASORsim Real-Time Transient Stability Simulator - The Ultimate Solution for Large-ScalePower System Simulations," 2016. [Online]. Available: http://www.opal-rt.com/en/ephasorsim

[90] *ISERINK platform for Cyber Defense Competitions*, Iowa State University, 2015. URL: http://www.iserink.org/.

[91] Western Electricity Coordinating Council (WECC), "WECC Remedial Action Scheme catalog summary," 2008.

[92] Aditya Ashok, Pengyuan Wang, Manimaran Govindarasu, *Cyber-physical-social system security testbeds for an attack-resilient smart grid*, ser. Energy Engineering. Institution of Engineering and Technology, 2016. [Online]. Available: http://digital-library.theiet.org/content/books/10.1049/pbpo081e_ch16

[93] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a cps security testbed," in *Power Energy Society General Meeting, 2015 IEEE*, July 2015, pp. 1–5.

[94] A. Ashok, S. Sridhar, A. D. McKinnon, P. Wang, and M. Govindarasu, "Testbed-based performance evaluation of attack resilient control for agc," in *2016 Resilience Week (RWS)*, Aug 2016, pp. 125–129.

[95] North American Electric Reliability Council(NERC), "Balancing and Frequency Control," January 2011. [Online]. Available: http://www.nerc.com/docs/oc/rs/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf

[96] Sridhar, S. and Govindarasu, M., "Data integrity attacks and their impacts on SCADA control system," in *Power and Energy Society General Meeting, 2010 IEEE*, july 2010, pp. 1 –6.

[97] "Scapy - An interactive packet manipulation program," 2015. [Online]. Available: http://www.secdev.org/projects/scapy/

[98] Anirudh Pullela, "CPS security testbed federation: architectural design, implementation and evaluation - Masters Thesis - Iowa State University," 2015.

APPENDIX PUBLICATIONS

Journals

- Adam Hahn, **Aditya Ashok**, Siddharth Sridhar, Manimaran Govindarasu, *"Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid*, IEEE Transactions on Smart Grid, Vol. 4, No. 2, June 2013.

- **Aditya Ashok**, Adam Hahn, Manimaran Govindarasu, *"Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment"*, Journal of Advanced Research, Vol. 5, Issue 4, July 2014.

- **Aditya Ashok**, Manimaran Govindarasu, Venkataramana Ajjarapu, *"Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation"*, in IEEE Transactions on Smart Grid , vol.PP, no.99, pp.1-1 (Early Access).

Conferences

- **Aditya Ashok**, Adam Hahn, and Manimaran Govindarasu, *"A Cyber Physical Security Testbed For Smart Grid: System Architecture And Studies"*, Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW 11), Oak Ridge National Laboratory, Tennessee, 2011.

- **Aditya Ashok**, Manimaran Govindarasu, *"Cyber attacks on power system state estimation through topology errors"*, Proceedings of IEE PES General Meeting 2012, San Diego, CA.

- **Aditya Ashok**, Pengyuan Wang, Matthew Brown and Manimaran Govindarasu, *"Experimental evaluation of cyber attacks on Automatic Generation Control using a CPS*

Security Testbed," 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.

- Pengyuan Wang, **Aditya Ashok** and Manimaran Govindarasu, *"Cyber-physical risk assessment for smart grid System Protection Scheme,"* 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015.

- **Aditya Ashok** and Manimaran Govindarasu, "Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach," 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, 2015.

- **Aditya Ashok**, Manimaran Govindarasu, and Venkataramana Ajjarapu, *"Attack-resilient measurement design methodology for State Estimation to increase robustness against cyber attacks,"* 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 2016.

- **Aditya Ashok**, Siddharth Sridhar, David McKinnon, Pengyuan Wang, and Manimaran Govindarasu, *"Testbed-based performance evaluation of attack resilient control for agc,* in 2016 Resilience Week (RWS), Aug 2016.

Book Chapter

- **Aditya Ashok**, Pengyuan Wang, Manimaran Govindarasu, *"Cyber-physical-social system security testbeds for an attack-resilient smart grid"*, In edited book titled: *'Cyber-Physical-Social Systems and Constructs in Electric Power Engineering'*, edited by: Siddharth Suryanarayanan, Robin Roche and Timothy M. Hansen, ser. Energy Engineering. Institution of Engineering and Technology, 2016.