Experimental Evaluation of Cyber Attacks on Automatic Generation Control using a CPS Security Testbed

Aditya Ashok, Pengyuan Wang, Matthew Brown, Manimaran Govindarasu
Department of Electrical and Computer Engineering
Iowa State University
Ames, IA 50011, USA.
Email: aashok, pywang, mrbrown, gmani@iastate.edu

Abstract—Cyber-Physical Security Testbeds serve as valuable experimental platforms to implement and evaluate realistic, complex cyber attack-defense experiments. Testbeds, unlike traditional simulation platforms, capture communication, control and physical system characteristics and their interdependencies adequately in a unified environment. In this paper, we show how the PowerCyber CPS testbed at Iowa State was used to implement and evaluate cyber attacks on one of the fundamental Wide-Area Control applications, namely, the Automatic Generation Control (AGC). We provide a brief overview of the implementation of the experimental setup on the testbed. We then present a case study using the IEEE 9 bus system to evaluate the impacts of cyber attacks on AGC. Specifically, we analyzed the impacts of measurement based attacks that manipulated the tie-line and frequency measurements, and control based attacks that manipulated the ACE values sent to generators. We found that these attacks could potentially create under frequency conditions and could cause unnecessary load shedding. As part of future work, we plan to extend this work and utilize the experimental setup to implement other sophisticated, stealthy attack vectors and also develop attack-resilient algorithms to detect and mitigate such attacks.

I. INTRODUCTION

As the electric power grid evolves into a Smart Grid to provide a reliable, secure and resilient electricity transmission and distribution system, the dependence on cutting edge automation and networking technologies has increased tremendously. The advent of high accuracy, time synchronized, high data-rate synchrophasor measurements and other modern substation automation systems over the grid, which are deployed to monitor, control and protect the power grid, has resulted in increased network connectivity and consequently, increased the potential attack surface. Several government reports in the recent past acknowledge the fact that the Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control the power grid are constant targets of sophisticated cyber attacks every day [1], [2]. They also identify the need to develop intelligent countermeasures to secure SCADA infrastructure elements and the fundamental applications they provide through a layered defense approach [3]. It is critical to develop attack-resilient algorithms for the critical applications that look beyond traditional information and infrastructure security by leveraging and correlating cyber and physical system information to detect measurement or control manipulations, which could otherwise go undetected.

Cyber-Physical Security Testbeds address the need of providing realistic test environments to perform complex cyber attack-defense experiments by providing a hybrid combination of simulated, emulated and real cyber-physical components. Testbeds, unlike traditional simulation platforms, capture communication, control and physical system characteristics and their interdependencies adequately in a unified environment. Testbed based research spans a broad range of topics from vulnerability assessment, impact analysis to development of counter-measures, etc. [4].

The main objective of this paper is to show a case study of how cyber-physical security testbeds can be leveraged to implement and evaluate various types of cyber attacks on WAMPAC applications like the AGC. The remainder of the paper is organized as follows. Section 2 identifies relevant literature about similar CPS testbeds. Section 3 discusses about the different types of cyber attacks on AGC. Section 4 provides an overview of the implementation of the experimental setup that was used to evaluate cyber attacks on AGC. Section 5 provides a detailed case study using the IEEE 9 bus system to show the impacts of different attack scenarios on AGC. Section 6 provides conclusions and directions for future work.
II. RELATED WORK

There has been a lot of recent work in the development of security testbeds to perform a variety of research and experimental validation pertaining to power grid cyber security. One of the foundational efforts was the National SCADA Testbed (NSTB), which is a collaborative project across multiple national labs where actual power system and cyber system components were used to perform vulnerability assessments and impact analysis studies [7]. Sandia National Laboratory has the Virtual Control System Environment (VCSE) testbed that integrates a combination of simulated, emulated and physical system components to realize a cyber-physical testbed [8]. The University of Illinois hosts the Virtual Power System Testbed (VPST) which also consists of a mix of simulated, emulated and physical components to perform cyber security research that includes vulnerability assessments, protocol testing and research validation [9]. The University College, Dublin also consists of a SCADA testbed which is used to perform experiments on intrusion detection and anomaly detection related to power grid cyber security [10]. Mississippi State University consists of a SCADA security testbed, which is used to perform intrusion detection and security testing of phasor measurement units and data concentrators [11].

The PowerCyber testbed at Iowa State University is a similar testbed compared to the other testbeds mentioned above [6]. The testbed consists of a hybrid mix of industry grade SCADA hardware and software, emulators for wide-area network routing and real-time power system simulators, thereby providing high-fidelity, hardware-in-the-loop, cyber-physical testbed environment for cyber security research and experimental validation studies.

The PowerCyber testbed has been leveraged to perform vulnerability assessment of SCADA devices, and communication protocols, impact analysis of coordinated attack scenarios and also to validate existing research that develops various application specific countermeasures. Recently, the PowerCyber testbed was linked with the DETER testbed at the University of Southern California to demonstrate a federated, coordinated cyber attack/defense experiment at the Smart America Challenge in Washington, D.C. [12]. In this paper, we describe how the PowerCyber testbed has been used to implement and evaluate various types of cyber attack scenarios on the AGC.

III. CYBER ATTACKS ON AGC

The previous section briefly described the research efforts that have been carried out using other similar CPS security testbeds. Also, the PowerCyber CPS security testbed was introduced. In this section, we provide a quick overview of the AGC algorithm, and then discuss how different types of cyber attacks impact the AGC, and consequently, the power system frequency and load.

The Automatic Generation Control (AGC) algorithm is the only wide-area control application that is completely automated, i.e. no operator in the loop to make control decisions. The AGC algorithm relies on wide-area measurement data, namely, the tie-line power flow measurements between the balancing areas, and frequency measurements to compute the Area Control Error (ACE) values, which are generator corrections to ensure generation-load balance and economic operation. The AGC algorithm runs every 2-4 seconds typically at each balancing area (BA), where ACE corrections are computed for each area generators on AGC. The ACE is calculated based on two terms, one depending on the deviation of actual tie-line power flows \( P_{act} \) and scheduled tie-line power flows \( P_{sch} \) between adjacent areas, the second one is based on the deviation of the overall system frequency from the nominal frequency (60 Hz), \( \beta \) is the frequency bias factor (MW/Hz), which varies for each balancing area and represents its obligation to support overall grid frequency.

![Fig. 1. Overview of AGC algorithm](image)

Figure 1 shows how the AGC algorithm depends on wide-area network for receiving the measurements and also sending the control commands back to the generators. Therefore, it is vulnerable to data manipulation either in the measurement or the control direction. ‘T’ and ‘F’ represent the tie-line flow and frequency measurements that are sent to the control center of each BA, where the AGC algorithm computes the ACE values for each generator taking part in AGC. It is to be noted that in each area some generators may not take part in AGC and may operate with a fixed loading depending on schedules.

Conceptually, the AGC algorithm can be impacted by attacks on measurements or control data. Measurement based attacks involve a modification of the tie-line and frequency measurements causing an incorrect computation of the ACE values for each area generators. Sridhar et al. show how such an attack can cause impacts on the power grid frequency and affect generation load balance in [5]. Further, the paper also identifies how a stealthy attacker can manipulate the tie-line measurements and frequency measurements consistently based on some knowledge about the underlying power system. In [13], the authors extend upon their earlier work to analyze the impact of such attacks in more detail and developed a model-based anomaly detection algorithm along with attack-resilient AGC algorithm.

Control attacks are attacks where the attacker manipulates...
the ACE corrections that are sent out to each generator in the BA. In this type of attack, the attacker tries to steer the system’s generation towards a certain operating condition, for example, creating constant generation ramp down eventually leading to an under frequency load shedding condition. The impact of such an attack can be quantified as lost load or in some cases as uneconomic generation dispatch, if the attacker changes individual generator set-points to control how each generator in a BA ramps up/down.

IV. EXPERIMENT IMPLEMENTATION ON THE POWERCYBER TESTBED

Figure 2 shows how the experimental setup has been implemented on the PowerCyber testbed. The power system model was configured to run on the RTDS, and the tie-line and frequency measurements were configured to be transmitted from the RTDS to the control center through the DNP3 protocol, similar to real-world implementations. At the control center, the tie-line power flow and frequency measurements are periodically polled from the outstations (RTDS) or the RTU’s and then the AGC algorithm is periodically triggered to compute the ACE values for the generators in the model. Once the values are computed, these are fed back to the outstations, in our case the RTDS again through the same DNP3 protocol. Based on the ACE values, the generators ramp up/down for the load changes in the power system model.

The attack vector that has been implemented is a classic man-in-the-middle (MITM) attack, where the attacker sits in between the control center and the substations, which is achieved through ARP poisoning. We implemented the MITM through the use of Scapy tool [14], which is an interactive packet manipulation program written in python and has several libraries to perform forging or decoding of packets of several network protocols and retransmitting them. Using this tool, we implemented both the control attacks (orange lightning bolt) and measurement attacks (red lightning bolt), where either the ACE values or the tie-line and frequency measurements were manipulated to demonstrate different types of attacks.

V. CASE STUDY USING IEEE 9 BUS POWER SYSTEM

In the previous section, we described how the experimental setup had been implemented to perform different attacks. In this section, we present a case study using the IEEE 9 bus power system to analyze the impacts of both measurement and control attacks on the AGC algorithm.

Figure 3 shows the IEEE 9-bus model split into three BA’s for the purpose of AGC implementation. Each area contains one generator and one regional load. The scheduled tie-line flows are set to the initial power flow distribution values. Out of the three BA’s, we show all the attack scenarios with AGC actions and load changes associated with only one (Area 1). Similar to real-world implementations, if the AGC fails to bring system frequency back to the normal level, we have implemented Under Frequency Load Shedding (UFLS) scheme and generator low frequency protection according to the frequency drop. When frequency goes below 59.8Hz, 20MW out of the total load will be shed as the first block in UFLS scheme. When it is below 59.6Hz, another 10MW will be shed as part of second block in UFLS scheme implemented.

A. Attack scenarios

We have implemented two attack strategies to analyze the performance of AGC under different attacks.

- Measurement attacks: This attack targets the tie-line flow and frequency measurements, i.e. measurements PL45, PL69 and the system frequency being sent to the control center. In this paper, we show a scenario where the attacker modifies the measurements by adding a random offset, though other complex attacks can also be easily implemented.

- Control attacks: This attack targets the ACE value after it’s sent out from AGC algorithm and before it arrives at the control center. In this paper, we show a scenario where the attacker modifies the sign of the ACE value leading to ramping up for load decrease and vice-versa.

B. Experimental results

Figure 4 and Figure 5 show the load profile in BA 1, and the corresponding frequency profile with only the governor control (no AGC) and with the AGC algorithm respectively. The top subplot shows the load profile and it keeps changing with time. We simulated the load profile in Area 1 with 4
different levels which are 40, 60, 90 and 110 MW. In our case study, we executed the AGC algorithm once every 4 seconds.

From Figure 4, we can see clearly that following a load change the system frequency either increases or decreases and does not return to the nominal frequency (60 Hz). It can be seen clearly that when the load level in Area 1 is at 90 MW, the frequency is at 60 Hz, as this is the base point operating condition and for any other load level the frequency is either above (load < 90 MW) or below (load > 90 MW).

The bottom subplot in Figure 5 shows the system frequency response to the load changes with the AGC algorithm implemented in Area 1. In this subplot, we can see that the system frequency tries to get back to the nominal value after load change. If there is no load change for a sufficiently long time, we can clearly see that the system frequency is at nominal frequency due to AGC.

Control attacks: Figure 6 shows the scenario where control commands are attacked, i.e. the ACE value going to the generator is manipulated by the attacker. In this case, the attack sends ramping commands to the generator in the opposite direction when compared to actual ACE values, i.e. ramp down for ramp up and vice versa. The top subplot shows the total load in Area 1, the middle subplot shows the frequency and the bottom subplot shows the generator output in BA1. We have shown the important events in the plots through the numbered red dots. Dot 0 indicates the normal load change from 90 MW to 110 MW, which is picked up by Area 1 generator.

As the AGC algorithm computes the ACE values for this load change, the normal control action would have been to ramp up the generation and improve the frequency. Dot 1 indicates the start of the attack, where in we can see the change in generator power and system frequency immediately. With the control attack described above (flipping the ACE signal), the frequency continues to decrease. When it goes below 59.8 Hz, 20 MW load is shed (Dot 2). As time progresses, the frequency worsens and another 10 MW load will be dropped when frequency goes to 59.6 Hz (Dot 3). The system frequency stays slightly above 59.6 Hz after the load drop and stays there as the attacker then sends zero ACE values to the generators until the end of the attack (Dot 4). After the attack ends, the real ACE values steer the frequency and tie-line flow back to nominal values immediately.

Measurement attacks: Figure 7 shows the scenario where the tie-line flow and frequency measurements are manipulated
by the attacker. In this case, the ACE values are determined by the based on the incorrect measurements which contain a constant offset. Similar to the previous case, the key events are indicated by the red dots. In this scenario, the load level increases from 90 MW to 110 MW (Dot 0). After the attack starts (Dot 1), instead of forwarding the real measurements corresponding to 110 MW load level, the fake measurements are sent to AGC which are actually replayed measurements when load level is 40 MW.

After AGC algorithm is run, a positive ACE value will be sent to ramp down the generator so that the frequency goes even lower. This can be clearly seen in the bottom subplot, where the output of generator 1 falls steeply due to the ACE values computed for tie-line flow and frequency measurements corresponding to a load level of 40 MW. Therefore, abruptly the frequency drops and eventually 20MW load will be shed after frequency is below 59.8 Hz (Dot 2). After the load shedding, the attacker denies the measurements from reaching the control center. Consequently, the frequency stays slightly above 59.8 Hz following the load drop until the attack ends (Dot 3). Once the attack is over the system frequency will recover after next cycle of AGC control.

![Fig. 7. Generation, Load, Frequency during measurement attacks](image)

VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we showed how cyber-physical security testbeds can be leveraged to implement realistic cyber attacks on critical WAMPAC applications like the AGC and analyze the impacts of such attacks. Specifically, we looked at related work done by other similar testbeds, and briefly introduced the PowerCyber testbed. We described two attack vectors and how these cyber attacks impact the AGC algorithm and consequently, the power system frequency and load. We also explained the implementation of the experimental setup on the PowerCyber testbed. We performed a case study of two types of cyber attacks, namely, measurement and control attacks and showed their impacts on system frequency and load.

Though the attack scenarios described in this paper are relatively simplistic, the main intent of this paper was to describe the implementation architecture of the experimental setup and show proof-of-concept attack scenarios as an evaluation. We plan to extend the basic attack scenarios described in this paper to develop more complex attack scenarios. We would also work on implementing and evaluating attack-resilient control algorithms on the testbed that can detect and mitigate complex, stealthy attack vectors such as the ones described in [13].

REFERENCES


