Attack Detection and Mitigation for AGC

Pooja A Kulkarni[1], Harshal A Karande[2]

Department Of Computer Engineering, Siddhant College of Engineering, Savitribai Phule University Pune, India

Abstract: ***Cyber systems play a critical role in improving the efficiency and reliability of power system operation and ensuring the system remains within safe operating margins. An adversary can inflict severe damage to the underlying physical system by compromising the control and monitoring applications facilitated by the cyber layer. There is a growing need for cyber-attack-resilient control techniques that look beyond traditional cyber defense mechanisms to detect highly skilled attacks. In this paper, we make the following contributions. We first demonstrate the impact of data integrity attacks on Automatic Generation Control (AGC) on power system frequency and electricity market operation. We propose a general framework to the application of attack resilient control to power systems as a composition of smart attack detection and mitigation. Finally, we develop a model-based anomaly detection and attack mitigation algorithm for AGC. We evaluate the detection capability of the proposed anomaly detection algorithm through simulation studies. Our results show that the algorithm is capable of detecting scaling and ramp attacks with low false positive and negative rates. The proposed model-based mitigation algorithm is also efficient in maintaining system frequency within acceptable limits during the attack period.***

Keywords: Anomaly detection, automatic generation control, intrusion detection systems, kernel density estimation, supervisory control and data acquisition.

1. Introduction

The scope of cyber attacks discovered in *Industrial Control Systems* (ICS) has revealed the level of sophistication of attackers. Firstly, recent cases of attacks (e.g., Stuxnet) have revealed that these attacks have been specifically written for ICS . Secondly, the attacks target specific critical control applications within the control system environment. This shows that sophisticated attackers have thorough knowledge of not only the control and automation computer systems and their vulnerabilities, but they also possess an understanding of the dynamics of the physical system to ensure maximum impact.

Intrusion Detection Systems (IDS) that classify data packets as true or anomalies are popularly used in computer systems to ascertain data integrity. The implications of a poor IDS in the IT environment might not be very serious. However, in the SCADA environment where false negatives are unacceptable and a low false positive rate is desired, poor IDS could cause serious problems to the dependent physical process. IDS solutions catering specifically to SCADA systems are still in early days of development. Intrusion detection systems are traditionally classified into *signature-based detection* and *anomaly-based detection*. Signature-based IDS look for known patterns of malicious activity. The database of the IDS is constantly updated with new attack signatures as and when they are discovered. Anomaly-based IDS, however, do not look to identify the actual sequence of intrusion, but look for deviations in the observed data. These IDS usually learn the normal behavior of the system based on statistical profiling. During real-time operation, the observations are compared to the learnt model and any deviation is marked as an anomaly. Most IDS in the IT domain are signature-based as there is an abundance of signatures available for this domain. However, in SCADA systems, the protocols, networks and architectures are unique to the environment. A limited signature database could make the IDS blind to certain attacks thus making it ineffective. The Automatic Generation Control (AGC) is a wide-area frequency control application that receives power flow and frequency measurements from remote sensors. It ensures system frequency remains within acceptable bounds and power ex-change between adjacent control areas is limited to scheduled value. This paper explores the potential impact of smart attacks on AGC. We also present an attack resilient control framework that employs an anomaly-based IDS and mitigation to maintain system stability during the attack period.

2. Literature Survey

This section reviews some of the related work followed by discussing their connections and differences with the proposed approach.

S. Sridhar and G. Manimara’8n introduced the impact of data integrity attacks directed at the AGC on operating frequency stability.

C-W. Ten and C-C. Liu discuss the impact of cyber attack on a power system in terms of load loss and the impact of cyber attacks on the total generation in a system through a graph based model.

V. Chandona , A. Banegree and V. Kumar have consolidated a classification of anomaly detection techniques and grouped this research efforts appropriately.

3. Control System Attack Model

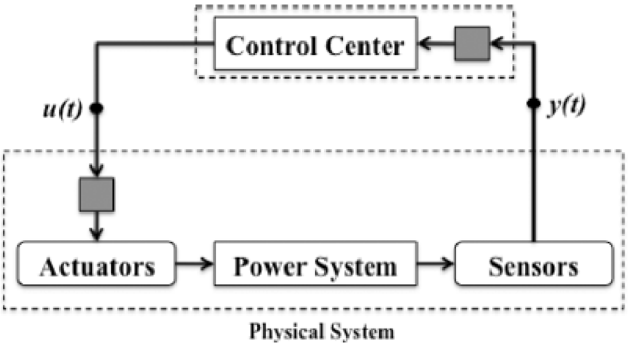

Figure 1: Control System Model

In automated control systems (Fig. 1), the control center accepts measurements y(t) as input from field devices and processes them to obtain the output control signal u(t). A smart attacker could manipulate measurements such that any operational decision made based on these measurements could trigger control actions that are unwarranted for the true syste'8m state. This could in turn cause instabilities in the underlying physical system or force the system to operate at uneconomical operating conditions due to non-optimal control actions. The need is for attack resilient control systems that are able to detect the presence of malicious data.

Following attacks on power system stability and electricity market operation represents the control system model.

1. Scaling Attack:

A scaling attack involves modifying true measurements to higher or lower values depending on the scaling attack parameter λs.

$$y^*(t) = \begin{cases} y(t) & \text{for t} \notin \tau_a \\ (1+\lambda_s) * y(t) & \text{for t} \in \tau_a. \end{cases}$$

2. Ramp Attack:

Ramp attacks involve gradual modification of true measurements by the addition of λr·t, a ramp function that gradually increases/decreases with time

$$y^*(t) = \begin{cases} y(t) & \text{for t} \notin \tau_a \\ y(t) + \lambda_r \cdot t & \text{for t} \in \tau_a. \end{cases}$$

3. Pulse Attack

As opposed to a scaling attack, where measurements are modified to higher/lower values during the entire duration of the attack, this type of attack involves modifying measurements through temporally-spaced short pulses with attack parameter λp .

4. Random Attack

This attack involves the addition of positive values returned by a uniform random function to the true measurements. The upper (a) and lower (b) bounds for selection are provided to the function as an input

$$y^*(t) = \begin{cases} y(t) & \text{for t} \notin \tau_a \\ y(t) + \text{rand}(a, b) & \text{for t} \in \tau_a. \end{cases}$$

.

4. Attack Resilient Control for Power Systems

The notion of attack resilient control for ICS was first presented. With reference to the cyber-attacks context, we define attack resilient control as a combination of *smart attack detection* and *mitigation*. Smart attack detection, for example, could be implemented through domain-specific anomaly detection algorithms that verify the integrity of received measurements based on simulated measurements obtained from equations that govern the functioning of the underlying physical system. Smart mitigation techniques should have the ability to function using forecasts when measurements cannot be trusted.

A. Anomaly Detection Engine

• Step 1: Density Estimation

Before every hour of operation, the anomaly detection engine receives the load forecast for the next hour. Based on this information and the generation schedule, an "ACE forecast" for the next hour of operation is made. The forecasted ACE(ACE_F) values are then fed into a *Kernel Density Estimator* module. The density estimator constructs a probability density $f(ACE_F)$ .The probability of a particular range of ACE_F values is obtained by integrating $f(ACE_F)$ between the range. The probability density helps identify the range of ACE values that are most probable during the next hour of operation.

• Step 2: Anomaly Detection

A bound δ_1 that corresponds to the probability of a range of ACE values, that is the area under the density graph, is specified to classify anomalies from true values. This is one of the tuning parameters of the anomaly detection engine. If δ_1 = 90% the anomaly detection algorithm identifies the range of ACE_F values,[$ACE_{F\ min}$, $ACE_{F\ max}$] that has a probability of 0.9. The range is calculated from the following equation.

$$\delta_1 = \int_{\mathrm{ACE}_{F_{\min}}}^{\mathrm{ACE}_{F_{\max}}} f(\mathrm{ACE}_F)$$

```
Algorithm: [$ACE_{F_{min}}$, $ACE_{F_{max}}$] Identifier
Input: $f(ACE_F)$, $\delta_1$
Output: [$ACE_{F_{min}}$, $ACE_{F_{max}}$]
begin
    i = j = index (max $f(ACE_F)$)
    Area = A(i, j)
    while Area < $\delta_1$ do
        if A(i-1, j) > A(i, j+1) then
            i = i-1
        else
            j = j+1
        end
        Area = A(i,j)
    end
end
```

B. Model Base Attack Mitigation

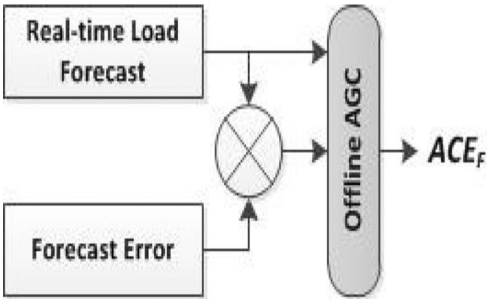

Figure 2: Generation of ACE_F

In scenarios where the meters or communication channels to the control center are compromised, the anomaly detection algorithm will be effective in identifying bad data. Under such circumstances, measurements from field sensors can no longer be trusted. The control center will be "flying blind" while trying to match the load and generation. The need is to make use of a technique that makes an educated guess based on system knowledge and appropriately issues ACE commands to generators without need for measurements. Real-time load forecasts are calculated using techniques such as regression models, neural networks and statistical learning algorithms. These approaches take into account variables that include weather forecasts and time factors (time of the day, year, etc.) to arrive at a load forecast.

5. False Positive And False Negative Analysis

1. False positive analysis

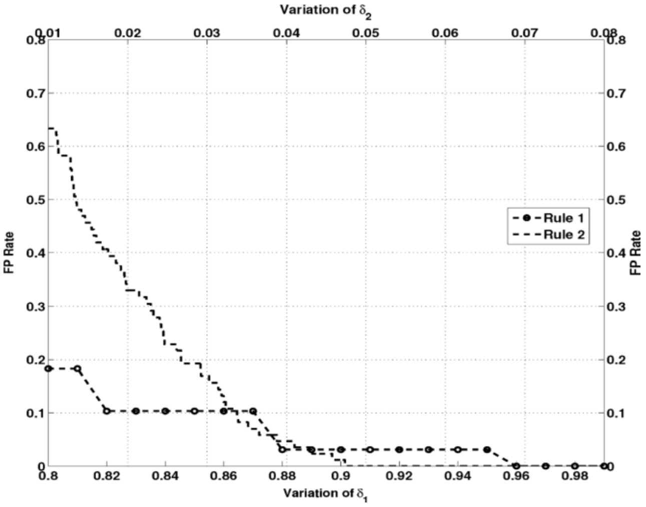

Figure 3: False Positive Analysis

Fig.3 presents the variation of false negative rate for different values of δ_1 and δ_2 . As the value of δ_1 increases from 0.8 to 0.99, the false positive rate decreases. This is because, at lower values of δ_1, even true ACE values are also identified as anomalies as they lie outside the, [$ACE_{F\ min,}$ $ACE_{F\ max}$] range. The FP rate beyond δ1=0.92 is minimum at zero. As in the case of δ_1, the FP rate decreases with as is varied between 0.01 and 0.08. The FP rate is significantly high in the region δ_2 <0.03. As the bound δ_2 is strict at this point, the condition Ψ> δ_2 is satisfied even for true measurements. The FP rate is zero in the region δ_2 >0.049.

1. False Negative Analysis

Fig. 4 presents the variation of false negative rate for different values of δ_1 and δ_2 . At a value of δ1=0.8 , the FN rate is non-zero at 0.14. This is because, even with a narrow [$ACE_{F\ min,}$ $ACE_{F\ max}$] band, some measurements anomalous introduced by the ramp attack template escape detection. As the value of δ_1 is increased from 0.8 to 0.99, the band [$ACE_{F\ min,}$ $ACE_{F\ max}$] widens. With this, more anomalous measurements introduced by the ramp attack template escape detection. This can be observed with the spike in FN rate after δ1=0.85. Scaling attack measurements are detected for all values of δ1.

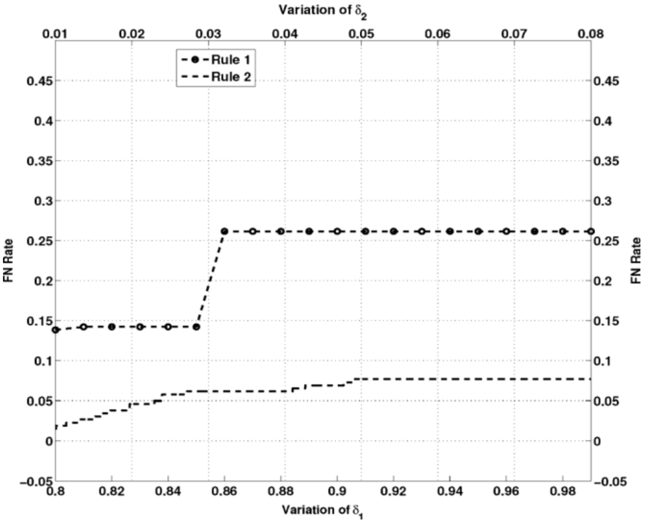

Figure 4: False Negative Analysis

6. Conclusion

In this paper, we showed the impacts of data integrity attacks on AGC operation. It was observed that scaling, ramp, pulse and random attacks severely affected power system stability and market operation. We proposed the notion of attack resilient control as a combination of smart attack detection and mitigation. Results from simulation studies have shown that the algorithm is efficient in mitigating attacks and maintaining the system within safe operating bounds. Our future work includes developing mitigation strategies for attacks that impact electricity market operation through AGC and coordinated cyber attacks on power system control.

References

[1] Siddharth Sridhar, Manimaran Govindarasu," Model-Based Attack Detection and Mitigation for Automatic Generation Control", 2, MARCH 2014.

[2] S. Sridhar and G.Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in Proc. IEEE Power Eng. Soc. General Meeting, Jul. 2011, pp. 1–6.

[3] C.-W. Ten, G.Manimaran, and C.-C. Liu, "Vulnerability assessment of cyber security for SCADA systems using attack trees," in Proc. IEEE Power Eng. Soc. General Meeting, Jul. 2007, pp. 1–8.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," Proc. ACM Comput. Surv., vol. 41, pp. 15:1–15:58, Jul. 2009.

[5] Density Estimation for Statistics and Data Analysis, School of Mathematics. London, U.K.: Chapman & Hall, 1986

Author Profile

Miss Pooja Kulkarni received the B.Tech. degree in Computer Science and Engineering from Shivaji University, Kolhapur. She is currently pursuing M.E. in Computer Engineering from Siddhant College Of Engineering, Pune.

Mr. Harshal A. Karande received the B.Tech. degree in Computer Science and Engineering from Shivaji University, Kolhapur. He is currently pursuing M.E. in Computer Engineering from Siddhant College Of Engineering, Pune.