Model-Based Attack Detection and Mitigation for Automatic Generation Control

Article *in* IEEE Transactions on Smart Grid · March 2014

DOI: 10.1109/TSG.2014.2298195

2 authors:

Siddharth Sridhar
Battelle Memorial Institute
21 PUBLICATIONS **1,921** CITATIONS
SEE PROFILE

Manimaran Govindarasu
Iowa State University
268 PUBLICATIONS **7,455** CITATIONS
SEE PROFILE

Model-Based Attack Detection and Mitigation for Automatic Generation Control

Siddharth Sridhar, *Student Member, IEEE*, and Manimaran Govindarasu, *Senior Member, IEEE*

***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. Protection of critical assets from electronic threats has traditionally been done through conventional cyber security measures that involve host-based and network-based security technologies. However, it has been recognized that highly skilled attacks can bypass these security mechanisms to disrupt the smooth operation of control systems. 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.**

***Index Terms*—Anomaly detection, automatic generation control, intrusion detection systems, kernel density estimation, supervisory control and data acquisition.**

I. 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 [1]. 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.

Present day ICS networks, such as the power system *Supervisory Control and Data Acquisition* (SCADA) systems, have increased connectivity to corporate IT networks to enable remote maintenance of field devices and provide critical information for decision making at the corporate center [2]. These connections were often created without an understanding of the potential consequences and thereby, have increased the attack surface of the system. Though attacks targeted at these systems are not frequent, their physical, economic and social impacts can be quite severe if successful [3].

The National Institute for Standards and Technology (NIST) recognizes that in order to protect ICS from cyber threats, it is important to have a *defense-in-depth* approach [2]. The Department of Homeland security recommends a combination of *Firewalls*, *De-militarized Zones* and *Intrusion Detection Systems* (IDS) to implement defense-in-depth [4]. Though the implementation of these technologies in traditional IT networks is well understood, their application to ICS is not straightforward [2]. Security solutions that specifically cater to ICS systems need to be developed with the limitations and constraints of the environment in mind.

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, a 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* [5]. 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-

Manuscript received February 11, 2013; revised June 20, 2013, October 07, 2013; accepted December 15, 2013. Date of current version February 14, 2014. This work was supported in part by the National Science Foundationunder Grants 0915945 and 1202542. Paper no. TSG-00099-2013.

The authors are with the Department of Electrical and Computer Engineering at Iowa State University, Ames, IA 50011 USA (e-mail: gmani@iastate.edu; sridhar@iastate.edu).

Digital Object Identifier 10.1109/TSG.2014.2298195

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.

II. Related Work

The following research efforts have looked into the impacts of cyber attacks on power system control applications. In our earlier work [6], the impact of data integrity attacks directed at the AGC on operating frequency stability was introduced. In [7], Esfahani *et al.* propose a technique to gauge the impact of an intrusion attack on a 2-Area power system. The impact of cyber attacks on *FACTS* are discussed in [8] and [9]. In [10], the impact of cyber attacks directed at wind farms on power system dynamics was presented. In [11], the authors present the impacts of data integrity and denial of service attacks on a chemical reactor system. The authors of [12] and [13] discuss the impact of a cyber attack on a power system in terms of load loss. In [14], the authors show the impact of a cyber attack on the total generation in a system through a graph-based model. The impact of data injection and manipulation on power system state estimation is presented in [15]. In [16], the impact of load redistribution attacks on state estimation is presented. The authors show that operational decisions made based on incorrect power flow and load measurements can cause uneconomic operation and stressed operating states. In [17], the authors explore the impact of compromised measurements on electricity markets. The attack-defense experiment is modeled using game theory.

The authors of [18] have consolidated a classification of anomaly detection techniques and grouped these research efforts appropriately. The authors of [19] apply the statistical anomaly detection technique to identify progressive faults in gearbox operation. In [20], the authors present a real-time payload-based anomaly detection for critical infrastructures. In [21], the authors use the rough set classification algorithm to develop an anomaly detection technique to identify errors introduced in the power flow meters. To the best of our knowledge, none of these efforts inspect the information conveyed by these packet at the application level. These detection techniques do not check if the reported measurements conform to power system theory. One such effort employs *invariant induction*, a technique that identifies power flow measurements that do not satisfy an underlying algebraic equation as anomalies [22]. However, no such technique exists for real-time control applications. The rest of this paper discusses the impact of malicious data injection on AGC, and the design and implementation of attack detection and mitigation.

III. Control System Attack Model and Impact Studies

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 system state. This could in turn cause instabilities in the underlying physical system or force the system to operate at uneconomical operating

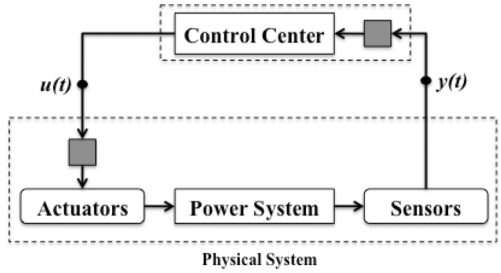

Fig. 1. Control System Model.

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.

A. Attack Templates

This section presents a formal model for the attack templates explored in this paper [11]. The impact of these attacks on power system stability and electricity market operation is presented. In the following definitions, t and τ_a represent time and attack period, respectively.

i) Scaling Attack: A scaling attack involves modifying true measurements to higher or lower values depending on the scaling attack parameter λ_s

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

ii) Ramp Attack: Ramp attacks involve gradual modification of true measurements by the addition of $\lambda_r \cdot t$, a ramp function that gradually increases/decreases with time

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

iii) 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 λ_p.

iv) 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

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

B. Impact of Data Integrity Attacks on AGC

The power system is divided into balancing areas that are connected by tie lines to facilitate exchange of power. Each balancing area has a control center in which the AGC application runs as a part of the energy management system. The AGC is responsible for maintaining system frequency at 60 Hz and limiting tie line power exchanges to their scheduled values. To this end, the algorithm calculates generator corrections based on frequency and tie line power flow measurements obtained from remote sensors via Inter-Control Center Communication Protocol (ICCP). These generator corrections, called the Area Control Error (ACE), are issued once every 5 seconds. The ACE for

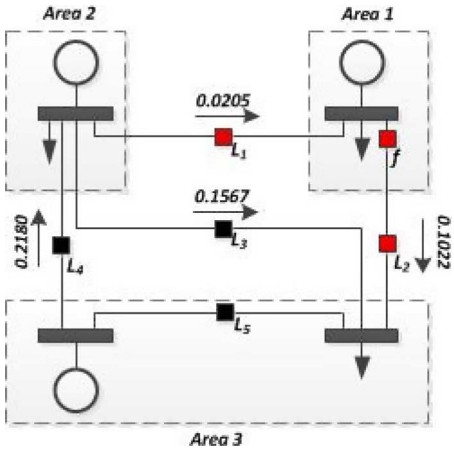

Fig. 2. 3-Area System.

balancing area $'i'$, calculated based on the following equation, instructs generators to either ramp up or down:

$$\mathrm{ACE}_i = (P_{\mathrm{tie}} - P_{\mathrm{sch}}) + \beta_i(f - 60). \tag{1}$$

In the above equation, P_{sch} is the scheduled tie-line power exchange between the balancing areas, β_i is the frequency bias for balancing area i and 60 (Hz) corresponds to the desired system frequency. The variables P_{tie} and f are the tie line power flow and system frequency measurements obtained from sensors in the system. The attack templates discussed in this paper involve injection of fabricated P_{tie} and f measurements in order to force the miscalculation of ACE. As the AGC is required to issue control commands once every 5 seconds, it is unable to benefit from existing measurement validation techniques such as the state estimation, which typically runs once every 5 minutes at the ISO/RTO level. This makes the AGC vulnerable to attacks that involve measurement corruption.

The impacts of attacks on the AGC will be demonstrated using the 3-area system shown in Fig. 2. The system consists of three balancing areas that are interconnected by tie lines. The attack templates require the compromise of sensors L_1, L_2 and f, the tie line power flow and frequency sensors that provide measurements to AGC. The attacker possesses knowledge to compromise these sensors at the corresponding substations compromising existing security mechanisms.

In order to inject the correct measurements according to the attack template, the attacker is required to know AGC operation as well as information on the target system. This information includes load forecasts, scheduled tie line flows, load frequency sensitivity parameter 'D', droop constant 'R' and frequency bias β for each area. The load forecast and scheduled tie line flow information are used to modify system load perception according to the attack template. Parameters D and R are used by the attacker in (2) to identify impactful attack parameters in the attack parameter selection process and to calculate attack frequency measurements as shown later. It is assumed that the maximum value of ACE that does not raise an alarm in the EMS is 0.05 pu. The attacker uses the frequency bias β in (1) to ensure that the ACE computed based on injected measurements remains within this value and that the attack remains undetected.

TABLE I
3-AREA SYSTEM SIMULATION PARAMETERS (FROM [23])

Area $'i'$	D (pu/Hz)	R (Hz/pu)	β (pu/Hz)
Area 1	0.015	3.00	0.3483
Area 2	0.016	2.73	0.3827
Area 3	0.015	2.82	0.3692

TABLE II
GENERATOR PARAMETER FOR LMP CALCULATION

Area	Cost	Per-unit Limit (min, max)
Area 1	33.07 $/MWhr	0.3, 0.8
Area 2	32.11 $/MWhr	0.2, 0.3
Area 3	32.54 $/MWhr	0.1, 0.4

These parameters for the 3-area system are provided in Table I. The following sections discuss the attack mechanism the corresponding physical system and market impacts.

1) Impact on Physical System Stability: The threat actors and for this type of attack could be disgruntled employees, insiders, nation states or terrorist organizations keen on affecting the reliability of the system. The goal of the attack is to cause a rapid decline in the system frequency in order to trigger load shedding schemes. Pulse and random attacks do not fit this purpose as the attacker would look to inflict a significant and definite impact.

In this scenario, the attacker modifies generator operating points through the AGC by providing a wrong perception of the system load. The attack mechanism can be explained with the following example. The power flows shown in Fig. 2 represent the scheduled tie line flow values. The attacker tricks Area 1 AGC into believing that the flow on L_2 has increased by 0.01 pu, which corresponds to an increase in system load ΔP_L. This is achieved by reporting a tie line power flow measurement of 0.1122 pu to the AGC. At the same time, the attacker plays normal measurements according to scheduled value to Area 3 AGC in order to prevent corrective action. The attacker then calculates the malicious frequency measurement to be reported to the AGC using the equation,

$$\Delta F = \frac{-\Delta P_L}{\sum_{i=1}^{3}\left(\frac{1}{R_i} + D_i\right)} = -0.0091 \tag{2}$$

On receiving the measurements, Area 1 AGC computes the ACE to a value of 0.0068 pu, and will instruct generators in Area 1 to ramp down. However, in reality, this action causes the system generation to reduce below the actual system load, thereby causing a generation imbalance. This generation imbalance would reduce system frequency. The following section introduces the attacker's procedure to identify a value for attack parameters λ_s and λ_r.

i) Attack Parameter Selection: The selection of λ_s and λ_r is critical from the attacker's perspective. The parameters have to be selected such that the attack creates the desired impact and at the same time does not trigger any data quality alarms in the control center. To be more precise, the attacker has to satisfy the following criteria.

1) It is assumed that data quality alarms would be triggered if the calculated ACE exceeds 0.05 pu. The ACE calculated

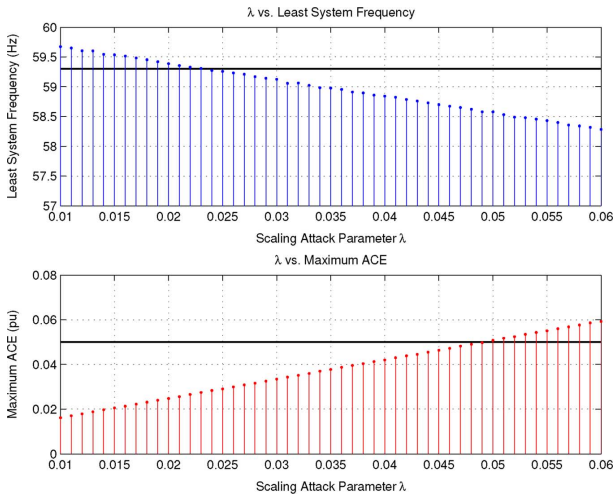

Fig. 3. Scaling Attack Parameter Selection.

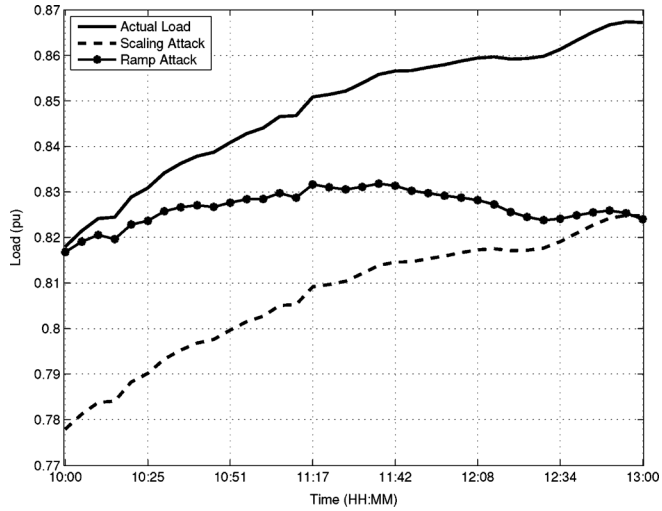

Fig. 4. Perceived Load during Attack.

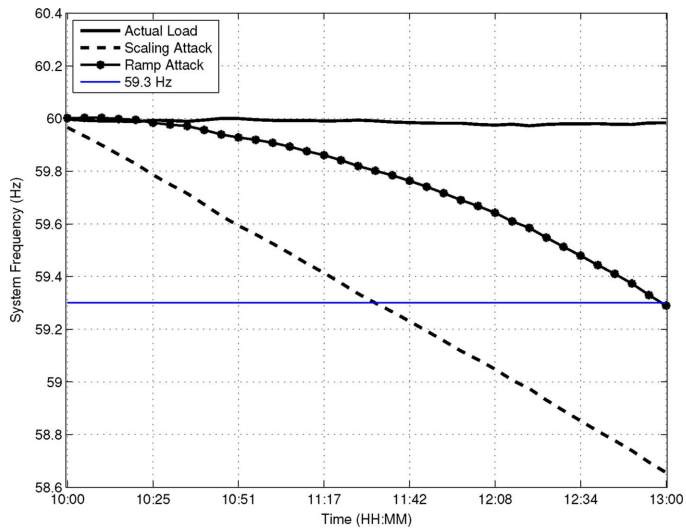

Fig. 5. System Frequency during Attack.

by the control center during the attack should not exceed this value.

2) Underfrequency load shedding schemes are triggered only when the system frequency reaches 59.3 Hz [24]. Hence, the attack parameters should be selected such that the system frequency declines to 59.3 Hz to cause an impact.

Intuitively, these criteria have contrasting requirements. Fig. 3 plots the variation of maximum ACE and the least system frequency during the attack period (10 AM–1 PM) against a range of λ_s. The attacker would construct these graphs based on (1) and (2) for attack parameter selection. The following observations can be made from these figures.

1) As the magnitude of λ_s increases, the least system frequency observed during the attack decreases. At a value of $\lambda_s = 0.023$, the system frequency declines to 59.3 Hz. This means, for this system under consideration, in order for the scaling attack to have an impact, the value of λ_s should be a minimum of 0.023. Thus, this analysis identifies the lower bound $\lambda_{s,\min}$ for the attack magnitude.
2) As the value of λ_s increases, the maximum ACE generated during the attack period increases. After a value of $\lambda_s = 0.049$, the maximum ACE increases beyond the threshold of 0.05 pu. This means, beyond a value of $\lambda_s = 0.049$, the data quality alarms in the control center would be triggered. Hence, for this system, in order for the attack to be stealthy, the maximum attack parameter $\lambda_{s,\max}$ should be below 0.049.

To summarize, in order for the scaling attack to be effective during this period, that is impactful and stealthy, the condition $(0.023 < \lambda_s < 0.049)$ has to be satisfied. A similar analysis for ramp attacks reveals that in order for the attack to be effective, the condition $(0.0022 < \lambda_r < 0.0024)$ has to be satisfied. In order to cause maximum impact, the attacker would use $\lambda_s = 0.049$ for scaling attacks and $\lambda_r = 0.0024$ for ramp attacks. Fig. 4 shows the variation between the actual system load and the perceived load during scaling and ramp attacks with these parameters. Fig. 5 shows the frequency of the system in response to the change in generation.

ii) Impact Analysis: The following observations can be made from Figs. 4 and 5 about the impact on physical system stability.

1) Firstly, the maximum ACE deviation during the scaling and ramp attacks is 0.0481 pu and 0.0476 pu, respectively. As these values remain within the 0.05 pu threshold, data quality alarms are not triggered in the control center (This is not shown in Fig. 4 and 5).
2) Secondly, it is observed the system frequency due to both scaling and ramp attacks declines to 59.3 Hz, thus leading to a load shedding scenario.
3) The system frequency due to scaling attack declines to 59.3 Hz much sooner when compared to ramp attacks. This is because the scaling attack instantly modifies the perceived load thereby triggering significant ACE correction. The ramp attack injects gradual deviations in perceived load and thereby creates a delayed impact.
4) Finally, it is observed that the magnitude of frequency decline caused by scaling attack is more severe when compared to the ramp attack despite similar perceived

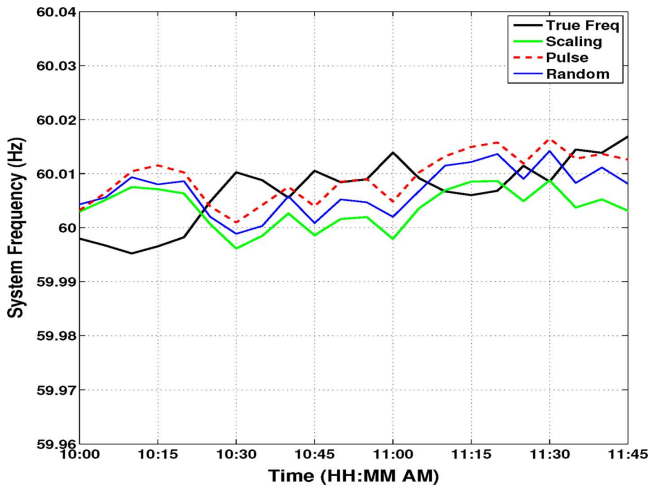

Fig. 6. Frequency during Electricity Market Attack.

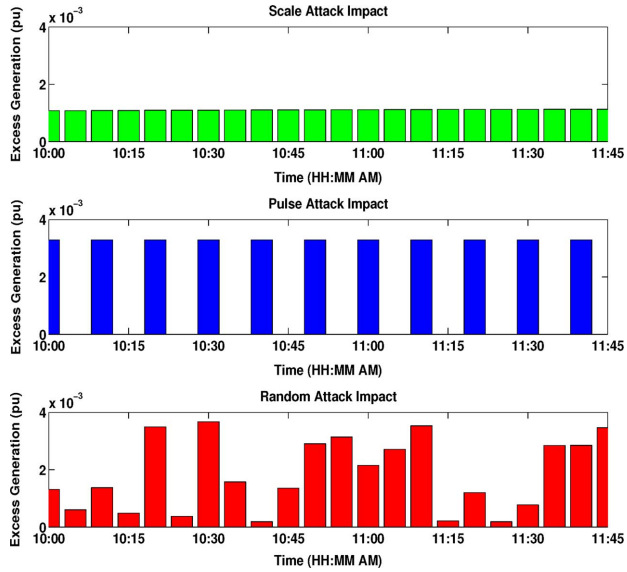

Fig. 7. Excess Generation during Electricity Market Attack.

loads towards the end of the attack period. This is because the scaling attack effects a significant difference between system load and generation for a longer duration when compared to the ramp attack.

From the above, it can be inferred that the impact from scaling attack is more severe when compared to ramp attack. For this period of operation, maximum impact will be caused if parameters $\lambda_s = 0.049$ for scaling and $\lambda_r = 0.0024$ for ramp were employed. An attacker would have to perform similar analysis in order identify effective λ_s and λ_r ranges for other periods of operation.

2) Impacts on Electricity Market Operation: The attack on electricity market operation involves modification of generator operating points identified by the security constrained economic dispatch (SCED). A market participant (utility) could use this type of attack to increase its generation and reduce generation in an adjacent balancing area. By doing so, the utility is able to increase revenue as it receives a greater financial settlement.

Using the same base case in Fig. 2, the attack mechanism can be explained as follows. The tie line flow between Area 2 and 1 is 0.0205 pu. In this case, the attacker modifies this measurement value to 0.0225 pu to indicate that Area 2 is supplying more than the scheduled value. The AGC in Area 2 calculates the ACE corresponding to this measurement as 0.0013 pu, which forces the generators in the area to ramp down. At the same time, the ACE computed by the AGC in Area 1 forces the generators in Area 1 to ramp up, thereby generating more than operating point suggested by the SCED. As a decrease in generation in Area 2 is compensated by an increase in Area 1, the system frequency is not impacted. This is confirmed in Fig. 6, where the system frequency is found to remain around 60 Hz even during attacks. However, the market participant in Area 1 will benefit from this scenario as it receives a greater settlement. In the following section, the impact of scaling, pulse and random attacks on calculation of settlements is shown.

The following parameters were used for the attacks—i) Scaling—$\lambda_s = 0.001$, ii) Pulse—$\lambda_p = 0.0025$, and iii) Random-$a = 0.03, b = 0$. Fig. 7 shows the additional generation from Area 1 as a result of the attack.

- The scaling attack forces the units in Area 1 to operate at 0.0011 pu higher than the correct operating point for a scaling factor $\lambda_s = 0.001$. As a result, the generator produces a total excess generation of 0.0266 pu during the attack period.
- The pulse attack causes Area 1 to have periods of excess generation of 0.0033 pu. This results in a total excess generation of 0.0395 pu during the attack period.
- The random attack results in a total excess generation of 0.0430 pu during the attack period.

This attack impacts the calculation of settlements to market participants. The settlement provided to a generation utility is a product of the power supplied by the utility to the system and the locational marginal price (LMP). The following generator parameters were assumed for LMP calculation.

For the load forecast during the period of simulation, the LMP was obtained to be 32.54 $/MWhr at all nodes. Assuming a system base of 1000 MW, the total excess generation during the attack period for scaling, pulse and random attacks is 26.6 MW, 39.5 MW and 43 MW. This corresponds to additional settlements of 865.56 $, 1285.33 $ and 1399.22$, respectively. Hence, for the attack scenarios presented in this section, the impact of random attack on market operation is the highest, followed by pulse and scaling attacks. An attacker could use these attacks periodically to consistently increase settlement.

IV. Attack Resilient Control for Power Systems

The notion of attack resilient control for ICS was first presented in [25]. 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

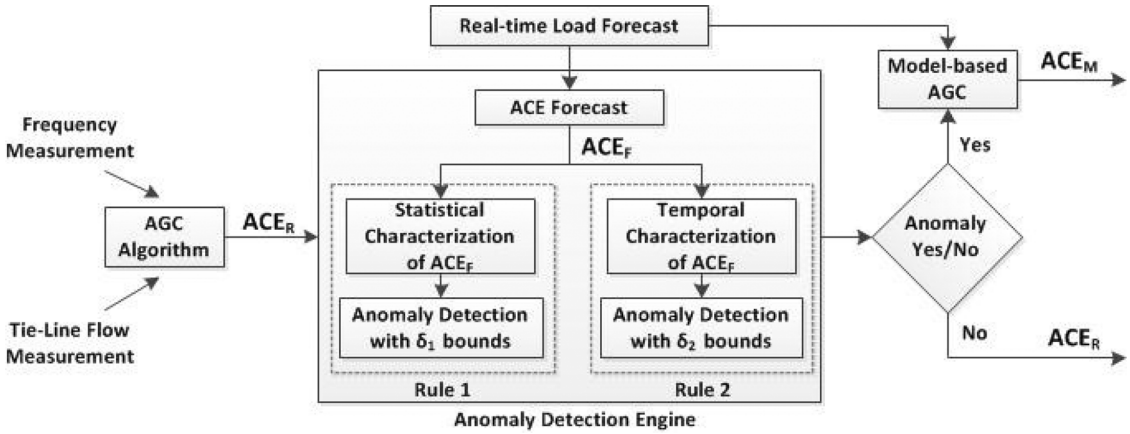

Fig. 8. Attack Resilient Control for AGC.

system. Smart mitigation techniques should have the ability to function using forecasts when measurements can not be trusted.

The power system is composed of several control systems that work in conjunction to ensure system stability [26]. Each control application has its own vulnerabilities depending on the type of protocol, network architecture and security technologies it uses. Similarly, the impact from a successful attack on a control system depends on the physical parameter it is monitoring and controlling [3]. Therefore, there may not be one single solution for an attack resilient power system. It is important for critical power system control applications to be provided with the required intelligence to detect attacks impactful in that domain. The following classes of information could be used to design attack resilient control modules.

- *Forecasts*: Load forecasts could be used to detect attacks that mimic unprecedented load changes. In [10], a scenario in which the attacker modifies P_{ref} (reference power) in a wind turbine to force a reduction in the active power output was shown. In this scenario, wind forecast information could have been used to detect the attack.
- *Situational Awareness*: Stability limits, system topology, geographic location, etc. could help identify attack scenarios. Situational awareness could also help the control module process mitigation strategies. E.g., Hospitals zones are given priority in scenarios where load shedding has to be performed.
- *System Resources*: System resources like generation reserves, VAR reserves, available transmission capacity, backup communication paths, etc. should be considered to process efficient mitigation strategies. E.g., if the the cyber logs of a substation reveal a potential attack, generation could be re-dispatched to prevent instabilities if the attack is successful.
- *Attack Templates*: The control module should be aware of effective attack templates and attack signatures for each control application. This could assist in early attack detection and defense at the cyber layer.
- *System Data*: System parameter data, such as inertia constants H, play a critical role in system response to disturbances. A control module provided with this information would be able to check for anomalous behavior in system performance.

Attack Resilient Control for AGC

The objective of the proposed attack resilient control mechanism for AGC is twofold—i) to detect the presence of malicious measurements and prevent the controller from performing incorrect ACE computations, and ii) to maintain the balance between generation and demand in the presence of untrusted measurements by using a model-based approach. In this paper, we propose a mitigation strategy for attacks that impact physical stability of the power system only. Fig. 8 presents a conceptual diagram for the implementation of attack-resilient AGC. The frequency and tie-line flow measurements received at the control center will be used by the AGC to calculate ACE_R, the real-time ACE. This ACE_R is checked by the anomaly detection engine to determine if the value is a anomalous. If ACE_R is identified as an anomaly, the model-based AGC is called upon.

A. Anomaly Detection Engine

Real-time load forecasts are calculated in 5-minute intervals for 60–180 minutes in the future [27]. The anomaly detection algorithm uses this real-time load forecast to predict AGC operation over a given time-period. During real-time operation, the performance of AGC is compared to this prediction to identify anomalies. The anomaly detection algorithm consists of two rules to detect anomalies. Rule 1 employs statistical characterization of forecasted ACE values and rule 2 uses temporal characterization of ACE performance. Rules 1 and 2 work in conjunction with one another to detect smart attacks that can cause frequency instabilities of the type described earlier. Details on rules 1 and 2 are provided below.

1) Rule 1—Statistical Characterization of ACE: This rule is incorporated to catch single exorbitant ACE values obtained from malicious measurements. The following steps explain this process in detail.

- *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

Algorithm: $[ACE_{F_{min}}, ACE_{F_{max}}]$ Identifier
Input: $f(ACE_F)$, δ_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

forecasted ACE (ACE_F) values are then fed into a *Kernel Density Estimator* module [28]. The density estimator constructs a probability density, $f(\mathrm{ACE}_F)$, for the inputed ACE_F values as shown in Fig. 9. The probability of a particular range of ACE_F values is obtained by integrating $f(\mathrm{ACE}_F)$ 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 δ_1 is one of the tuning parameters of the anomaly detection engine. If $\delta_1 = 90\%$, the anomaly detection algorithm identifies the range of ACE_F values, $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$, that has a probability of 0.9. The range $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ is calculated from the following equation.

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

  The following algorithm ensures the area indicated by δ_1 is determined over the most probable values of ACE_F. Once the probability density is constructed, the algorithm identifies the index of the ACE_F which has the highest value for $f(\mathrm{ACE}_F)$ and assigns the value to variables i and j. Next, the area under the graph, which gives the probability, is determined using the function $A(i, j)$. The *while* loop is executed as long as $A(i, j) < \delta_1$. The algorithm compares $A(i-1, j)$ and $A(i, j-1)$. If $A(i-1, j) > A(i, j-1)$, the value of i is changed to $i-1$. If $A(i, j-1) > A(i-1, j)$, j is incremented by 1. This ensures that area is identified across the most probable ACE_F values. Once $A(i, j) < \delta_1$ is false, the values of ACE_F at i and j are identified as $\mathrm{ACE}_{F_{\min}}$ and $\mathrm{ACE}_{F_{\max}}$, respectively.

During operation, if ACE_R computed by the AGC algorithm falls outside $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$, the measurement is identified as an anomaly.

2) Rule 2—Temporal Characterization of ACE: In some cases such as ramp attacks, smart attackers may manipulate measurements such that the system is gradually deviated from the correct state of operation to conceal the attack effectively. In such scenarios, rule 1 alone is insufficient as successive ACE_R values could fall within $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ range obtained from δ_1. Under such circumstances, it becomes important to observe a series of measurements to identify an attack. Rule 2 of the anomaly detection algorithm observes a series of ACE_R measurements to detect ramp attack type scenarios that gradually modify operating points of generators.

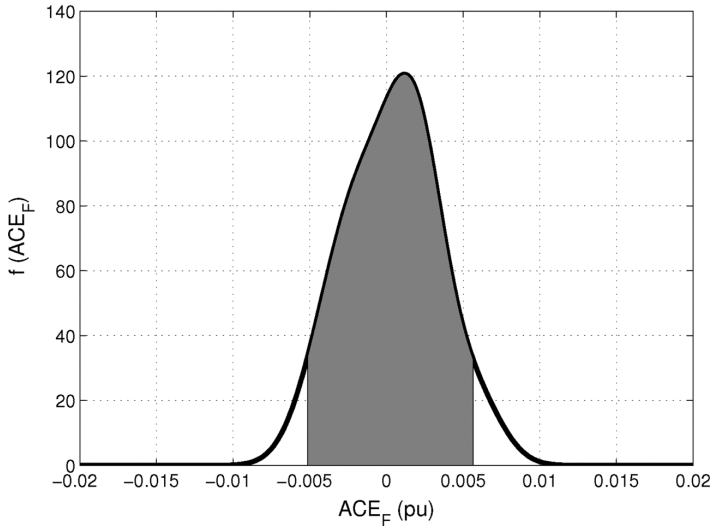

Fig. 9. PDF of Forecasted ACE Values ($\delta_1 = 90\%$).

The ACE is a corrective signal sent to generating units to adjust operating points once every five seconds. During a period of operation the final operating points of generating units are a result of successive ACE corrections added to the initial operating point. The ACE corrections are generated as a result of load changes. Hence, an algebraic sum of ACE signals will reflect the load change during that period of operation.

- *Anomaly Detection*
  A comparison of the algebraic sum of ACE_R and ACE_F values will reveal the difference between the expected final operating point and actual final operating point during a time-period of operation, $t \cdot \Psi$ is defined as,

$$\Psi = |\Sigma_t \mathrm{ACE}_F - \Sigma_t \mathrm{ACE}_R|$$

  A δ_2 bound is defined such that, if $\Psi > \delta_2$, $\mathrm{ACE}_R \in t$ are marked as anomalies.

During real-time operation, the time taken to check if ACE_R and $\Sigma\mathrm{ACE}_R$ satisfy rules 1 and 2, respectively, should be less than a second in modern computers. Therefore, the proposed anomaly detection algorithm will operate within the AGC cycle.

3) Anomaly Detection Engine Parameter Selection: The performance of the anomaly detection engine is tied to parameters δ_1 and δ_2. System operators or software programs should use the following guideline to tune δ_1 and δ_2 for low False Positive (FP) and False Negative (FN) rates.

- ***Step 1:*** The following data should be generated from the real-time load forecast—i) $f(\mathrm{ACE}_F)$ and $\Sigma_t \mathrm{ACE}_F$ data and ii) effective $\lambda_{s,\min} < \lambda_s < \lambda_{s,\max}$ and $\lambda_{r,\min} < \lambda_r < \lambda_{r,\max}$ ranges for the period of operation under consideration.

- ***Step 2:*** Create a dataset that consists of true values and measurements corrupted with $\lambda_{s,\min}$ and $\lambda_{r,\min}$ that were identified in the previous step. This is to ensure that any attack with $\lambda > \lambda_{\min}$ is detected. This dataset will be used in the next step to tune δ_1 and δ_2 for low FP and FN rates.
- ***Step 3:*** Run the AGC algorithm offline with the dataset created in the previous step in order to identify ACE and $\Sigma_t\mathrm{ACE}$. Some of these values are a result of true measurements and some of them are derived from corrupt measurements. For every value of δ_1, identify $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ from $f(\mathrm{ACE}_F)$ and observe if ACE is identified as anomaly or true according to rule 1 check. Similarly, for every value of δ_2 calculate Ψ from $\Sigma_t\mathrm{ACE}$ and $\Sigma_t\mathrm{ACE}_F$ and observe if $\Sigma_t\mathrm{ACE}$ is identified as anomaly or true according to rule 2 check. Depending on the nature of the original data and result of the anomaly check, calculate the *False Positive* (FP) and *False Negative* (FN) rates for every value of δ_1 and δ_2. Select δ_1 and δ_2 values corresponding to low FP and FN rates.

The FP and FN rates are calculated from (3) and (4), where TN and TP refer to true negatives and true positives, respectively. An efficient anomaly detection algorithm should have low FP and FN rates. If the FP rate is too high, there will be too many false alarms and the operators will lose their trust in the system. A high FN rate means that the anomaly detection algorithm will fail to catch malicious measurements and attacks will not be detected. Therefore, it becomes important to determine the optimal amount of δ_1 and δ_2 to avoid situations of this type.

$$\text{FP Rate} = \frac{\text{FP Count}}{\text{FP Count} + \text{TN Count}} \tag{3}$$

$$\text{FN Rate} = \frac{\text{FN Count}}{\text{FN Count} + \text{TP Count}} \tag{4}$$

B. Model-Based Attack Mitigation

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.

The proposed model-based mitigation strategy uses this load forecast in order to predict AGC performance and thereby obtain the ACE forecast (ACE_F). As shown in Fig. 10, an error is added to the forecast in order to generate a simulated real-time load. The simulated real-time load and the forecast are then fed into an offline AGC module. As system generation resources are planned based on the load forecast, running the AGC algorithm offline using this forecast and simulated real-time load as input would generate ACE_F.

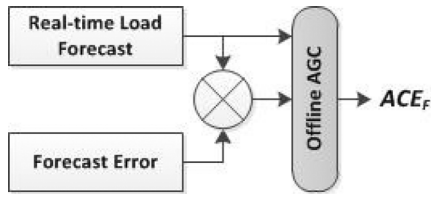

Fig. 10. Generation of ACE_F.

As explained earlier, the ACE_F obtained from this block is fed into the Kernel Density Estimator module for the purposes of attack detection. For mitigation, the mean of the ACE_F for the forecast period is used to issue generator correction during an attack. As the real-time load forecast is made for every 5 minutes for the next one hour of operation, the mitigation will pre-compute 12 ACE_F corrections for the time period. When an anomaly is detected, the mean of these forecasted ACE values would be issued as generator corrections. This approach is followed until the trust in sensors or communication channels is restored.

V. Simulation Studies

The goal of this section is to analyze the performance of the anomaly detection and model-based mitigation during attack scenarios. The study involves two components—i) Anomaly detection engine tuning for the period of operation under consideration and ii) Performance analysis of attack resilient control during attack scenarios. The attack-defense experiments on AGC was performed using the 3-Area power system introduced in Section III. Additionally, the following data are required to perform these studies.

- *Real-time load forecasts*—Real-time load forecasts are used to schedule generation resources during real-time operation [27]. The New England ISO website provides 5-minute load data for their system. As corresponding load forecast information is unavailable, the actual load data was per-unitized and assumed to be the real-time load forecast for the 3-Area power system. The real-time load forecast is used to calculate $f(\mathrm{ACE}_F)$ and $\Sigma_t(\mathrm{ACE}_F)$ for anomaly detection tuning and mean of ACE_F for model-based mitigation.
- *Load data*—The load data for the same time period as above is obtained by adding an error to the real-time forecast. Reference [29] characterizes the error from real-time load forecast into a truncated normal distribution with mean -1.15, min/max ∓ 349, standard deviation 98 and autocorrelation 0.61. Load data generated using this technique is made use of in the following cases—i) to generate dataset for anomaly detection engine tuning and ii) to generate corrupted load data for performance analysis of attack resilient control.

The performance of attack resilient control was analyzed using data for one day of operation obtained from [30]. The scaling and ramp attacks were implemented between 10 AM–1 PM and 1 PM–4 PM, respectively. Table III summarizes the effective λ_r and λ_s range for this period of operation along

TABLE III
SIMULATION CASE STUDY SUMMARY

Attack	Time	λ	δ_1, δ_2
Scaling	$10\,AM - 1\,PM$	$0.024 < \lambda_s < 0.05$	0.92, 0.049
Ramp	$1\,PM - 4\,PM$	$0.0021 < \lambda_r < 0.0024$	0.94, 0.05

with δ_1 and δ_2 used by the anomaly detection engine for the first hour. The following section explains anomaly detection engine tuning for the scaling attack time period.

A. Anomaly Detection Engine Tuning

The parameters δ_1 and δ_2 have to be selected for every hour of operation in order to maintain acceptable FP and FN rates. Based on the guideline presented in Section IV.A3, this process is demonstrated for the period from 10 AM–11 AM from the test data.

1) ***Step 1:*** From the load forecasts for this period, $f\,(\mathrm{ACE}_F)$ and $\Sigma_t \mathrm{ACE}_F$ were generated. Through the λ selection procedure shown in Section III.B, the λ_s and λ_r ranges for this period were identified as—i) $0.024 < \lambda_s < 0.05$ and ii) $0.0021 < \lambda_r < 0.0024$.
2) ***Step 2:*** A dataset was created with a hundred load data subsets by adding noise to the real-time load forecast. Each load data subset is a representation of the load curve for the period under consideration. Of these, twenty subsets were corrupted with scaling attack template with $\lambda_{s,\min} = 0.024$ and another twenty subsets were corrupted using the ramp attack template with $\lambda_{r,\min} = 0.021$.
3) ***Step 3:*** The objective of this step is to identify values of δ_1 and δ_2 that result in low FP and FN rates. For this purpose, the FP and FN rates for the ranges $0.8 < \delta_1 < 0.99$ and $0.01 < \delta_2 < 0.08$ were analyzed. Each subset of load data was run through an offline AGC program in order to determine the individual ACE values and $\Sigma_t \mathrm{ACE}$. Based on rules 1 and 2, anomalies were identified in the attack data set for every value of δ_1 and δ_2. The FP and FN rates were then calculated based on the results of anomaly detection. In these studies, the impact of δ_1 on FP and FN rates was evaluated with rule 1 only implemented. Similarly, studies for impact of δ_2 on FP and FN rates was performed with only rule 2 implemented. The following section discusses these results.

- ***False Positive Analysis:*** Fig. 11 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 $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ range. The FP rate beyond $\delta_1 = 0.92$ is minimum at zero. As in the case of δ_1, the FP rate decreases with as δ_2 is varied between 0.01 and 0.08. The FP rate is significantly high in the region $\delta_2 < 0.03$. As the δ_2 bound is strict at this point, the condition $\Psi > \delta_2$ is satisfied even for true measurements. The FP rate is zero in the region $\delta_2 > 0.049$.
- ***False Negative Analysis:*** Fig. 12 presents the variation of false negative rate for different values of δ_1 and δ_2. At a value of $\delta_1 = 0.8$, the FN rate is non-zero at 0.14. This is because, even with a narrow $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ 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 $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ band 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 $\delta_1 = 0.85$. Scaling attack measurements are detected for all values of δ_1.

  The value of δ_2, which represents the maximum tolerated cumulative ACE variation the period of operation, was varied between 0.01 to 0.08. At a value of $\delta_2 = 0.01$, the FN rate is 0.015. At this point, the algorithm fails to detect some anomalous measurements introduced by scaling attack. As the value of δ_2 is increased, more anomalies introduced by the scaling attack template are not detected. At a value of $\delta_2 = 0.05$, all the anomalies introduced by the scaling attack are missed. However, all anomalies introduced by ramp attacks are identified at all points.

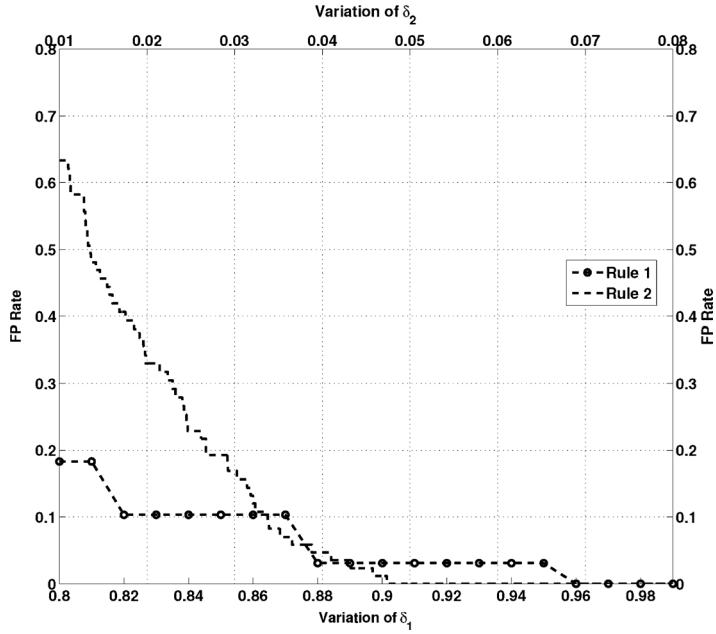

Fig. 11. False Positives Analysis.

The analysis reveals that scaling and ramp attacks are identified at all values of δ_1 by rule 1 and δ_2 by rule 2. However, the FP rates are least in the region $\delta_1 > 0.92$ and $\delta_2 > 0.049$. Hence, for this period of operation, the anomaly detection engine should be set to $\delta_1 = 0.92$ and $\delta_2 = 0.049$ for the best performance. Similar analysis for the period 1 PM–2 PM resulted in $\delta_1 = 0.94$ and $\delta_2 = 0.05$.

B. Online Performance Analysis

The attack dataset that was used to test online performance involved measurements corrupted with scaling and ramp parameters of $\lambda_s = 0.05$ and $\lambda_r = 0.0024$. This is justified as the attacker would have identified these values as the most impactful and stealthy. In this section, we present results from the operation of attack-resilient AGC during attacks. The principle of operation is that when an anomaly is detected, model-based

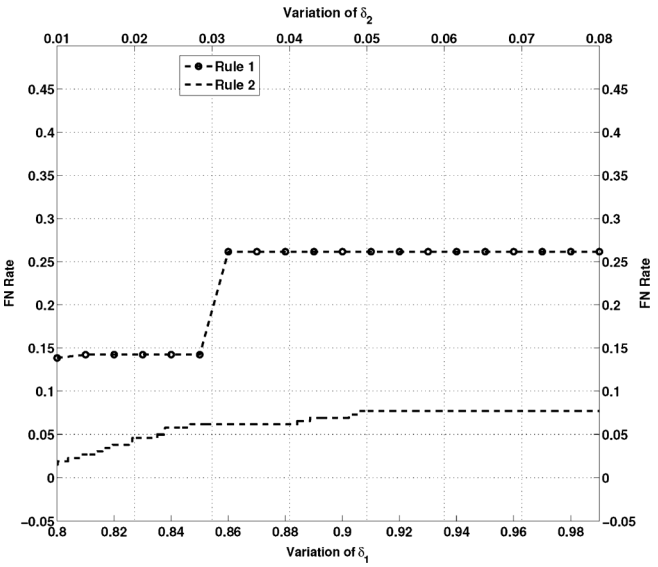

Fig. 12. False Negatives Analysis.

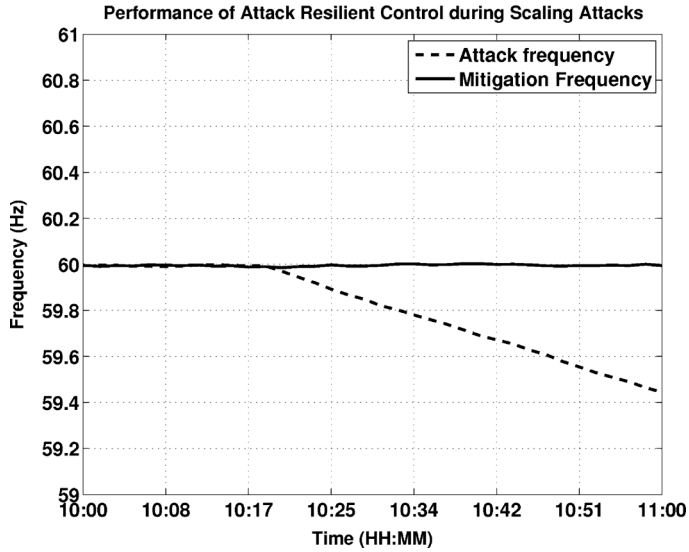

Fig. 13. Frequency Performance during Scaling Attacks.

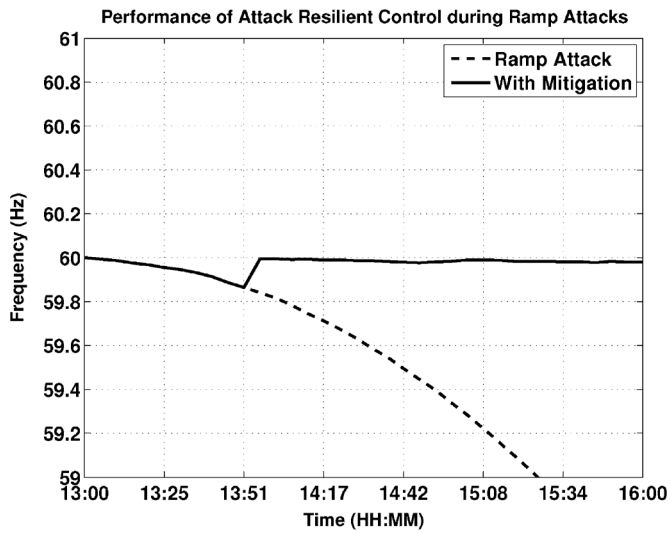

Fig. 14. Frequency Performance during Ramp Attacks.

AGC is employed until the end of the hour. It is assumed that during this time, the source of the cyber threat is identified and negated. At the end of the hour, AGC returns to the traditional measurement-based operation.

Performance During True Positives: i) Mitigation of Scaling Attacks: Fig. 13 shows system performance during the scaling attack period. The anomaly detection engine is successful in identifying the scaling attack through the ACE forecast calculated at 10.00 AM. The algorithm calculated the value for $\mathrm{ACE}_{\min}$ and $\mathrm{ACE}_{\max}$ as -0.0070 and 0.0065, respectively, based on $\delta_1 = 0.92$. However, the scaling attack forces the calculated real-time ACE to 0.0282, which is not within the range defined by $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$. Hence the field measurements for rest of the hour are marked anomalous and the AGC operation is carried out based on real-time load forecasts. From Fig. 13 it is observed that the model-based mitigation is effective in maintaining system frequency within reasonable limits.

ii) Mitigation of Ramp Attacks: Fig. 14 shows the frequency performance of the system during the ramp attack period (1–4 PM). It is observed that the actual system frequency, indicated by the solid line, deviates initially for some period of time before returning to 60 Hz. This is because, the anomaly detection algorithm is able to identify ramp attacks only after observing a series of measurements to determine the algebraic sum of ACE. Once the attack is identified, AGC is operated for the next hour based on the real-time load forecast.

For the first hour of the ramp attack, between 1–2 PM, the algebraic sum of ACE from the forecast (ACE_F) was determined to be -0.0002 pu. With the inclusion of the tolerance bound given by $\delta_2 = 0.050$, the acceptable range of algebraic ACE sum is between -0.0502 pu and 0.0498 pu. However, the algebraic sum of ACE during real-time operation for the same hour was determined to be 0.0595 pu, which is outside the acceptable limit. This anomaly triggers model-based AGC operation for the next hour. From Fig. 14, it is observed that the frequency deviation is arrested and the brought back to acceptable values for the next hour during the attack period.

Performance During False Positives: During the simulation, the anomaly detection algorithm identified a true measurement as an anomaly. A real-time ACE of -0.0071 was generated at around 6.14 AM. However, the $[\mathrm{ACE}_{F_{\min}}, \mathrm{ACE}_{F_{\max}}]$ range was evaluated to be $[-0.0065, 0.0070]$ for this period of operation. This triggered unwarranted model-based mitigation. Fig. 15 shows the frequency performance of the system during this period. It is observed that there is a difference in frequency performance when model-based AGC is used. However, the system frequency is still maintained within acceptable limits.

VI. Conclusion

In this paper, we showed the impacts of data integrity attacks on AGC operation. It was observed that scaling, ramp,

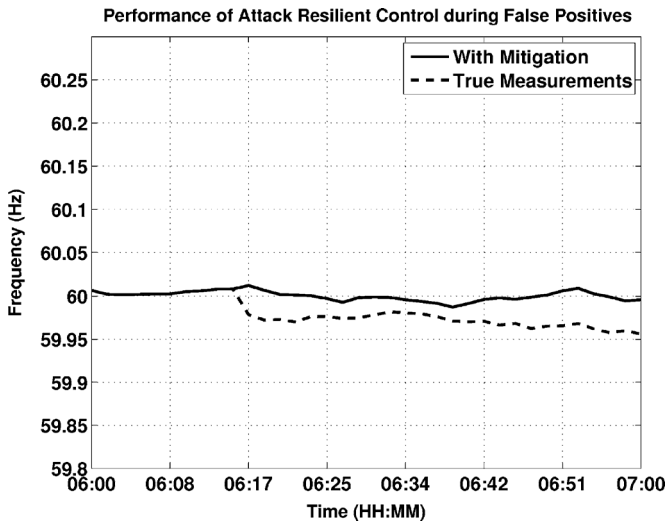

Fig. 15. Frequency Performance during False Positives.

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. The idea was to develop detection and mitigation techniques based on knowledge of power system operation. The idea was extended to an attack resilient AGC that detects malicious data injection based on real-time load forecasts. The performance of the anomaly detection algorithm was measured in terms of false positive and negative rates and the performance of the mitigation was observed through frequency performance of the power system. 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] N. Falliere, L. O'Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec, Tech. Rep., Feb. 2011.

[2] J. F. Keith Stouffer and K. Kent, "Guide to supervisory control and data acquisition (SCADA) and industrial control systems security—Recommendations of the national institute of standards and technology," Special Publication 800-82, Initial Public Draft Sept. 2006.

[3] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[4] M. F. David Kuipers, "Control Systems Cyber Security: Defense in Depth Strategies," Department of Homeland Security, Tech. Rep., May 2006.

[5] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," Dept. Computer Engineering, Chalmers Univ. Technol., 2000.

[6] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on scada control system," in *Proc. IEEE Power Eng. Soc. General Meeting*, Jul. 2010, pp. 1–6.

[7] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. American Control Conference (ACC), 2010*, Jul. 2010, pp. 962–967.

[8] L. R. Philips, M. Baca, J. Hills, J. Margulies, B. Tejani, B. Richardson, and L. Weiland, "Analysis of Operations and Cyber Security Policies for a System of Cooperating Flexible Alternating Current Transmission System (FACTS) Devices," Sandia National Lab., Dec. 2005.

[9] 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.

[10] J. Yan, C.-C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm SCADA system and its impact analysis," in *Proc. Power Systems Conference and Expo. (PSCE)*, Mar. 2011, pp. 1–6.

[11] Y.-L. Huang, A. A. Cardenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *Int. J. Critical Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.

[12] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man Cybern. A*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

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

[14] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010, pp. 244–249.

[15] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," 2009.

[16] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[17] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–10, 2013.

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

[19] M. J. Desforges, P. J. Jacob, and J. E. Cooper, "Applications of probability density estimation to the detection of abnormal conditions in engineering," *Proc. Inst. Mech. Eng. Part C: J. Mech. Eng. Sci.*, vol. 212, no. 8, pp. 687–703, 1998.

[20] P. Dssel, C. Gehl, P. Laskov, J.-U. Buer, C. Strmann, and J. Kstner, "Cyber-critical infrastructure protection using real-time payload-based anomaly detection," in *Critical Information Infrastructures Security*, E. Rome and R. Bloomfield, Eds. New York, NY, USA: Springer, 2010, vol. 6027, pp. 85–97.

[21] M. Coutinho, G. Lambert-Torres, L. da Silva, H. Martins, H. Lazarek, and J. Neto, "Anomaly detection in power system control center critical infrastructures using rough classification algorithm," in *Proc. DEST*, Jun. 2009, pp. 733–738.

[22] J. Bigham, D. Gamez, and N. Lu, "Safeguarding SCADA systems with anomaly detection," in *Computer Network Security*, V. Gorodetsky, L. Popyack, and V. Skormin, Eds. New York, NY, USA: Springer, 2003, vol. 2776, pp. 171–182, ser. Lecture Notes in Computer Science.

[23] H. Bevrani, *Robust Power System Frequency Control*, 1st ed. New York, NY, USA: Springer, 2009.

[24] MRO Under-Frequency Load Shedding (UFLS) Program Midwest Reliability Organization, , Tech. Rep., Dec. 2005.

[25] D. Wei and K. Ji, "Resilient industrial control system (rics): Concepts, formulation, metrics, and insights," in *Proc. 3rd ISRCS*, Aug. 2010, pp. 15–22.

[26] K. Tomsovic, D. Bakken, V. Venkatasubramanian, and A. Bose, "Designing the next generation of real-time control, communication, and computations for large power systems," *Proc. IEEE*, vol. 93, no. 5, pp. 965–979, May 2005.

[27] D. Trudnowski, W. McReynolds, and J. Johnson, "Real-time very shortterm load prediction for power-system automatic generation control," *IEEE Trans. Contr. Syst. Technol.*, vol. 9, no. 2, pp. 254–260, Mar. 2001.

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

[29] Integration of Renewable Resources: Technical Appendices for California ISO Renewables Integration (Version 1).

[30] New England Independent System Operator—Five-Minute Data.

Siddharth Sridhar received the B.E. degree in electrical and electronics engineering from The College of Engineering, Guindy (Anna University), India, in 2004. He is currently working towards the Ph.D. degree in computer engineering at the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA.

His research interests are in the application of intelligent cybersecurity methods to power system monitoring and control.

Manimaran Govindarasu is currently the Mehl Professor of Computer Engineering in the Department of Electrical and Computer Engineering at Iowa State University. He received his Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT), Chennai, India, in 1998 and has been on the faculty of Iowa State since 1999.

His research expertise is in the areas of CPS security for the smart grid, cyber security, and real-time systems/networks. He has co-authored over 125 peer-reviewed research publications, and has given invited talks and tutorials at reputed IEEE conferences and delivered several industry short courses on the subject of cyber security. He is a co-author of the text *Resource Management in Real-Time Systems and Networks* (MIT Press, 2001).

Dr. Govindarasu served as the co-chair of the Super Session on Communications Innovations for Power Systems at IEEE Power and Energy Society (PES) General Meeting, 2012. He has served as guest co-editor for several journals including leading IEEE magazines (IEEE *Network*, Jan. 2004; IEEE *Power and Energy*, Jan. 2012; IEEE Network, 2013) and serving as an Editor for IEEE TRANSACTIONS ON SMART GRID since 2011. He has contributed to the U.S. DOE NASPInet (Synchrophasor network) Specification project. He currently serves as the founding chair of the Cyber Security Task Force at IEEE Power and Energy Society (PES) CAMS subcommittee and also serves as the Vice-Chair of CAMS.