Optimized Predictive Control for AGC Cyber Resiliency

Muhammad Nouman Nafees
Cardiff University
Cardiff, United Kingdom
nafeesm@cardiff.ac.uk

Neetesh Saxena
Cardiff University
Cardiff, United Kingdom
saxenan4@cardiff.ac.uk

Pete Burnap
Cardiff University
Cardiff, United Kingdom
burnapp@cardiff.ac.uk

ABSTRACT

Automatic Generation Control (AGC) is used in smart grid systems to maintain the grid's frequency to a nominal value. Cyber-attacks such as time delay and false data injection on the tie-line power flow, frequency measurements, and Area Control Error (ACE) control signals can cause frequency excursion that can trigger load shedding, generators' damage, and blackouts. Therefore, resilience and detection of attacks are of paramount importance in terms of the reliable operation of the grid. In contrast with the previous works that overlook ACE resiliency, this paper proposes an approach for cyber-attack detection and resiliency in the overall AGC process. We propose a state estimation algorithm approach for the AGC system by utilizing prior information based on Gaussian process regression, a non-parametric, Bayesian approach to regression. We evaluate our approach using the PowerWorld simulator based on the three-area New England IEEE 39-bus model. Moreover, we utilize the modified version of the New England ISO load data for the three-area power system to create a more realistic dataset. Our results clearly show that our resilient control system approach can mitigate the system using predictive control and detect the attack with a 100 percent detection rate in a shorter period using prior auxiliary information.

CCS CONCEPTS

• **Security and privacy** → **Intrusion detection systems**;

KEYWORDS

automatic generation control; resiliency; anomaly detection

ACM Reference Format:
Muhammad Nouman Nafees, Neetesh Saxena, and Pete Burnap. 2021. Optimized Predictive Control for AGC Cyber Resiliency . In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21), November 15–19, 2021, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3460120.3485358

1 INTRODUCTION

The Automatic Generation Control (AGC) is a wide-area frequency control application that ensures frequency stability and keeps the power interchange between Balancing Authority (BA) areas at the scheduled values [7]. The control of the AGC mechanism relies on geographically dispersed sensing devices that are remotely controlled. The tie-line power flow between BA areas and frequency measurements from these sensing devices are sent to supervisory control and data acquisition (SCADA) systems and control centers. State Estimation (SE) ensures the data measurement integrity for power flow, and frequency measurements and Bad Data Detection (BDD) algorithm are applied. SE can reduce measurement noise and detect faulty sensor data. However, Area Control Error (ACE) measurement, an integral part of the AGC algorithm, is vulnerable to integrity attacks due to no estimation mechanism for such measurements. Such underlying vulnerability may significantly degrade system performance under cyber-attacks; false data injection and time delay attacks over the communication channels may mislead the AGC performance, triggering improper actions such as load shedding and even cascading outages.

The Department of Homeland security and the National Institute for Standards and Technology (NIST) recommends Intrusion Detection Systems (IDS) and De-militarized zones to protect the critical infrastructures [4, 5]. Implementing these technologies in Information Technology (IT) is well understood; however, much of what is known about the applicability to the AGC is still anecdotal due to the intrinsic constraints such as stringent timing requirements, non-synchronicity of signals, and other inescapable non-linearities. In addition, the existing diagnosis approaches for attack-resilient algorithms in AGC typically cover measurement noise and other anomalous factors only in state estimation for tie-line power flow and frequency measurements. Recent works focus on a model-based AGC cyber-attack resiliency approach that involves correlating all the required parameters. In [7], Zhang et al. proposed an attack impact evaluation framework by utilizing stochastic system analysis methods to evaluate the statistics of system state variables in the AGC. However, the resilience and detection of cyber-attacks was not the scope of the work. Similar to our work, Tan et al. [6] derived an attack impact model consisting of a series of false data injections and developing an efficient algorithm to detect the attacks. However, the work only considers the consistency between the observed frequency deviation and the predicted frequency deviation and ignores the ACE measurement integrity.

Contributions. Our aim in this paper is to introduce an approach for cyber-attack detection and resiliency in the AGC process: Resiliency refers to the capability of a system to maintain low estimation error under cyber-attacks. In this direction, we propose a state estimation-based detection approach for the AGC system by utilizing prior information based on Gaussian process regression, a non-parametric, Bayesian approach to regression. We use the information to boost state estimation and resiliency and enforce properties about how the algorithm identifies the anomalous measurements. Specifically, our approach utilizes the model-based and

CCS '21, November 15–19, 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8454-4/21/11.
https://doi.org/10.1145/3460120.3485358

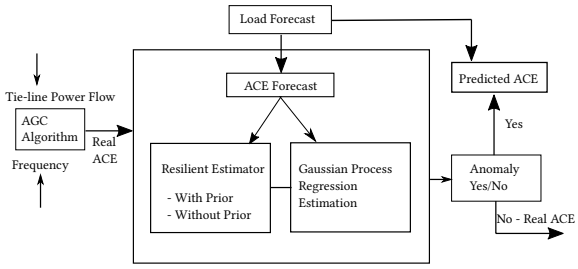

Figure 1: Conceptual resilient control model for AGC.

data-driven algorithm to boost the resiliency and detection performance: Properties of the model-based method and the accuracy of the data-driven method provide further redundancy, which can enhance the overall system performance. To validate our approach, we used the PowerWorld simulator based on the three-area New England IEEE 39-bus model. Furthermore, we also utilized and modified the New England ISO load data for a 3-area power system to create a more realistic dataset.

2 AGC RESILIENCE USING PRIOR INFORMATION

This section presents the AGC model details adopted in this work. Furthermore, we provide the prior model and anomaly detection engine estimation, seeking to correlate between tie-line power flow, frequency, and ACE measurements. Lastly, we present the threat model.

System Model. As in the smart grid AGC literature, we consider a standard electric power AGC system; where the function of the system is to maintain the system frequency at its nominal value, e.g., 60 Hz in North America, and to regulate the net scheduled value of power flow across different BAs. The state variables are represented by the system's tie-line power flow and frequency measurements: The AGC controller computes the ACE using these measurements after receiving them over a communication network. For the i^{th} area, $ACE_i = a_i \cdot P_{E_i} + b_i \cdot f_i$, where P_{E_i} and f_i are the i^{th} area's power export and frequency deviation of the grid, whereas a_i and b_i are the constants. The ACE values are sent to the generators to adjust the primary control loop set-points, and the process is repeated every 2-4 seconds, also referred to as the AGC cycle.

Prior Model. The objective of the prior model is to provide an extra layer of resiliency to the AGC system. We use auxiliary models such as transformer ratings, historical information of generator capacity, statistical characterization of tie-line power flow, frequency, and ACE values to map them with the real-time measurements by building Gaussian process regression with hyper-parameters tuning in the machine learning algorithms and data pre-processing tool known as Weka. Specifically, the prior information and load data are fed into our proposed model to correlate with the forecast values of power flow, frequency, and ACE values.

Anomaly detection Engine Estimation. We now describe how our approach instantiates each of the phases in the cyber-attack detection and resilience architecture. Figure 1 presents a conceptual diagram of our proposed model for the AGC. Throughout the resilient control and detection mechanism, we integrate model-based and data-driven techniques to boost the performance of our proposed approach: We use Gaussian Process for the data-driven scheme for the predicted estimation of the AGC relevant measurements. The final ACE measurement is correlated with the prior information to identify any anomalous measurements throughout the real-time process. If the ACE value does not get to zero due to any frequency fault or cyber-attack, the system utilizes the prior auxiliary information to compute the probability of the error and compare it with the real-time values. For liveness, the framework relies on the sum of two terms: The significant difference between the actual and forecasted values; and the temporal characterization of the control signal to identify the cyber-attacks such as ramp attacks where the adversary gradually deviates the system frequency to conceal the attack.

Threat model. We can envision that an adversary has gained initial access to the communication system via social engineering techniques. Next, an adversary can mount time delay attacks between the controller and actuator to delay control commands. For example, an attacker can compromise a communication path such as a router to delay the control commands. Similarly, adversaries can access remote sensors to mount false data injection attacks on power flow measurements. In this scenario, the attacker tries to provide a wrong perception of the system load. For example, the attacker can trick any area of AGC into believing that the power flow has increased/decreased; the action can cause the incorrect computation of an ACE value sent to the generators. Consequently, the wrong ACE value sent to the generator will falsely ramp up/down the generator. Any of the mentioned scenarios can adversely impact the performance of the AGC system, which can cause generation imbalance and destabilize systems' frequency.

3 EVALUATION - AGC AND SIMULATION SETTINGS

To evaluate our approach, we conduct PowerWorld [2] simulations - an industry-class high-class fidelity simulator – based on the three-area New England IEEE 39-bus model [1]. The complete system contains 10 generators with the same value of nominal power 1000 MVA, 19 loads, and 39 buses. Furthermore, each generator is equipped with 4 second AGC cycle length and Multi-Band Power System Stabilizer (MBPSS). Frequency deviation and the measurement of tie-line active power exchanged are utilized to compute the ACE. Moreover, we collect frequency values locally using a rotor speed deviation of all generators; frequency is a global signal that does not have significant variations throughout the power system, and a rotor speed deviation is equal to a frequency deviation.

To validate our approach, we consider two simulation scenarios: The first is a false data injection to the tine-line power flow measurements in which we increase the power flow values with small magnitude to cause grid frequency fluctuations; in the second scenario, we consider the delay of ACE values to the generators in which we employ the OpenSSL 1.0.1 to mimic a control center

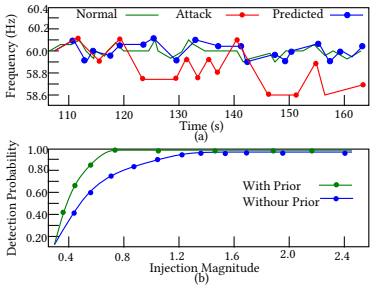

Figure 2: (a) Validating prediction for AGC frequency under false data injection attack. (b) Efficacy of prior information in detection probability.

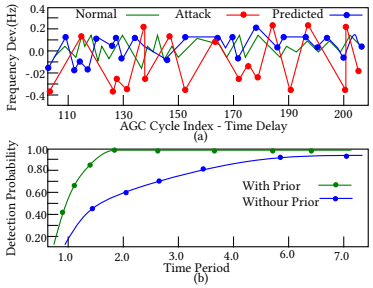

Figure 3: (a) Predicted frequency deviation using the regression model. (b) Impact of prior information on detection probability over time.

and a substation. An SSL session is established every 4 seconds to transmit sensor readings. The simulation of AGC under no attack starts at t = 15s and terminates at t = 340s, and data is collected with a frequency of 0.25, which is equivalent to 4 seconds. The simulation generates zero-mean process and measurement noises as the default settings.

To create a dataset for evaluation, we also utilize the New England ISO load data for a 3-area power system [3]; we modified the load data by adding unavailable line load information from our simulation results. Moreover, we duplicated the data with the simulation results of attack scenarios: The corrupted load data with the standard deviation of 97 was correlated with actual simulation results for the accuracy of the dataset. To reduce the size of the dataset, we used a smaller range of ACE delay attacks. The data is then fed into Gaussian process regression with hyper-parameters tuning in the Weka tool to produce mean and covariance matrix of the corresponding power flow and frequency deviation measurements. Towards this end, auxiliary variables and prior information are fed into the model to correlate the corresponding measurements with the historical values accurately.

Simulation Results. Figure 2 (a) shows the results of our proposed resilient control approach during the false data injection attack on power flow measurements. The horizontal axis is time in seconds, while the vertical axis is the gird's frequency. During the injection attack to power flow and frequency readings, the gird's frequency fluctuates and decreases to a minimum of 58.6 Hz. As seen from the figure, the system's predicted value is closer to the actual values, the performance of the resilient control system clearly suggests an anomaly; therefore, it maintains the system's frequency according to the predicted values using the combination of prior auxiliary information and independent power system attributes. Furthermore, Figure 2 (b) shows the detection probability against the magnitude of the false data injection attack. The results show that resilient control using prior information has a better attack detection probability compared to the results of detecting an attack without utilizing prior information and attributes.

Figure 3 (a) compares the predicted frequency deviation values during the time delay attacks. The algorithm calculates the frequency deviation based on prior information and historical data of local measurement of frequency and tie-line power flow. The prediction improves with an increasing number of AGC cycles; it means there will be more waiting time for the detection of an attack, leading to a longer reaction time to counteract the attack. However, the system remains stable under lower frequency fluctuation in stealthy attacks as it marks the field measurements as anomalous after identifying the attack; this means the accuracy of detection becomes better for the stealthy time delay attack after some AGC cycles. Similarly, Figure 3 (b) compares the detection probability against time. The approach with prior information clearly identifies the attack with a 100 % detection rate in a shorter period than using without prior auxiliary information.

4 CONCLUSION

In this paper, we proposed an approach based on prior information for the AGC cyber-attack detection and resiliency. Specifically, we showed that specific power system attributes in conjunction with prior auxiliary information could improve the system's resiliency against cyber-attacks. To validate our approach, we used the PowerWorld simulator based on the three-area New England IEEE 39-bus model. The results demonstrate that incorporating prior information based on Gaussian process regression can significantly improve the system's resiliency and probability of predicting cyber-attacks correctly. Our future work will aim to investigate the performance of our approach for malicious and natural load disturbances. Moreover, we plan to add more power systems attributes and prior information to evaluate this approach against a wide variety of cyber-attacks.

REFERENCES

[1] 2021. New-England-IEEE-39-bus-system. (2021). https://electricgrids.engr.tamu.edu/
[2] 2021. PowerWorldThe visual approach to electric power systems. (2021). https://www.powerworld.com/
[3] 2021. Pricing Reports. (2021). https://www.iso-ne.com/isoexpress/web/reports/pricing
[4] David Kuipers and Mark Fabro. 2006. *Control systems cyber security: Defense in depth strategies.* Technical Report. Idaho National Laboratory (INL).
[5] Victoria Y Pillitteri and Tanya L Brewer. 2014. Guidelines for smart grid cybersecurity. (2014).
[6] Rui Tan, Hoang Hai Nguyen, Eddy YS Foo, Xinshu Dong, David KY Yau, Zbigniew Kalbarczyk, Ravishankar K Iyer, and Hoay Beng Gooi. 2016. Optimal false data injection attack against automatic generation control in power grids. In *2016 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. 1–10.
[7] Jiangmeng Zhang and Alejandro D Domínguez-García. 2016. On the impact of measurement errors on power system automatic generation control. *IEEE Transactions on Smart Grid* 9, 3 (2016), 1859–1868.