Physics- and Learning-based Detection and Localization of False Data Injections in Automatic Generation Control

Ana Jevtic* Fengli Zhang** Qinghua Li** Marija Ilic*

* Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: ajevtic, ilic@mit.edu)
** University of Arkansas, Fayetteville, AR 72701 (e-mail: fz002, qinghua@uark.edu)

Abstract: In this paper, we propose two complementary methods of detecting False Data Injection (FDI) attacks in Automatic Generation Control (AGC). The first is a physics-based method which relies on Interaction Variables, and is derived by using a more detailed spatial dynamic model of the control area than the currently used Area Control Error (ACE). The second method of detecting FDI attacks in AGC is based on Deep Learning. This method mainly depends on historical data (tie-line flow, and frequency) and ACE data, and employs a Long Short Term Memory (LSTM) neural network to build a model using the available historical data to learn the data patterns, and then predict ACEs through the learned patterns. The performance of both methods is verified through simulations on a 5-bus power system. Our results show that both methods yield high detection accuracy. The physics-based method performs better than the learning-based method, although, at the cost of requiring significantly more noise-free measurements.

Keywords: electric power grid, cyber security, deep learning, attack detection, Automatic Generation Control

1. INTRODUCTION

Automatic Generation Control (AGC) is one of the most critical parts of the operation in today’s power systems. Its main function is to automatically control power generation in response to slow, hard-to-predict area control imbalances. Each control area has its own AGC system, with the task of regulating local area frequency to nominal value (60 Hz in USA), and the exchange of power with the neighboring areas to the values agreed upon during economic dispatch. The net power imbalance is represented as the Area Control Error (ACE). ACE is calculated every 2-4 sec in today’s operation, and is used to change set-points of generator governors participating in AGC every minute so that the ACE crosses zero every 10 minutes. This is known as the A1 performance criteria. When one views effects of adjusting governor set points as a discrete time process driven by disturbances, it can be shown that this process is marginally stable (Ilic and Skantze, 2000). This further implies that cyber-attacks could destabilize the AGC process and cause significant operating problems.

The increasing number of smart devices deployed on demand side and their connectivity to external networks, as well as operation of the grid through corporate networks on generation side, open new doors to malicious intrusions. In this new environment, power systems’ control processes become vulnerable to cyber-attacks, such as False Data Injection (FDI) attacks. Existing methods implemented in Control Centers may no longer be able to provide system reliability, as they rely only on having redundant measurement communication paths and components, used by State Estimator (SE) and Bad Data Detection (BDD) schemes to detect sensor failures. Recent research has shown that these existing methods can be bypassed by a coordinated FDI attack on power systems (Xie et al., 2011). They could potentially lead to the major blackouts created by the “hidden” failures, much the same way as many blackouts in the past were caused by the hidden relay protection malfunctioning (Bae and Thorp, 1999).

In today’s system operation, measurements of local area frequencies and of tie-line power flows are collected in the Control Center. Based on those, AGC calculates and dispatches new set-points to the generators. An FDI attack on tie-line flows and local frequency measurements used by the AGC will cause inaccurate calculation of ACE and, subsequently, wrong adjustment of power generation set-points. This will, in turn, lead to imbalance in the area that will go undetected and might eventually cause cascading failures in the system.

Contributions. In this paper, we propose two methods of detecting FDI attacks on AGC, which are meant to complement one another in order to increase the detection rate. The first is a physics-based method which provides an alternative computation of ACE by using a more detailed model of the control area than is used currently in control centers. To achieve this, we use the notion of

* This material is based upon work supported by the Department of Energy under Award Number DE-OE0000779. Part of this work (the deep learning-based detection method) appeared in our preliminary workshop paper (Zhang and Li, 2017)
Interaction Variables (IntVar), which is derived by using a more detailed spatial dynamic model of the control area. A significant mismatch between the traditional ACE and IntVar-based ACE therefore alerts to the presence of attacks in the system. The second method of detecting FDI attacks in AGC is based on Deep Learning. This method mainly utilizes historical measurements (tie-line flow, and frequency) and ACE data, which are available in most control areas. In this method, we first adopt Long Short Term Memory (LSTM) neural network to build a model with the historical data to learn the data patterns, and then predict ACEs through the learned patterns. A difference between the ACE predictions and real ACE data indicates presence of attacks.

The rest of the paper is organized as follows. The physics-based method of detecting FDI attacks is formulated in Section 2 for general control systems, and in Section 3 for AGC system in power grids. Physics-based localization and mitigation of FDI attacks are described in Section 4. Section 5 describes the deep learning-based approach to detection and localization of FDI attacks. Finally, Section 6 shows numerical results on a small grid.

2. PROBLEM FORMULATION - DETECTION OF FDI ATTACKS IN CONTROL SYSTEMS

We first pose the problem of attack detection for linear dynamic systems, relevant for detection of FDI attacks in AGC. We start by first formulating the problem for general linear time-invariant (LTI) systems with a control input and an exogenous input (disturbance). We consider a system with following dynamics:

\[
\dot{x}(t) = Ax(t) + Bu(t) + Hd(t) \tag{1}
\]

where \(x(t) \in \mathbb{R}^n\) is the vector of state variables, \(u(t) \in \mathbb{R}^k\) is the control input, and \(d(t) \in \mathbb{R}^p\) is the vector of disturbances. Matrices \(A, B,\) and \(H\) are the system matrices of appropriate dimensions. We consider a set of measurements given by a vector \(y(t) = Cx(t)\) collected by field sensors to monitor the system (1). Based on these measurements, a control signal \(u(t)\) is then calculated as

\[
u(t) = f(y) \tag{2}
\]

where \(f(\cdot)\) is a linear function of \(y\).

We assume that an attacker can modify the measurement signal \(y\) by adding a value \(y_a\), so that the measurement received by the controller is:

\[
y^*(t) = y(t) + y_a(t) \tag{3}
\]

If there is no attack on the system, \(y_a\) will be equal to 0. Otherwise, \(y_a \neq 0\), and its value will depend on the type of attack (different types of attacks will be discussed in following sections). The controller will then produce a control signal from the received measurements, based on (2) and (3) as \(u(t) = f(y^*)\).

For a system defined as above, we propose a method of detecting FDI attacks on measurements \(y\).

**Proposition 1.** Consider the control system in (1) that is attacked through the measurements \(y\) as in (3). If there exists a set of measurements \(\bar{y} \neq y\) and a linear function \(g(\cdot)\) such that

\[
g(\bar{y}) = \bar{u}(t) \quad \text{and} \quad \bar{u}(t) = u(t), \forall t
\]

where the asterisk denotes received measurements, and the residual \(r\) satisfies

\[
r = |f(y^*) - g(\bar{y})| > \epsilon
\]

for some threshold \(\epsilon\), then the system in (1) is under an FDI attack.

Section 3.3 will provide an appropriate choice for \(\bar{y}\) and \(g(\cdot)\) for application of this method in power systems.

3. DETECTION OF CYBER-ATTACKS ON AGC IN POWER SYSTEMS

In order to detect attacks on AGC in power systems, we will first introduce the relevant component models, and derive the interconnected system model. Then, we will introduce an alternative method of computing ACE, based on interaction variables. It is reviewed that, in quasi-static operation, the IntVar, much the same as ACE, represents net power imbalance. As such, the two should be the same at the rate AGC is implemented.

3.1 Modeling of power systems divided into control areas

We consider a power system divided into control areas equipped with AGC. We denote the set of control areas by \(\mathcal{A}\), the set of generators participating in AGC by \(\mathcal{G}\), and set of load buses by \(\mathcal{L}\). The cyber-physical architecture of a typical power system with two interconnected control areas is depicted in Figure 1. In this paper, we model the power system dynamics using the structure-preserving load model (Ilic et al., 2010), (Bergen and Hill, 1981) given in (5) in addition to the well-known generator model with governor control (Ilic and Zaborszky, 2000) given in (4). We model the loads explicitly, as the load side is more exposed to the general public through new smart devices, such as smart meters, electric vehicles and other smart appliances connected to the Internet (Campbell, 2015). Thus, the grid model must be expanded to accommodate these new devices that greatly affect the behavior of the system.

We begin with the model of generators with governor control in the interconnected system.

![Fig. 1. Illustration of cyber and physical layers of today’s AGC](image-url)
\[
\begin{align*}
\dot{\omega}_L &= -M_L^{-1}(D_L \omega_L + (P_L - L)) \\
\dot{P}_T &= T_w^{-1}(-P_T + K\alpha) \\
\dot{\alpha} &= T_g^{-1}(-\alpha - \omega_G + \omega^{\text{ref}}) \\
\dot{P} &= B_{bus} \omega - gF
\end{align*}
\]

(4)

State variable \( \omega \in \mathbb{R}^n \) is composed of all bus frequencies, where \( \omega = [\omega_G \omega_L]^T \), and \( P_T \in \mathbb{R}^n \), \( \alpha \in \mathbb{R}^n \) denote mechanical powers and turbine valve positions of the generators, and \( P = [P_G P_L]^T \in \mathbb{R}^n \) are net real power injections at all buses. The control input of the model is the vector of frequency set-points provided by AGC. Using these two component models, a control system can be designed. The state variables \( \omega \) are given by the diagonal matrix \( M_R \), with the elements corresponding to generators that do not participate in AGC set to zero. The generator inertias are given by diagonal matrices \( M_G \in \mathbb{R}^{n_G \times n_G} \), the damping coefficients by \( D_G \in \mathbb{R}^{n_G \times n_G} \), and time constants of the governors and the turbines by \( T_G \in \mathbb{R}^{n_G \times n_G} \) and \( T_p \in \mathbb{R}^{n_G \times n_G} \). Vector of rates of change of tie-line flows is denoted by \( F \in \mathbb{R}^n \), and \( g \in \mathbb{R}^{n \times n} \) indicates connection of tie-lines to each generator bus, where \( n_p \) is the number of tie-lines that connect the given area with its neighbors. Lastly, we assume a lossless system, so matrix \( B_{bus} \in \mathbb{R}^{n \times n} \) is the imaginary part of the admittance matrix of the area.

Unlike the commonly-used impedance loads, the frequency-dependent loads do not get included into a reduced network, and therefore, the network topology is explicitly represented in the interconnected system. Among other benefits, this preserves the sparsity of the system. We represent them as aggregate loads at the substation level with the following dynamical equations:

\[
\dot{\omega}_L = -M_L^{-1}(D_L \omega_L + (P_L - L))
\]

(5)

where the state variables \( \omega_L \in \mathbb{R}^{(n-n_G)} \) represent the frequency of load buses, and \( L \in \mathbb{R}^{(n-n_G)} \) is the vector of actual load consumption of each bus. \( M_L \) and \( D_L \) are nonphysical values that represent inertia and damping coefficients. Using these two component models, a control area \( i \) composed of \( n_G \) generators and \( (n-n_G) \) loads can be represented with a following state space model with states \( x_i = [\omega_i^T P_i^T \alpha_i^T \theta_i^T]^T \in \mathbb{R}^{(n+1)n_G} \) in matrix form (Ilic and Zaborszky, 2000):

\[
\dot{x}_i = A_i x_i + B_i \omega^{\text{ref}} + C_i \dot{E} + H_i L_i, \quad i \in \mathcal{A}
\]

(6)

where \( A_i, B_i \) and \( H_i \) are instances of matrices described below corresponding to an area \( i \), and \( G_i \) is an incidence matrix mapping the connections of tie-lines to each bus:

\[
A = \begin{bmatrix}
-M_i^{-1}D & M_i^{-1}E & M_i^{-1}e_T E^T & -M_i^{-1}T_w^{-1}K_i & 0 & -T_g^{-1}r_i \\
0 & -T_g^{-1}r_i & T_g^{-1}r_i & 0 & 0 & 0 \\
-T_g^{-1}e_T & 0 & -T_g^{-1}r_i & 0 & 0 & 0 \\
B_{bus} & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

\[
B = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}^T
\]

\[
H = [-e_{T_n}^T 0 0 0]^T
\]

3.2 Interaction variable of a control area

**Definition 2.** (Ilic and Zaborszky, 2000) Interaction variable of control area \( i \) is defined as any linear combination of interaction values, \( z^i = T^i x^i, T^i \neq 0 \), such that:

\[
z^i(t) \equiv 0
\]

in the absence of reference signal changes (\( \omega^{\text{ref}} = 0 \)), load disturbances in the area (\( L^i = 0 \)), and interactions with other areas (\( F^i = 0 \)).

From this definition, it is obvious that any dynamics of interaction variable \( z^i \) will be driven externally through interconnections with other areas or set-point changes. The interaction variables are defined for disconnected regions, so they are completely local variables associated with each area. In power systems, the system matrix \( A_i \) of any area \( i \) has inherent structural singularity, as a direct consequence of general power conservation law of the area, so \( T^i \) will always exist. From the definition of interaction variables we have \( z^i \equiv 0 = T^i A_i x, \) so \( T^i \) can be easily found as the left eigenvector of \( A_i \) corresponding to the zero eigenvalue. More specifically, the interaction variable of a lossless system can always be defined as a linear combination of net real power injections of the components in the area (Ilic and Zaborszky, 2000), i.e.

\[
T^i = [0 \ 0 \ldots t^i_p]^T, \quad t^i_p \in \mathbb{R}^{1 \times n} \implies z^i = t^i_p F^i
\]

(7)

A slightly more involved method for deriving \( T^i \) when grid losses are included can be found in the same reference.

To derive the dynamics of the interaction variable \( z^i \) within one cycle of AGC (i.e. \( \omega^{\text{ref}} \) remains constant at zero) for the interconnected area, we combine (6) and (7):

\[
z^i = t^i_p F^i + t^i_p H^i L^i
\]

(8)

Having derived the interaction variable and its dynamic properties, we will use it to develop our detection method for cyber-attacks on AGC.

3.3 Detection of FDI attacks in AGC

Following the problem formulation and notation introduced in Section 2, for a power system equipped with AGC, we will have the disturbance \( d \) as the deviation of load from forecast value, i.e. \( d(t) = L \in \mathbb{R}^{(n-n_G)} \).

Further, \( u(t) = f(y) = \omega^{\text{ref}} \in \mathbb{R}^k \) where \( y \) will represent an ACE signal of area \( i \), and \( k \) is the number of generators participating in AGC. Traditionally, ACE is computed as a linear combination of frequency deviation from the nominal system frequency (60 Hz in USA) and net tie-line flow deviation from scheduled flows:

\[
ACE^i = F^i + \frac{\beta^i}{2\pi} \omega^i, \quad i \in \mathcal{A}
\]

(9)

where \( \omega^i \) and \( F^i \) represent deviations from scheduled values, and \( \beta^i \) is a frequency bias of area \( i \). In today’s AGC, frequency is measured at one location, usually at the location of the Control Center, and is assumed to be uniform throughout the area. Therefore, ACE is a coarse aggregated signal that does not contain any information about the components within the area and of the electrical distances between them.

On the other hand, measurements \( \tilde{y}^i \) will be net power injections at every bus \( P^i \) and an alternative frequency
Finally, we can define the residual from the interconnected system model (6) as all tie-line flows from other areas (which can be seen about the area. This is true because, ultimately, the value measurement \( \bar{\omega} \) to us, and

\[ P_j + T^T P_{jk} + F_j = 0 \]  

Here we denote with \( T \) the incidence matrix of the area, with \( P_{jk} \) power flows to bus \( j \) from buses \( k \) in the same area, and with \( F_j \) the power flow of the tie-line connected to bus \( j \). Since the measurements of \( P_j \) and \( F_j \) are available to us, and \( P_{jk} \)s are functions of them, the equation (11) will be violated in case of a FDI attack on tie-line flow measurements. To accommodate for the losses in the system, another threshold can be introduced, and residuals

\[ r_j = |ACE^i - \bar{\omega}_i| \]

and use the condition in Proposition 1 to detect FDI attacks on AGC when \( r > \epsilon \).

4. LOCALIZATION OF FDI ATTACKS IN AGC

Once an attack is detected using the procedure described in Proposition 1, it would be desirable to know where the attack originated, so that appropriate mitigation procedures can be set in motion. Two possible ways to launch an FDI attack on AGC are either falsifying the frequency measurement at the control center location or the tie-line flow measurements. Therefore, a method is needed to discern between these two possibilities. In normal operation, the collected measurements have to satisfy the power conservation law at every bus. For a lossless system we considered in the rest of this paper, we can write a following equation for each bus \( j \) that has a tie-line incident to it:

\[ P_j + T^T P_{jk} + F_j = 0 \]  

The approach first trains a LSTM model with historical data. It is assumed that all the historical data used in training are collected from normally running power system. If any accident or attack occurs, the corresponding data should not be included in historical data. Then the trained model is used to predict the next several ACEs and compare them with calculated/observed ACEs. In particular, the current ACE data sequence \( \langle ACE_{i-m}, ..., ACE_i \rangle \) is fed into the trained model to do the prediction for next ACE \( ACE_{i+1} \). \( m \) is the length of the input data sequence, which can be adjusted based on the datasets to achieve better prediction results. \( ACE_i \) means the observed ACE data at AGC cycle \( i \). It is found that one predicted ACE is insufficient to detect attacks, since the difference between one predicted ACE and the corresponding observed ACE is small. Thus \( n \) successive ACE predictions are made, and then the distance between the predictions and corresponding observed ACEs are calculated. It implies presence of attacks if the distance is larger than a preset threshold. The detailed steps of the method are shown as follows.

**Step 1**: Predict the next data sequence using the trained model.

\[ ACE_{i-m-1}, ACE_{i-m-2}, ..., ACE_i \rightarrow ACE_{i+1} \]

\[ ACE_{i-m}, ACE_{i-m-1}, ..., ACE_{i+1} \rightarrow ACE_{i+2} \]
Step 2: Use Manhattan Similarity to compute the distance between the predicted sequence and the measurements.

\[ d = \frac{1}{n-1} \sum_{j=1}^{n} |ACE_{i+m+j} - \hat{ACE}_{i+m+j}| \]

Step 3: Compare the distance with the threshold \( \theta \). If it is larger than the threshold \( d > \theta \), it is regarded as attacked data. Otherwise, it is normal data.

5.2 Attack localization

After detecting existence of attacks, it is also needed to know where the attacks come from or which sensor is compromised. The detection method is borrowed to detect abnormal patterns of the measurements used in ACE calculations and thus localize attacks. For each used measurement (e.g., frequency of a control area), an LSTM model is built, and trained with historical data of the measurements. When an attack is detected by the detection model, each measurement’s model will be run to check its pattern. If some measurement’s pattern are detected as abnormal, it means this measurement is under attack.

6. SIMULATION RESULTS

In this section, we will present some numerical examples of the methods proposed in this paper. We have used the 5-bus system (Liu, 1994) shown in Fig 1. In this system, buses 1-3 are generator buses, and 4-5 are load buses. The model of the interconnected system was derived as explained in Section 3.1. As can be seen in Fig 1, the system is divided in two areas, where Area I contains buses 1, 2 and 4, and Area II contains buses 3 and 5.

6.1 Synthetic data generation

In order to generate realistic attack scenarios on AGC, we first simulated the system without any attacks with real load consumption data used at the load buses. That way, realistic ACE patterns were inserted into this synthetic AGC system. We used real time actual load measurements and the load forecast data from two areas in NY-ISO (NY-ISO, 2018), and generated load deviation values for our system by subtracting the forecast values from actual load values. We also scaled the load deviations down to fit the parameters of our small example grid. Then each one of those signals was placed on each of our load buses to simulate the load deviations. We simulated the AGC system, driven by these disturbances - deviations in loads, and generated realistic measurements of frequency, tie-line flows, as well as a realistic ACE signal, to which various FDI attacks can be added easily.

6.2 Attacked data generation

Although both the physics-based method and the deep learning-based method are general approaches, due to the space limitation, our methods are mainly tested on three different attack types: random attack, ramp attack and scale attack, which were proposed in (Huang et al., 2009) and used in (Sridhar and Govindarasu, 2011), (Sridhar and Govindarasu, 2014). These attacks add a value \( y_a(t) \) to measurement \( y(t) \) as discussed in (3). Random attack aims to add a random positive value \( y_a(t) = rand(a,b) \) in a range with lower bound \( a \) and upper bound \( b \) to \( y(t) \) during the attack period; ramp attack modifies measurements gradually by adding \( y_a(t) = \lambda_r \cdot t \) with ramping parameter \( \lambda_r \) in the attack period, and scale attack modifies measurements with \( y_a(t) = \lambda_s \cdot y(t) \) by scaling up or down them with parameter \( \lambda_s \). Since no real attacked data are available, attacked data are generated manually by injecting the three types of attacks into tie-line flow measurements, and ACEs are calculated based on the attacked measurements.

The FDI attacks were injected to tie-line measurements periodically and every injection lasts for 10 cycles. Three different levels of attacks were generated for each attack type: high-level, medium-level and low-level. High-level attacks mean doing more changes on measurements and vice versa. In our generated attack data, on average, one high-level FDI attack changed the ACE value by 2.5%. One medium-level and low-level attack changed ACE value by 2.0% and 1.5%, respectively.

6.3 Performance of physics-based method

In Figure 2 we show the performance of the physics-based method in the presence of ramp, scale and random FDI attacks. For the IntVar-based ACE calculation, the measurements of real power injections on buses 1, 2, and 4 were used, as well as local frequency of generator on bus 2. The threshold (red line) was chosen based on the parameters of the system, and the same value was used for all three scenarios. For the appropriate choice of threshold, the physics-based method of detection is able to detect all attacks whose amplitude is larger than the chosen threshold. In general, the threshold should be chosen such that physical system dynamics do not trigger false alarms.

6.4 Performance of deep learning-based method

The simulation data was split into two parts: 67% as training data and 33% as testing data. The training data was used to train the LSTM model, which has a hidden layer with 100 neurons and an output layer to make the prediction. The tanh activation function is used for the LSTM neurons. Here \( n \) and \( m \) are both set as 5 which means we use 5 cycles’ data to do one prediction and do attack detection on a 5-data sequence. \( \theta \) was set as 0.005 where the False Positive (FP) detection rate, which is defined as the fraction of normal data sequences falsely detected as attacked data, is 1.27%.

The attack detection accuracy is shown in Figure 3. It shows that the method performs better on higher level attacks and all the detection rates are above 90%. The detection accuracy of low-level random attacks, ramp attacks, and scale attacks are 92.6%, 95.1% and 96.3% respectively. Figure 4 describes the localization accuracy which means the percentage of the attacks that can be localized correctly. The results show that most of the attacks (more than 92%) can be localized. The accuracy for high-level attacks is over 98%.
7. CONCLUDING REMARKS

Two complementary methods of detecting FDI attacks on AGC, a physics-based method which relies on Interaction Variables and a deep-learning based method are proposed in this paper. The physics-based method relies on an alternative procedure for computing the ACE by using Interaction Variables (IntVar). The deep-learning based method relies on historical measurements (tie-line flow, and frequency) and ACE data, and exploits a Long Short Term Memory (LSTM) neural network to build a model using the available historical data to learn the data’s patterns, and then predict ACEs through the learned patterns. We evaluate the performance of both methods through numerical simulations on a 5-bus power systems where we show that both methods yield high detection accuracy.

REFERENCES

Bae, K. and Thorp, J.S. (1999). A stochastic study of hidden failures in power system protection. Decision Support Systems, 24(3-4), 259–268.
Bergen, A.R. and Hill, D.J. (1981). Structure preserving model for power system stability analysis. IEEE Trans. Power Appar. Syst.
Campbell, R.J. (2015). Cybersecurity issues for the bulk power system. Technical report, Congressional Research Service Report.
Hochreiter, S. and Schmidhuber, J. (1997). Long short-term memory. Neural computation, 9(8), 1735–1780.
Huang, Y.L., Cardenas, A.A., Amin, S., Lin, Z.S., Tsai, H.Y., and Sastry, S. (2009). Understanding the physical and economic consequences of attacks on control systems. International Journal of Critical Infrastructure Protection, 2(3), 73–83.
Ilic, M.D. and Skantze, P. (2000). Electric power systems operation by decision and control, the case revisited. IEEE Control Systems, 20(4), 25–39.
Ilic, M.D., Xie, L., Khan, U.A., and Moura, J.M.F. (2010). Modeling of future cyber-physical energy systems for distributed sensing and control. IEEE Transactions on Systems, Man and Cybernetics: Part A.
Ilic, M.D. and Zaborszky, J. (2000). Dynamics and Control of Large Electric Power Systems. John Wiley & Sons, Inc.
Liu, X.Z. (1994). Structural modeling and hierarchical control of large-scale electric power systems. Ph.D. thesis, MIT.
NY-ISO (2018). Real-time actual load data reports. URL http://www.nyiso.com/public/markets_operations.
Sridhar, S. and Govindarasu, M. (2014). Model-based attack detection and mitigation for automatic generation control. IEEE Transactions on Smart Grid, 5(2), 580–591.
Sridhar, S. and Manimaran, G. (2011). Data integrity attack and its impacts on voltage control loop in power grid. In Power and Energy Society General Meeting, 2011 IEEE, 1–6. IEEE.
Tan, R., Nguyen, H.H., Foo, E.Y., Yau, D.K., Kalbarezky, Z., Iyer, R.K., and Gooi, H.B. (2017). Modeling and mitigating impact of false data injection attacks on automatic generation control. IEEE Transactions on Information Forensics and Security, 12(7), 1609–1624.
Xie, L., Mo, Y., and Sinopoli, B. (2011). Integrity data attacks in power market operations. IEEE Transactions on Smart Grid, 2(4).
Zhang, F. and Li, Q. (2017). Deep learning-based data forgery detection in automatic generation control. In International Workshop on Cyber-Physical Systems Security (CPS-Sec).