On the Failure of Power System Automatic Generation Control due to Measurement Noise

Jiangmeng Zhang and Alejandro. D. Domínguez-García
University of Illinois at Urbana-Champaign Urbana, Illinois 61801
Email: {jzhang67, aledan}@illinois.edu

***Abstract*—This paper discusses a class of measurement noise that has the potential to destabilize power systems with automatic generation control (AGC). AGC is responsible for maintaining nominal frequency and interchange power between balancing areas as scheduled. The results in this paper show that AGC is robust to measurement white noise. However, when the intensity of the measurement noise depends on the system state, the AGC system fails to meet its performance requirements. The measurement noise is modeled as a stochastic process, while the overall power system dynamic behavior is described by a stochastic differential equation (SDE) model. The impact of measurement noise is evaluated through a set of differential equations describing the evolution of the statistics of the system states, which are derived from the SDE model. Mitigation strategies to address this problem are also discussed.**

I. Introduction

Information technology (IT) systems are increasingly being incorporated into power systems as a result of visions such as the US Department of Energy *Smart Grid*. As a consequence, there is a tighter coupling between physical and cyber components, which raises new challenges in power system operations. There is a concern that if the interaction of cyber and physical components is not clearly understood, the electric grid could become more vulnerable to failures in both cyber and physical components, and intentional attacks on the cyber components. Automatic generation control (AGC), as the only system-level automatic closed-loop control system over the IT infrastructure of a power system [1], is sensitive to such cyber events, which, in turn, would influence power system performance. The AGC system takes as inputs measurements of: (i) the power system frequency, (ii) the real interchange power between balancing authority (BA) areas, and (iii) the generation profile of units online; and sends out control signals to the generators through the IT infrastructure. The processing algorithms in AGC aim at regulating the system frequency, and maintaining the interchange power to scheduled values.

The AGC system algorithms are part of the Supervisory Control and Data Acquisition (SCADA) system that resides in a centralized location (typically a control center). However, due to the lack of authentication capabilities in SCADA communication protocols, it is possible for adversaries to manipulate sensor measurements, inject false control commands, develop denial of service attacks, and resort to other malicious actions [2]. Various false data detection techniques based on state estimation (SE) have been developed [3]. Following this line of work, false date injection attacks against SE [4] (and its countermeasures [5]) have been widely investigated. However, as one of the inputs to AGC, the integrity of frequency measurements is difficult to assure due to the fact that steady-state operation is assumed when conducting state estimation, and the frequency is not included in SE. Alternatively, the measurements provided by synchrophasor measurement units (PMUs) in the Wide-Area Measurement System (WAMS)—an advanced infrastructure that complements the SCADA system—can also be used as inputs to the AGC system [6]. However, some work in the literature have demonstrated the feasibility of manipulating PMU measurements by spoofing the clocks that they use for synchronization [7].

Apart from malicious manipulations to measurements, noise in the communication channel, as another contributor to measurement uncertainty, cannot be avoided. In [8], we proposed a framework to evaluate the impact of measurements noise on power system dynamic performance. In this paper, we adopt the same stochastic differential equation (SDE) framework that we proposed in [8] to model the power system dynamics as well as the AGC system, and utilize it to calculate the statistics of system state variables, such as frequency, when measurements are corrupted by noise. The results demonstrate that AGC is robust to additive, fixed-intensity, white noise imposed on the measurements. However, we also show that a class of measurement noise, where the intensity of the noise affecting the measurements is a function of the system state, may cause system instability. To analyze its impact on power system dynamic performance, the noise model is formulated and incorporated into the aforementioned framework. We find that the mean of the system states are not affected. However, by properly choosing the intensity factors, the evolution equations on the second moments of the system state deviation (from its nominal value) become unstable, meaning that the second moments of the system state would diverge if no mitigation actions are performed. The purpose of this paper is to raise the awareness of the importance of measurement integrity, and the integration of the WAMS with the SCADA system so as to ensure the integrity of the measurements used by the AGC system.

II. Modeling Framework

In this section, we present the modeling framework, which includes the canonical power system electromechanical nonlinear differential algebraic equation (DAE) model with AGC, and the measurement model, including the effect of random noise. Then, we linearize the DAE model around the nominal trajectory to obtain a linear stochastic differential equation (SDE) model.

A. Power System Model with AGC

The electromechanical behavior of a power system can be described by a set of differential algebraic equations (DAEs) of the form (see, e.g., [9]):

$$\begin{aligned} \dot{x} &= f(x, y, u), && (1) \\ 0 &= g(x, y), && (2) \end{aligned}$$

where $x \in \mathbb{R}^n$ contains the dynamic states of synchronous generators, including rotor electrical angular position, angular velocity and mechanical torque; $y \in \mathbb{R}^m$ denotes the system algebraic states, including bus voltage magnitudes and angles; $u \in \mathbb{R}^l$ includes the generator set points; $f : \mathbb{R}^{n+m+l} \mapsto \mathbb{R}^n$ describes the evolution of the dynamic states; and $g : \mathbb{R}^{n+m} \mapsto \mathbb{R}^m$ describes the power flow equations.

The generator set point vector u can be determined by the secondary frequency control mechanism, i.e., AGC. The AGC system takes the measurements of the BA area frequency, real interchange power between BA areas and the generators' output; calculates the area control error (ACE); and determines the generator set points. The AGC system dynamics can be described by

$$\begin{aligned} \dot{z} &= h_1(\gamma, z), && (3) \\ u &= k(z), && (4) \end{aligned}$$

where $z \in \mathbb{R}^p$ represents the states involved in AGC; $\gamma \in \mathbb{R}^q$ indicates the measurements serving as inputs to the AGC system; $h_1 : \mathbb{R}^{p+q} \mapsto \mathbb{R}^p$ describes the evolution of z; and $k : \mathbb{R}^p \mapsto \mathbb{R}^l$ describes how the generator set point vector u is determined based on a set of participation factors [8].

B. Measurement Model

The actual values of the measurements used as inputs to the AGC system are evaluated as a function of the synchronous generator dynamic states x, and the system algebraic states y. Note that the derivative of bus voltage angles may appear when calculating the BA area frequency. However by using (1)-(2), the derivative of y can be expressed as a function of x and y. The noise affecting a particular measurement is assumed to be a white Gaussian process. Thus, the measurement model can be described by

$$\gamma = h_2(x, y) + \eta\dot{w}, \tag{5}$$

where $\eta \in \mathbb{R}^q$ with one nonzero element corresponding to the affected measurement and representing the intensity of the noise, and w is a Wiener process. The validity of (5) lies in the fact that White noise can be viewed as the generalized mean-square derivative of the Wiener process [10].

C. Linearization

Assuming the augmented DAE system in (1)-(5) evolves from a set of initial conditions with no measurement noise (i.e., $\eta = 0$), a nominal trajectory $(x^*, y^*, z^*, \gamma^*, u^*)$ results. Let $x(t) = x^*(t) + \Delta x(t)$, $y(t) = y^*(t) + \Delta y(t)$, $z(t) = z^*(t) + \Delta z(t)$, $u(t) = u^*(t) + \Delta u(t)$, $\gamma(t) = \gamma^*(t) + \Delta\gamma(t)$, where Δx, Δy, Δz, $\Delta\gamma$, and Δu appear as a consequence of the measurement noise vector η. Assume that Δx, Δy, Δz, $\Delta\gamma$, and Δu are sufficiently small. Linearizing (1)-(5) around the nominal trajectory $(x^*, y^*, z^*, \gamma^*, u^*)$, we obtain a set of linear DAEs of the form

$$\begin{aligned} \Delta\dot{x} &= A_1(t)\Delta x + A_2(t)\Delta y + A_3(t)\Delta u, && (6) \\ \Delta\dot{z} &= A_4(t)\Delta\gamma + A_5(t)\Delta z, && (7) \\ \Delta\gamma &= A_6(t)\Delta x + A_7(t)\Delta y + \eta\dot{w}, && (8) \\ \Delta u &= A_8(t)\Delta z, && (9) \\ 0 &= C_1(t)\Delta x + C_2(t)\Delta y, && (10) \end{aligned}$$

where $A_1(t)$–$A_8(t)$, $C_1(t)$, and $C_2(t)$ are matrices obtained from the partial derivatives of the functions f, g, h_1, h_2, and k evaluated along the nominal trajectory. In subsequent developments, we drop the dependence on t for notational convenience.

Assuming C_2 is invertible and substituting Δy, $\Delta\gamma$ and Δu into (6)-(7), we obtain a stochastic differential equation (SDE) of the form

$$\dot{X} = AX + B\eta\dot{w}, \tag{11}$$

where $X = [\Delta x^T, \Delta z^T]^T \in \mathbb{R}^{n+p}$; A and B are defined as

$$A = \begin{bmatrix} A_1 - A_2C_1C_2^{-1} & A_3A_8 \\ A_4A_6 - A_4A_1C_1C_2^{-1} & A_5 \end{bmatrix}, B = \begin{bmatrix} 0_{n\times q} \\ A_4 \end{bmatrix}.$$

III. Assessing the Impact of Measurement Noise

In this section, we introduce the assessment method to quantify the impact of measurement noise on power system dynamics. The impact of standard white noise, and state-dependent intensity noise in one measurement is investigated. The extension to multiple state-dependent measurement noise is also discussed.

A. Dynkin's Formula

By using the system model described in (11), we can evaluate the impact of measurement noise on system performance; to this end, we can use Dynkin's formula (see, e.g., [10]). Let a function $\psi : \mathbb{R}^{n+p} \mapsto \mathbb{R}$ be twice continuously differentiable; then, Dynkin's formula states that

$$\frac{d\mathbb{E}[\psi(X)]}{dt} = \mathbb{E}[(L\psi)(X)], \tag{12}$$

where $\mathbb{E}[\cdot]$ is the expectation operator, and the operator $\psi \mapsto L\psi$ is called the generator of the system and is defined as

$$(L\psi)(X) := \frac{\partial\psi(X)}{\partial X}AX + \frac{1}{2}\mathrm{Tr}(B\eta\frac{\partial^2\psi(X)}{\partial X^2}\eta^T B^T). \tag{13}$$

Therefore, a set of ODEs governing the evolution of states' statistics can be obtained by properly choosing the function ψ; the idea is illustrated next.

B. The Impact of White Noise

For non-state-dependent white noise in the measurement, we set η to be a constant. Then, according to Dynkin's formula, as stated in (12)-(13), the first and second moments of system states in (11) evolve according to

$$\begin{aligned} \frac{d\mathbb{E}[X]}{dt} &= A\mathbb{E}[X], && (14) \\ \frac{d\Sigma}{dt} &= A\Sigma + \Sigma A^T + B\eta\eta^T B^T, && (15) \end{aligned}$$

where $\Sigma = \mathbb{E}[XX^T]$. Assume that the original system without measurement noise is stable, meaning that the real part of all the eigenvalues of A is negative. Then, (14) shows that the mean of X is not affected by the measurement noise and will converge to zero as $t \to \infty$. Letting the left-hand side in (15) be zero results in a Lyapunov equation. Since the matrix $B\eta\eta^T B^T$ is symmetric and positive definite, the Lyapunov stability theorem guarantees that there exists a positive definite matrix Σ satisfying this Lyapunov equation [11], meaning that the steady-state covariance of the state vector exists and is finite. However, a class of measurement noise, where the intensity of the noise affecting the measurements is a function of the system state, may result in (15) not having a positive definite solution, which means that the system would become unstable as we discuss next.

C. Impact of Random Noise with State-Dependent Intensity

Here, we show that state-dependent noise affecting one measurement will cause instability of the system state covariance matrix, which means that the system trajectory will diverge from the nominal trajectory for every realized sample path. As discussed in the previous section, AGC, as a closed-loop control system, is robust to standard white noise. However, if the intensity of the noise affecting the measurements is a function of the system state, it is possible to destabilize the system in (15). In the measurement model in (5), we construct the nonzero element of η as $\alpha[h_2(x, y) - h_2(x^*, y^*)]$. By linearization and substitution using (10), we obtain that

$$\eta = \alpha H X, \tag{16}$$

where $\alpha \in \mathbb{R}$ and the elements of $H \in \mathbb{R}^{q\times(n+p)}$ are zero except one row corresponding to the affected measurement. The system in (11) becomes

$$\dot{X} = AX + \alpha BHX\dot{w} = AX + \alpha\hat{B}X\dot{w}, \tag{17}$$

where $\hat{B} \in \mathbb{R}^{(n+p)\times(n+p)}$ equals BH.

According to Dynkin's formula in (12), the evolution equations for the first and second moments of the system states are now given by

$$\frac{d\mathbb{E}[X]}{dt} = A\mathbb{E}[X], \tag{18}$$

$$\frac{d\Sigma}{dt} = A\Sigma + \Sigma A^T + \alpha^2\hat{B}\Sigma\hat{B}^T. \tag{19}$$

In this case, it is possible that system in (19) becomes unstable due to the state-dependent noise term.

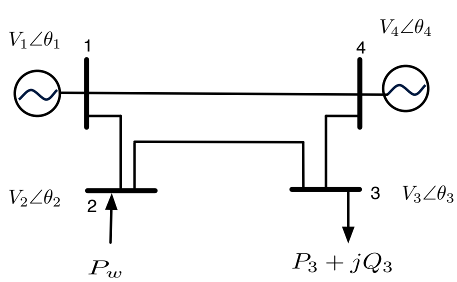


Figure 1: 4-bus 2-machine system [8].

In order to find the value of α that makes (19) unstable, we rearrange the entries of the matrix Σ into a vector Φ. To this end, denote the ith row of Σ by Σ_i; then $\Phi = [\Sigma_1\Sigma_2\cdots\Sigma_{n+p}]^T$. Thus, we can rewrite (19) as

$$\frac{d\Phi}{dt} = D\Phi, \tag{20}$$

where the elements in D are defined using Kronecker algebra, and depend on α, A, and $\hat{B}$. By properly choosing α, it is possible to make some of the eigenvalues of D positive, which would make the system in (20) unstable. Note that, at this point, even though the system state mean is still stable, the system state covariance becomes unstable. Eventually, this causes the divergence of the system states in each realized sample path.

D. Extension: multiple measurement noise

The above formulation analyzes the impact of one measurement noise; this can be easily generalized to the case where more than one measurement is affected. To this end, the measurement model in (5) can be generalized as follows:

$$\gamma = h_2(x, y) + \sum_{i=1}^{r} \eta_i\dot{w}_i, \tag{21}$$

where $r \leq q$ is the number of measurements of interest with random noise and w_i's are a set of independent Wiener processes. Subsequently, (19) becomes

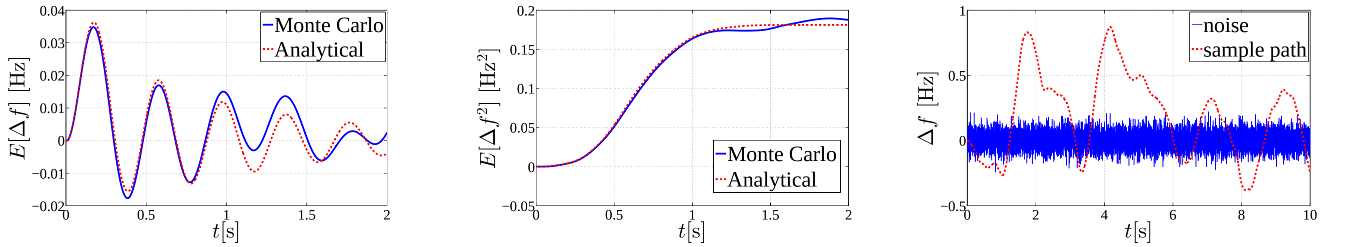
$$\frac{d\Sigma}{dt} = A\Sigma + \Sigma A^T + \sum_{i=1}^{r} \alpha_i^2\hat{B}_i\Sigma\hat{B}_i^T. \tag{22}$$

Now, the matrix D in (20) is determined based on the noise intensity factors, i.e., the α_i's. Multiple measurement noise tends to cause significant influence on the system performance with relatively small intensity factors, as illustrated next.

IV. Numerical Example

In this section, we illustrate the ideas described in the previous section by using the 4-bus power system depicted in Fig. 1. This power system model consists of two synchronous generators, one renewable generation unit and one load. A complete list of its dynamic and static parameters, as well as the AGC parameters can be found in [8]. The dynamics of each synchronous machine is described by a third-order model that captures the governor dynamics and the mechanical equations of motion [12]; we choose the angle of machine 1 as the reference angle. Thus, there are 5 dynamic states associated with the synchronous machines, and 1 state for the AGC system. Without loss of generality, the AGC system takes measurements of the frequencies and power output of machine 1 and 2. Therefore, in this system, $n = 5$, $p = 1$, and $q = 4$. As expected, all the eigenvalues of the matrix A for this system have negative real parts.

First, we consider the frequency measurement of machine 1. As a comparison, we first model the noise as white noise with fixed intensity, meaning that η is a constant vector as discussed in Section III-B. In this case, all the entries of η are zero except for the first one, which is $\eta_1 = 12.56$. The mean



(a) Mean value of frequency deviation.

(b) Second Moment of frequency deviation.

(c) One sample path of frequency deviation and imposed noise.

Figure 2: Fixed intensity noise in frequency measurement on machine 1.

and second moment of the frequency variation are depicted in Figures 2(a) and 2(b). The results obtained from Monte Carlo simulations, depicted with a solid line, match with those obtained by analytical method, i.e., Dynkin's formula, depicted with a dashed line; this demonstrates the validity of the analytical method. Consistent with the discussion in Section III-A, the variance of frequency deviation converges to $0.18\,\mathrm{Hz}^2$, which agrees with the results obtained by solving (15). The frequency variation of one arbitrary sample path obtained using the nonlinear model in (1)-(5), as well as the imposed noise, are depicted in Fig. 2(c), which illustrates that the measurement noise affects the system performance and, at the same time, AGC is able to limit the influence to an acceptable margin.

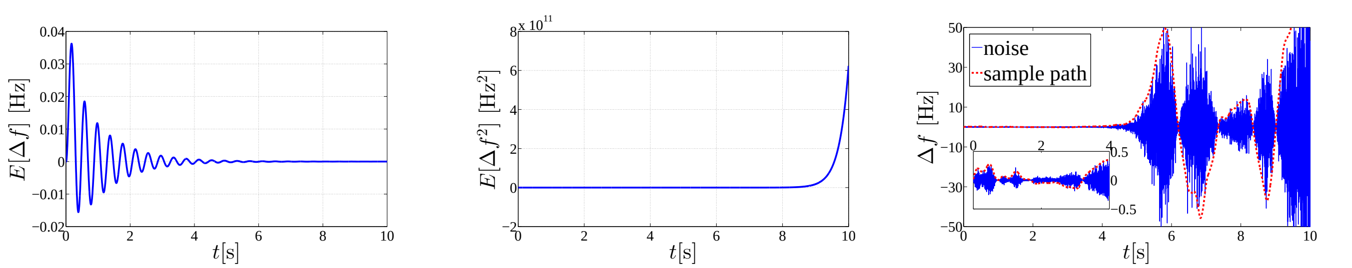
Now, we consider the random noise described in Section III-C. In this case, H in (16) is a 4×6 matrix with all elements being zero except the first row, which corresponds to the first measurement, i.e., the frequency measurement. The value of α is set to be 12.56 so that matrix D in (20) has a positive eigenvalue. For the sample path in Fig. 3(c) obtained from one Monte Carlo simulation using the nonlinear model, we can observe that the values of the added noise processes are in the same order of the frequency variation. Note that other control mechanisms will be certainly triggered before the system frequency variation becomes larger than a certain threshold; however, the added noise causes the system performance to degrade significantly. Furthermore, the response of other control and protection mechanisms, e.g., under-frequency or over-frequency protection relays, may lead to load shedding, and generator tripping.

Similarly, we investigate the impact of the noise in the frequency measurement of machine 2. The mean and second moment, as well as a sample path of the frequency variation are shown in Fig. 4. Comparing Fig. 3 and 4, one can observe that the added noise does not affect the mean of the system states; however, it affects the second moment and any realized sample path. Now, we look at the impact of the random noise in the frequency measurements of two machines. Following the formulae in (21)-(22), we set $\alpha_1 = \alpha_2 = 6.28$, which make one of the eigenvalues of D positive. One sample path of the frequency variation is plotted in Fig. 5. Note that in this case, the random noise with smaller intensity in each measurement, compared to the case where a single measurement noise is considered, causes system instability.

V. Mitigation Strategies

The severe impact of measurement noise demonstrated in this paper highlights the importance of measurement integrity in AGC systems. There are two approaches to maintain measurement integrity. The first one is to ensure the measurement quality and protect measurements from being manipulated. The second one is to develop bad data detection algorithms to eliminate bad data.

In regards to the first approach, i.e., measurement integrity protection, both the processes of measuring and transmitting the values of system variables need to be considered. For example, the GPS clock is a crucial element in both traditional time/frequency devices and PMUs to measure the system frequency. Various techniques against GPS spoofing have been discussed (see, e.g., [7] and the reference therein). The

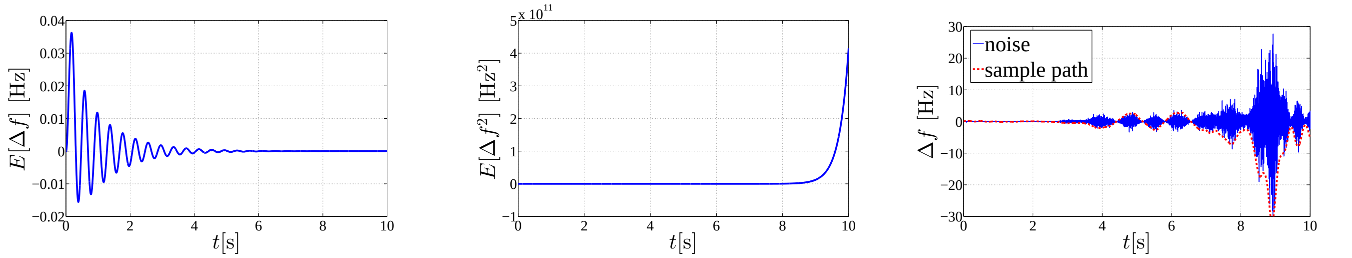


(a) One sample path of frequency deviation and imposed noise.

(b) Mean value of frequency deviation.

(c) Second Moment of frequency deviation.

Figure 3: Various intensity noise in frequency measurement on machine 1.



(a) Mean value of frequency deviation.

(b) Second Moment of frequency deviation.

(c) One sample path of frequency deviation and imposed noise.

Figure 4: Various intensity noise in frequency measurement on machine 2.

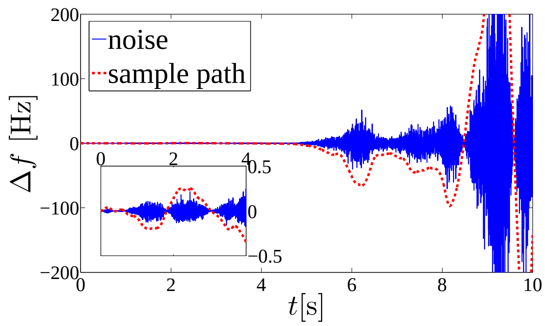


Figure 5: Various intensity noise in both frequency measurements.

security of the communication channel has also been highly addressed in a large amount of recent literature (see, e.g., [2] and the references therein). For instance, in the Critical Infrastructure Protection (CIP) Standards, the National Electric Reliability Council (NERC) has regulated critical cyber assets to be protected within an electronic security perimeter [2]. In addition, IEEE Std 1815-2012, as a new standard for the distributed network protocol in SCADA systems, includes secure authentication features and is capable of using public-key infrastructure [13].

Second, although it is difficult to ensure integrity of the system frequency measurement used by the SCADA system, bad measurements due to natural noise, unintentional failures or malicious actions can be detected by integrating measurements provided by the WAMS into the SCADA system. One intuitive way is to compare the frequency measurement from the SCADA system and that provided by PMUs. But when there exists discrepancy, it is difficult to assess which of the two measurements is incorrect. To address this issue, we utilize the fact that PMUs measure frequencies based on the values of voltage angles, the integrity of which can be detected via state estimation using SCADA measurements. In other words, PMUs couple together the frequency measurements and other variables used in state estimation. If the frequency measurement from a PMU is offset, the voltage angle measurement will also be inaccurate, which can be directly detected through the bad data detection algorithms in the state estimator [3]. Finally, the state-dependent noise described in this paper, which causes large mismatch with the actual values, would be easily detected if SCADA and WAMS systems are integrated.

VI. Concluding Remarks

The AGC system plays an essential role in maintaining satisfactory performance of a power system. We have shown that AGC is robust to additive, fixed intensity, white noise imposed on the measurements that the AGC system uses as inputs. However, we have shown that the class of random noise with state-dependent intensity will destabilize the ODE system that governs the evolution of the second moments of the system states, and subsequently cause divergence of the power system states for any realized sample paths. Mitigation strategies from the perspective of data protection and bad data detection have been discussed; further analysis on defense techniques is part of ongoing research.

References

[1] P. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. of IEEE Conference on Decision and Control*, 2010, pp. 5973–5978.

[2] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *eCrime Researchers Summit*, 2010, pp. 1–9.

[3] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 329–337, 1975.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM Conference on Computer and Communications Security*, 2009, pp. 21–32.

[5] R. Bobba, K. Rogers, Q. Qang, H. Khurana, K. Nahrstedt, and T. J. Oberbye, "Detecting false data injection attacks on dc state estimation," in *Proc. of Workshop on Secure Control Systems*, 2010.

[6] A. Chakrabortty and P. Khargonekar, "Introduction to wide-area control of power systems," in *Proc. of American Control Conference*, 2013, pp. 6758–6770.

[7] X. Jiang, J. Zhang, B. Harding, J. Makela, and A. Dominguez-Garcia, "Spoofing gps receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.

[8] D. Apostolopoulou, Y. Chen, J. Zhang, A. Dominguez-Garcia, and P. Sauer, "Effects of various uncertainty sources on automatic generation control systems," in *Proc. of Bulk Power System Dynamics and Control*, 2013, pp. 1–6.

[9] Y. Chen and A. Dominguez-Garcia, "A method to study the effect of renewable resource variability on power system dynamics," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 1978–1989, 2012.

[10] B. Øksendal, *Stochastic Differential Equations: An Introduction with Applications*. U.S. Government Printing Office, 2003.

[11] H. Khalil, *Nonlinear Systems*. Prentice Hall PTR, 2002.

[12] A. D. Domínguez-García, *Models for Impact Assessment of Wind-Based Power Generation on Frequency Control*. in Control and Optimization Methods for Electric Smart Grids, Power Electronics and Power Systems, M. Ilić and A. Chakrabortty, Springer, 2012.

[13] "IEEE standard for electric power systems communications-distributed network protocol (dnp3)," *IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010)*, pp. 1–821, 2012.