Combating False Data Injection Attacks in Smart Grid Using Kalman Filter

Kebina Manandhar
Dept. of Computer Science
Georgia State University
Email: kmanandhar1@cs.gsu.edu

Xiaojun Cao
Dept. of Computer Science
Georgia State University
Email: cao@cs.gsu.edu

Fei Hu
Dept. of Electrical and Computer Engineering
University of Alabama
Email: fei@eng.ua.edu

Yao Liu
Dept. of Computer Science and Engineering
University of South Florida
Email: yliu@cse.usf.edu

***Abstract*—The security of Smart Grid, being one of the very important aspects of the Smart Grid system, is studied in this paper. We first discuss different pitfalls in the security of the Smart Grid system considering the communication infrastructure among the sensors, actuators, and control systems. Following that, we derive a mathematical model of the system and propose a robust security framework for power grid. To effectively estimate the variables of a wide range of state processes in the model, we adopt Kalman Filter in the framework. The Kalman Filter estimates and system readings are then fed into the χ^2-square detectors and the proposed Euclidean detectors, which can detect various attacks and faults in the power system including False Data Injection Attacks. The χ^2-detector is a proven-effective exploratory method used with Kalman Filter for the measurement of the relationship between dependent variables and a series of predictor variables. The χ^2-detector can detect system faults/attacks such as replay and DoS attacks. However, the study shows that the χ^2-detector detectors are unable to detect statistically derived False Data Injection Attacks while the Euclidean distance metrics can identify such sophisticated injection attacks.**

I. Introduction

As one of the important infrastructural backbones, the secluded power grid system is gradually being transformed into a smart Cyber Physical System (CPS) having more embedded intelligence and networking capability. In such a Smart Grid system, cyber and physical components work in a complex co-ordination to provide better performance and stability. In specific, the Smart Grid is equipped with many sensors to monitor various aspects of the grid such as the meter and voltage fluctuations. The collected information from the sensor networks can then help providing feedbacks or control commands to the physical power grid devices. Hence, it involves a two-way communication between the controller system and the physical components. The Smart Grid system incorporates the traditional security measures (e.g., intrusion detection and firewall) to prevent rudimentary attacks in traditional data networks. Most of the study in literature revolves around the security of data communication from the physical components to the central controller or among different elements (e.g., sensors and actuators) (e.g. [1–4]). The security measures discussed in these studies use the rudimentary techniques such as intrusion detection [1], cryptography and authentication [2][3], defense against network analysis [4], physical layer security enhancement, and the utilization of recommendation based social network infrastructure. These papers on the security of data communication in Smart Grid, can roughly be categorized into three groups. The work in the first category deals mostly with the wired/wireless networking security among cyber components in the Smart Grid [1–4]. The papers in the second category are concerned with the early detection of anomalies in the system. Smart Grid is a real time system and faults/attacks must be handled as soon as possible, the early anomaly detection schemes can pro-actively protect the system [5][6]. The work in the third category applies the control theories in the security process using various state estimation and detection techniques [7] [8] [9].

An attack/fault in the Smart Grid system is always reflected in the form of change in either voltage, current or phase, hence the work in [7] proposed a control-theoretic adaptation framework for the system level security of Smart Grid. The control-theoretic framework uses the state estimation technique to estimate the data from the remote terminal units and applies power security analysis tools to detect attack on the system. Similarly, the protection for the set of meter measurements was discussed in [8] [9].

As stated in [4], the existing security approaches are either i) not viable; ii) or incompatible with Smart Grid; iii) or not appropriately scalable; iv) or not adequate. Particularly, the existing techniques did not address the new class of attack called False Data Injection Attack [10]. This type of injection attack is undetectable by detectors used in the existing state-estimation security frameworks [10],[11]. Hence, this work presents a framework, based on a state space model derived from the voltage flow equations, to defend different types of attacks and faults including the False Data Injection Attack. In addition, we show that the False Data Injection attack cannot be detected using a traditional combination of estimator

978-1-4799-2358-8/14/$31.00 ©2014 IEEE

and detector (i.e., KF and χ^2-detector). Then, we propose a different detector based on Euclidean distance metric to detect the complicated False Data Injection Attack on the power grid system.

The rest of the paper is organized as follows. Section II describes the proposed framework, then derives the mathematical model of the power grid system and discusses the Kalman Filter estimator in the proposed framework. Section III presents the two detectors implemented in the framework in order to detect various attacks and failures in the system. In Section IV, performance results of the proposed framework and the observations are discussed. Finally, Section V presents the conclusion and future work.

II. Proposed Framework For Smart Grid using Kalman Filter

In this section, we present a security framework for Smart Grid which can detect various attacks including random attack, replay attack and DoS attack along with the powerful False Data Injection Attack on the power system. The framework utilizes Kalman Filter estimators to estimate state variables.

To apply the Kalman Filter (KF) technique, we have to develop a state space model (as to shown in next section) from the 3-phase sinusoidal voltage equations. The Kalman Filter model estimates the values for the state variables based on the reports from the numerous sensor readings and the past state values. Without loss of generality, we assume the use of voltage sensors to measure the state variables (amplitude and phase of the voltage) in the framework. As stated in [12], the sampling rate for the sensors should be around 16 samples per 60 Hz cycle, i.e. about 960 samples per second for medium to low data rate production. Now, the estimated values generated by KF and the observed values for the state variables are fed into the detector as shown in Figure 1. The detector compares the two state vectors (including all the state variables) and if the two differ from each other significantly, when the difference is above a certain precomputed threshold, the detector triggers an alarm to signify a possible attack on the Smart Grid. As the literature study shows, the χ^2-detector is a typical choice for the Kalman Filter estimators [13] when the residue of the KF equations follows gaussian distribution and g(t), (as in Equation (17, in Section III-A)) follows the χ^2 distribution [11]. However, False Data Injection Attacks can bypass such detectors and may remain undetected [11]. Hence, we propose to use an additional detector, based on the euclidean distance, along with χ^2-detector. The Euclidean distance detector reconstructs the sinusoidal voltage signal from the state parameters and calculates the difference between the estimated and observed voltage signals. If the difference is larger than a precomputed threshold, the detector triggers an alarm.

A. State Space Model

Meters or sensors such as PMUs that are able to measure current phase and amplitude [14] are used in the power system to measure the system state at various locations and

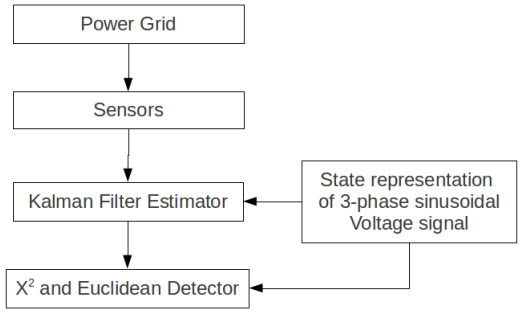

Fig. 1: Security framework for the Smart Grid system

time to ensure a smooth operation of the power system. The measurements obtained from these meters/sensors are the state variables that are reported to the central controller via the wired/wireless communication infrastructure. As stated in [10], the state variables include bus voltage, angles and magnitudes. Furthermore, an attack or fault in the power system is always reflected in the form of change in either voltage, current or phase [7]. Without loss of generality, we derive the state space model from the power grid voltage signal.

The voltage signal can be represented as a sinusoidal wave [15] as shown in Equation (1) [1]. The equation represents voltage as a function of amplitude (A_v), angular frequency wt and phase ϕ at discrete time.

$$V_1(t) = A_v sin(\omega t + \phi) \tag{1}$$

Equation (1) can be expanded as follows,

$$V_1(t) = A_v * sin\omega t * cos\phi + A_v * cos\omega t * sin\phi \tag{2}$$

Assuming the angular frequency is relatively constant over time, we consider amplitude and phase as the variables in the state space representation. The equation then becomes,

$$V_1(t) = x_1 * sin\omega t + x_2 * cos\omega t \tag{3}$$

where, $x_1 = A_v * cos\phi$ and $x_2 = A_v * sin\phi$ are defined as the state variables. Assuming there is no additional delay in the system and considering random noise as well as small error picked up by the system, we have Equation (4) representing the state equation over the time.

$$\begin{bmatrix} x_1(t+1) \\ x_2(t+1) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + w(t) \tag{4}$$

Equivalently,

$$x(t+1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x(t) + w(t) \tag{5}$$

where, $x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}$ and $w(t)$ represents the process noise. Note both A_v and ϕ are non-time-varying components of the sinusoidal wave and the state variables and if any change

[1]The other two phases of the voltage signal can be similarly considered. For simplicity we only consider Eq. (1) in the process of developing the model

is detected in these components, it signifies either attack or fault in the system.

The actual voltage signal for the current state using non stationary deterministic vector $[sin\omega t\ cos\omega t]$ can be obtained using Equation (2) and can be written as shown in Equation (6), where $v(t)$ represents the measurement noise.

$$y(t) = [sin\omega t\ cos\omega t] \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + v(t) \tag{6}$$

B. Kalman Filter

In this section, we introduce the Kalman Filter [16] technique to obtain estimates for the state space vector $x(t)$ described in the above section. To apply the Kalman Filter technique, the state equation can be written as,

$$x(t+1) = Ax(t) + w(t) \tag{7}$$

where, A = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ The observation equation for Kalman Filter from Equation (6) can be written as:

$$y(t) = C(t)x(t) + v(t) \tag{8}$$

Here, $y(t)$ is the measurement vector collected from the sensors, $C(t) = [sin\omega t\ cos\omega t]$, $v(t)$ is the measurement noise which is independent of the initial conditions and process noise. Both $w(t)$ and $v(t)$ are assumed to be white Gaussian noise with zero mean and standard deviation σ.

Kalman Filter can then be applied to compute state estimations $\hat{x}(t)$. Let the mean and covariance of the estimates be defined as follows:

$$\begin{aligned} &\hat{x}(t|t) = E[x(t), y(0), ..., y(t)] \\ &\hat{x}(t|t-1) = E[x(t), y(t), ..., y(t-1)] \\ &P(t|t-1) = \Sigma(t|t-1) \\ &P(t|t) = \Sigma(t|t-1) \end{aligned} \tag{9}$$

Here, $\hat{x}(t|t)$ is the estimate at time t using measurements up to time t, $\hat{x}(t|t-1)$ is the estimate at time t using measurements up to time $t-1$. Similarly, $P(t|t)$ is the covariance of the estimates at time t using data up to time t and $P(t|t-1)$ is the covariance of the estimates at time t using data up to time $t-1$. Now, the iterations of Kalman Filter can be written as:

Time Update:

$$\hat{x}(t+1|t) = A\hat{x}(t) \tag{10}$$

$$P(t|t-1) = AP(t-1)A^T + Q \tag{11}$$

The Equation (10) projects the state and covariance estimates at $t+1$ time step from t time step. Here, A is obtained from the state space model in Equation (4) and Q is the process noise covariance matrix.

Measurement Update:

$$\begin{aligned} &K(t) = P(t|t-1)C(t)^T(C(t)P(t|t-1)C(t)^T + R)^{-1} \\ &P(t|t) = P(t|t-1) - K(t)C(t)P(t|t-1) \\ &\hat{x}(t) = \hat{x}(t|t-1) + K(t)(y(t) - C(t)\hat{x}(t|t-1)) \end{aligned} \tag{12}$$

Equations (12) represents the measurement updates of the Kalman Filter. $K(t)$ is the Kalman gain and R is the measurement noise covariance matrix. The last two formulae in Equation (12) are used to generate a more accurate estimate by incorporating the measurements $y(t)$. The initial condition is $x(0|-1) = 0, P(0|-1) = \Sigma$, [7].We assume that the Kalman gain converges in a few steps and is in a steady state. Finally, a training period is assumed such that the filter knows the Kalman gain before the estimation, then,

$$\begin{aligned} P &\triangleq \lim_{k\to\infty} P(t|t-1), \\ K &= PC^T(CPCT + R)^{-1} \end{aligned} \tag{13}$$

Equation (12) can be further updated as:

$$\hat{x}(t+1) = A\hat{x}(t) + K[y(t+1) - C(A\hat{x}(t))] \tag{14}$$

The estimation error $e(t)$ is defined as:

$$e(t) \triangleq \hat{x}(t) - x(t) \tag{15}$$

III. Attack/Failure Detector

After the KF estimator calculates the next state of the system and the sensors readings are available, the projected estimates and the actual sensor readings are compared by the detector to detect any disagreement. If the detector detects that the difference between the two are significant, as dictated by a precomputed threshold, it triggers an alarm for a possible attack or failure. As discussed earlier, the framework proposed in this paper implements two types of detectors: The χ^2-detector and the detector implementing the Euclidean distance metric.

A. χ^2-detector

The χ^2-detector is a conventional detector used with Kalman Filter. As described in [13] the χ^2-detector detector constructs a χ^2 test statistics from the Kalman Filter and compares them with a pre-computed threshold. Now, the residue z_{k+1} at time $k+1$ is defined as:

$$z(t+1) \triangleq y(t+1) - \hat{y}(t+1|t)$$

From Equation (8), (10) and (16), we get,

$$z(t+1) \triangleq y(t+1) - C(A\hat{x}(t)) \tag{16}$$

Then, the χ^2-detector test consists of comparing the scalar test statistics given by:

$$g(t) = z(t)^T B(t) z(t) \tag{17}$$

Where, $B(t)$ is the covariance matrix of $z(t)$. The χ^2 detector compares $g(t)$ with a precomputed threshold obtained using the χ^2-detector-table [13] to identify a failure or attack. The χ^2-detector for the Kalman Filter was first studied in [13].

χ^2 test is long-term test because, at each detection step, all integrated effects since system start time are considered. This property makes it very useful for the fault detection in Smart Grid which consists of sensors that are subject to soft failures like instrument bias shift. Another advantage of χ^2

detector is its computational straightforwardness. The parameters required to perform the test are already generated by the Kalman Filter making it compatible with the KF. Furthermore, the threshold for the detector can be easily obtained from the χ^2-table making the threshold computation relatively easy. However, as mentioned previously, this detector fails to detect False Data Injection attack on the sensors and thus is not sufficient [11].

B. Detector implementing the Euclidean Distance Metrics

As can be seen from the simulations in the next section, the χ^2-detector fails when the adversary performs a False Data Injection Attack on the Smart Grid system. The False Data Injection Attack is a class of attack which is carefully crafted to bypass the statistical detector like χ^2-detectors. Hence, we propose an Euclidean-based detector, which will calculate the deviation of the observed data from the estimated data. To apply the Euclidean detector, we need to reconstruct the sinusoidal signals from the state estimates and compare them with the measurements obtained from the sensors. As shown in Equation (18), if the deviation is large enough, it means that the system is under a possible attack or there are some faults in the system. Without loss of generality, we assume that an appropriate threshold is obtained using the data obtained in the past when the system is functioning normally.

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + ... + (p_n - q_n)^2} \tag{18}$$

Since we are actually regenerating the signal to see how much it deviates from what is expected/estimated, we can detect attacks and faults that results from the manipulation of the measured signal. Nonetheless, this approach can be computation intensive in the process of reconstructing the signal.

IV. Implementation and Performance Evaluation

The Kalman Filter estimator, the χ^2-detector and the Euclidean distance metrics are implemented using Matlab. Table I shows the experimental setup and the initial values. A 60Hz Sinusoidal voltage signal with random Gaussian noise was generated and fed to the Kalman Filter estimator as the input. Matlab function randn() was used to produce normally distributed noise with mean value zero. The input signal and the resulting sinusoidal signal obtained using the state estimates are plotted in Figure 2-6. Each of these figures contain two graphs and show the results of the simulation plotted against time. The left sub graph shows how the amplitude varies with time for the input sinusoidal signal and the signal constructed using estimated state variables. In the second graph, the value for $g(t)$ from Equation (17) are plotted against time. The straight horizontal line is the threshold obtained from the χ^2 table. For the Euclidean detectors, $d(p,q)$ from Equation (18) is plotted against time.

A. Attack/Fault detection using χ^2 detector

The simulation results, using χ^2 detector, for a certain time frame is shown in Figure 2. As seen in Figure 2, the estimated

TABLE I: Experimental setup

Frequency	60Hz
Amplitude	1 Volt
Sampling frequency	2 KHz
Initial value for $x_1(0)$	0
Initial value for $x_2(0)$	0
Initial covariance matrix $P(0\|0)$	Identity matrix

values obtained from the Kalman Filter estimator agrees with the input signal when there are no attacks/faults. Hence the value for g(t) obtained from the detector stays within the threshold. Since our simulations also consider the random noise in the system, there is a slight difference between the estimates and the input signal at the beginning. As Kalman Filter works iteratively by correcting its estimates using both the state space model and the measurements obtained, the estimates gradually converge with the input signal. Figure

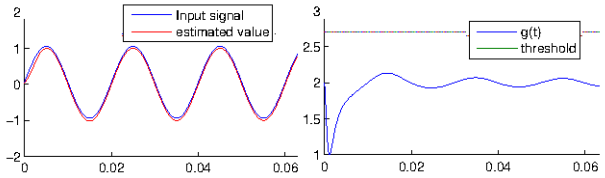

Fig. 2: Simulation results without attack/fault

3 shows when there is a random attack on the system, the estimated values do not correspond with the input signal and g(t) exceeds the threshold. The detector triggers an alarm signifying an attack/fault in the system. Similarly, short-timed attack is also detectable as depicted in Figure 4. The replay attack and DoS attack can also be detected in the similar manner.

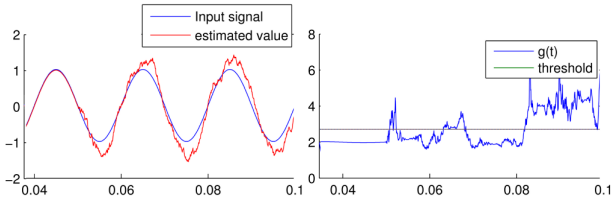

Fig. 3: Simulation results with a continuous random attack

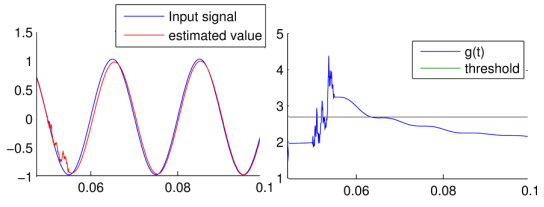

Fig. 4: Simulation results when there is a random attack for a short period of time

B. False Data Injection Attack

The generation of attack sequence for a CPS using Kalman Filter is described in [17]. The attack sequence ensures that it

can by pass the detector and at the same time increase the error in the state estimation. The second sub graph in Figure 5 shows how the system behaves when the system is attacked using the false data injection technique. We can see the estimates do not agree with the measured values in the top sub graph in Figure 5. However, the g(t) curve never exceeds the threshold. In other words, the statistical tests in χ^2-detector fail in the detection of such a False Data Injection Attack. In the next section, we show that the proposed Euclidean Distance metric, Equation (18) can identify such an attack by constantly monitoring the difference between the estimated values and the measured values.

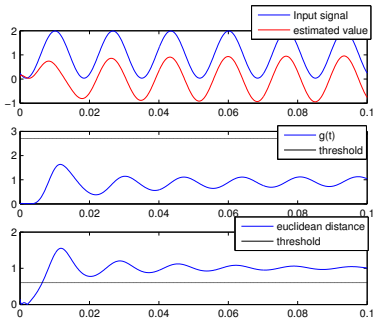

Fig. 5: False Data Injection Attack using χ^2-detector and Euclidean Detector

C. False Data Injection Attack detection using Euclidean Distance Metric

For the detector implementing Euclidean distance metric, we use Equation (18) to measure the deviation of the measured data from the estimated data. Since the state variables only consider the time-invariant components of a sinusoid the state variables remain relatively constant. Hence, change in state variables could mean either attack or fault in the system and can be easily detected. However, to avoid false alarms due to measurement or system errors, it is important to set a proper threshold. As mentioned in Section II-B, the noise in the system is considered white Gaussian with 0 mean and standard deviation σ. To prevent the false positives due to noise in the bus, we set the threshold to 3σ, σ being the standard deviation of the noise from Section II-B. Due to the properties of Gaussian distribution, this filters out 99.73% false positives due to noise. Figure 6 shows the plot of the Euclidean Distance metric when there is no attack in the system and the bottom sub graph in Figure 5 shows the plot when there is a False Data Injection Attack in the system. When there is an attack in the system the difference between the two curves is large and exceeds the threshold, hence the False Data Injection Attack can be detected by the Euclidean distance metric.

V. Conclusion

A robust framework has been designed for the Smart Grid system using Kalman Filter estimator together the χ^2-detector and Euclidean detectors. It has been shown that the χ^2-detector

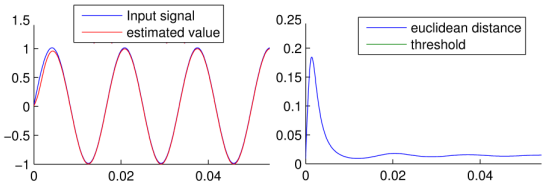

Fig. 6: Simulation results using Euclidean distance metric when there is no attack

is efficient in detecting different types of faults and attacks on the system such as replay and DOS attacks. However, the χ^2-detector fails to detect the False Data Injection Attack on the system. Thus we have proposed to use Euclidean distance metric to detect the False Data Injection Attack on the system.

References

[1] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809 –818, Dec. 2011.

[2] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675 –685, Dec. 2011.

[3] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 686 –696, Dec. 2011.

[4] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 476 –486, Sept. 2011.

[5] C. Alcaraz, C. Fernandez-Gago, and J. Lopez, "An early warning system based on reputation for energy control systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 827 –834, Dec. 2011.

[6] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865 –873, Dec. 2011.

[7] H. Qi, X. Wang, L. Tolbert, F. Li, F. Peng, P. Ning, and M. Amin, "A resilient real-time system design for a secure and reconfigurable power grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 770 –781, Dec. 2011.

[8] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, Dec. 2011, pp. 1162 –1167.

[9] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *First Workshop on Secure Control Systems (SCS 2010),CPSWEEK2010*, Apr. 2010.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011. [Online]. Available: http://doi.acm.org/10.1145/1952982.1952995

[11] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *2010 49th IEEE Conference on Decision and Control (CDC)*, Dec. 2010, pp. 5967 –5972.

[12] V. Sood, D. Fischer, J. Eklund, and T. Brown, "Developing a communication infrastructure for the smart grid," in *Electrical Power Energy Conference (EPEC), 2009 IEEE*, Oct. 2009, pp. 1 –7.

[13] B. Brumback and M. Srinath, "A chi-square test for fault-detection in kalman filters," *IEEE Transactions on Automatic Control*, vol. 32, no. 6, pp. 552 – 554, Jun 1987.

[14] R. Wilson, "Pmus [phasor measurement unit]," *Potentials, IEEE*, vol. 13, no. 2, pp. 26–28, 1994.

[15] M. Djerf, "Power grid integration using kalman filtering," *Uppsala University, Signals and Systems Group*, no. 12003, p. 55, 2012.

[16] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal Of Basic Engineering*, vol. 82, pp. 35–45, 1960.

[17] Y. Mo and B. Sinopoli, "False data injection attacks in control system," in *First Workshop on Secure Control Systems, CPS Week*, 2010, pp. 5967 –5972.