Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter

Kebina Manandhar, Xiaojun Cao, *Member, IEEE*, Fei Hu, *Member, IEEE*, and Yao Liu

***Abstract*—By exploiting the communication infrastructure among the sensors, actuators, and control systems, attackers may compromise the security of smart-grid systems, with techniques such as denial-of-service (DoS) attack, random attack, and data-injection attack. In this paper, we present a mathematical model of the system to study these pitfalls and propose a robust security framework for the smart grid. Our framework adopts the Kalman filter to estimate the variables of a wide range of state processes in the model. The estimates from the Kalman filter and the system readings are then fed into the χ^2-detector or the proposed Euclidean detector. The χ^2-detector is a proven effective exploratory method used with the 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 DoS attack, short-term, and long-term random attacks. However, the studies show that the χ^2-detector is unable to detect the statistically derived false data-injection attack. To overcome this limitation, we prove that the Euclidean detector can effectively detect such a sophisticated injection attack.**

***Index Terms*—Cyber physical system, false data injection attack, Kalman filter smart grid, security.**

I. Introduction

THE POWER grid is one of the important infrastructural backbones that has a deep impact on economy as well as our daily activities. Failures in the power grid often lead to catastrophic effects as the ones in New York (2003) and Mumbai (2012). Though both of these failures resulted due to faults in the system, security failures can also result in similar consequences, if not worse. With the advent of new technologies, the secluded power grid system is being replaced by a grid, which is a typical smart cyber physical system (CPS) that has more embedded intelligence and networking capability. In such smart-grid systems, cyber and physical components work in a complex coordination to provide better performance and stability. Sensors are equipped throughout the system to monitor various aspects of the grid, such as the meter and voltage fluctuations in these systems. The collected information from the sensor networks helps provide feedback to the physical power grid devices. Hence, such a CPS involves two-way communication between the controller system and the physical components as shown in Fig. 1.

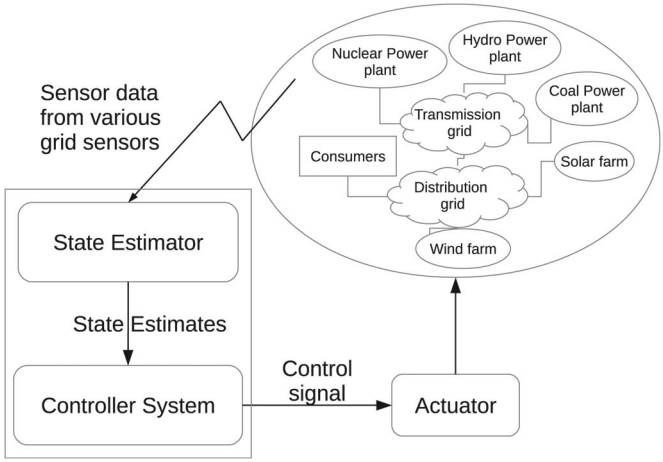


Fig. 1. Block diagram for a smart-grid system.

Since the smart grid relies on wired/wireless networking infrastructures to integrate the control system and physical power grid system, it is important to understand and defend cyberattacks that emerge from the networking and control infrastructures. The addition of wired/wireless communication capabilities in the existing power grid system results in increasing complexity and potentially more holes in security. The smart-grid system can incorporate traditional security measures (e.g., intrusion detection and firewall) to prevent rudimentary attacks, such as the ones in traditional data networks. Lots of studies in the literature revolve around the security of data communication from the physical components to the central controller or among different elements (e.g., sensors and actuators). For example, the authors in [1] propose an intrusion detection system to detect malicious nodes in the smart-grid wireless network. Similarly, a distributed intrusion detection system is discussed in [2].

Recently, many emerging attacks specifically targeting the communication and control systems in smart grid are exposed [3]–[8]. For example, security threats include the tampering of physically unguarded monitoring sensors in the grid system leading to false data. A general strategy to identify physical tampering is to deploy an estimator and a detector in the controller. The estimator compares the calculated estimates with the actual readings and verifies them [3], [4]. The detector triggers an alarm when the estimated states and measured states do not agree with each other. In other words, a remarkable

Manuscript received April 7, 2014; revised July 12, 2014 and August 6, 2014; accepted August 20, 2014. Date of publication September 12, 2014; date of current version December 15, 2014. Recommended by Associate Editor P. A. Iglesias.

K. Manandhar and X. Cao are with the Department of Computer Science, Georgia State University, Atlanta, GA 30303 USA (e-mail: kmanandhar1@cs.gsu.edu; cao@cs.gsu.edu).

F. Hu is with the Department of Electrical and Computer Engineering, University of Alabama, Tuscaloosa, AL 35487 USA (e-mail: fei@eng.ua.edu).

Y. Liu is with the Department of Computer Science and Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail:yliu@cse.usf.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCNS.2014.2357531

difference between the estimated and measured states signifies either a fault or a possible attack on the system. However, the studies in [3] and [4] show that a new type of attack called a False Data Injection attack can be directed at the system if some system parameters are known to the attacker. To the best of our knowledge, no existing estimator and detector combination has been examined in the literature to effectively detect different types of attacks in the power grid including the False Data Injection attack.

In this paper, we present a security framework for smart grid using the Kalman filter (KF). The Kalman filter generates estimates for state variables using the mathematical model for the power grid and the data obtained from the sensor network deployed to monitor the power grid. A χ^2-detector can then be employed to detect the discrepancies between the estimated data and the measured data, and trigger alarms. The χ^2-detector can effectively detect attacks, such as the DoS attack and random attack, even though the states of the system do not remain constant at various time periods. However, the study shows that the χ^2-detector cannot detect the statistically derived False Data Injection attack. For the first time, we comprehensively investigate the sophisticated False Data Injection attack, together with the proposed KF framework and propose an additional detection technique using the Euclidean distance metric. Our primary contributions include: 1) we propose a mathematical model together with the KF to detect possible attacks and faults on the smart-grid system; 2) we investigate the performance of the exploratory method χ^2-detector, in identifying faults and random attacks; 3) we analyze the limitation of the χ^2-detector in detecting the statistically derived False Data Injection attack and accordingly propose a new Euclidean detector to be coupled with KF; and 4) we demonstrate the effectiveness of the proposed approaches via extensive simulations and analysis on practical systems.

The rest of this paper is organized as follows. Section II presents the motivation and the related work on smart-grid security. Section III describes the proposed framework, the mathematical model of the power grid system, and the Kalman filter estimator. Section IV presents the two detectors implemented in the framework in order to detect various attacks and failures in the system. In Section V, performance results of the proposed framework and the observations are discussed. Finally, Section VI presents the conclusion.

II. Motivation and Related Work

In this section, we review various security schemes studied in the literature. Most of the papers discussed in this section deal with the security of data communication using the rudimentary techniques, such as intrusion detection, cryptography, physical layer security enhancement, and the utilization of recommendation-based social network infrastructure (for example, [6]–[10]). The existing studies on the security of the smart grid can be broadly categorized into three categories. The work in the first category deals with the wired/wireless networking security among cyber components in the smart grid [1], [2], [5]–[9]. The papers in the second category investigate 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 [10], [11] can proactively protect the system. The work in the third category applies the control theories in the security process using various state estimation and detection techniques [12]–[14].

A wireless mesh network architecture was proposed in [1] for the smart-grid system and an intrusion detection scheme called smart tracking firewall was introduced. To overcome the security pitfalls, such as signal jamming and eavesdropping, the authors in [1] also investigated the anti-jamming, physical-layer security technique coupled with the smart-tracking firewall. The proposed firewall consists of two agents: 1) intrusion detection agent and 2) response agent. The agents maintain two lists of misbehaving nodes called the black list and the gray list. These lists keep tracking the malicious nodes in the network. Another distributed intrusion detection scheme was discussed in [2], which deploys an intelligent module and an analyzing module along with an artificial immune system to detect and classify malicious data as well as possible attacks on the smart grid. In [5], secure estimation of the system states is discussed. The channel capacity requirement to ensure negligible information leakage to the adversary regarding the system states and control message is studied in this paper. A message authentication scheme was proposed in [6] to achieve the mutual authentication among the smart meters in the smart grid using shared keys and hash-based authentication techniques. Another signature-based message authentication scheme was proposed in [7], which employs the multicast authentication to reduce the signature size and communication bandwidth at the cost of increased computation. As suggested in this paper, such an authentication scheme is more desirable in the smart grid, where there is a limitation in the storage size and bandwidth. The work in [8] uses the data concatenation and random drop schemes to defend a traffic analysis attack, and the study in [9] is about defending the Internet-based load altering attack.

Unlike the papers discussed before that focus mainly on the protection of data communication in the smart grid, the authors in [10] presented an early warning scheme to predict/prevent anomalous events in advance. The proposed approach consists of detection, reaction, data recollection, and alarm-management components. Anomaly detection in the existing power grid substation was studied in [11], which presents an anomaly inference algorithm based on the combination of the transaction-based model, hidden Markov model, and feature-aided tracking.

An attack/fault in the smart-grid system is always reflected in the form of change in either voltage, current, or phase [12]. The work in [12] proposed a control-theoretic adaptation framework for the system-level security of the 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 attacks on the system. However, the proposed distributed state estimation owns slightly larger data estimation error [12]. Similarly, the protection for the set of meter measurements or changes was discussed in [13] and [14]. The identification and verification of the set of sensor measurements that are required to be protected in order to detect

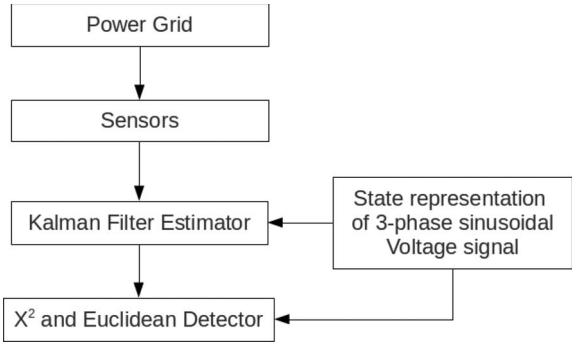


Fig. 2. Security framework for the smart-grid system.

the existence of a False Data Injection attack in the smart grid are discussed in [14].

As discussed before, much of the present work is based on various security techniques that are originally developed for securing the Internet data communication. While these techniques are effective in securing the Internet, these security techniques alone are not sufficient to deal with attacks in a more complex CPS, such as the smart-grid system [5]. As stated in [5], the existing security approaches are either 1) not viable; 2) incompatible with the smart grid; 3) not appropriately scalable; or 4) not adequate. Particularly, the existing techniques did not address the new class of attack called the False Data Injection attack [3]. This type of injection attack is undetectable by detectors used in the existing state-estimation security frameworks [3], [4]. Hence, this paper 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. We show that the False Data Injection attack cannot be detected using a traditional combination of estimator and detector (i.e., KF and χ^2-detector). Then, we propose a different detector based on the Euclidean distance metric to detect the complicated False Data Injection attack on the power grid system.

III. Proposed Framework for Smart Grid Using the Kalman Filter

In this section, we present the detailed description of the security framework for smart grid using the Kalman filter (KF). The framework is capable of detecting various attacks, including short-term and long-term random attacks along with the powerful False Data Injection attack on the power system. We develop a state-space model (as shown in Section III-A) from the three-phase sinusoidal voltage equations, to integrate the technique of the Kalman filter. Without loss of generality, we assume the use of voltage sensors to measure the state variables (e.g., amplitude and phase of the voltage) in the framework. The sampling rate for the sensors is assumed to be around 16 samples per 60-Hz cycle, that is, about 960 samples/s for medium-to-low data-rate production [15].

Fig. 2 shows the proposed security framework where the KF estimates the values for the state variables based on the system state and the data from numerous sensor readings. The estimated values generated by KF and the observed values for the state variables are fed into the detector. The detector compares two state vectors (consisting of all the state variables). If the two differ from each other significantly and are 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 KF estimators [16] when the residue of the KF equations follows Gaussian distribution and $g(t)$ (as in (32)) follows the χ^2 distribution [4]. Attacks such as the DoS attack and random attack are readily detected by the KF and χ^2-detector combination. However, the False Data Injection attack can bypass such detectors and may remain undetected [4]. Hence, we use an additional detector, based on the Euclidean distance, along with the 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

The power system deploys sensors or meters, such as phasor measurement units, to measure the system state at various locations and time to ensure smooth operation of the power system. These meters are able to measure current phase and amplitude [17]. 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 [3], the state variables may include bus voltage, angles, and magnitudes. Therefore, the state-space model should reflect these properties of the power system. The study in [12] indicates that an attack or fault in the power system is always reflected in the form of change in either voltage, current, or phase. 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 [18] as shown in (1). The equation represents voltage as a function of amplitude (A_v), angular frequency wt, and phase ϕ at discrete time. Equations (2) and (3) are mentioned here to represent the three-phase voltage signal. For simplicity, we only consider (1) in the process of developing the model

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

$$V_2(t) = A_v \cos\left(\omega t + \phi - \frac{2\pi}{3}\right) \tag{2}$$

$$V_3(t) = A_v \cos\left(\omega t + \phi - \frac{4\pi}{3}\right). \tag{3}$$

Equation (1) can be expanded as follows:

$$V_1(t) = A_v^* \cos\omega t * \cos\phi - A_v * \sin\omega t * \sin\phi. \tag{4}$$

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

$$V_1(t) = x_1 * \cos\omega t - x_2 * \sin\omega t \tag{5}$$

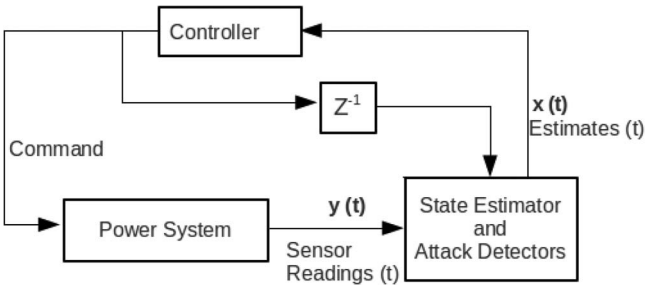


Fig. 3. Power grid system.

where $x_1 = A_v^* \cos\phi$ and $x_2 = A_v^\circ \sin\phi$ are defined as the state variables. Assuming there is no additional delay in the system and considering random noise or small errors picked up by the system, we have (6) representing the state equation over time

$$\begin{bmatrix} x_1(t+1) \\ x_2(t+1) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + w(t). \tag{6}$$

Equivalently

$$x(t+1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x(t) + w(t) \tag{7}$$

where $x(t) = \left[\begin{smallmatrix} x_1(t) \\ x_2(t) \end{smallmatrix}\right]$ and $w(t)$ is the process noise. Process noise represents the unmodeled system dynamics or the disturbance inputs in the system model.

The actual voltage signal for the current state using the nonstationary deterministic vector $[\cos\omega t - \sin\omega t]$ can be obtained using (4) and can be written as shown in (8), where $\gamma(t)$ represents the measurement noise

$$y(t) = [\cos\omega t \ -\sin\omega t] \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \gamma(t). \tag{8}$$

B. Kalman Filter

Fig. 3 shows the control system with the KF embedded for the estimation of the state vector and detector for the detection of attacks or faults. As shown in Fig. 3, $x(t)$ denotes the output of the state estimator that is fed to the controller and Z^{-1} is the control system feedback. The observations or sensor readings $y(t)$ are forwarded to the estimator at a regular time interval denoted by Δt. At each time step Δt, the estimator of the system generates estimated readings based on the estimates $x(t-1)$ from the previous time step and the real-time sensor readings $y(t)$.

To apply the KF technique, the state equation can be written as

$$x(t+1) = Ax(t) + w(t) \tag{9}$$

where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

From (8), the observation equation for the KF can be written as

$$y(t) = C(t)x(t) + v(t). \tag{10}$$

Here, $y(t)$ is the measurement vector collected from the sensors $C = [\cos\omega t - \sin\omega t]$; $v(t)$ is the measurement noise and assumed to be white Gaussian noise with mean 0 and standard deviation σ, which is independent of the initial conditions and process noise.

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

$$\hat{x}(t|t) = E\left[x(t), y(0), \ldots, y(t)\right] \tag{11}$$

$$\hat{x}(t|t-1) = E\left[x(t), y(t), \ldots, y(t-1)\right] \tag{12}$$

$$P(t|t-1) = \Sigma(t|t-1) \tag{13}$$

$$P(t|t) = \Sigma(t|t-1). \tag{14}$$

Here, $\hat{x}(t|t)$ is the estimate at time t using measurements up to time t, and $\hat{x}(t|t-1)$ 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 readings 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 the KF can be written as

Time update

$$\hat{x}(t+1|t) = A\hat{x}(t) \tag{15}$$

$$P(t|t-1) = AP(t-1)A^T + Q. \tag{16}$$

Equation (15) projects the state and covariance estimates at the $t+1$ time step from the t time step. Here, A is obtained from the state-space model in (6), and Q is the process noise covariance matrix.

Measurement update

$$K(t) = P(t|t-1)C(t)^T\left(C(t)P(t|t-1)C(t)^T + R\right)^{-1} \tag{17}$$

$$P(t|t) = P(t|t-1) - K(t)C(t)P(t|t-1) \tag{18}$$

$$\hat{x}(t) = \hat{x}(t|t-1) + K(t)\left(y(t) - C(t)\hat{x}(t|t-1)\right). \tag{19}$$

Equations (17)–(19) represent the measurement updates of the KF. $K(t)$ is the Kalman gain, and R is the measurement noise covariance matrix. Equation (19) is used to generate a more accurate estimate by incorporating the measurements $y(t)$. The initial condition is $x(0|-1) = 0$, $P(0|-1) = \Sigma$ [12]. As shown in [16] and [19], the Kalman gain can converge in a few steps and operate in a steady state. Given a training period such that the filter knows the Kalman gain before the estimation, we have

$$P \triangleq \lim_{k\to\infty} P(t|t-1), \tag{20}$$

$$K = PC^T(CPCT + R)^{-1}. \tag{21}$$

Equation(19) can be further updated as

$$\hat{x}(t+1) = A\hat{x}(t) + K\left[y(t+1) - C\left(A\hat{x}(t) + Bu(t)\right)\right]. \tag{22}$$

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

$$e(t) \triangleq \hat{x}(t) - x(t). \tag{23}$$

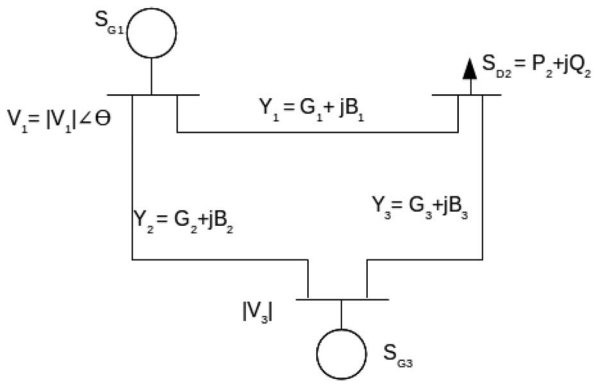


Fig. 4. Three-bus system.

C. Generalization of the Model

The state-space model described in Section III-A can be generalized for power grid measurements. The voltage at any given bus can be obtained in the form of a sinusoidal wave (or phasor representation) using Kirchoff's Voltage Law (KVL) and/or Kirchoff's Current Law (KCL). Let us consider a three-bus system as shown in Fig. 4 as an example. The voltage amplitude ($|V_i|$), phase (ϕ_i), active power (P_i), and reactive power (Q_i) are the variables in this system. Given a set of known initial values, the values for the unknown variables at each bus are obtained by solving (24) and (25) [20]. These equations are produced by applying KCL at each node. Hence, by solving the power-flow problem for the three-bus system, the voltage amplitude $|V_i|$ and phase ϕ_i at each bus are calculated. For any bus $'i'$

$$P_i = \sum_{k=1}^{n} |V_i||V_k| \left(G_{ik}\cos(\phi_i - \phi_k) + \sin(\phi_i - \phi_k)\right) \quad (24)$$

$$Q_i = \sum_{k=1}^{n} |V_i||V_k| \left(G_{ik}\sin(\phi_i - \phi_k) - \cos(\phi_i - \phi_k)\right) \quad (25)$$

where $|P_i|$ and $|Q_i|$ are the active and reactive power at bus i. $|V_i|$ and ϕ_i are the voltage magnitude and phase at bus i, and $Y_{ik} = G_{ik} + jB_{ik}$ are the Y-bus elements.

As described in Section III-A, the state variables are $x_1 = A_v * \cos\phi$ and $x_2 = A_v * \sin\phi$. Assuming the system has reached the stable state, these values of $|V_i|$ and ϕ_i for bus i, obtained by solving the power-flow equations, can be plugged in to obtain the initial values for the state variables at $t = 0$. Once the initial states are known, (7) and (8) for the KF of bus i can be used to estimate values for the next time step

$$At \text{ bus } i:$$

$$x_1(0) = |V_i|\cos\phi_i \quad (26)$$

$$x_2(0) = |V_i|\sin\phi_i. \quad (27)$$

Equations (24) and (25) account for the effect of all generators and loads in the system at each bus. Hence, for any bus i, $|V_i|$ and ϕ_i, obtained after solving this equation, reflect the effect of all system parameters. An attack/fault on any bus or branch in the system is reflected in the form of change in the values of these variables. Since the KF described before uses the values of $|V_i|$ and ϕ_i that are obtained by solving (24) and (25) as its initial state, any deflection in the values due to any attack/fault will cause the values of the state variables to deviate from the estimated values.

D. Attack Model

It is assumed that the attacker is able to control a subset of the sensor readings in the system. Three types of attacks are considered in this paper: 1) DoS attack; 2) random attack; and False Data Injection attack.

1) Denial-of-Service (DoS) Attack: The denial-of-service (DoS) attack is a form of attack where an adversary renders some or all the components of an inaccessible control system. The DoS attack can be launched by jamming the communication channels, flooding packets in the network, and compromising devices to prevent data transfer, etc. by the adversary [21]. The DoS attack could be on sensor data, control data, or both. In this paper, we model the DoS attack as the lack of available sensor data.

2) Random Attack: In this case, the attacks are not crafted to overcome the detection mechanism implemented by the central system. As described in (28), the attacker simply manipulates the sensor readings

$$y'(t) = C(t)x'(t) + v(t) + y_a(t) \quad (28)$$

where $y_a(t)$ is the random attack vector generated by the attacker. When the system is under attack, $y'(t)$ and $x'(t)$ denote observations and states. These random attacks could be generated at any point in time and could be a long-term continuous attack or a short attack.

3) False Data-Injection Attack: In case of a False Data Injection attack, it is assumed that the attacker knows the system model, including parameters A, B, C, Q, R, and gain K [22]. The attacker can also control a subset of sensors (S_{bad}). The attack model can then be described as

$$y'(t) = C(t)x'(t) + v(t) + \tau y_a(t) \quad (29)$$

where $\tau = \text{diag}(\gamma_1, \ldots\ldots \gamma_m)$ is the sensor selection matrix; $\gamma_i = 1$ if and only if $i \in S_{bad}$; otherwise, $\gamma_i = 0$; and $y_a(t)$ is the malicious input from the attacker.

IV. Attack/Failure Detector

The KF estimator calculates the following state of the system using the equations described in Section III-B. As the meter readings for that state become available, the projected estimates and the actual meter readings are compared by the detector. If the difference between the two is above a precomputed threshold, an alarm is triggered to notify a possible attack or failure. As previously discussed, the framework proposed in this paper implements two types of detectors: 1) the χ^2-detector and 2) the detector implementing the Euclidean distance metric.

A. χ^2-detector

The χ^2-detector is a conventional detector used with KF. As described in [16], the χ^2-detector constructs χ^2 test statistics from the KF and compares them with the threshold obtained from the standard χ^2 table.

Now, the residue z_{k+1} at time $k+1$ is defined as

$$z(t+1) \triangleq y(t+1) - \hat{y}(t+1|t). \tag{30}$$

Equivalently,

$$z(t+1) \triangleq y(t+1) - C\left(A\hat{x}(t)\right). \tag{31}$$

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

$$g(t) = z(t)^{TB}(t)z(t) \tag{32}$$

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 [16] to identify a failure or attack. The χ^2 test is a 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 the smart grid which consists of sensors that are subject to soft failures, such as instrument bias shift. Another advantage of the χ^2 detector is its computational complexity. The parameters required to perform the test are already generated by the KF, 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. In our experiments, the threshold is chosen such that error rate is less than 5%.

The False Data Injection attack is characterized by an attack sequence y_a such that $\limsup \|\Delta x(t)\| = \infty$, $\|\Delta z(t)\| \leq 1$, and $t = 0, 1, \ldots$, where $\|\Delta x(t)\| = x_a(t) - x(t)$, $\|\Delta z\| = z_a(t) - z(t)$, and $x_a(t)$ and $z_a(t)$ are state variables and residue of the compromised systems [22]. This definition shows that the χ^2-detector may fail to detect the False Data Injection attack on the sensors [4]. Thus, we introduce the Euclidean-based detector in the following section.

B. Detector Implementing the Euclidean Distance Metric

Though χ^2 detectors have a high noise tolerance and work in most cases, attacks such as the False Data Injection attack fail to get detected [4]. This phenomenon is also visualized in the simulation results in Section V. The False Data Injection attack is a class of attack which is carefully crafted to bypass the statistical detector, such as χ^2-detectors. Thus to detect these types of attacks, we propose an Euclidean-based detector, which calculates the deviation of the observed data from the estimated data. To apply the Euclidean detector, we first reconstruct the sinusoidal signals from the state estimates and then compare them with the measurements obtained from the sensors as shown

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \ldots\ldots + (p_n - q_n)^2} \tag{33}$$

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

where p is the amplitude of the voltage signal and q is the amplitude of the estimated voltage signal.

If the difference between the two is greater than the threshold, as in the case of the χ^2 detector, an alarm is triggered. The aforementioned KF estimator (and detectors) cannot differentiate the state variable changes due to an attack/fault from the noise such as system disturbance. To minimize the false positives caused due to the noise, we set the threshold to 3σ (σ is the standard deviation of the noise from Section III-B). As stated earlier, given the Gaussian noise with zero mean, setting the threshold to 3σ can filter out 99.73% false positives due to the noise [23].

Under steady state, the input signal can be reconstructed by applying the values of state variables in (5). Similarly, the estimated signal can be reconstructed using (5) and $\hat{x}(t)$ from (17).

Hence, the following corollary can be obtained from the definition of the False Data Injection attack in Section IV-A.

Corollary 1: Given $\limsup \|\Delta x(t)\| = \infty$

$$\lim_{t\to\infty} d\left(V_a(t), V(t)\right) = \infty$$

where $d(V(t), V_a(t)) = \sqrt{(C(t)\hat{x}_a(t) - C(t)x'(t))^2}$.

As $\|\Delta x(t)\|$ tends to ∞, $d(V(t), V_a(t))$ approaches ∞ as well. Therefore, we can detect attacks and faults that result from the manipulation of the measured signal, such as the False Data Injection attack.

V. IMPLEMENTATION AND PERFORMANCE EVALUATION

We implemented the KF estimator, χ^2-detector and Euclidean detector using Matlab. The experimental setup and the initial values are shown in Table I. A 60-Hz sinusoidal voltage signal with random Gaussian noise is generated and fed to the KF estimator as the input. Matlab function $randn()$ is 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 Figs. 5–9 and 11. Each of these figures contains two graphs and shows the results of the simulation plotted against time. The top subgraph shows how the amplitude varies with time for the input sinusoidal signal and the signal constructed using estimated state variables. In the bottom subgraph, the value for $g(t)$ from (32) is plotted against time. The straight horizontal line is the threshold obtained from the χ^2 table. For the Euclidean detectors, $d(p,q)$ from (33) is plotted against time.

A. Attack/Fault Detection Using the χ^2 Detector

Fig. 5 shows the simulation results using the χ^2-detector in the absence of attacks/faults for a certain period of time. It can

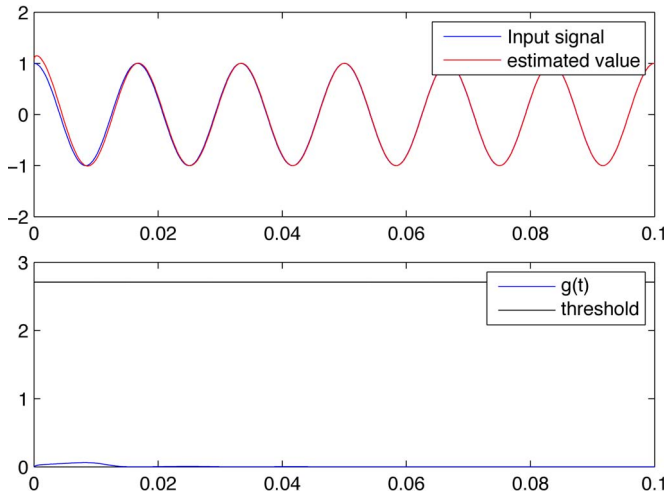


Fig. 5. χ^2-detector when there is no attack/fault.

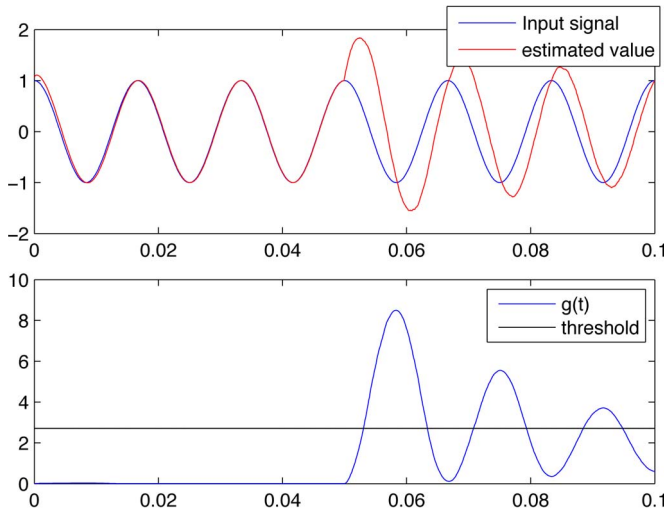


Fig. 6. Continuous random attack detected using χ^2-detector.

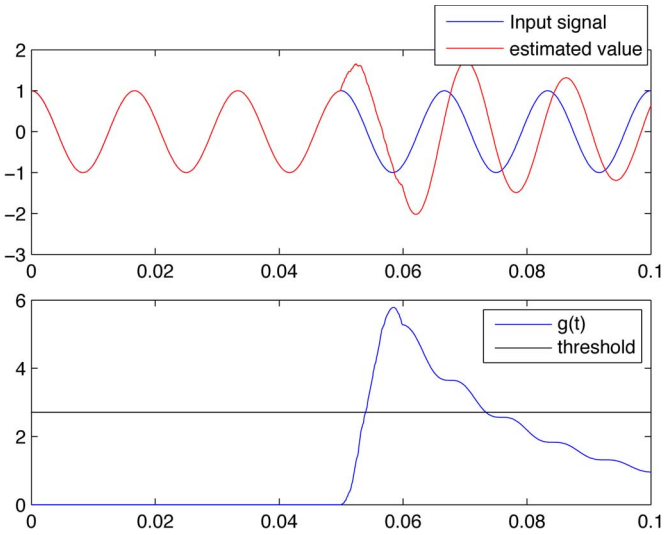


Fig. 7. Random attack for a short period of time detected using the χ^2-detector.

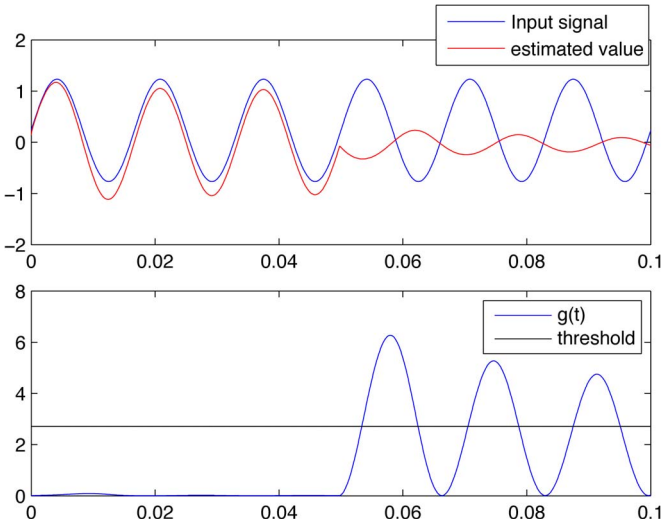


Fig. 8. DoS attack detected using the χ^2-detector.

be seen that the estimated values obtained from the KF estimator overlap with the input signal denoting there is no difference between the estimated and the observed value. Hence, 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 in the beginning. However, the KF works iteratively by correcting its estimates using the state-space model and the measurements obtained, and the estimates gradually converge with the input signal.

In case of attacks, the estimated values do not match with the observed values and $g(t)$ exceeds the threshold as shown in Fig. 6. As a result, the detector triggers an alarm signifying an attack/fault in the system. Similarly, Fig. 7. shows a short-timed attack being detected by the framework. Fig. 8. shows the detection of the DoS attack.

B. False Data Injection Attack

The False Data Injection attack injects fake sensor measurements that can fool the system by implementing the KF estimator with the χ^2-detector as described in [22]. The attack sequence can be obtained from

$$y_a(n+t) = y_a(t) - \frac{\lambda^{(i+1)}}{M} y^* \tag{34}$$

where n is the dimension of state space, $y^* = Cv$, $v =$ eigenvector of A, $|\lambda| >= 1$, $M = max_{k=0..n-1}\|\Delta z(k)\|$, and $\Delta z(k) = z'(k) - z(k)$. $z'(k)$ is the residue when the system is under attack.

The derivation of the attack sequence [22] ensures that it bypasses the detector and increases the error in the state estimation. The second subgraph in Fig. 9 shows the behavior of the χ^2-detector under the False Data Injection attack. We can see the estimates do not agree with the measured values in the top subgraph in Fig. 9. However, $g(t)$ never exceeds the threshold. In other words, the graph shows that the statistical tests in the χ^2-detector fail to detect the False Data Injection attack. We address this drawback in the next section by using the Euclidean detector, which can identify such an attack by

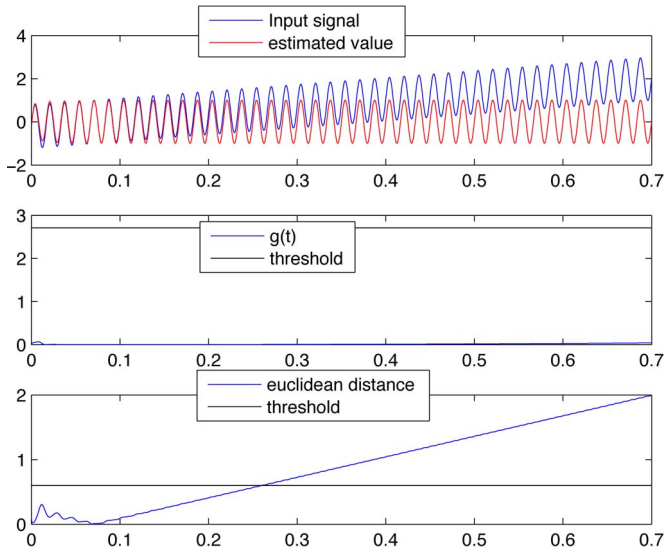


Fig. 9. False Data Injection attack using the χ^2-detector.

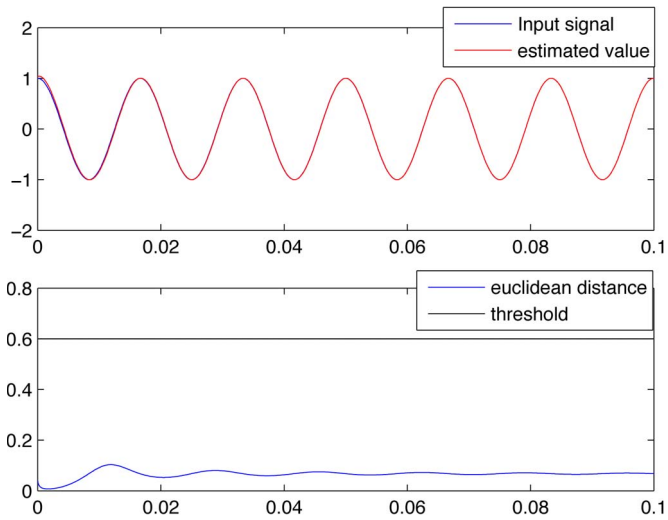


Fig. 10. Euclidean detector when there is no attack/fault.

constantly monitoring the difference between the estimated values and the measured values.

C. False Data Injection Attack Detection Using the Euclidean Detector

The Euclidean detector compares the difference between the measured data and the estimated data based on the Euclidean distance metric as shown in (33). Since the state variables only consider the time-invariant components of a sinusoid, the state variables remain relatively constant as described in Section III-A. Thus, a change in state variables could mean either an attack or a fault in the system. However, to avoid false alarms due to measurement or system errors, we set the threshold to 3σ as discussed in Section IV-B. Fig. 10 shows the plot of the Euclidean Distance metric when there is no attack in the system and the bottom subgraph in Fig. 10. 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

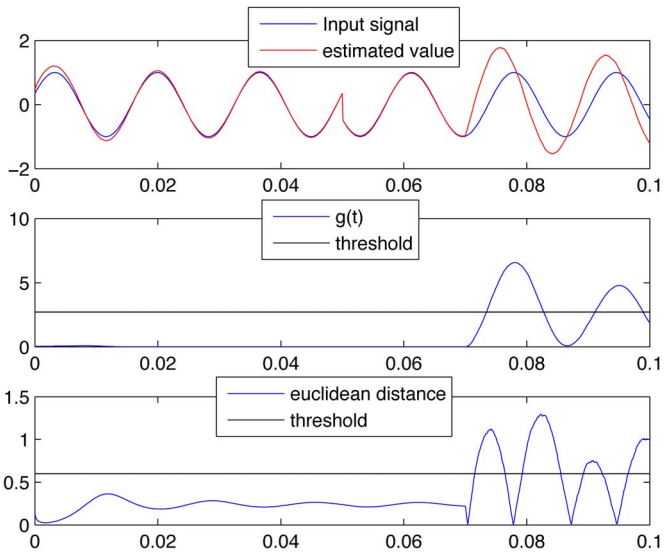


Fig. 11. Change in voltage due to load change.

curves exceeds the threshold, hence, the False Data Injection attack can be detected by the Euclidean distance metric.

D. Load Change

In the model derived in this paper, it is assumed that the load in the system remains constant. In case there is a change in load, there will be a change in the voltage signal across the buses. If the load profile is known, then the change in voltage amplitude/phase caused due to the load change can be predicted. Assume there is a change in the voltage due to load change as shown in Fig. 11. The parameters in the KF can be adjusted to reflect the change in the voltage due to the load change. This allows us to obtain estimates for the state variables after the load change. Fig. 11. shows that the estimates closely follow the signal with the load change. At time step 0.07, the random attack is detected by the χ^2 detector and Euclidean detector in this scenario.

E. χ^2-Detector versus Euclidean Detector

The probability of attack detection in both detectors is largely dependent on the value of the threshold. In the case of the χ^2-detector, the threshold is obtained from the standard χ^2 table. Similarly, in the case of the Euclidean detector, the threshold is obtained from the standard deviation of Gaussian distribution. In this experiment, we set the value of the thresholds in both detectors to filter 99% of noise. Thus, the probability of false alarms due to noise is less than 1%.

In general, the Euclidean detector is more sensitive towards changes than the χ^2-detector. As can be seen in Fig. 12, the Euclidean detector is faster in responding to the changes. Hence, if noise parameters for the system are known, the Euclidean detector gives better results. If the noise parameters are not known in advance, the χ^2-detector is preferable since it handles the soft errors better. However, a disadvantage of the χ^2-detector relative to the Euclidean detector is its inability to detect a False Data Injection attack. Fig. 9 shows the reaction

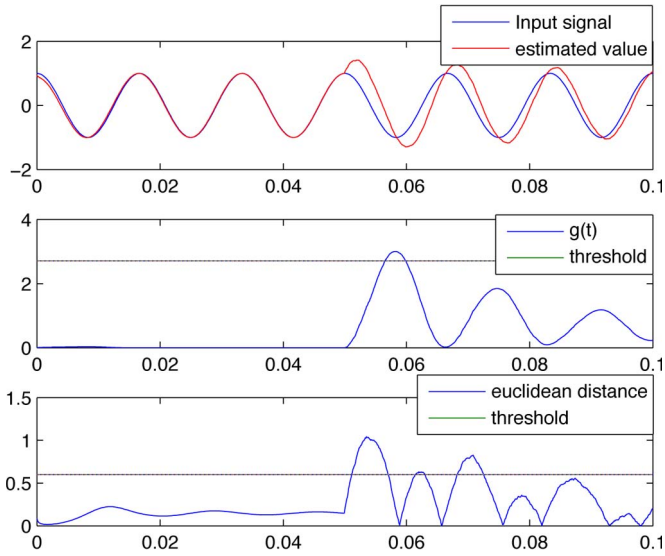


Fig. 12. Performance of both detectors under the random attack.

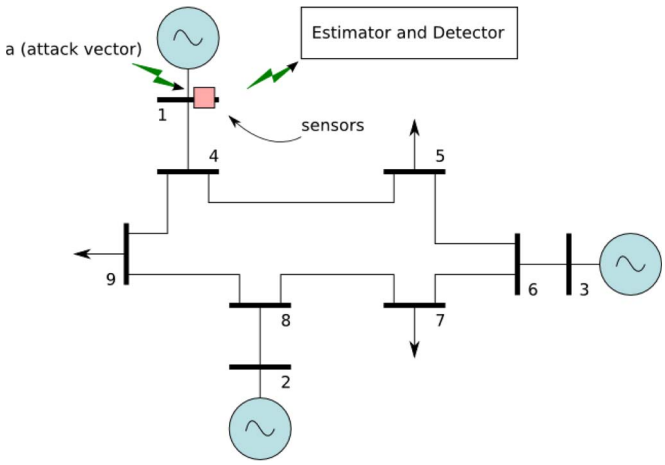


Fig. 13. IEEE 9-bus system under the False Data Injection attack.

of the χ^2 detector and Euclidean detector when the system is under the False Data Injection attack.

The Euclidean detector reconstructs the signal from the state estimates and compares it with the measured signal whereas the χ^2-detector only computes the residue vector. Since reconstruction requires more computation, the Euclidean detector is more resource intensive than the χ^2-detector.

F. Implementation of the Proposed Framework in the IEEE 9-Bus System

Fig. 13. shows an IEEE 9-bus system with sensors to monitor the state parameters and the estimator/detector for bus 3. The 9-bus system is simulated using the MATPOWER [24] package in MATLAB. The voltages and phases, obtained by solving the IEEE 9-bus power system in MATPOWER, are used as the state parameters in the KF estimator. A similar structure can be assumed for each bus in the system. For the simplicity, only bus 3 is discussed here. The attack sequence y_a is generated by the adversary as discussed in [22]. The sensors in the bus report their readings to the corresponding KF estimators and

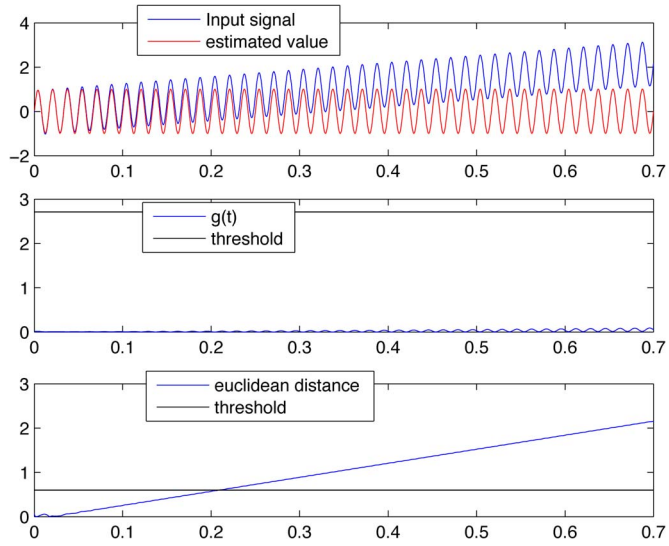


Fig. 14. False data attack detection for bus 3 in the IEEE 9-bus system.

Euclidean detectors. The successful detection of the False Data Injection attack on bus 3 is shown in Fig. 14.

VI. Conclusion

In this paper, a framework for the smart-grid system using the KF estimator together with the χ^2-detector and Euclidean detector has been designed. It has been shown that the χ^2-detector is efficient in detecting different types of faults and attacks, such as DoS attacks and random attacks on the system. Further, to handle attacks on the system, such as False Data Injection, which evades the χ^2-detector, we have proposed the Euclidean detector which uses the Euclidean distance metric for detection. We have also shown that the false positives due to noise for the Euclidean detector can be reduced to less than 1% with the proper selection of the threshold. Our extensive simulation and analysis have demonstrated the effectiveness of the proposed Euclidean detector in detecting various types of attacks, including the False Data Injection attack.

References

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

[2] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[4] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. 49th IEEE Conf. Dec. Control*, Dec. 2010, pp. 5967–5972.

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

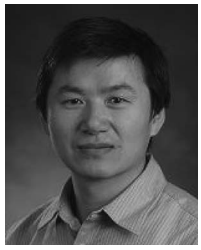
[6] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

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

[8] B. Sikdar and J. Chow, "Defending synchrophasor data networks against traffic analysis attacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 819–826, Dec. 2011.
[9] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.
[10] C. Alcaraz, C. Fernandez-Gago, and J. Lopez, "An early warning system based on reputation for energy control systems," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 827–834, Dec. 2011.
[11] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.
[12] 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 Trans. Smart Grid*, vol. 2, no. 4, pp. 770–781, Dec. 2011.
[13] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *Proc. IEEE GLOBECOM Workshops*, Dec. 2011, pp. 1162–1167.
[14] 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," presented at the 1st Workshop on Secure Control Syst., Stockholm, Sweden, Apr., 2010.
[15] V. Sood, D. Fischer, J. Eklund, and T. Brown, "Developing a communication infrastructure for the smart grid," in *Proc. IEEE Elect. Power Energy Conf.*, Oct. 2009, pp. 1–7.
[16] B. Brumback and M. Srinath, "A chi-square test for fault-detection in Kalman filters," *IEEE Trans. Autom. Control*, vol. 32, no. AC-6, pp. 552–554, Jun. 1987.
[17] R. Wilson, "Pmus [phasor measurement unit]," *IEEE Potentials*, vol. 13, no. 2, pp. 26–28, Apr. 1994.
[18] M. Djerf, "Power grid integration using kalman filtering," *Uppsala University, Signals and Systems Group*, no. 12003, p. 55, 2012.
[19] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Basic Eng.*, vol. 82, pp. 35–45, 1960.
[20] R. C. Dorf and J. A. Svoboda, *Introduction to Electric Circuits*. Hoboken, NJ, USA: Wiley, 2010.
[21] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*. New York, USA: Springer, 2009, pp. 31–45.
[22] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6, preprints.
[23] W. J. Dixon and F. J. Massey, *Introduction to statistical analysis*, vol. 344. New York, USA: McGraw-Hill, 1969.
[24] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, "Matpower: Steady-state operations, planning, analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

Kebina Manandhar received the M.Sc. degree in computer science from Georgia State University, Atlanta, GA, USA, in 2013, where she is currently pursuing the Ph.D. degree in computer science at Georgia State University, Atlanta, GA, USA.

Her primary research is related to security in cyberphysical systems, chiefly involving water and smart-grid systems. Her research also extends to the design of schemes to provide anonymity in current and upcoming networks.



Xiaojun Cao (M'05) received the B.S. degree in engineering physics from Tsinghua University, Beijing, China, in 1996, the M.S. degree in digital signal processing from Chinese Academy of Sciences, Beijing, China, in 1999, and the Ph.D. degree in computer science from the State University of New York at Buffalo, Buffalo, NY, USA, in 2004.

Currently, he is an Associate Professor in the Department of Computer Science at Georgia State University, Atlanta, GA, USA, where he leads the Advanced Network Research Group (aNet). Prior to joining Georgia State University, he was an Assistant Professor in the College of Computing and Information Sciences at Rochester Institute of Technology, Rochester, NY, USA. He is the co-author of the book *Wireless Sensor Networks: Principles and Practice* (CRC, 2010). His primary research interests include optical, datacenter and cyberphysical networks, as well as related network modeling and security.

Prof. Cao is a recipient of the National Science Foundation CAREER Award.

Fei Hu (M'13) received the Ph.D. degree in electrical and computer engineering in the field of signal processing from Tongji University, Shanghai, China, in 1999, and the Ph.D. degree in electrical and computer engineering from Clarkson University, Potsdam, NY, USA, in 2002.

Currently, he is an Associate Professor in the Department of Electrical and Computer Engineering at the University of Alabama (main campus), Tuscaloosa, AL, USA. He has published more than 200 journal/conference papers, books, and book chapters. His research has been supported by the U.S. National Science Foundation (NSF), U.S. Department of Defense (DoD), Cisco, Sprint, and other sources. So far, he has obtained more than U.S.$5 million research grants (average U.S.$500K per year). He also holds a few U.S. patents. He has served the editorial board for more than five international journals. He has chaired a few international conferences. His research interests are security, signals, and sensors. With security, this is about how to overcome different cyberattacks in a complex wireless or wired network. Recently, he focused on cyberphysical system security and medical security issues. With signals, this mainly refers to intelligent signal processing, that is, using machine-learning algorithms to process sensing signals in a smart way in order to extract patterns (i.e., achieve pattern recognition). With sensors, this includes microsensor design and wireless-sensor networking issues. He has taught more than 10 major electrical and computer engineering (ECE) courses and developed five brand new courses for ECE students (some of those new offered courses were sponsored by the U.S. National Science Foundation).

Yao Liu received the Ph.D. degree in computer science from North Carolina State University, Raleigh, NC, USA, in 2012.

Currently, she is an Assistant Professor in the Department of Computer Science and Engineering, University of South Florida, Tampa, FL, USA. Her research is related to computer and network security, with an emphasis on designing and implementing defense approaches that protect emerging wireless technologies from being undermined by adversaries. Her research interest also lies in the security of cyberphysical systems, especially in smart-grid security.