A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids

Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski,
Ju Bin Song, and Husheng Li, *Member, IEEE*

***Abstract*—Recent investigations have revealed the susceptibility of phasor measurement units (PMUs) to the time synchronization attack by spoofing its global positioning system (GPS). This paper proposes a cross-layer detection mechanism to fight against simultaneous attacks toward multiple PMUs. In the physical layer, we propose a GPS carrier-to-noise ratio (C/No) based spoofing detection technique. We apply the patch-monopole hybrid antenna to two GPS receivers and compute the difference between the standard deviation of each receiver's C/No. The priori probability of spoofing is calculated from the distributions of the difference. A counter is embedded in the physical layer to identify the most suspicious PMU. In the upper layer, the spoofing attack is considered similarly to the bad data injection toward the power system. A trustworthiness evaluation, which is based on both the physical layer information and power grid measurements, is applied to identify the PMU being attacked. An experiment has been carried to validate the proposed algorithm.**

***Index Terms*—Cross-layer mechanism, global positioning system (GPS) spoofing, multiple attacks detection, phasor measurement units (PMU).**

I. Introduction

THE PHASOR measurement units (PMUs) have been widely installed in power grids recently and are expected to be massively used in the future [1], for its outstanding performance compared with the traditional supervisory control and data acquisition (SCADA) system. PMUs make various measurements in power systems and attach time stamps to provide precise timing information. According to the IEEE standard [2], the total vector error (TVE) between the measurements, e.g., phasor, and the theoretical value should be less than 1%. This requires precise time synchronization among components in the power system, which is usually provided by the global positioning system (GPS).

Manuscript received March 5, 2014; revised June 11, 2014; accepted August 1, 2014. The work of Y. Fan and H. Li was supported in part by the National Science Foundation under Grant CNS-1116826, Grant CNS-1237834, and Grant CNS-1239366, and in part by the University of Tennessee-Battelle under Grant R011344513. Paper no. TSG-00203-2014.

Y. Fan is with the University of Tennessee, Knoxville, TN 37996-2250 USA.

H. Li is with the University of Tennessee, Knoxville, TN 37996-2250 USA; he is also an International Scholar of Kyung Hee University, South Korea (e-mail: husheng@eecs.utk.edu).

Z. Zhang is with Ji Nan University, Guangzhou 510632, China.

M. Trinkle is with University of Adelaide, Adelaide, SA 5005, Australia.

A. D. Dimitrovski is with Oak Ridge National Laboratory, Oak Ridge, TN 37831-6070 USA.

J. B. Song is with Kyung Hee University, South Korea.

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/TSG.2014.2346088

However, the time alignment from GPS may not be reliable [3] when it is being spoofed. GPS spoofing is the process of generating a faked version of GPS signal to disturb the navigation and time synchronization process of the receiver. GPS spoofing field tests [4] toward PMUs have been already implemented by researchers, which revealed its vulnerability against malicious attack. By spoofing the GPS embedded in the PMUs, the attacker could introduce an error of more than tens of microseconds time and cause variations in the PMUs phase angle at a rate of 1.73 degrees per minute [4], which violates the maximum phase error allowed by the applicable standard [2] and could be considered as a bad data injection. Therefore, the spoofing attack introduces severe problems in the real-time monitoring and control of smart girds.

Although the Volpe National Transportation System Center [5] has first published the report on the vulnerabilities of the GPS system in 2001 to warn about the lack of method against spoofing, most of civilian GPS receivers today still do not have the capability to detect or prevent spoofing attacks. Some previous studies focused on this topic have confirmed this problem. For example, Zhang *et al.* [6] have demonstrated the effectiveness of spoofing attack on three applications of PMUs in smart grids. Jiang *et al.* [7] have demonstrated the feasibility of a spoofing attack on PMUs formatted as an optimization problem. Humphreys *et al.* [8] demonstrated that it is feasible to build an inexpensive portable software defined GPS spoofer using the off-the-shelf components. As PMUs play a critical role in secure wide area monitoring system (WAMS) of the next-generation smart grid infrastructure [9] and are considered to be part of the control systems [10] or remedial schemes [11] in the future, these vulnerabilities may produce high potential risk toward the stability of the future power system. Some previous literature has already investigated this issue and considered it similarly to the bad data injection problem (see [23], [24]).

In this paper, we focused on such a novel potential attack toward PMUs in smart grid using GPS spoofing. We found that traditional defensive mechanisms are unable to prevent such an attack. From the viewpoint of signal structure, since the GPS signal does not have any encryption or authorization mechanism [12], spoofers could generate the counterfeit GPS signals that current commercial GPS receivers are unable to distinguish from real GPS signal. Besides, since the malicious attackers need not be physically connected to the communication network or near the monitoring device [8], simply enhancing the firmware of the monitoring devices could not

improve the system's reliability toward such an attack. Since the security of the power system is closely related to many critically important aspects in modern society, there is a pressing need to establish a defense scheme against GPS spoofing attacks in smart grids [13].

Aware of the extreme importance of the security of PMU in smart grid, we study the detection of spoofing attack to ensure the reliability of the monitoring system. In this paper, we propose an innovative cross-layer method that could detect multiple spoofers. In the physical layer, we improve the efficiency of detecting spoofing attack using traditional GPS techniques, which can be implemented in each individual GPS receiver. These techniques are based on the GPS signal parameters that are directly obtained from the GPS receiver, which have been examined in [14] in the aspect of Amplitude discrimination, Time-of-arrival discrimination, Consistency of navigation inertial measurement unit (IMU) cross-check, Polarization discrimination, Cryptographic authentication and Angle-of-arrival discrimination in detail. The first two solutions apply only when the spoofing attack strategy is straightforward and simple. They are proven to be inefficient when the attacker uses the receiver-spoofer mechanism [8]. The method with IMU requires high budget due to the price of IMU, which is not practical. The cryptographic authentication needs to modify the structure of civil GPS signal, which appears hardly possible in the near future, as it requires the whole GPS industry to adopt to the modification. Therefore, angle-of-arrival (AOA) based spoofing detection (AOASD) has been considered as the optimal technique to detect a GPS spoofing attack considering both efficiency and feasibility. The idea of AOA detection method is based on the fact that a typical GPS receiver would receive navigation signal from multiple GPS satellites with different AOAs. On the contrary, as in the most common receiver-spoofer based spoofing strategy, the spoofer itself is a GPS receiver. It firstly receives true GPS signals from different satellites and manipulates them into spoofing signals to transmit to the target victim. In this case, from the victim side, the signals from different satellites would have the same AOA. However, the AOA based techniques also requires an antenna array with extra GPS receiver device to estimate the AOA of the GPS signals, which limits its application as the result of the increasing size and cost.

Therefore, in our paper, we first propose a low-cost and efficient AOASD. Instead of using an antenna array with traditional AOASD, we mount a monopole-patch hybrid antenna to the device. The monopole antenna and the patch antenna are separately connected to different GPS receivers. Because the monopole and patch antennas have different radiation patterns in elevation, it is expected that we can distinguish the signal from different AOAs by calculating the difference of the signal's carrier-to-noise ratio (C/No) between the two antennas. As the C/No could be directly obtained from the GPS receiver, in our method, the only modification toward the PMU with civil GPS is to install an extra GPS connected to specific antenna. With a reduced cost, our AOASD is still effective against the common spoofing attack and even cooperative attack, as it is sensitive to the signal from the same elevation angle near the horizon. Besides, a prior probability could be obtained in this layer to help the upper layer to evaluate the possibility of which PMU is spoofed.

The prior probability obtained in the physical layer is then fed to the upper layer, where we use the state estimation based detection method to dynamically detect the bad data injection caused by GPS spoofing. A trustworthiness value is proposed to measure the possibility of spoofing. The two methods from physical layer and upper layer are integrated to a cross-layer detection mechanism to improve the efficiency and reliability against one or more simultaneous spoofing attack. The byproduct of our proposed method is to distinguish the bad data produce by the system fault with the spoofing attack, which helps the control center tackle with the bad data problem.

The remainder of this paper is organized as follows. Section II introduces the general background about GPS, the spoofing attack and its impact on smart grid. Section III presents the physical layer detection method based on AOA. Section IV introduces the trustworthiness evaluation mechanism based on the power system model. Section V provides the details of the cross-layer detection algorithm. The experiment result is presented in Section VI. Conclusions and future work are provided in Section VII.

II. GPS and Spoofing

The global position system (GPS) provides accurate location information to military and civil users all around the world. To calculate the precise position of the user, GPS needs to synchronize the time at the device with the satellites' time [the coordinated universal time (UTC)]. With its availability in all weather conditions and anywhere near the earth where four or more satellites are visible and the time accuracy around 100 ns, GPS becomes the ideal access to synchronize time stamp of the distributed components in the system. In power systems, the increasing complexity and capacity challenges the control and monitoring part of the system, which demands the distributed sensors in the monitoring system with more accurate time stamp in their measurements. PMU is considered as the optimal solution for its time accuracy provided by the built-in GPS.

However, as the civil GPS signal has no encryption or authorization mechanism and the detailed information about GPS signal is open to the public, it is feasible for malicious user to build devices that generate faked GPS signal. Once the target GPS receiver receives the faked signal, false location and time information would be extracted and reported to the user. In power systems, the PMU with spoofed GPS would report measurement with wrong time stamp and the accuracy of the measurements will be declined, which causes bad data problem in the power system.

In this section, we will briefly introduce GPS timing and the mechanism of GPS spoofing.

A. GPS Timing

The time information is embedded in the GPS signal. In the radio frequency (RF), the received GPS signal

could be described as [15]

$$r(t) = \sum_{k=1}^{n} H_k (2P_c)^{\frac{1}{2}} (C_k(t) D_k(t)) cos(2\pi (f_{L1} + \Delta f_k)t) + n(t) \tag{1}$$

where H_k and P_c are the channel matrix for the kth satellite and the channel power, respectively. $C_k(t)$ stands for the spread spectrum sequence (C/A code) and $D_k(t)$ is the navigation data. f_{L1} is the carrier frequency and Δf_k is the doppler frequency shift. $n(k)$ is noise. By demodulating the GPS signal, the receiver could align its time in the target receiver with UTC in two parts.

1) *Coarse Timing:* Coarse time information is stored in navigation data in subframe 1, whose detailed structure could be found in [9]. The parameter, time of clock for the satellite, T_{oc}, could be read directly from the subframe 1.
2) *Precise Timing:* Precise position navigation requires all the receivers to synchronize their time with the system time (UTC). The time difference between receiver and the UTC could be derived from the GPS signal propagation time. In order to demodulate the GPS signal, the local receiver would generate one replica of the C/A code. In the tracking procedure, the local C/A code generator adjusts its phase to match the received signal. Using this phase, the propagation time is obtained and consequently the time difference could be calculated

$$\Delta t = t_{rcv} - t_p - t_{UTC} \tag{2}$$

where Δt is the time difference between the receiver and UTC, t_{rcv} is the time on receiver and t_p is the propagation time, respectively. t_{UTC} is the system reference time.

B. Spoofing

As described above, the structure of GPS signal is simple and its technical detail is open to the public, which provides the feasibility for malicious users to deploy spoofing attacks. The common spoofing strategy is based on the mechanism of GPS signal acquisition, which is called receive-transmit mechanism. It has the following two steps.

1) In the first step, the spoofer itself receives real signal and calculates the position information and the time difference. Then it copies the real signal and transmits it to the target receiver in low power. The target receiver would not recognize this process because in its viewpoint, the only change is the small increase in the signal power.
2) Then, the spoofer gradually increases the its duplicated signal's power until it exceeds the real signal to take the control of the receiver. Then it slowly shifts the phase of the copied signal. In this condition, the signal becomes the spoofing signal but treated as the "real" signal while the authentic signal is treated as the noise by the target receiver. Thus, the receiver would adjust its signal generator to align with the spoofing signal, which deviates its phase from the true signal. As the phase is critical to calculate the propagation time and consequently the time difference, the spoofing will break the time synchronization between the receiver and system time by randomly shifting the phase in the GPS signal.

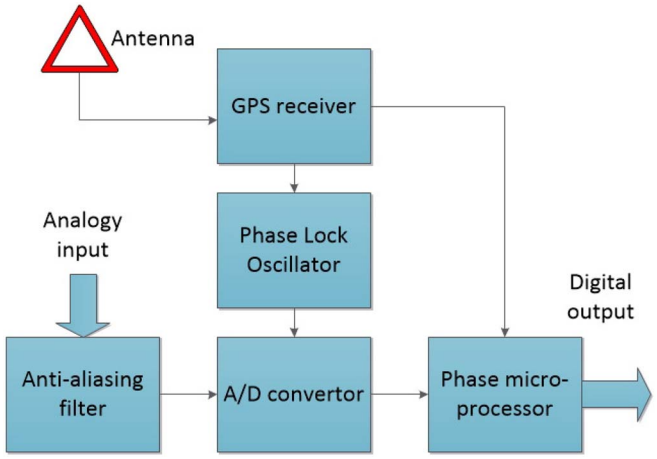

Fig. 1. Flowchart of PMU.

The efficiency and accuracy of the monitoring system in smart grid would be seriously affected when spoofed. Fig. 1 demonstrates that GPS spoofing could influence the work of PMU in two ways by changing the interval of A/D convertor and its time stamp on measurement. It's negative effects have been investigated by [3] as follows.

1) For transmission line fault detection, as the data from PMU could be applied to estimate the state of other parts of the system without PMUs, spoofing will increase the measurement error of PMU and deteriorate the performance of fault location.
2) For voltage monitoring system, spoofing provides false time stamps on the PMUs measurements, resulting in voltage instability alarms.
3) For the locationing of fault in power grid, spoofing can cause a substantial location error because the spoofed GPS delivers wrong geographical information to PMU. For example, a fault occurring in Tennessee may be misled to Kentucky.

The detailed analysis and numerical results can be found in our previous work [6].

III. Physical Layer Detection Mechanism

In this section, we propose a C/No based mechanism to detect the potential spoofing attack. A counter, based on this detection mechanism, is embedded in this layer to define the suspicious level of a certain PMU, which will be fed to the cross-layer detection against multiple spoofing attack. Our mechanism can be easily implemented by installing another commercial GPS receiver close to the existing GPS receiver in the PMU.

A. C/No Based Detection Mechanism

In our mechanism, two GPS receivers are installed closely and are connected to independent antennas, which have different radiation patterns, namely $G_1(\theta_i, \phi_i)$ and $G_2(\theta_i, \phi_i)$. The

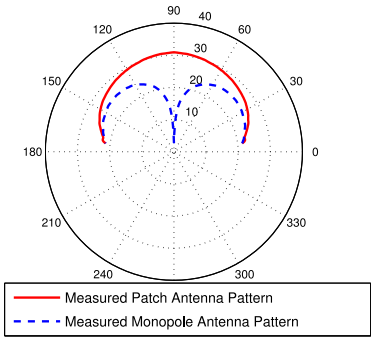

Fig. 2. Radiation patterns of monopole and patch antenna.

power ratio between the two antennas is defined as follows:

$$R_i = 10\log_{10}\left(\frac{G_1(\theta_i,\phi_i)}{G_2(\theta_i,\phi_i)}\right) \tag{3}$$

where R_i indicates the direction of the ith satellite's GPS signal, θ_i and ϕ_i represents for the azimuth direction and elevation direction of the ith satellite's GPS signal, respectively. In an authentic GPS signal, different channels come from different satellites, which are distributed sparsely in the open air and result in the difference between the power ratio. However, in spoofing signal, all the channels are transmitted from one spoofer and therefore they share the same direction as $\theta_1 = \theta_2 = \cdots = \theta_n$ and $\phi_1 = \phi_2 = \cdots = \phi_n$. Hence, the power ratio should be the same.

The standard deviation of R_i for all satellites observed at a given time t is used to describe how the power ratios of the antennas are closed to each other. A spoofing signal is expected to have a low standard deviation because of the same arrival direction of all signal channels. We first calculate the power ratio difference of each channel using the C/No values that are estimated by the GPS receiver

$$R_i = (C/No)_{i,1}(dB) - (C/No)_{i,2}(dB) \tag{4}$$

where $(C/No)_{i,n}$ is the estimated C/No value for the ith satellite from the nth GPS receiver in the dB scale. With all the power ratios of observable satellites are available, the standard deviation is calculated and compared with the threshold to determine the presence of a spoofing signal. The threshold is based on the distribution of the standard deviation of the R_i of authentic signal and spoofing signal, which can minimize the probabilities of false alarm and miss detection. The distribution of the standard deviation is obtained from the field test experiment introduced in the subsequent subsection.

B. Field Test

A field test is implemented to verify the proposed physical layer detection mechanism. Two GPS receivers were installed, one connected to a patch antenna and the other to a monopole antenna. The antenna gain patterns of these two antennas are significantly different. The patch antenna has the maximum gain at 90 degrees elevation and the monopole antenna has the opposite pattern. Fig. 2 shows the radiation patterns of the patch and monopole antennas in elevation, which were measured in an anechoic chamber. The devices are firstly

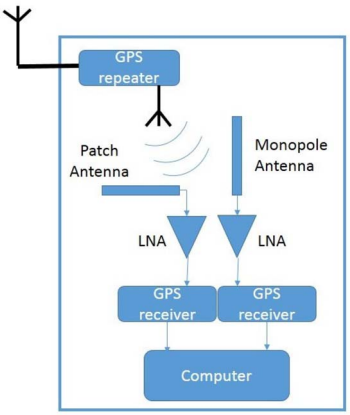

Fig. 3. Laboratory setup.

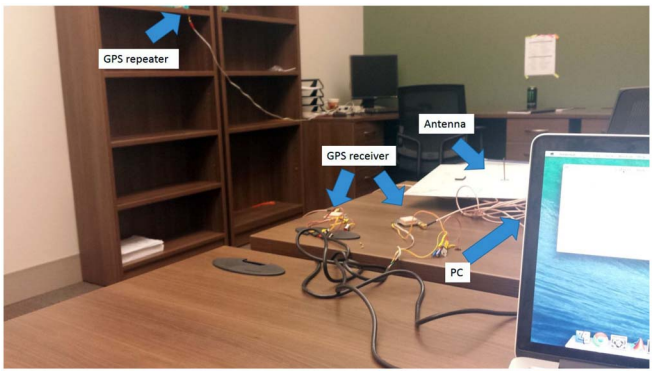

Fig. 4. Field test experiment.

exposed to the authentic GPS signal. When begin in good work condition, the receivers estimated the C/No of the authentic signal and logged it into PC in fixed time interval. With these measurements, R_i is calculated and used to generate the histogram to obtain the distribution of authentic signal's standard deviation.

The spoofing environment is illustrated in Figs. 3 and 4. The authentic GPS signal was collected by an antenna installed outside the laboratory and sent to the GPS signal repeater, which is installed in the blocked laboratory. Then the repeater transmits the received signal using a single antenna to spoof target GPS receivers. The receivers estimated the C/No of spoofing signal and logged it into the computer. Similarly to the authentic signal, the distribution of R_i's standard deviation for spoofing signal was obtained.

The primary errors in the estimation of C/No are the white noise introduced in the measuring process, and the calculation of C/No within the GPS receiver includes a rooting operation. Hence, it is reasonable to use the Chi distribution to fit the standard deviation of R_i. As shown in Fig. 5, a noncentral Chi distribution was applied to the authentic signal and a Chi distribution was fitted to the spoofing signal. It is clear that the two distributions, namely the authentic and spoofing signals, have a good separation. As spoofing signal's standard deviation is more concentrated in left side, it is intuitive to find a good threshold for the detection.

In Fig. 6 we carry out the search for the optimal threshold with the least sum of false alarm probability and miss detection

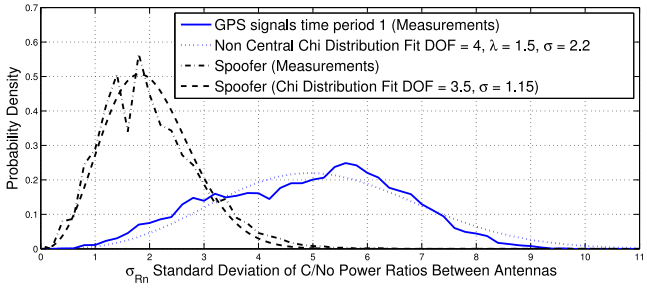

Fig. 5. Estimated PDF of the standard deviation of the power ratio Rn between antennas for real GPS signals and spoofer.

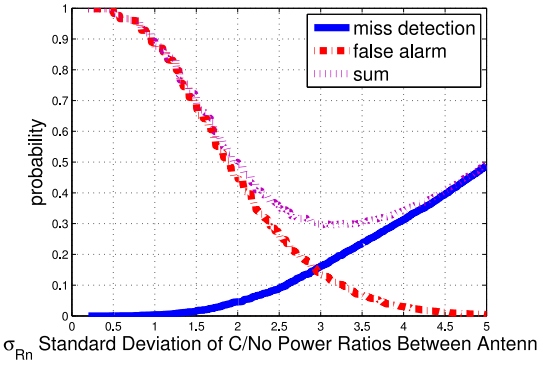

Fig. 6. Probabilities of false alarm, miss detection and their sum under different σ_{R_n}.

probability. Based on this threshold, we define a random variable $D_i(m,t)$ to describe the status of the standard deviation in physical layer

$$D_i(m,t) = \begin{cases} 1 & m < threshold \\ 0 & m > threshold \end{cases} \tag{5}$$

where m is the estimated value of the standard deviation for R_i. Let S represent the event that the GPS is under spoofing and $\bar{S}$ represents the event that the GPS is under a good working condition. With these definitions, four conditional probabilities are obtained from the distribution of the standard deviations

$$P_{i,sd} = P(D_i(m,t) = 1|S) \tag{6}$$

and

$$P_{i,md} = P(D_i(m,t) = 0|S) \tag{7}$$

and

$$P_{i,fa} = P(D_i(m,t) = 1|\bar{S}) \tag{8}$$

and

$$P_{i,gd} = P(D_i(m,t) = 0|\bar{S}) \tag{9}$$

where $P_{i,sd}$, $P_{i,md}$, $P_{i,fa}$, $P_{i,gd}$ are the probabilities of spoofing detected, miss detection, false alarm and good condition detected for the ith GPS receiver, respectively. These probabilities provide primary reference to distinguish whether the GPS receiver is under spoofing, and are fed to the upper layer as the prior probabilities for the trustworthiness evaluation, which will be discussed in the next section.

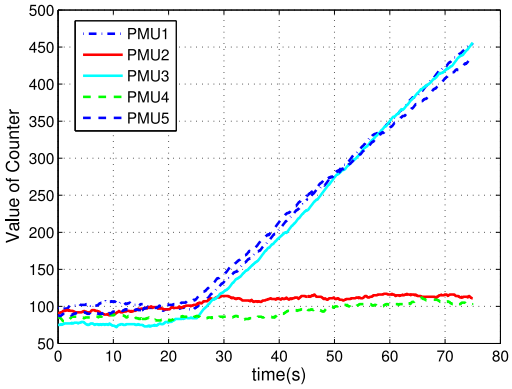

Fig. 7. Counter embedded in physical layer which reflects the suspicious level of PMU being spoofed.

C. Suspicious Level Counter

As shown in Fig. 6, when using the optimal point as threshold to define the random variable $D_i(m,t)$, the sum of false alarm probability and miss detection probability reaches approximately 0.3, which is not satisfying in practical applications. Besides, the threshold based detection mechanism cannot not provide the suspicious level of certain value of measurement, since any value on the same side of the threshold would be treated as the same regardless of how far away the value is from the threshold. To address these concerns, a counter is introduced. We believe that the spoofing attack is continuous in the time. Then we define

$$Cnt_i = \sum_{k=t}^{t+n} D_i(m,k) \tag{10}$$

where $D_i(m,k)$ is the ith random variable (defined as before) at time slot k and n is the observation window size. It is intuitive that the GPS receiver under spoofing would have a larger counter, which indicates a high suspicious level of this receiver. The key to implement the counter is the choice of the observation window size. A larger window size provides good reliability because more samples could average and eliminate the influence of randomness and noise. However, more samples require more initialization time. In our experiment, the choice of the window size is influenced by the threshold of standard deviation for C/N difference described above according to our simulation as well as the requirement for the detection response time. We set the sampling rate as 50 times per second and believe 6 s is reasonable for the response time. Therefore, the window size is 300. Fig. 7 shows the performance of the counter under normal and spoofing conditions.

IV. Upper Layer Detection Mechanism

In this section, we discuss the GPS spoofing detection in the upper layer. A linear system model is introduced to describe the power grid around the equilibrium point. Based on this linear system model, we propose a mechanism for evaluating the trustworthiness of each PMU.

A. Linear System Model

Basically, the power system is a nonlinear interconnected system with small signal stability and damping control for low-frequency oscillations [16]. However, in many cases, linear model could be considered to approximate the operation of the power grid system when it is around the equilibrium point [17]. In this paper, we would focus on the linear model and will extend it into nonlinear models in the future.

The dynamics of the linearized power system could be expressed as the following state space model, which is given by:

$$\boldsymbol{x}(t+1) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{w}(t) \tag{11}$$

$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{n}(t) \tag{12}$$

where $\boldsymbol{x}(t)$ and $\boldsymbol{y}(t)$ are the $N \times 1$ state vector and $M \times 1$ measurement vector of the power system, respectively. $\boldsymbol{A}$ is the linearized matrix that describe the system model and $\boldsymbol{B}$ is the control matrix which adds the control vector $\boldsymbol{u}(t)$ from the control center to the power grid system. $\boldsymbol{w}(t)$ and $\boldsymbol{n}(t)$ are considered to be the Gaussian noise. For simplicity, instead of continuous system model, the discrete model is considered in our paper. Some specific details and assumptions are set in our system for the simulation of spoofing attack and the implementation of the detection mechanism.

1) Every node in the system is connected to one PMU and a reliable communication network is installed for PMU to transmit the collected measurement to the control center with its own time stamp.
2) The controller adopts the linear quadratic regulation (LQR) control [18] in an infinite time horizon with the cost function given by

$$J = E\left[\sum_{t=0}^{i} nf\beta(t)\left(\boldsymbol{x}^T(t)\boldsymbol{Q}\boldsymbol{x}(t) + \boldsymbol{u}^T\boldsymbol{P}\boldsymbol{u}(t)\right)\right] \tag{13}$$

where $\boldsymbol{Q}$ and $\boldsymbol{P}$ are positive definite matrices and β is a weighting factor for control [19].
3) The spoofing attack may not only change PMUs time stamp via disconnecting the PMUs time synchronization from UTC, but also influence the collecting time interval of the A/D converter inside the PMU, which is equivalent to change the measurement value collected by spoofed PMU due to the time misalignment between the PMUs.

B. Trustworthiness Evaluation

The idea of our trustworthiness evaluation is, when given some value of the parameter derived from power grid system's measurements (phase from PMU in our paper), we use the prior probabilities from another source to calculate the corresponding conditional probability which evaluates the possibility that the event (spoofing in this paper) happens when such value is obtained. In this paper, we define the trustworthiness level of the system at time slot t $\pi_n(t)$, which is given by

$$\pi(t) \triangleq P(S|E(t)) \tag{14}$$

where S represents the event that the spoofing attack happens and $E(t)$ is the system's measurement error at time slot t, which will be further discussed in detail later. Obviously, a larger $\pi(t)$ indicates a higher suspicious level of the system being spoofed.

We first use a state estimation method to obtain the error between the measurements and the estimated value. As the measurements from all nodes in the system are coupled with each other and thus provide redundancies, we can predict the system's future state with some uncertainty using Kalman filter. At time slot $t+1$, the predicted state vector $\hat{\boldsymbol{x}}(t+1)$ is calculated from the state vector $\boldsymbol{x}(t)$ and measurement vector $\boldsymbol{y}(t)$ as

$$\hat{\boldsymbol{x}}(t+1) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{P}(t+1)\left[\boldsymbol{y}(t) - \boldsymbol{C}_{-n}\boldsymbol{A}\boldsymbol{x}(t)\right] \tag{15}$$

where $\boldsymbol{x}(t)$ includes several system states such as the phase, voltage and amplitude and $\boldsymbol{y}(t)$ is the phase measured from each PMU. $\boldsymbol{C}_{-n}$ denotes the matrix C excluding the nth row. The covariance matrix $\boldsymbol{P}(t+1)$ is given by [21], and

$$\boldsymbol{K}(t+1) = \boldsymbol{F}(t+1|t)\boldsymbol{C}_{-n}^T\left[\boldsymbol{C}_{-n}\boldsymbol{F}(t+1|t)\boldsymbol{C}_{-n}^T + \boldsymbol{R}\right] \tag{16}$$

where $\boldsymbol{R}$ is the measurement noise matrix and $\boldsymbol{F}(t+1|t)$ is the prediction covariance, which is given by

$$\boldsymbol{F}(t+1|t) = \boldsymbol{A}\boldsymbol{F}(t|t)\boldsymbol{A}^T + \boldsymbol{B}\boldsymbol{Q}\boldsymbol{B}^T \tag{17}$$

where $\boldsymbol{Q}$ is the system process noise matrix.

As the spoofing attack will significantly influence PMUs measurement on the phase, we focus on the error of phase in our case. The measurement error is calculated as

$$E(t) = \sqrt{\sum_{i=1}^{n} r_i(t)^2} \tag{18}$$

where $r_i(t)$ is computed as the normalized residuals

$$r_i(t) = \frac{y_i(t) - \hat{x}_i(t)}{\sigma_i}. \tag{19}$$

Normally, the measurement error is fitted to the Chi-square distribution, because the noise introduced in the Kalman filter is Gaussian noise, and thus $r_i(t)$ has the standard normal distribution. Similar to the bad data detection [20], any error exceeds the preset threshold would be treated as an abnormal one, because under the Chi-square distribution the conditional probability $P(E(t) > threshold|M)$ would be so small that the event $\{E(t) > threshold|M\}$ is considered to hardly happen.

We apply the Bayes' theorem to (14) and obtain

$$\pi(t) = P(S|E(t)) \tag{20}$$

$$= \frac{P(E(t)|S)P(S)}{P(E(t))} \tag{21}$$

$$= \frac{P(E(t)|S)P(S)}{P(E(t)|S)P(S) + P(E(t)|\bar{S})P(\bar{S})} \tag{22}$$

where $P(S)$ $(P(\bar{S}))$ is the prior probability that spoofing attack happens (or not), which determines the sensitivity and reliability of our algorithm. The larger $P(S)$ is, the larger trustworthiness value the algorithm outputs. However, the trustworthiness of system under the normal condition will also increase, because with the increase of sensitivity, any small

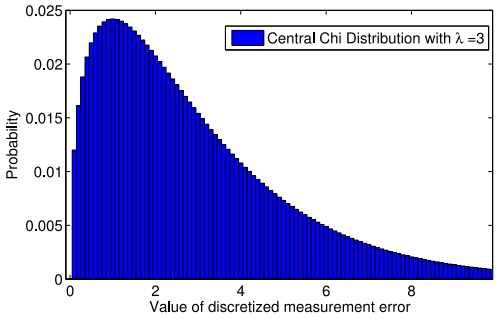

Fig. 8. Probability density function of discrete measurement error when system is under normal operation.

turbulence in measurements under normal condition may be considered as the error resulted from spoofing attack.

$P(E(t)|\bar{S})$ in (22) is the conditional probability depicting the possibility that $E(t)$ is obtained under normal condition, which could be fitted to the chi-square distribution. However, as the distribution of $E(t)$ under normal condition is continuous, we cannot obtain the accurate probability of a certain point. In this paper, we define a discrete random variable to approximate $E(t)$. By dividing the value field of $E(t)$ $[E_{\min}(t), E_{\max}(t)]$ into n_g equivalent grids, we have

$$M(t) \triangleq E_{\min}(t) + \frac{E_{\max}(t) - E_{\min}(t)}{n_g} n_c \tag{23}$$

where n_c is defined as

$$n_c = \left\{ n \in Z | E(t) \leq \frac{nE_{\max}(t) - (n_g - n)E_{\min}(t)}{n_g} \&\& \right.$$
$$\left. E(t) \geq \frac{(n+1)E_{\max}(t) - (n_g - n - 1)E_{\min}(t)}{n_g} \right\}. \tag{24}$$

Then the probability of $M(t)$ could be calculated as

$$P(M(t)|\bar{S}) = \int_n^{n+1} pdf_{C(t)|\bar{S}}(m)dm. \tag{25}$$

The probability density function (pdf) of $M(t)$ has approximately the same shape as $E(t)$ as shown in Fig. 8, a chi-square pdf curve with different scaling, which is resulted from the integration among the grid. We replace $E(t)$ with $M(t)$ in (22) and obtain the conditional probability in (22) by (25)

$$\pi(t) = \frac{P(M(t)|S)P(S)}{P(M(t)|S)P(S) + P(M(t)|\bar{S})P(\bar{S})}. \tag{26}$$

Essentially, the upper layer detection mechanism can efficiently detect the abnormal measurement error in the power system. However, this mechanism cannot distinguish the source of the error. In other words, the measurements error caused by spoofing attack or power system itself will be treated as the same situation, such that the control center may take incorrect or unnecessary actions toward such a problem. In the next section, cross layer detection algorithm is proposed to solve this problem.

V. Cross-Layer Detection

In this section, the cross-layer detection algorithm is presented. We first propose an improved version of trustworthiness value that combines the information from both physical layer and upper layer probabilistically. Then a detection scheme based on the trustworthiness value is proposed with the awareness of possibly more than one PMUs being spoofed.

A. Improved Trustworthiness Value

As both physical layer and upper layer have probabilistic structures, it is intuitive to integrate these two frameworks. The information from physical layer could help the upper layer to distinguish the source of the measurement error while the information from upper layer could help to improve the accuracy of physical layer in detection.

We redefine (14) as

$$\pi(t) \triangleq P(S|M(t), D_{i,t}(m), i = 1...n). \tag{27}$$

Again, by applying the Bayes' rule, we have

$$\begin{aligned} \pi(t) &= P(S|M(t), D_{i,t}(m), i = 1...n) \\ &= \frac{P(S)P(M(t), D_{i,t}(m), i = 1...n|S)}{P(M(t), D_{i,t}(m), i = 1...n)} \end{aligned} \tag{28}$$

where $D_{i,t}(m)$ is the random variable defined in (5) and n is the number of the PMU.

We assume that the measurements in the upper layer and physical layer are mutually independent, then we have

$$\pi(t) = \frac{P(S)P(M(t)|S)P(D_{i,t}(m), i = 1...n|S)}{P(M(t))P(D_{i,t}(m), i = 1...n)}. \tag{29}$$

As PMUs are distributed separately and a single spoofer cannot spoof multiple PMUs at the same time (although in our system multiple PMUs could be spoofed by multiple spoofers simultaneously), it is reasonable that the measurements from different PMUs in physical layer are mutually independent, thus resulting in

$$\pi(t) = \frac{P(S)P(M(t)|S)\prod_{i=1}^{n} P(D_{i,t}(m)|S)}{P(M(t))\prod_{i=1}^{n} P(D_{i,t}(m))}. \tag{30}$$

Using the law of total probability, we extend (30) to

$$\pi(t) = \frac{P(S)P(M(t)|S)}{P(M(t)|S)P(S) + P(M(t)|\bar{S})P(\bar{S})} \prod_{i=1}^{n} \frac{P(D_{i,t}(m)|S)}{P(D_{i,t}(m)|S)P(S) + P(D_{i,t}(m)|\bar{(S)})P(\bar{S})}. \tag{31}$$

Components in (31) are obtained from both physical layer and upper layer.

B. Multiple Attackers Spoofing Scheme

Based on the trustworthiness value introduced above, we design the detection scheme against multiple spoofing attackers. At every time slot t when a new measurement is collected (normally 0.1 s in PMU), the calculation of trustworthiness value is invoked to detect whether the power system is under spoofing and the counter is investigated to detect which PMUs are being suspicious to be spoofed. The steps of the scheme are given as follows.

1) Calculate the corresponding $\pi(t)$ with present data.
2) If $\pi(t)$ is small, the system is considered to be in a good condition. Update the counter Cnt_i.

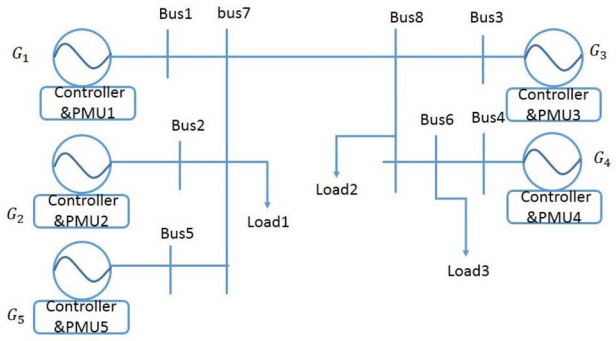

Fig. 9. Illustration of the five-bus power network used in the numerical simulations.

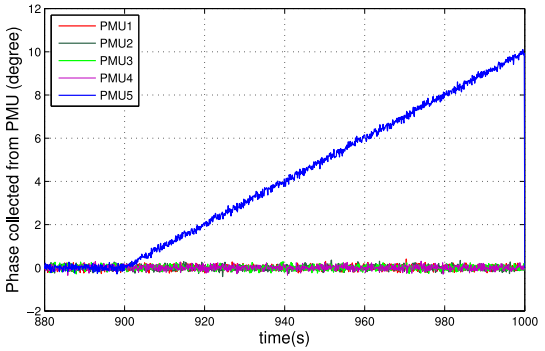

Fig. 10. Change of the phase measurement from PMU. PMU 5 is being spoofed at the 900th second and the phase deviates ten degree within 2 min.

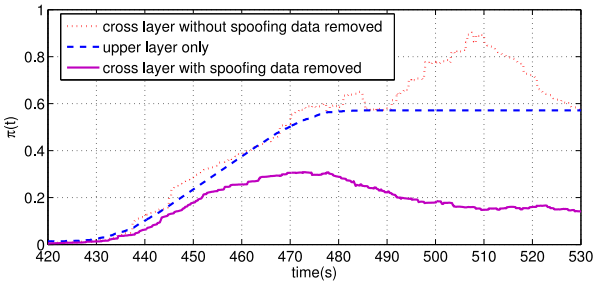

Fig. 11. Suspicious level under the attack strategy with one spoofer.

3) If $\pi(t)$ is beyond the normal range of the value, then a spoofing attack will be suspected.
4) Look up the counters in the physical layer, find the PMU with the largest counter to be the most dubious. Delete this PMUs measurement data and go back to the first step. In other words, our scheme works iteratively on the certain time slot until all the spoofing PMUs are detected.

VI. Experimental Results

In this section, the experiment result is presented to verify our proposed detection mechanism. We first introduce the experiment environment, then we will apply the mechanism to the scenario that the there is only one attacker and extend it to the case of multiple attackers.

A. Experiment Environment

We consider a five-node power network illustrated in Fig. 9. It has five generators (G1, G2, G3, G4, G5), eight buses and three loads. As the physical layer environment with hardware has been introduced in Section III, this subsection will focus on the upper layer. The five PMUs collect the measurement every 0.1 s and by assumption the measurement from all the PMUs are transmitted to the control center simultaneously. Then the spoofer attacks one of the PMUs and modifies its measurement before transmitted to the control center. The spoofing strategy is similar to the field test result implemented in [4], shown in Fig. 10. The modified phase measurement deviates its true value at the speed of about 0.8 degree per second, which breaks the IEEE C37.118 Standard [2] of PMU within 2 min.

B. Cross Layer Detection

Given the spoofing scenario, we deploy our detection scheme to the system. In Fig. 11, at time slot $t = 430$ s, the spoofing attack is launched and the phase deviation will increase as time progresses. The trustworthiness value $\pi(t)$ in both upper layer and cross-layer schemes increase. We first run our detection algorithm without removing detected spoofed PMU data. In this case, $\pi(t)$ from the cross-layer scheme outperforms the detection only using the data in upper layer, when the deviation becomes large. This is obvious because in the physical layer it takes some time to sample and calculate the counter, which is explained above, and when the deviation becomes large, due to (31), the factor given by

$$\prod_{i=1}^{n} \frac{P(D_{i,t}(m)|S)}{P(D_{i,t}(m)|S)P(S) + P(D_{i,t}(m)|(\bar{S}))P(\bar{S})} \tag{32}$$

becomes larger, consequently increasing the whole trustworthiness value.

When the removing scheme is included, the trustworthiness value will significantly decrease when the data of the spoofed PMU is removed.

To further test the efficiency of proposed algorithm, we set the scenario that three of the five PMUs in the system are spoofed. Fig. 12 shows the detailed detection process. When a new PMU is detected to be spoofed and its data is removed, $\pi(t)$ will suffer a period of decreasing process before being steady again. The three spoofed PMUs are detected one by one until the trustworthiness value $\pi(t)$ recovers to a normal value. Besides, in our algorithm, the time interval for the detection of two spoofed PMUs is within 20 s, which is acceptable because normally the spoofing process would last more than 200 s before it could create obvious negative influence on the power system.

In Fig. 13, we deploy our detection mechanism to another scenario where the measurement from some PMUs is abnormal because of systematic problem within the power system instead of spoofing attack at the $t = 650$ s. It demonstrates that without the help of the prior probability from the physical layer, $\pi(t)$ in upper layer is large in both conditions, such that it cannot distinguish the source of measurement error, while our cross-layer mechanism obtains obviously different results in two scenarios. Notice that the spoofing stops at about $t = 550$ s. $\pi(t)$ from the cross-layer scheme decreases

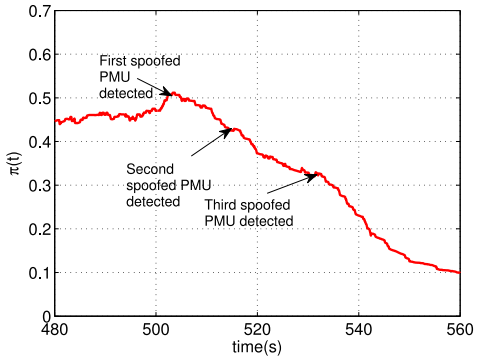

Fig. 12. Detect the suspicious PMU one by one.

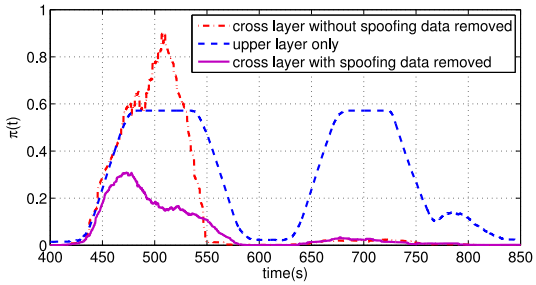

Fig. 13. Suspicious level under the attack strategy and system fault.

significantly, while $\pi(t)$ from upper layer takes much more time. This is because, once the spoofing is stopped, the spoofed PMU can resynchronize its time and its measurement is back to normal. It takes some time for the Kalman filter to track the system state.

VII. Conclusion

In this paper, we have proposed a cross-layer detection mechanism to detect multiple spoofing attacks against smart grid. In physical layer, we propose the angle-of-arrival based mechanism. By obtaining the distribution of the normal and spoofed standard derivation of the difference of the C/No from different antennas, we calculate the prior probability of spoofing, which is fed to the upper layer for further detection. In the upper layer, we apply the Kalman filter to estimate the state of power system and use the measurement error to calculate the trustworthiness value of being spoof. Finally, we combine the information from both physical layer and upper layer to integrate the cross-layer mechanism. Numerical results have demonstrated that the cross-layer detection scheme can efficiently detect the spoofing attack.

References

[1] A. G. Phadke, "Synchronized phasor measurements in power systems," *IEEE Comput. Appl. Power*, vol. 6, no. 2, pp. 10–15, Apr. 1993.
[2] *IEEE Standard for Synchrophasors for Power Systems, 2005*, IEEE Std. C37.118 Revision 1344, 1995.
[3] H. Wen, P. Y. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. 18th Int. Tech. Meeting Satell. Divis. Inst. Navig. (ION GNSS)*, Long Beach, CA, USA, Sep. 2005, pp. 1285–1290.
[4] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protect.*, vol. 5, no. 3, pp. 146–153, Dec. 2012.
[5] (2001). "Vulnerability assessment of the transportation infrastructure relying on the global positioning system," John A. Volpe Nat. Transport. Syst. Center, U.S. Dept. Transp, Cambridge, MA, USA, Tech. Rep. [Online]. Available: http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf
[6] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.
[7] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.
[8] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Divis. Inst. Navig. (ION GNSS)*, vol. 55. Savannah, GA, USA, 2008, pp. 2314–2325.
[9] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar./Apr. 2009.
[10] H. J. A. Ferrer and E. O. Schweitzer, III, *Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems*. Pullman, WA, USA: Schweitzer Engineering Labs, 2010.
[11] C. Taylor, D. Erickson, K. Martin, R. Wilson, and V. Venkatasubramanian, "WACS-wide-area stability and voltage control system: R&D and online demonstration," *Proc. IEEE*, vol. 93, no. 5, pp. 892–906, May 2005.
[12] T. E. Humphreys. (2012, Jul.). *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing* [Online]. Available: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf
[13] R. Lemos. (2007). "SCADA system makers pushed toward security," *Security Focus* [Online]. Available: http://www.securityfocus.com/news/11402
[14] E. L. Key, "Techniques to counter GPS spoofing," Internal memorandum, MITRE Corporation, Bedford, MA, USA, Feb. 1995.
[15] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver*. Boston, MA, USA: Birkhfauser, 2007.
[16] J. Liu, A. Gusrialdi, S. Hirche, and A. Monti, "Joint controller communication topology design for distributed wide-area damping control of power systems," in *Proc. 18th IFAC*, Milan, Italy, 2011, pp. 519–525.
[17] J. Machowski, J. Bialek, and J. Bumby, *Power System Dynamics: Stability and Control*. Hoboken, NJ, USA: Wiley, 2008.
[18] H. Kwakernaak and R. Sivan, *Linear Optimal Control Systems*, 1st ed. Hoboken, NJ, USA: Wiley, 1972.
[19] B. Wu and O. P. Malik, "Multivariable adaptive control of synchronous machines in a multimachine power system," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1772–1781, Nov. 2006.
[20] J. Lin and H. Pan, "A static state estimation approach including bad data detection and identification in power systems," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Los Alamitos, CA, USA, 2007, pp. 1–7.
[21] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. New York, NY, USA: Springer, 1994.
[22] Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "Combating time synchronization attack: A cross-layer defense mechanism," in *Proc. ACM/IEEE Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Philadelphia, PA, USA, 2013, pp. 141–149.
[23] A. Giani *et al.*, "Smart grid data integrity attacks: Characterizations and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, Oct. 2011, pp. 232–237.
[24] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

Yawen Fan received the B.S. degree in electronics engineering from Fudan University, Shanghai, China, in 2013. He is currently pursuing the Ph.D. degree in electronic and electrical engineering from the Department of Electrical Engineering and Computer Science (EECS), University of Tennessee, Knoxville, TN, USA, under the supervision of Dr. H. Li.

He is currently a Research Assistant with the Department of EECS, University of Tennessee. His current research interests include global positioning systems, area communication, and communications for distributed learning with big and distributed data.

Zhenghao Zhang received the B.S. degree in telecommunication engineering and the Ph.D. degree in information system and telecommunication engineering from Xidian University, Xi'an, China, in 2005 and 2011, respectively. He is currently pursuing the Ph.D. degree from the Department of Electrical Engineering and Computer Science (EECS), University of Tennessee, Knoxville, TN, USA, under the supervision of Dr. H. Li.

From 2011 to 2012, he was a Research Assistant with EECS, University of Tennessee. He is currently a faculty member with the Electrical and Information College, Jinan University, Guangzhou, China. His current research interests include wide-band cognitive radio, compressed sensing, and Internet of things.

Dr. Zhang was the recipient of the Chinese National Scholarship.

Matthew Trinkle received the B.Eng. (Hons.) degree in electrical electronic engineering, and the B.Sc. degree in mathematical and computer science from the University of Adelaide, Adelaide, SA, Australia, in 1994 and 1995, respectively.

From 1996 to 2004, he was with the Cooperative Research Centre for Sensor Signal and Information Processing, where he joined the area of adaptive algorithms for global positioning system (GPS) interference suppression. Since 2005, he has been with the University of Adelaide, SA, Australia, where he was involved in a number of research projects in the area of phased array processing for GPS, radar, and accoustics.

Aleksandar D. Dimitrovski received the B.Sc. and the Ph.D. degrees in electrical engineering with emphasis on power from the University Saints Cyril and Methodius, Skopje, Macedonia, and the M.Sc. degree in applied computer sciences from the University of Zagreb, Zagreb, Croatia.

He is a Chief Scientist of Power and Energy Systems, Oak Ridge National Laboratory and a Joint Faculty with the University of Tennessee, Knoxville, TN, USA. He was with Schweitzer Engineering Laboratories, Pullman, WA, USA, and with Washington State University, Pullman, first as a Post-Doctoral Fellow and then as a Visiting Professor. He was a Tenured Professor with the University Saints Cyril and Methodius. His current research interests include uncertain power systems, their modeling, analysis, protection, and control.

Ju Bin Song received the B.Sc. and the M.Sc. degrees in 1987 and 1989, respectively, and the Ph.D. degree in electronic and electrical engineering from the Department of Electronic and Electrical Engineering, University College London (UCL), London, U.K., in 2001.

From 1992 to 1997, he was a Senior Researcher with the Electronics and Telecommunications Research Institute, Daejeon, Korea. He was a Research Fellow with the Department of Electronic and Electrical Engineering, UCL, in 2001. During 2002–2003, he was an Assistant Professor with the School of Information and Computer Engineering, Hanbat National University, Daejeon. He is currently a Professor with the Department of Electronics and Radio Engineering, Kyung Hee University, Seoul, Korea, since 2003. He served as Head of the Department of Radio Engineering, Kyung Hee University, in 2005. From 2009 to 2010, he was a Visiting Professor with the Department of Electrical Engineering and Computer Science, the University of Houston, Houston, TX, USA. His current research interests include resource allocation in communication systems and networks, cooperative communications, game theory, optimization, cognitive radio networks, and smart grid.

Dr. Song serves as a member of the Technical Program Committee for international conferences on communications and networks and is an Editor of the *International Journals on Communications and Networks*. He was the recipient of the Kyung Hee University Best Teaching Award in 2004 and 2012.

Husheng Li (S'00–M'05) received the B.S. and the M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1998 and 2000, respectively, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2005.

From 2005 to 2007, he was a Senior Engineer at Qualcomm Inc., San Diego, CA, USA. In 2007, he joined the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA, as an Assistant Professor, and was promoted to Associate Professor in 2012. He is also an International Scholar of Kyung Hee University, Seoul, Korea. His current research interests include wireless communications and smart grid.

Dr. Li was the recipient of the Best Paper Award of the *The European Association for Signal Processing Journal of Wireless Communications and Networks* in 2005 (together with his Ph.D. Advisor: Prof. H. V. Poor), the Best Demo Award of Globecom in 2010, and the Best Paper Awards of Internation Conference on Communications and SmartGridComm in 2011 and 2012.