Smart Grid Conference 2015
SGC 2015
23-24 December 2015
Iran University of Science and Technology

کنفرانس شبکه‌های هوشمند ۹۴
دانشگاه علم و صنعت ایران، ۱ و ۲ دی‌ماه ۱۳۹۴

A Novel PMU Anti-Spoofing Algorithm Based on Smart Grid Infrastructures

Mohammad Yasinzadeh*, Dr. Mahdi Akhbari**

*Engineering Faculty of Shahed University, m.yasinzadeh@shahed.ac.ir

** Engineering Faculty of Shahed University, Akhbari@shahed.ac.ir

Abstract: *Phasor measurement unit (PMU) GPS receiver spoofing has been addressed in the recent literatures. Having spoofed GPS signals, the spoofer can inject bad data into power system control center and consequently the protection system will face serious problems. The existing anti spoofing techniques are all based on GPS signal analysis and are just able to detect spoofing. However, as PMUs are placed in optimum numbers, refining the bad data without any PMU outage is also an important case. It should be notified that some of the existing methods require additional infrastructures besides power grid infrastructures which are not economically attractive.*

In this paper, a novel anti spoofing algorithm has been proposed based on smart grid infrastructures. The algorithm is not only able to detect PMU GPS receiver spoofing, but also is able to refine counterfeit measurements. Vestigial signal analysis is also applied to remove fake signals. The defects of the existing anti spoofing algorithms have been discussed and the effectiveness of the proposed algorithm has been proved through simulation.

Key words: PMU, Spoofing, GPS signal, Bad data.

1. Introduction

Power grid's safety is an important issue. Many investigations and efforts have been made to make power grid as secure as possible using the existing infrastructures. Any defective measurements or cyber risks threaten power grid's security. Hence, many authors have proposed valuable algorithms to deal with bad data and consequently, ensure grid security, e.g. [1-6].

Application of computers in supervisory control and data acquisition (SCADA) has made power grid vulnerable to cyber risks [7]. It will be so threatening if a hacker gets access to power system control network, computers and protection hardware. As the hacker can inject bad data by manipulating the measurements and subsequently cause protection system to malfunction. A threat which has been recently addressed by some literatures is PMU GPS receiver spoofing.

PMUs provide us with synchronic voltage and current phasors from remote parts of the power grid using a common time reference.

PMUs are considered one of the most important measuring devices in the future of power systems. They are also being applied in smart grids due to the increased interest in measures of phase angle. The great dynamism of loads and high penetration of distributed energy resources, make phase angle measurement important for smart grid's real time monitoring and control [8].

Thus, the validity of synchrophasors plays an important role in power system's security. In some literatures, the vulnerability of PMUs to time synchronization attacks has been studied [9-12].

PMUs from dispersed locations of the power grid are synchronized using common time reference of a global positioning system (GPS). The GPS receiver of a PMU receives GPS signals from different satellites in radio frequency (RF). These signals contain unencrypted C/A code, which is basically used in civilian applications, e.g. PMU receivers, and the encrypted P(Y) code, which is basically applied for military aims. Unfortunately, unencrypted civil GPS signals are vulnerable to spoofing attack [13].

A GPS spoofing attack tires to deceive a GPS receiver by broadcasting fake GPS signals, which resemble a set of authentic GPS signals, or by rebroadcasting authentic signals which are recorded at a different time.

A variety of methods have been proposed to deal with GPS spoofing. Some of these methods use external hardware like low cost inertial and magnetic sensors, odometers, stable clocks with high precious and cellular networks [14-15]. The aim is to deal with the problem based on the existing infrastructures and with the lowest price, thus, external assistance is not recommended. In some research works, authors attempt to use signal characteristics, rather than external hardware. Like

signal's power [16-17], quality [18] and angle of arrival (AOA) [10, 19-20].

In [17] a monitoring mechanism is applied in the RF front end using automatic gain control to detect spoofing. In the spoofing process, the fake signal has to overpower the authentic one so that a victim receiver will lock on to the more powerful fake signal. Thus, an abrupt increase in signal power implies the possibility of a spoofing attack. Therefore, checking for signal's power can be regarded as a countermeasure against spoofing. The main drawback of this method is the low certainty due to the stochastic nature of GPS signal power.

[10] proposes a cross-layer defense mechanism. The proposed mechanism uses angle of arrival (AOA) of the received signals to detect spoofing attack. The idea of AOA detection method is based on the fact that authentic signals from different satellites have different AOA. However, fake signals which are broadcasted from spoofer antenna have the same AOA.

The methods which are based on AOA, e.g. [10, 19-20], need an extra antenna array which is not economically attractive. The drawback of this technique is also highlighted when a skilled spoofer uses different antennas in dispersed positions to broadcast the fake signals.

Some other literatures are based on cryptographic techniques [13, 21-23]. [13] for example, proposes a signal authentication architecture based on a network of cooperative receivers. The idea is based on the fact that a receiver in the network correlates its received military P(Y) signal with those received by other receivers. This can be an affective countermeasure against spoofing. However, some cryptographic authentication techniques basically require the modification of civil GPS signal structure, which may not be adopted by the whole GPS industry [10].

All the mentioned methods are valuable research works which deal with spoofing attack. However, this paper doesn't suggest using the above methods to deal with the spoofing of PMUs. Because the existing infrastructures of smart grids can easily act against spoofing attacks. At the same time PMU GPS receiver is a static receiver and its operation can easily be evaluated by PMU measurements.

There are many bad data processing (BDP) algorithms which have previously been proposed in different literatures. Some of the BDP algorithms are also affective algorithms which may treat spoofing attack like any other bad data injection attacks. One may argue that some of the proposed BDP algorithms have the ability of detecting bad data caused by spoofing attacks. It should be pointed out that spoofing is more dangerous and probable than any bad data injection attacks as the attacker doesn't need to have access to power grid hardware. The attacker can easily perform the spoofing at anywhere outside the substations. Therefore, detecting bad data is not the only goal here. Refining the manipulated measurements and finding their origin are also crucial goals. Having detected spoofing attack, it is essential to stop spoofing process. This may not be possible unless spoofing is investigated separately from bad data injection attacks.

In this paper, a novel algorithm is proposed to deal with the spoofing through smart grid infrastructure and measurement analysis. Not only is it able to detect spoofing, but also it refines the bad data produced by spoofing.

The organization of this paper is as follows. Section two describes the spoofing process. The effect of spoofing on power grid is discussed in section three. The proposed anti spoofing algorithm is explained in Section four. Section five and six contain, respectively, simulation results and conclusions.

2. The Description of Spoofing Process

In the spoofing attack, the attacker first receives authentic GPS signals and then manipulates them in order to generate fake signals. Having generated the fake signals based on the threatening aims; it's time to rebroadcast them. The signal acquisition of the GPS receiver is designed to search for the signals with highest signal to noise ratio (SNR) in a two dimensional space of code phase and carrier frequency. The GPS receiver tracks these signals and uses their information. To carry out the spoofing of GPS receiver, the spoofer needs to generate the signal which has higher SNR than the authentic one. Therefore, the spoofer first searches in the mentioned two dimensional space so that the fake signal overlaps the authentic one. Then a slight increase in fake signal's SNR, causes the GPS receiver to lock on the fake signal and lose the track of the authentic one. Having misled the receiver, the spoofer can launch the threatening plans by changing clock offset or position information of the receiver. As PMUs are static devices with certain positions, manipulating the position information is not the case here. However, changing the clock offset of the GPS receiver will result in erroneous data in the power grid.

3. The Effect of Spoofing in Power Grid

PMUs are installed at power grid buses and are able to measure the voltage phasor of the bus with all the current phasors of the adjacent lines. These measurements will be labeled by their relative time stamps and will be used in protection and control systems. When a spoofer changes the clock offset of the GPS receiver, the time stamps of the measurements are modified and consequently, phase angles of the measurement are modified. There are several types of spoofing attack which will have different effects on the measurements. [24] describes three spoofing models which are as follows: data-level spoofing, signal-level spoofing and bent pipe spoofing (also called *meaconing* or *replay attack*).

In both data-level and signal-level spoofing, the receiver's time solution is modified while its position solution is not. A skilled spoofer can launch a data-level spoofing without significantly changing the computed receiver position from its pre-attack value. Depending on the number of spoofed satellite signals, the spoofer can cause significant phase angle errors. The phase angle error resulting from this type of spoofing can reach to 52 degrees in a 60-Hz power system [24- 25].

In the signal-level spoofing, the spoofer transmits fake signals that carry the same navigation data as concurrently broadcast by the GPS satellites. In the replay attack, the authentic GPS signals are recorded and rebroadcasted with a time delay while the position solution is as the same of spoofer receiver's position solution. Therefore, the calculated time by the victim receiver is delayed and an error will be imposed to clock offset. The phase angle error resulting from this type of spoofing can be as high as 20 degrees in a 60-Hz power system [24-25].

This paper highlights some key points which reveal spoofing through measurement analysis. It should be notified that the spoofing doesn't change the magnitude of the measurements and it just affects their phase angle. On the other hand, the phase angles of the bus voltage and all the current phasors of the adjacent lines are shifted in the same way. Thus, all the phasors of the victim PMU, face a certain shift in their phase angles. It should also be pointed out that the power flows of the lines are case sensitive to voltage phase angles and these angles cannot change significantly like current phase angles.

4. The Proposed Anti-Spoofing Algorithm

4.1 The Description of Algorithm

The proposed approach is based on smart grid infrastructures, as conventional power grids may not be able to provide us with needed data redundancy. To launch the algorithm, the phasor measurements of each PMU are analyzed independently. Both current and voltage phasors are checked for tricky phase angle shift in short time intervals. The phase angle changes are either caused by power flow changes or by spoofing. Therefore, calculating the real phase angle changes caused by power flow changes, let us detect the tricky angle shifts. This can be easily carried out using well-known load flow algorithms, e.g. Newton-Raphson algorithm. Depending on the required precise and size of the grid one can chose between these algorithms. Having applied Newton-Raphson algorithm, the conventional power flow measurements are used to calculate phase angles. Smart grid infrastructures can easily provide us with power flow measurements from conventional instruments, therefore, bus voltages and angles are calculated using equation (1).

$$[J]\times\begin{bmatrix}\Delta\delta\\ \frac{\Delta V}{V}\end{bmatrix}=\begin{bmatrix}\Delta P\\ \Delta Q\end{bmatrix} \tag{1}$$

Where, *[J]* is the Jacobian matrix. $\Delta\delta$ and $\frac{\Delta V}{V}$ represent, respectively, angle and relative voltage changes of buses. ΔP and ΔQ represent, respectively, real and reactive power matrices which have been defined for Newton-Raphson algorithm.

As line parameters are known, line currents can be easily calculated using equation (2).

$$\begin{bmatrix}I_S\\ I_R\end{bmatrix}=[Y]\times\begin{bmatrix}V_S\\ V_R\end{bmatrix} \tag{2}$$

Where, I_s and I_R are sending and receiving currents of the line, respectively. And V_s and V_R are sending and receiving bus voltages. *[Y]* is the admittance matrix of the line and its elements are chosen based on the line model.

Let Φ_i^m be the measured phase angle matrix and Φ_i^c the calculated phase angles from equations (1) and (2) which are associated with the *i*th PMU. *D* will be a $(n+1)\times 1$ matrix which is defined as follows:

$$D_i=\Phi_i^m-\Phi_i^c \tag{3}$$

Where *n* is the number current phasors which are measured by *i*th PMU. If no spoofing occur, all the elements of *D* are zero. However, if a spoofing is in the process, all the elements of *D* are equal and non zero. This condition is shown in the following constraint:

$$D_i(1)=D_i(2)=\cdots=D_i(n+1)=\varepsilon_\theta\neq 0 \tag{4}$$

Where ε_θ is the tricky phase angle shift caused by spoofing. Constraint (4) is checked continuously in short time intervals. It reveals whether a spoofing is in the process or not. Using this method, not only spoofing is detected but also the bad data is refined by subtracting angle shift from measured phase angles. This is illustrated in equation (5).

$$\Phi_i^r=\Phi_i^m-\varepsilon_\theta[1]_{(n+1)\times 1} \tag{5}$$

Having detected spoofing and refined the bad data, it's time to stop spoofer. In this paper, a novel method has also been considered to stop any PMU spoofers. The idea is based on the fact that the authentic GPS signals, while less powerful than the spoofed ones, are still present in the environment. Therefore, when spoofing is detected there is chance to stop spoofer.

The receiver clock offset, t_u, is calculated using equation (6) as follows:

$$t_u = \frac{-1}{nc}\sum_{i=1}^{n}(\rho_i - r_i) \quad (6)$$

Where, r_i and ρ_i are *i*th satellite's pseudorange and true range, respectively. n is the number of visible satellites and c is the speed of light (299792458 m/s).

If spoofing changes the receiver clock offset from its pre-spoofing value, t_u^p , to t_u^s , a phase shift will be imposed to phase angle according to equation (7) [25].

$$\varepsilon_\theta = f \times (t_u^p - t_u^s) \times 360^o \quad (7)$$

Where, f is the power grid frequency.

As t_u^s is known and ε_θ is calculated from constrain (4), t_u^p , which is the true clock offset, can be calculated from equation (7). Having calculated the true receiver clock offset, algorithm searches for low power signals and calculates clock offset them using equation (6). If the calculated clock offset, t_u^c, matches the true clock offset, the receiver will track the low power signal and spoofing will be removed.

4.2 Flowchart of the Proposed Algorithm

The follow chart of the algorithm is shown in figure 1. This algorithm runs for each PMU separately.

In the first step, initial values for *[P],[Q],[V]* and *[I]* matrices are saved as authentic values for all the PMUs. In step 2, the mentioned matrices are updated using refined data or authentic data from previous stage. And phase angles are calculated using equation (1) and (2). In step 3, *[P],[Q],[V]* and *[I]* are updated by new measurements which are obtained from conventional power flow devices and PMUs. In the next step, D_i is calculated for the *i*th PMU and decision is made in step 5. If constrain (4) is not satisfied, then algorithm starts with step 2, updating the matrices. However, if any spoofing is detected, the data is refined using equation (5) and subsequently vestigial signal analysis is carried out to search for authentic low power signals.

In the last step, if authentic signals are found, the GPS receiver is ordered to track them.

5. Simulation Results

The simulation is carried on IEEE 14 bus system and the algorithms effectiveness is proved. Figure 2 illustrates IEEE 14 bus system with three PMUs which are placed on bus 2, 6 and 9 to ensure observablity of the system.

First, the sensitivity of phase angles to load changes is analyzed. Table 1 illustrates the changes of phase angles measured by PMU-2 in a scenario that the load of bus 3 experiences fast changes during seven minutes.

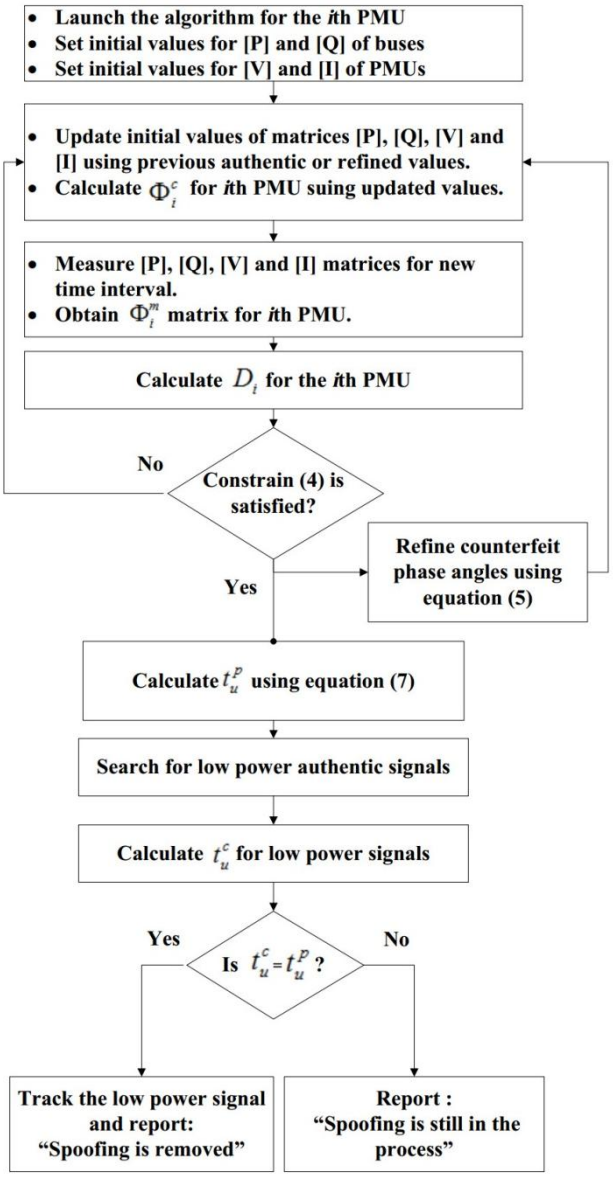

Fig. 1: The follow chart of the algorithm

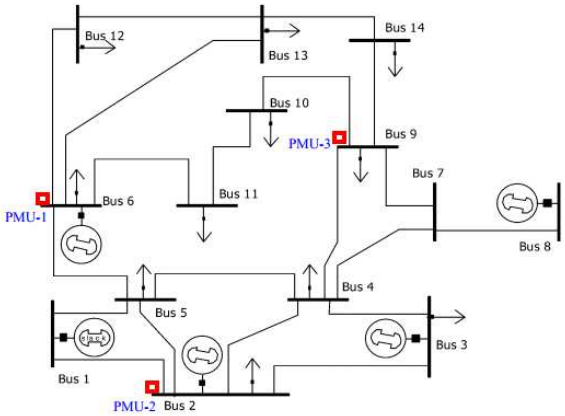

Fig. 2: IEEE 14 bus system with three PMUs for monitoring

Table 1: Sensitivity of phasor angles to load changes

Time (min)	Load3 (MW)	Voltage angle (deg.)	Line current angle(deg.)			
			L2-4	L2-5	L2-1	L2-3
0	5	-2.49	-3.40	-5.29	+171	-30.0
0.5	15	-2.55	-3.21	-5.30	+160	-25.3
1	16	-2.57	-3.20	-5.30	+165	-24.2
0.5	25	-3.08	-2.88	-5.31	-178	-18.5
2	40	-3.30	-2.81	-5.32	-176	-13.5
2.5	44	-3.50	-2.75	-5.35	-176	-12.5
3	50	-3.71	-2.6	-5.40	-177	-12.2
3.5	40	-3.30	-2.81	-5.32	-176	-13.5
4	74	-4.36	-2.53	-5.64	-175	-9.2
4.5	75	-4.36	-2.52	-5.65	-175	-9.1
5	80	-4.42	-2.55	-5.71	-175	-8.8
5.5	100	-5.03	-2.66	-6.07	-174	-7.7
6	100	-5.03	-2.66	-6.07	-174	-7.7
6.5	103	-5.05	-2.7	-6.10	-173	-7.2
7	74	-4.36	-2.53	-5.64	-175	-9.2

The algorithm checks for spoofing every 30 seconds and calculates D_2 for PMU-2 in a time interval of 30 seconds. In this case all the elements of D_2 are zero and constrain (4) is not satisfied, hence, the algorithm doesn't report any spoofing. Table 2 shows the results provided by the algorithm.

Table 2: Provided results of the algorithm in normal condition

D_2 elements	$D_2(1)$	$D_2(2)$	$D_2(3)$	$D_2(4)$	$D_2(5)$
Corresponding angle shift in 30 s	Bus voltage angle shift	L2-4 Current angle shift	L2-5 Current angle shift	L2-1 Current angle shift	L2-3 Current angle shift
Time (min)					
0	0	0	0	0	0
0.5	0	0	0	0	0
1	0	0	0	0	0
0.5	0	0	0	0	0
2	0	0	0	0	0
2.5	0	0	0	0	0
3	0	0	0	0	0
3.5	0	0	0	0	0
4	0	0	0	0	0
4.5	0	0	0	0	0
5	0	0	0	0	0
5.5	0	0	0	0	0
6	0	0	0	0	0
6.5	0	0	0	0	0
7	0	0	0	0	0

Another scenario is considered in which load 3 experiences fast changes and a spoofer has spoofed PMU-2. The spoofer imposes up to 1.6 degrees angle shift per minute to the measured data while no anti-spoofing algorithm exist. Table 3 depicts this scenario and shows how threatening the spoofing can be.

Table 3: Phasor angles under spoofing attack

Time (min)	Load3 (MW)	Voltage angle (deg.)	Line current angle(deg.)			
			L2-4	L2-5	L2-1	L2-3
0	5	-2.49	-3.4	-5.29	171	-30.0
0.5	15	-3.35	-4.01	-6.1	159.2	-26.1
1	16	-4.17	-4.80	-6.9	163.4	-25.8
0.5	25	-5.28	-5.08	-7.51	-180.2	-20.7
2	40	-5.9	-5.41	-7.92	-178.6	-16.1
2.5	44	-6.6	-5.85	-8.45	-179.1	-15.6
3	50	-7.41	-6.30	-9.10	-180.7	-15.9
3.5	40	-7.8	-7.31	-9.82	-180.5	-18.0
4	74	-9.66	-7.83	-10.94	-180.3	-14.5
4.5	75	-10.26	-8.42	-11.55	-180.9	-15.0
5	80	-11.02	-9.15	-12.31	-181.6	-15.4
5.5	100	-12.33	-9.96	-13.37	-181.3	-15.0
6	100	-12.73	-10.36	-13.77	-181.7	-15.4
6.5	103	-13.55	-11.20	-14.60	-181.5	-15.7
7	74	-13.66	-11.83	-14.94	-184.3	-18.5

The last scenario is also considered when proposed algorithm is applied. Table 4 shows that the proposed anti spoofing algorithm can effectively deal with spoofing. As shown in table 4, constraint (4) is satisfied in each thirty second time interval and subsequently, spoofing is reported.

Having detected the phase angle shift, counterfeit angles can easily be refined. Each of the D_2 elements reveals the tricky shift which is imposed in thirty seconds.

In table 3, it's also observed that the spoofer have successfully shifted the phase angles of measured data slowly and in a tricky way so that it cannot be easily detected. After seven minutes an angle shift around 9.3 degrees has been imposed to measured data.

This much phase angle shift can easily cause protection system to malfunction. The threat is also highlighted for bus voltage angle. Hence, a proper anti-spoofing algorithm is crucial to deal with such a threat.

Table 4: Provided results of the algorithm in spoofing condition

D_2 elements	$D_2(1)$	$D_2(2)$	$D_2(3)$	$D_2(4)$	$D_2(5)$
Corresponding angle shift in 30 s / Time (min)	Bus voltage angle shift	L2-4 Current angle shift	L2-5 Current angle shift	L2-1 Current angle shift	L2-3 Current angle shift
0	-0.6	-0.6	-0.6	-0.6	-0.6
0.5	-0.5	-0.5	-0.5	-0.5	-0.5
1	-0.5	-0.5	-0.5	-0.5	-0.5
0.5	-0.6	-0.6	-0.6	-0.6	-0.6
2	-0.4	-0.4	-0.4	-0.4	-0.4
2.5	-0.5	-0.5	-0.5	-0.5	-0.5
3	-0.6	-0.6	-0.6	-0.6	-0.6
3.5	-0.8	-0.8	-0.8	-0.8	-0.8
4	-0.8	-0.8	-0.8	-0.8	-0.8
4.5	-0.6	-0.6	-0.6	-0.6	-0.6
5	-0.7	-0.7	-0.7	-0.7	-0.7
5.5	-0.7	-0.7	-0.7	-0.7	-0.7
6	-0.4	-0.4	-0.4	-0.4	-0.4
6.5	-0.8	-0.8	-0.8	-0.8	-0.8
7	-0.8	-0.8	-0.8	-0.8	-0.8

6. Conclusions

In this paper, a novel PMU anti-spoofing algorithm has been proposed based on smart grid infrastructures. The proposed algorithm detects spoofing by analyzing phase angles of the measured data. Despite previous anti-spoofing algorithm methods, the proposed method is able to refine counterfeit measurements. At the same time no additional hardware is required and the algorithm is completely software based. Permanently spoofing removal has also been considered using vestigial signal analysis.

Acknowledgements

The authors sincerely thank Dr. Sarvari for his word processing comments.

References

[1]. O. Kosut, L. Jia, R. J. Thomas, and L, Tong, "Malicious data attacks on the smart grid," *IEEE Trans. On Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[2]. M. Yasinzadeh, and H. Seyedi, "Fake measurement identification in power substations based on correlation between data and distance of the evidence," *IET Generation, Transmission & Distribution*, vol.9, no.5, pp. 503-512, Sep. 2014.

[3]. G. Dán, and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," *Smart Grid Communications* (SmartGridComm), 2010.

[4]. Y. Huang, H. Li, K. A. Campbell and Z. Han, "Defending false data injection attack on smart grid network using adaptive CUSUM test," *Information Sciences and Systems* (CISS), 2011.

[5]. T. Liu, Y. Gu, D. Wang, X. Guan and Y. Gui, "A Novel Method to Detect Bad Data Injection Attack in Smart Grid," *IEEE* INFOCOM Workshop on CCSES, 2013.

[6]. M. Esmalifalak, G. Shi, Z. Han and L. Song, "Bad data injection attack and defense in electricity market using game theory study", *IEEE Trans. on Smart Grid*, vol.4, no.1, pp. 106-169, Jan 2013.

[7]. Ericsson, G.N., "Toward a framework for managing information security for an electric power utility–CIGRÉ experiences," *IEEE Trans. Power Deliv.* , vol. 22, no. 3, pp. 1461–1469, 2007.

[8]. T.A. Rizzetti, L.N. Canha, R. Milbradt, P. B. Zorrilla, A. Abaide, C. Arend, "Methods of availability assurance for communication of PMU in a smart grid based on IP protocol," *Power Engineering Conf.* (UPEC), 49th International Universities, pp. 1-6, 2014.

[9]. Zh. Zhang, Sh. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: impact and analysis," *IEEE Trans. On Smart Grid*, vol.4, no.1, pp. 87-98, 2013.

[10]. Y. Fan, Zh. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. on Smart Grid*, vol. pp, no. 99, Aug. 2014.

[11]. 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.

[12]. 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. on Power Syst.*, vol.28, no.3, pp. 3253-3262, Aug. 2013.

[13]. L. Heng, D. Chou, and G. X. Gao, "Cooperative GPS signal authentication from unreliable peers," Inside GNSS, vol. 8, no. 5, pp. 70–75, Sep. 2013.

[14]. J. Krumm, and K. Hinckley, "The NearMe wireless proximity server," in UbiComp 2004: Ubiquitous Computing, ser. Lecture Notes in Computer Science, N. Davies, E. Mynatt, and I. Siio, Eds. Springer Berlin Heidelberg, vol. 3205, pp. 283–300, 2004.

[15]. Y. Bardout, "Authentication of GNSS position: An assessment of spoofing detection methods," in Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, pp. 436–446, Sep. 2011.

[16]. V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/No estimates," in Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, pp. 2878–2884, Sep. 2012.

[17]. D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," NAVIGATION, vol. 59, no. 4, pp. 281–290, Winter 2012.

[18]. M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, pp. 1888–1896, Sep. 2011.

[19]. S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS antispoofing method using a multi-antenna array," in Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, pp. 1233–1243, Sep. 2012.

[20]. D. Borio, "Panova tests and their application to GNSS spoofing detection," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 49, no. 1, pp. 381–394, 2013.

[21]. L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), Portland, pp. 1543–1552, Sep. 2003.

[22]. S. Lo, D. D. Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," Inside GNSS, Sep. 2009.

[23]. M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, Oct. 2013.

[24]. L. Heng, J.J. Makela, A. D. Dominguez-Garcia, R. B. Bobba, W.H. Sanders, and G. X. Gao, "Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture," Power and Energy Conference at Illinois (PECI), pp. 1-6, 2014.

[25]. 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 Transactions on Power Systems, vol. 28, no. 3, pp. 3253–3262, 2013.