A GPS Spoofing Resilient WAMS for Smart Grid

Alessia Garofalo, Cesario Di Sarno, Luigi Coppolino, and Salvatore D'Antonio

Department of Technology, University of Naples Parthenope, Naples, Italy
{alessia.garofalo,cesario.disarno,
luigi.coppolino,salvatore.dantonio}@uniparthenope.it
http://www.dit.uniparthenope.it/FITNESS/

Abstract. Smart grids provide efficiency in energy distribution, easy identification of disturbance sources, and fault prediction. To achieve these benefits a continuous monitoring of voltage and current phasors must be performed. Phasor Measurement Units (PMUs) allow measurements of the phasors. A Wide Area Measurement System uses PMUs placed in different locations to assess the status of the power grid. To correctly analyze the phasors provided by PMUs, phasors must refer to the same time. For this reason each PMU uses the clock provided by a GPS receiver. GPS receiver is vulnerable to spoofing attack and it is a single point of failure. In this context we examined Network Time Protocol (NTP) as an alternative time source when the GPS receiver is compromised. In this paper a resilient architecture is proposed that is able to detect and react to the GPS spoofing attack. Experimental tests have shown the effectiveness of our solution.

Keywords: Smart Grid, Wide Area Monitoring System, GPS Spoofing Attack, Phasor Measurement Unit.

1 Introduction

Power grids were designed in order to meet requirements that were defined in the 20th century when the goal was "to keep lights turned on". Today, the requirements expected to be fulfilled by power grids have changed. The increasing load and consumption demands increase electricity issues, such as blackouts, and overloads. In July, 2012 for two days, India experienced blackouts that involved a large portion of the country's power grid. Specifically, a 9% gap was estimated between the effective energy requirements and the available energy amount [1] [2]. In the afternoon of September 8, 2011, an 11 minutes-long system disturbance occurred in the Pacific Southwest, leading to cascading outages and leaving approximately 2.7 million customers without power. The failure of the power grid was due to the bad redistribution of the power flow caused by the failure of a transmission line. Other examples of power grid blackouts due to different types of failure are reported in [3] [4] [5] [6] whereas a security analysis of the technologies which enable data collection in power grid and in other critical infrastructures is provided in [7] [8] [9].

M. Vieira and J.C. Cunha (Eds.): EWDC 2013, LNCS 7869, pp. 134–147, 2013.

Smart Grid systems represent the natural evolution of the power grid. The term smart grid defines a self healing network equipped with dynamic optimization techniques that use real time measurements to minimize network losses, maintain voltage levels, and increase reliability. Operational data collected by the smart grid are analyzed and they allow system operators to rapidly identify the best strategy to secure against attacks, vulnerabilities, faults and so on, caused by various contingencies [10]. In order to monitor the status of the smart grid Wide Area Monitoring Systems (WAMSs) are used. WAMSs make use of devices distributed throughout the power grid that measure the key parameters to detect anomalous conditions.

Today Phasor Measurement Units (PMUs) are the most commonly used devices in WAMS. In particular, PMUs are devices that perform measurements of real-time phasors of voltages and currents to provide information about power grid status. The time synchronization between different PMUs is required to understand the global status of the power grid at the same time. This is because events occurring in one part of the grid affect operations elsewhere, and they also extend to other systems beyond the grid that rely on stable power. Time synchronized measurements produced by PMUs are called synchrophasors. In order to obtain simultaneous measurements of phasors detected from different PMUs installed across a wide area of the power system, it is necessary to synchronize these times, so that all phasor measurements belonging to the same time are truly simultaneous. Each PMU uses a Global Positioning System (GPS) receiver [11] to take a unique timestamp within the global system. One of the main problems affecting smart grid monitoring is the spoofing of the GPS signal provided to the GPS receiver [12]. The GPS signal can be forged in order to mislead the GPS receiver that uses it. This type of attack is called "GPS spoofing" [13] and more details are provided in Section 4. If an attacker forges the timestamps provided by GPS to a PMU, it could cause variations in measured phase angles. The difference in the phase angle between two PMUs indicates that the power between the regions measured by each PMU has changed. These variations could compromise the stability of the system in such a way that grid operators or automatic response systems would make incorrect decisions as powering up or shutting down generators. Incorrect decisions can cause blackouts or damages.

Many techniques are available in order to detect the GPS spoofing attack. These techniques are based on different approaches as: monitoring the absolute GPS signal strength; monitoring the relative GPS signal strength; monitoring satellite identification codes and the number of satellite signals received [14]. While different techniques are available to detect GPS spoofing attack no remediation technique was proposed.

In this paper we propose an architecture resilient to GPS spoofing attack. In particular our architecture provides capabilities of detection and remediation for the GPS spoofing attack. To design this architecture we analyzed requirements in terms of maximum time delay required by PMUs to avoid loss of synchronization. Also we analyzed the time accuracy provided by the GPS receiver to the PMUs. Thus we identified a particular implementation of the Network Time

Protocol (NTP) that offers the same accuracy as GPS receiver and that satisfies the PMU time requirements to avoid synchronization losses. So we developed a new component called "Spoofing Detector" placed between PMU device and the two time sources. The main time source is provided by the GPS receiver while backup time source is provided by NTP. Spoofing Detector detects the GPS spoofing attack and activates the remediation i.e. it switches from main to backup time source to provide PMU device with correct timestamp even under attack. Our architecture provides intrusion tolerance capabilities using both detection techniques of GPS spoofing attack and two external time sources.

The paper is organized as follows. Section 2 provides an overview about WAMS with reference to power grid. Section 3 describes the PMU devices and the way how they perform measurements of the synchrophasors. Section 4 presents the GPS spoofing attack that affects each PMU that uses a GPS receiver. In this section several techniques are discussed to detect this attack. Section 5 presents the synchronization protocol NTP as a candidate backup time source to use when the GPS receiver is compromised. Section 6 describes the resilient architecture proposed to detect and react to the GPS spoofing attack. Section 7 provides details about the implementation of the proposed architecture. Section 8 describes an attack model on the architecture proposed and presents the experimental results obtained.

2 Background

2.1 Wide Area Monitoring System

The power grid is composed of three main components: power plant, transmission substation and distribution grid. The power plant produces simultaneously three different phases of AC power with 120 degrees offset from each other. The three-phase power feeds a transmission substation. This substation uses large transformers to increase the generator's voltage up to extremely high voltages to reduce transmission line losses on long-distance. Distribution grid is the final stage of energy conversion before the electricity is supplied to end users.

The simplified architecture adopted today to monitor the power grid is shown in Figure 1.

PMUs are devices that use GPS signals as a common time source and analyze the waveforms of different transmission lines at different locations across a wide-area system at the same moment. In particular they perform a sampling of the waveforms provided by transmission lines and generate the phasors. These phasors are timestamped using the same clock provided by the GPS receiver. These synchronized phasors are called synchrophasors. Such timestamps can be used to compare collected synchrophasors with microsecond precision. In fact, the Phasor Data Concentrator (PDC) gathers the data provided by different PMUs and it performs a comparison between the synchrophasors to assess the status of power grid. A PDC can exchange phasors with PDCs at other locations to perform wide are monitoring.

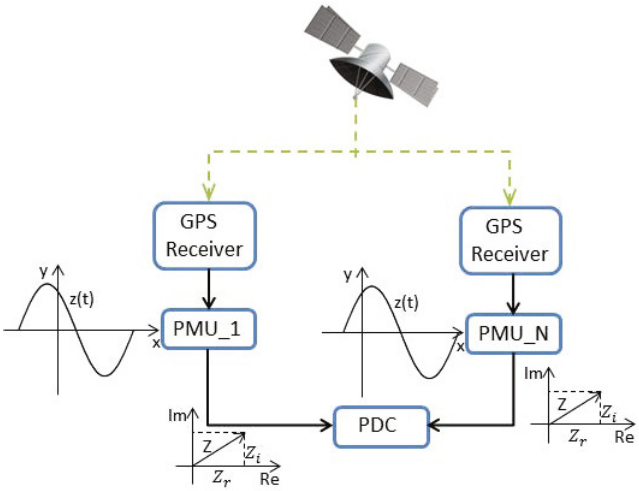

Fig. 1. Smart Grid Monitoring Architecture

The reference standard for PMU is IEEE Standard C37.118 [15]. It discusses about the definition of a synchronized phasor, time synchronization, method to verify compliance of measurements with the reference standard, and message formats for communication with a Phasor Measurement Unit (PMU).

3 Phasor Measurement Unit (PMU)

PMU devices are used in WAMSs in order to monitor power grids. In particular, PMUs analyze the 50/60 Hz AC waveforms provided by the power grid and they calculate the synchrophasors. The typical sinusoidal waveform analyzed by a PMU is:

$$z(t) = A_m * \cos(\omega t + \phi); \quad \omega = 2\pi f; \tag{1}$$

where f is the instantaneous frequency and A_m is the magnitude of the sinusoidal waveform. Waveform (1) can be represented as the phasor:

$$\bar{z} = Z_r + jZ_i = \frac{X_m}{\sqrt{2}} * e^{j\phi}; \tag{2}$$

where $\frac{X_m}{\sqrt{2}}$ represents the Root Mean Square (RMS) value of the waveform and ϕ is its phase angle relative to a cosine function at the frequency of the nominal system synchronized to Universal Time Coordinated (UTC). The time synchronization is provided by a GPS receiver. The advantage of referring phase angle to a global reference time is helpful in capturing the wide area snapshot of the power grid. The most common technique for determining the phasor representation of an input signal is to use data samples taken from the waveform,

and apply the Discrete Fourier Transform (DFT) to compute the phasor. Also, the obtained representation of the phasor is independent from the frequency of the signal $z(t)$.

So, the PMU calculates the voltage and current synchrophasors. Different PMUs are installed in different locations in order to obtain the global status of the power grid. In particular, the IEEE Standard C37.118 standard [15] defines the transmission rate of data generated by PMU. This rate changes if the system is 50 or 60 Hz. In Figure 2, the number of frames per second transmitted by PMU is shown for different types of systems.

System Frequency	50 Hz		60 Hz		
Frame per second	10	25	10	20	30

Fig. 2. PMU: phasor data transmission rate

Important topics covered by the mentioned standard concern the application of timestamps, the definition of the message format for communications between PMUs and the method to verify the measurement accuracy. The accuracy is expressed as the magnitude of the vector difference between the theoretical phasor and the phasor estimated by the measuring device, expressed as a fraction of the magnitude of the theoretical phasor. The magnitude of the vector difference is called Total Vector Error (TVE) and it is given by the following formula:

$$TVE = \sqrt{\frac{(Z_r(n) - Z_r)^2 + (Z_i(n) - Z_i)^2}{(Z_r^2 + Z_i^2)}} \tag{3}$$

where n represents the measurement time, $Z_r(n)$ and $Z_i(n)$ are the values measured by PMU, while Z_r and Z_i are the theoretical values of the input signal at the instant of time of measurement, determined by (2). The loss of synchronization occurs when the TVE value exceeds the value limit of 1%. There are three types of errors that can increase the TVE value: phase-angle measurement error; magnitude measurement error and time synchronization error. In this paper we analyze only the case of error in time synchronization. This is because when a GPS spoofing attack is performed successfully, the remediation architecture that we propose must satisfy specific time constraints to avoid losses in synchronization.

If a PMU is not accurately synchronized with UTC, then the measured phase will not match the true signal phase. In particular a phase error of 0.01 radians in (3) will cause 1% TVE. So we can calculate the maximum allowed time error before the synchronization loss using the following equation:

$$\Delta t = \frac{\phi}{2\pi f} \tag{4}$$

In (4), if we replace ϕ with the phase error that generates the maximum TVE value allowed and we consider power systems with nominal frequency of 50 Hz, then the maximum time error is $\Delta t = 31.8\mu s$. If the power system works with 60 Hz as nominal frequency then the maximum time error is $\Delta t = 26.5\mu s$.

Today, GPS systems represent the most commonly adopted method to provide time synchronization with the PMU devices. In particular, they provide a accuracy of about 100 ns that satisfies the requirements described above.

4 GPS Spoofing Attack and Detection Techniques

In section 3 we have argued about the importance of the PMUs synchronization. We showed how even a small time error can cause loss of synchronization. For this reason, PMU devices rely on the GPS receiver to obtain high accuracy. The GPS receiver is known to be vulnerable to GPS spoofing attacks. The goal of GPS spoofing attacks is to provide a forged version of the GPS signal to take control of a GPS receiver. So if an attacker successfully performs a GPS spoofing attack he/she can compromise the monitoring system of the power grid. This attack was discovered and highlighted in 2001 by U.S. Department of Transportation during a study performed on vulnerabilities of the transportation infrastructure that uses GPS signal [16].

The first step needed to perform a GPS spoofing attack is to acquire and to track the GPS signals to obtain a reference signal. Then a forged signal is generated and summed to the original GPS signal. The new signal is used to synchronize the spoofed signal with the authentic signal received. So the attacker produces a signal perfectly aligned with the authentic signals but with lower power. The generated spoofed signal is comparable to the noise of the target receiver in terms of power. Then the attacker increases the power of the forged signal until it overcomes the authentic signal. In this way, the forged signal shows higher Signal-to-Noise Ratio (SNR). So, the GPS receiver tracks the fake GPS signal (instead of the authentic signal) due to its higher SNR. After that, the attacker has successfully taken control of the GPS receiver. Then he/she slowly moves the spoofed signal from the authentic signal. The GPS signal received is considered to be completely captured when the spoofed signal is delayed by $2\mu s$ from the authentic signal as described in [17].

Thus the attacker could increase the time delay until it overcomes the 1% TVE as defined in the section 3.

Several techniques have been proposed in order to detect the GPS spoofing attack. These techniques are based on:

- monitoring the absolute GPS signal strength. This technique is based on comparisons between the observed signal strength and the expected signal strength. If their difference is greater than a fixed threshold, an alert is generated;
- monitoring the signal strength received from each satellite. The idea is to compare the observed signal strength with the expected signal strength for each satellite. The attacker will generate forged signal of equal strength for

each artificial satellite through the GPS satellite simulator. Instead, the signals provided by real satellites will change over time for each satellite. So an alert is generated if the signal characteristics are constant over time for each satellite;
- monitoring the relative GPS signal strength. This technique implies that the average signal strength is recorded and compared periodically. An alert is generated if a large change in relative signal strength is detected.

Further techniques that can be used to detect GPS spoofing attack are provided in [18] [19].

5 Network Time Protocol

Network Time Protocol (NTP) is widely used to synchronize system clocks among a set of distributed time servers and clients. NTP architecture is organized in layers, where synchronization flows from primary servers (higher layer) to the secondary servers and clients (lowest layer). The primary servers must be reliably synchronized to a GPS receiver and they must provide accurate and precise timestamps, even in case of a significant network jitter. Also the protocol must mitigate errors due to network disruptions or server failures. The synchronization process between a client and a server starts with a request from the client as shown in Figure 3. In particular the client sends current time T_1 to the

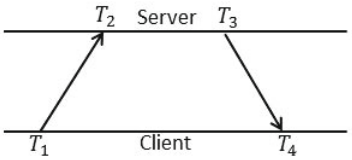

Fig. 3. NTP: client-server synchronization

server. The server saves this time T_1 together with the current time T_2. Then the server sends the client the current time T_3 together with the saved times T_1 and T_2. When the client receives the message, it reads its time T_4 and computes two values: offset of the clock α and round-trip delay β related to the server. The offset is computed as: $\alpha = \frac{1}{2}[(T_2 - T_1) + (T_3 - T_4)]$ whereas the round-trip delay is computed as: $\beta = (T_4 - T_1) - (T_3 - T_2)$. Both values α and β are minimized by a clock filter algorithm to obtain the synchronization of the client. More details about NTP are provided in [20] [21].

6 Anti GPS Spoofing Architecture

In this section we describe our architecture for remediation when a GPS spoofing attack is successfully performed. The proposed architecture is shown in Figure 4.

The idea is to increase the resilience to attacks using the concepts of redundancy and diversity. In fact, GPS spoofing attack can succeed because each PMU uses the timestamps provided by a unique time source i.e. GPS receiver. Also GPS receiver is a single point of failure for each PMU. Our approach is to use multiple time sources to provide timestamps to PMUs. To identify which technology can be used as a backup time source for PMUs, we analyzed PMUs requirements in terms of maximum time delay to avoid synchronization losses. Also we analyzed the accuracy provided by the GPS receiver so that the backup time source can provide coherent timestamps. We selected NTP as a technology that satisfies both requirements of maximum allowed delay by PMUs and expected accuracy by GPS receiver. The resulting NTP precision depends on the communication network behavior.

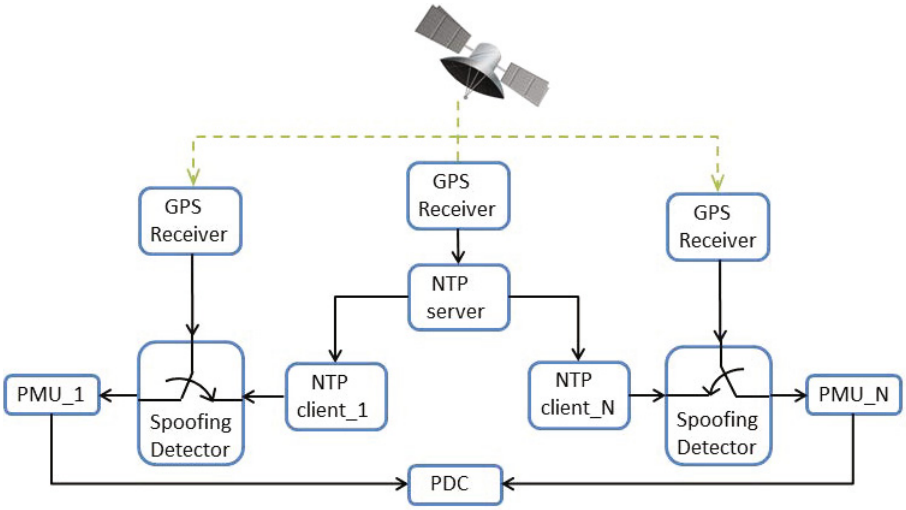

Fig. 4. GPS Spoofing Remediation Architecture

In the following, we assume that an NTP server is available and provides synchronization to many clients. The NTP server in Figure 4 is synchronized through a GPS receiver. NTP clients are synchronized with the correct time provided by NTP server. In our architecture we can see that PMU devices are not directly connected to the GPS receiver as in the standard monitoring model shown in Figure 1, but they are linked to the Spoofing Detector component. Of course the redundancy with two time sources is not sufficient to ensure intrusion tolerance. In fact to perform a voting with quorum at least three time sources are required. However we obtained the same results through only two time sources i.e. GPS Receiver and NTP client, because the Spoofing Detector uses a technique that allows to detect clock anomalous behaviours. In fact, Spoofing Detector component implements one of the techniques described in Section 4 to detect the GPS spoofing attack. The Spoofing Detector listens to the signal provided by the GPS receiver in order to recognize the characteristics

of the GPS spoofing attack. When an anomalous condition according to the chosen detection technique is found, then the remediation technique is activated. In particular, the Spoofing Detector component performs a switch of the timing source from GPS receiver to the NTP client. The NTP client replaces the compromised GPS receiver. In this way, PMUs always use a correct time source while measuring synchrophasors. NTP client is warm component i.e. it is always enabled and synchronized with NTP server.

The PDC component monitors the difference between the phases provided by different PMUs. Also the PDC uses information provided by Spoofing Detectors to avoid the generation of false alerts when an unexpected delay occurs during the synchronization of NTP clients.

In the proposed architecture, each PMU and NTP server uses a different GPS receiver. Also the GPS receiver of the NTP server is located very far from other GPS receivers. Then, when a spoofed GPS signal is propagated to compromise a GPS receiver belonging to a PMU device, we assume that the spoofed signal does not affect the GPS receiver of the NTP server.

7 Implementation Details

As we have shown in section 3, PMUs require strong time constraints to avoid synchronization losses. Our architecture works correctly when NTP protocol provides the same or better accuracy compared to GPS receiver. To obtain the maximum accuracy in NTP, modifications to operating system kernel are required. In particular the clock discipline algorithm in the synchronization daemon must be replaced with a module that offers the same functionality and operates in the kernel module. The clock discipline algorithm is the algorithm used to adjust the system clock in accordance with a final offset. While clock corrections are performed once per second in the classic synchronization daemon, they are performed every tick interrupt in the kernel. Using a specific implementation of NTP, it is possible to get an accuracy of the order of nanoseconds when an accurate reference clock is available [22] [23].

We use a dedicated network to reduce the network communication delay. Also all clients are linked to the primary NTP server to obtain a better accuracy.

Spoofing Detector component implements one of the techniques mentioned in section 4 to detect the GPS spoofing attack. The implemented technique is based on monitoring relative GPS signal strength. In particular, initially the component records a valid signal for a defined time interval. Then, it calculates the average value of the recorded signal and stores it. Finally, the alert threshold must be chosen. The choice of the threshold is very important because if it is set too low the component will perform many wrong switches of the chosen reference source; at the other side, if the threshold is too high the attack detection will be slow. Since the maximum time error allowed for PMUs to avoid the synchronization loss is about $20\mu s$, then a slow detection can compromise the synchronization of PMUs.

The component was developed in C++ in order to obtain good performances.

8 Attack Model and Experimental Results

In the first experiment we used two PMUs with a power grid that works at 60 Hz. The GPS receiver of a PMU is compromised by a spoofing attack. Instead, the GPS receiver of the other PMU works correctly and we use it as reference. In Figure 5 we show the attack model. In Figure 6 we show the difference

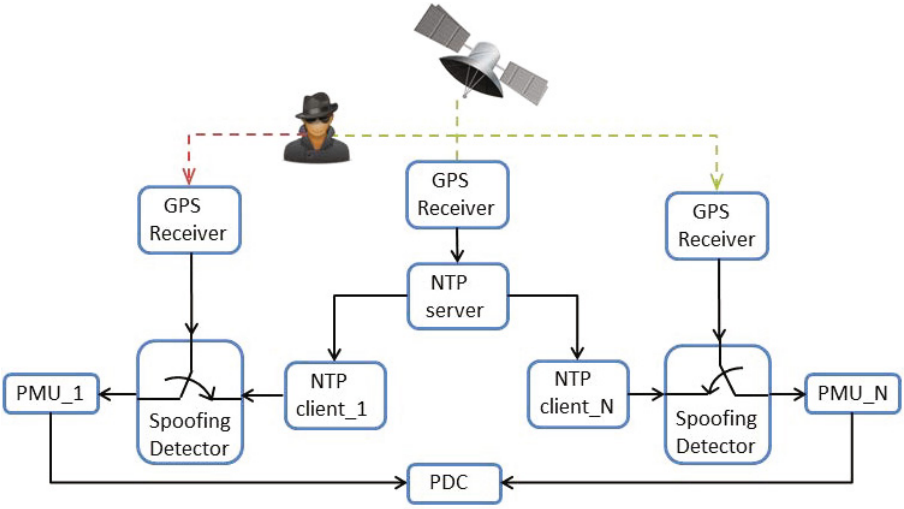

Fig. 5. Attack model used to compromise a GPS receiver of the PMU

between the phase angle measured by the compromised PMU and the phase angle measured by the reference PMU over time. Before the attack occurs, the synchrophasors measured by the two PMUs are overlapping vectors. This means that the phase angles of the two PMUs are aligned, so their difference is equal to zero.

At time $t = 300$ seconds the attacker tries to compromise the GPS receiver of a PMU through a spoofing attack. We have done many experiments in order to find the time required to perform a spoofing attack. In particular, in our case the time required is 2 minutes and 20 seconds. This time is in agreement also with another study [24], where the authors claim that about 2 minutes are needed to perform a spoofing attack. So at time $t = 440$ seconds the GPS receiver is completely compromised and the error time introduced for perfect synchronization with the attacker is $2\mu s$. The relation between phase angle and time error is provided by (4).

From now on, the purpose of the attacker is to introduce a higher error in the phase angle of the synchrophasors generated by the compromised PMU to overcome the maximum time error allowed before losing the synchronization. To achieve this goal, the attacker provides a constant acceleration of $3\frac{m}{s^2}$. A higher acceleration could desynchronize the GPS receiver from the attacker. We can see

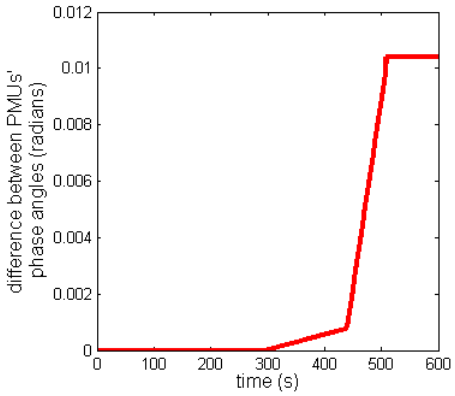

Fig. 6. Difference between PMUs' phase angles when one of them is compromised

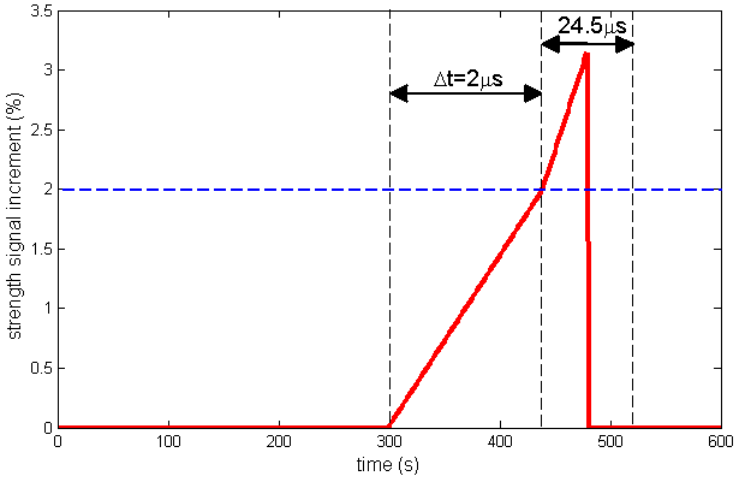

Fig. 7. Performance of the proposed resilient architecture

that at time $t = 470$ seconds the time error introduced is about $12.65\mu s$ and the difference of phase angles is about 0.0048 radiants. As described in section 3, the maximum tolerated error phase before the loss of synchronization is 0.01 radiants so, no loss of synchronization is occurring yet. At time $t = 510$ seconds, the difference between phase angles is greater than the maximum error phase allowed to obtain a TVE value under 1%. So the synchronization of the PMU attacked is lost. In Figure 7 we show the performance of our resilient architecture. In particular, we show the detection and remediation activities performed when spoofing attack occurs. At the time when the signal strength measured by Spoofing Detector overcomes 2% (blue line) of the average signal strength, our resilient architecture performs a change of time source. The threshold that allows the remediation to be activated was estimated through experimental tests. So at time $t = 440$ seconds the architecture has successfully detected the attack.

The detection delay causes a time error of $2\mu s$. At this time the attacker increases the acceleration of $3\frac{m}{s^2}$ to quickly reach the desynchronization from the correct time source. It is possible to use the available error time (i.e. $24.5\mu s$) to activate the remediation before the loss of synchronization. During the change of the timing source from GPS receiver to NTP client, the strength of the spoofed signal grows because the attacker tries to complete the spoofing attack. After the reference source time is changed, then the correct time is again provided to the PMU by the NTP client.

9 Conclusions

In this paper we discussed the usage of WAMS in smart grid. WAMSs use measurements of different PMUs to obtain information about power grid status. The comparison between measurements provided by different PMUs are useful if referred to the same time. So all PMU devices use a unique reference clock provided by GPS receivers. GPS receivers are vulnerable to GPS spoofing attacks. We reviewed several techniques to detect this type of attack. Also we presented a new resilient architecture that implements one of the proposed techniques to detect the spoofing attack. Also, the architecture implements a remediation technique when the attack is detected. The remediation technique is based on the use of the synchronization protocol NTP. When the attack is detected the time source switches from GPS receiver to NTP client. Experimental tests show the effectiveness of our solution.

In the future we plan to improve the detection time of spoofing attack. In fact, we think that times provided by NTP client and GPS receiver can be used together, to reduce detection latency. However the Spoofing Detector component of the proposed architecture could become more complex. We will perform other experimental tests in order to evaluate the impact of a greater complexity of the Spoofing Detector component on the reaction time of the architecture.

Acknowledgments. This work has been partially supported by the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research.

The research leading to these results has received funding from the European Commission within the context of the Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. 257644 (MAnagement of Security information and events in Service Infrastructures, MASSIF Project).

References

1. Romero, J.J.: Blackouts illuminate india's power problems. IEEE Spectrum 49(10), 11–12 (2012), doi:10.1109/MSPEC.2012.6309237
2. Singh, A., Aasma, S.: Grid failure in Northern, Eastern and North-Eastern grid in 2012: Cause & its effect on economy of India An Review. SAMRIDDHI-A Journal of Physical Sciences, Engineering and Technology (S-JPSET 2012) 3(2) (2012) ISSN: 2229-7111

3. FERC/NERC Staff Report on the September 8, 2011 Blackout. Arizona-Sourthem California Outages on September 8, 2011 (April 2012)
4. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations. Technical report, U.S.-Canada Power System Outage Task Force (April 2004)
5. Larsson, S., Danell, A.: The black-out in southern Sweden and eastern Denmark, September 23, 2003. In: 2006 IEEE PES Power Systems Conference and Exposition, PSCE 2006, October 29-November 1, pp. 309–313 (2003), doi:10.1109/PSCE.2006.296324
6. Oral, B., Donmez, F.: The Impacts of Natural Disasters on Power Systems: Anatomy of the Marmara Earthquake Blackout. Acta Polytechnica Hungarica (2010)
7. D'Antonio, S., Coppolino, L., Elia, I.A., Formicola, V.: Security issues of a phasor data concentrator for smart grid infrastructure. In: Proceedings of the 13th European Workshop on Dependable Computing, EWDC 2011, pp. 3–8. ACM, New York (2011), doi:10.1145/1978582.1978584
8. Coppolino, L., D'Antonio, S., Elia, I.A., Romano, L.: Security analysis of smart grid data collection technologies. In: Flammini, F., Bologna, S., Vittorini, V. (eds.) SAFECOMP 2011. LNCS, vol. 6894, pp. 143–156. Springer, Heidelberg (2011)
9. Coppolino, L., D'Antonio, S., Esposito, M., Romano, L.: Exploiting diversity and correlation to improve the performance of intrusion detection systems. In: International Conference on Network and Service Security, N2S 2009, June 24-26, pp. 1–5 (2009)
10. Momoh, J.: Smart Grid: Fundamentals of Design and Analysis. IEEE Press Series on Power Engineering, vol. 63. Wiley (2012)
11. Doberstein, D.: Fundamentals of GPS Receivers. Springer ISBN 978-1-4614-0409-5
12. Hadley, M.D., McBride, J.B., Edgar, T.W., O'Neil, L.R., Johnson, J.D.: Securing Wide Area Measurement Systems. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability (June 2007)
13. Humphreys, T.: Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing, submitted to the Subcommittee on Oversight, Investigations and Management of the House Committee on Homeland Security, U.S. House of Representatives, Washington, DC (July18, 2012), `http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf`
14. Warner, J.S.: GPS Spoofing Countermeasures. Appeared in Homeland Security Journal (December 12, 2003)
15. IEEE Standard C37.118-2005: IEEE Standard for Synchrophasors for Power Systems (2006)
16. Volpe National Transportation Systems Center, Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, U.S. Department of Transportation Research and Innovative Technology Administration, Cambridge, Massachusetts (2001), `http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf`
17. Shepard, D.P., Humphreys, T.E., Fansler, A.A.: Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection 5(3-4), 146–153 (2012)
18. Warner, J.S., Johnston, R.G.: GPS Spoofing Countermeasures. Vulnerability Assessment Team Los Alamos National Laboratory Los Alamos, New Mexico, 87545
19. Humphreys, T.: Statement on the vunerability of civil unmanned aerial vehicle and other systems to civil GPS spoofing. University of Texas at Austin (July 18, 2012)

20. Hinden, R., Deering, S.: Internet Protocol Version 6 (IPv6) Addressing Architecture, Network Working Group report RFC-3513. Nokia, 26 p. (April 2003)
21. Partridge, C., Mendez, T., Milliken, T.: Host Anycasting Service, Network Working Group report RFC-1536, Bolt Beranek Newman, 9 p. (November 1992)
22. Mills, D.L.: Unix kernel modifications for precision time synchronization, Electrical Engineering Department Report 94-10-1, University of Delaware, 24 p. (October 1994)
23. Mills, D.L.: Adaptive hybrid clock discipline algorithm for the Network Time Protocol. IEEE/ACM Trans. Networking 6(5), 505–514 (1998)
24. Warner, J.S., Johnston, R.G.: A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. Journal of Security Administration (2002)