Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture

Liang Heng, Jonathan J. Makela, Alejandro D. Domínguez-García,
Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao
University of Illinois at Urbana-Champaign, Urbana, IL 61801
Email: {heng, jmakela, aledan, rbobba, whs, gracegao}@illinois.edu

***Abstract*—Synchronized voltage and current phasor measurements provided by phasor measurement units (PMUs) have the potential to augment power system monitoring, control, and protection functions. PMUs use the Global Positioning System (GPS) to synchronize measurements across a wide geographical area. Unfortunately, low-received-power, unencrypted civil GPS signals are vulnerable to jamming and spoofing attacks. Accidental receiver malfunction can also lead to incorrect position/time solutions. This paper presents a multi-layered multi-receiver architecture that hardens GPS-based timing against jamming, spoofing, and receiver errors. Our architecture integrates eight countermeasures in all layers of receiver signal and data processing; most of the countermeasures exploit the static and networked nature of time reference receivers. We define five threat models, and qualitatively analyze the effectiveness of each countermeasure against each threat model. The analysis demonstrates that the redundant, independent but complementary countermeasures provide high reliability and robustness.**

I. Introduction

Efficient power transmission and distribution would benefit from synchronized near-real-time measurements of voltage and current phasors at widely dispersed locations in an electric power grid [1]. Such measurements also have the promise to enable effective real-time system monitoring and control, which have been considered to be the key to preventing wide-scale cascading outages like the 2003 Northeast Blackout [2]. A phasor measurement unit (PMU), also known as synchrophasor, is a device capable of measuring power system voltage and current phasors at a rate of thousands of samples per second [3], [4]. The samples are time-stamped with 1 microsecond or better accuracy to a common absolute time reference provided by the Global Positioning System (GPS) receivers attached to PMUs [5], [6].

Unfortunately, low-received-power, unencrypted civil GPS signals have been proven to be vulnerable to jamming and spoofing attacks [7]–[11]. A jammer emits a high-power interfering signal at the GPS frequency in order to deny nearby GPS receivers access to the GPS signal. A spoofer broadcasts a counterfeit GPS signal that overpowers the authentic signal so as to manipulate a victim receiver's reported position, time, or both. In a future scenario where PMU data play a significant role in power system operations, an attacker may disturb or bring down the system by attacking the GPS receivers attached to PMUs. Shepard et al. [12] have shown that an attacker could cause a generator trip by spoofing a GPS time reference receiver.

Even without being jammed or spoofed, a GPS receiver does not always yield correct position and time solutions due to accidental receiver malfunctions. Heng et al. [13] have shown that 0.34% of the navigation messages collected by the geodetic-grade GPS receivers in the International GNSS Service (IGS) [14] network throughout the year 2009 were incorrect. Another surprising instance is that on 31 July 2006, 29 out of 245 GPS receivers in the IGS network missed or misinterpreted a navigation message. As a result, the 29 receivers miscalculated their positions and clocks for more than one hour [15].

So far, a variety of countermeasures have been proposed to enhance civil GPS receivers' robustness against jamming and spoofing attacks and accidental receiver errors. These methods can be generally categorized into four groups: external assistance, signal features, redundant measurements, and cryptography. The first group utilizes the information from the sensors external to the GPS subsystem, such as accelerometers, gyroscopes, odometers, and cellular networks [16], [17]. The second group makes use of the features inherent in GPS signals, including angle-of-arrival (spatial sparsity) [18]–[20], time-frequency sparsity [21], signal quality [22], signal power [23], and multipath [24]. The third group exploits the redundancy of pseudorange measurements [25], [26] and the correlation among multiple cooperative receivers [27]–[29]. The fourth group uses cryptographic, unpredictable information carried by the GPS signal to ensure its authenticity [30], [31].

Most of the methods mentioned above were designed for stand-alone kinematic receivers, and their objective was mainly reliable positioning but not necessarily reliable timing. There is still a dearth of countermeasures designed for static, networked GPS time reference receivers in power systems. In this paper, we present a multi-layered multi-receiver architecture that hardens GPS-based timing against jamming, spoofing, and receiver errors. Our architecture integrates eight countermeasures in all layers of receiver signal and data processing; most of the countermeasures exploit the static and networked nature of time reference receivers.

The remainder of the paper is organized as follows. Section II briefly explains how GPS works. Section III introduces five threat models considered in this paper. Section IV describes our proposed multi-layered multi-receiver architecture and elaborates on the countermeasures used in each layer. Section V compares the effectiveness of the countermeasures and discusses implementation of the architecture in current power systems. Finally, concluding remarks are presented in Section VI.

II. GPS Fundamentals

The Global Positioning System (GPS) is a satellite-based passive radio navigation system. It provides accurate position and time information to any number of users on or near the Earth wherever four or more GPS satellites are in sight. Each GPS satellite continuously transmits a direct-sequence spread spectrum (DSSS) ranging signal which contains two codes: an unencrypted C/A code, which is freely available to the public, and an encrypted P(Y) code, usually reserved for military applications. Navigation messages are modulated on top of ranging codes. A navigation message includes an ephemeris and a clock dataset; the former is used to calculate the satellite position, and the latter is used to calculate the satellite clock bias [32].

Figure 1 shows a simplified block diagram of most GPS receivers used nowadays. The signal conditioning circuit converts the raw radio frequency (RF) signal into intermediate frequency (IF) samples, which are processed by multiple tracking loops. Each tracking loop tracks one satellite and generates the pseudorange measurements and raw bits, from which the decoding module extracts the navigation data.

The GPS receiver uses *multilateration* (also referred to as *trilateration*) to determine its position [33]. The satellite-to-receiver *pseudorange*[1] is calculated by multiplying the speed of light by the time the signal has taken from the satellite to the receiver. The pseudorange to the kth satellite is given by

$$\rho_k = \|\boldsymbol{x}_k - \boldsymbol{x}\|_2 + c(b - b_k) + \epsilon_k, \tag{1}$$

where the satellite position $\boldsymbol{x}_k$ and clock bias b_k are calculated from the navigation message from the kth satellite, c is the speed of light, and ϵ_k represents the range measurement error. When pseudoranges to K satellites are available, $K \geq 4$, the receiver's position $\boldsymbol{x}$ and clock bias b can be uniquely determined by minimizing the mean squared error:

$$\min_{\boldsymbol{x},b} \sum_{k=1}^{K} \left(\epsilon_k\right)^2 = \min_{\boldsymbol{x},b} \sum_{k=1}^{K} \Big(\rho_k - \|\boldsymbol{x}_k - \boldsymbol{x}\|_2 + c(b - b_k)\Big)^2. \tag{2}$$

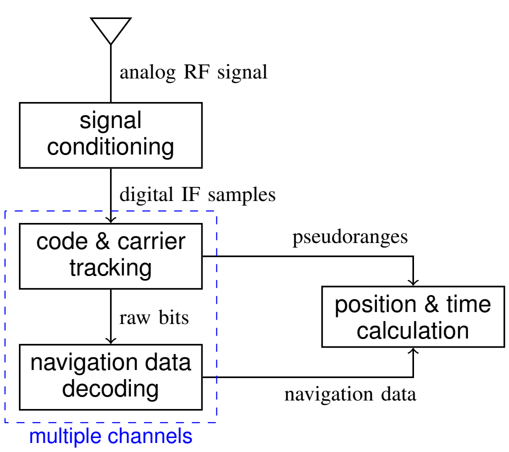


Fig. 1. GPS receiver block diagram.

[1]The range measurement is called "pseudorange" because the one-way time-of-arrival ranging includes satellite and receiver clock biases, as well as other errors caused by propagation effects.

III. Threat Models and Design Goals

Equation (2) indicates the following prerequisites for a correct position and time solution:

- correct pseudorange measurement ρ and
- correct navigation message so that the receiver can obtain correct $\boldsymbol{x}_k$ and b_k, $k = 1, \ldots, K$.

This paper is concerned with the threats that render any of the above prerequisites unavailable or incorrect. Specifically, we consider the following five threat models:

[J] Jamming: a jammer transmits high-power interfering signals in the GPS frequency band so as to stop nearby GPS receivers from acquiring and tracking GPS signals.

[S1] Data-level spoofing: a data-level spoofer synthesizes and transmits counterfeit GPS signals in order to manipulate a victim receiver's time solution without affecting its position solution. The spoofer achieves this goal by modifying several parameters in the navigation data (e.g., the spoofing attacks described in [11]).

[S2] Signal-level spoofing: a signal-level spoofer synthesizes and transmits counterfeit GPS signals that carry the same navigation data as concurrently broadcast by the GPS satellites. By carefully tuning the delay of each code (e.g., the spoofing attacks conducted in [10]), the spoofer is able to manipulate a victim receiver's time solution without affecting its position solution.

[S3] Bent-pipe spoofing (also referred to as *meaconing*): a bent-pipe spoofer conducts a replay attack, namely, it records authentic GPS signals and rebroadcasts them (with a delay τ) as spoofing signals. The time calculated by a victim receiver is delayed by τ, while the position solution is always equal to the position of the attacker's antenna used to record the GPS signals.

[E] Accidental receiver malfunctions: accidental GPS receiver malfunctions yield incorrect pseudorange measurements or incorrect navigation messages, resulting in incorrect position solution or time solution, or both.

Under the threat model [J], we want the receiver to be able to continue operating. For the other threat models, the goal is to detect the threat with a high confidence in a timely manner. The next section describes our multi-layered multi-receiver architecture and how it achieves these goals.

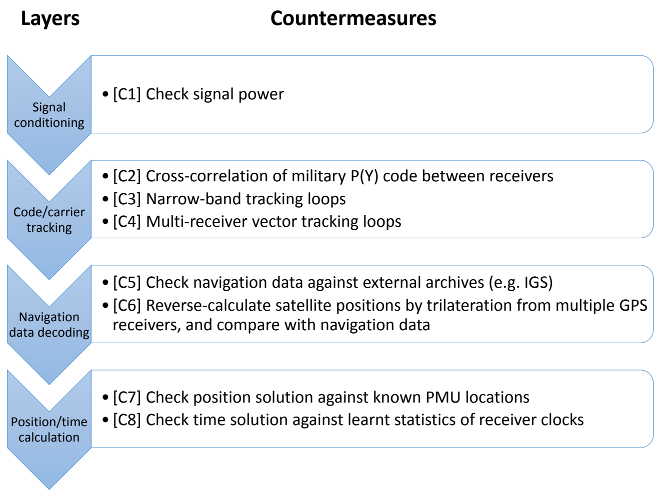


Fig. 2. Our proposed multi-layered multi-receiver architecture for reliable GPS-based timing for power system applications.

IV. System Architecture

Figure 2 shows our proposed multi-layered multi-receiver architecture which enables reliable GPS-based timing. Our architecture employs comprehensive countermeasures in all layers of receiver signal and data processing. In the signal conditioning layer, statistical tests on signal power serve as early spoofing detection [22], [34]. In the signal tracking layer, cross-correlation of the noisy P(Y) signals from two receivers is used to ensure that the received signals are broadcast by the GPS satellites rather than generated by a spoofer [31], [35], [36]. Thanks to the static nature of GPS receivers, a narrow-band tracking loop is used to improve the receiver's robustness against jamming attacks. Multi-receiver vector tracking loops are also employed in this layer to enhance a receiver's capability of continuing operating under against jamming attacks [37]. In the GPS navigation data processing layer, the navigation messages collected by a receiver are compared against others' to ensure the correctness of navigation data. The pseudorange measurements from multiple receivers are used to reverse-calculate satellite positions, which are expected to match the satellite positions calculated from the navigation data. Finally, in the position/time calculation layer, the solutions are checked against a priori statistics in order to detect any spoofing attacks missed in previous layers.

The list below summarizes the main purpose of the countermeasures performed in each layer:

- Signal conditioning layer: Early spoofing detection;
- Tracking loop layer: Continuous operation under jamming;
- Navigation data layer: Spoofing detection and receiver malfunction detection; and
- Position/time calculation layer: Final spoofing detection and receiver malfunction detection.

The remainder of this section is devoted to a detailed description of eight specific countermeasures within this architecture.

[C1] Check signal power

In a spoofing attack, the counterfeit signal has to overpower the authentic signal so that a victim receiver will lock on to the more powerful counterfeit signal. Therefore, an ascent of received signal power implies the possibility of a spoofing attack. In GPS receivers which use two or more bits sampling, automatic gain control (AGC) is used to adjust the front-end gain to a level suitable for the analog-to-digital converter (ADC). Experiments in [34] have shown that AGC level is a low-computational-complexity, low-cost means to detect potential spoofing attacks.

Our architecture integrates the signal power check as an early spoofing detection. Advantages of this countermeasure include low computational complexity and independence (not relying on other receivers). A major disadvantage is the low detection confidence due to the stochastic nature of signal power. Therefore, the signal power check is considered as an auxiliary countermeasure against threats [S1]–[S3].

[C2] Cross-correlation of military P(Y) code between receivers

As mentioned in Section II, the GPS signal contains the unencrypted C/A code and the encrypted P(Y) code, which are modulated onto the L1 carrier in-phase and quadrature, respectively. This countermeasure is based on the fact that a spoofer cannot generate the P(Y) code.

As shown in Fig. 3, two receivers track the C/A code from a satellite visible to both of them. Each receiver uses the C/A code phase and timing relationships to the P(Y) code to take a snippet of the same part of the received P(Y) code. The spoofing detection correlates two snippets of the GPS signals from two receivers. Although the P(Y) code is encrypted and thus unknown to non-military receivers, and although its received versions are noisy and may be distorted by narrow-band RF front-ends, when conducting cross-correlation, the P(Y) code components in the two snippets are similar enough to create an obvious correlation peak if neither receiver is spoofed. An

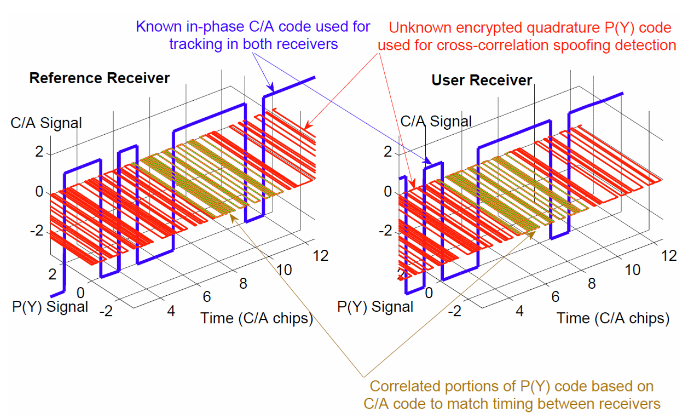


Fig. 3. Principle of cross-correlation spoofing detection (adapted from Fig. 1 in [35]). The publicly-known C/A signal and encrypted P(Y) signal are modulated onto the L1 carrier in-phase and quadrature, respectively. Each receiver tracks the C/A code, and uses its phase and timing relationships to the P(Y) code to take a snippet of the same part of the P(Y) code. A high correlation will appear if the two snippets contain the same P(Y) code.

obvious correlation peak may also appear if both receivers are spoofed by the same spoofer, but this scenario can be precluded by choosing reference receivers far (e.g., at least one kilometer) away from the user receiver.

Psiaki et al. [35] have shown that the probability of detection errors decreases exponentially with the length of the snippet. In general, a one-second or longer snippet is required to achieve a high detection performance. Heng et al. [36] have shown that if multiple reference receivers are available, the probability of detection errors decreases exponentially with the number of reference receivers.

Therefore, this anti-spoofing method has provable effectiveness against synthesized spoofing attacks, including threat models [S1] and [S2]. Unfortunately, it is ineffective against threat [S3] because bent-pipe spoofer rebroadcast the authentic GPS signals which contains the correct P(Y) code.

To implement this countermeasure, the receiver ought to have the capability to output baseband samples, and these samples need be transmitted over a data network. Due to the high sampling rate (usually greater than 2 Msps), we recommend performing this spoofing detection periodically rather than continuously.

[C3] Narrow-band tracking loops

In a GPS receiver, tracking loops are used to continuously follow the code and carrier parameters of the incoming signal. The bandwidth of loop filters is an important design parameter because the variance of code tracking errors is proportional to the loop bandwidth [33]. In general, a narrower bandwidth is better at suppressing noise, while a wider bandwidth allows faster response to receiver dynamics.

A jamming attack is equivalent to raising the noise floor. Since PMUs are static, we propose using narrow-band tracking loops to improve the robustness against jamming attacks (threat model [J]).

[C4] Multi-receiver vector tracking loops

In conventional GPS receivers, tracking loops operate independently, as each of them is assigned to a satellite; from an information-theoretic view, the channel is single-input single-output (SISO). In a vector tracking loop, information from all satellites is shared, and the user state is coupled to the pseudorange measurements via a Kalman filter; the channel can be seen as multiple-input single-output (MISO). Vector tracking loops enable a receiver to operate at a lower signal-to-noise ratio (SNR) [38] and thus increase immunity to jamming attacks (threat model [J]).

Since there are multiple networked receivers available in a power system, we propose using multi-receiver vector tracking loops to collaboratively process information from multiple receivers. The channel can be seen as multiple-input multiple-output (MIMO). Multi-receiver signal accumulation improves acquisition and tracking performance in low SNR [37]. Multi-receiver phased arrays greatly improve the robustness against jamming/spoofing attacks (threat models [J], [S1]–[S3]) by forming beams to satellites and steering nulls to jammers/spoofers. In addition, multi-receiver signal processing helps detect receiver errors (threat model [E]) because a malfunctioning receiver is usually inconsistent with other receivers.

Similar to countermeasue [C2], multi-receiver processing requires receivers to output baseband samples. The high-sampling-rate data need to be continuously transmitted between receivers (or to a central processing server). In practice, we recommend choosing receivers within a local vicinity and transmitting the data over a local area network.

[C5] Check navigation data against external archives

This countermeasure cross-checks the navigation messages collected by one PMU GPS receiver with others, and compares them against external references such as the IGS navigation data archive. This method can easily detect the data-level spoofing attacks (threat model [S1]) in which the navigation data are modified. This method also ensures that a receiver does not miss or misinterpret a navigation message (threat model [E]). Under jamming attacks (threat model [J]), a receiver may be able to track satellites but cannot correctly decode navigation messages. Using the navigation data from external archives enables the receiver to continue operating.

[C6] Reverse-calculate satellite positions by trilateration from multiple GPS receivers, and compare with navigation data

Since the PMU GPS receivers are static and their positions are known, we propose using the pseudorange measurements from multiple receivers to reverse-calculate satellite positions by multilateration. The reverse-calculated satellite positions match the satellite positions calculated from the navigation data only when both the navigation data and the pseudorange measurements are correct. Therefore, this countermeasure can easily detect bent-pipe spoofing attacks (threat model [S3]) and receiver errors (threat model [E]). This countermeasure also makes the synthesized spoofing attacks (threat models [S1] and [S2]) much more difficult because it imposes more constrains on “valid” spoofing signals.

The accuracy of multilateration depends on the satellite-to-users geometry. We recommend choosing receivers at dispersed locations to improve accuracy (see, e.g., the discussion on dilution of precision in [33]).

[C7] Check position solution against known PMU locations

For a single PMU GPS receiver, checking the position solution against its location known a priori can detect a bent-pipe spoofer (threat model [S3]). Receiver errors (threat model [E]) can also be detected if the errors result in an incorrect position solution. However, this method cannot detect the synthesized spoofing attacks (threat models [S1] and [S2]) because, when formulated properly, these attacks ensure unaltered position solutions.

In this paper, we argue that this countermeasure is effective against threat models [S1] and [S2] if multiple receivers are deployed in close vicinity and all the receivers are synchronized to a common clock. As shown in Fig. 4, several receivers

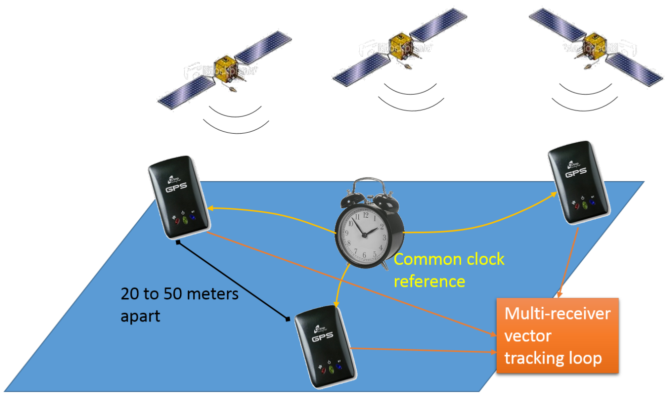


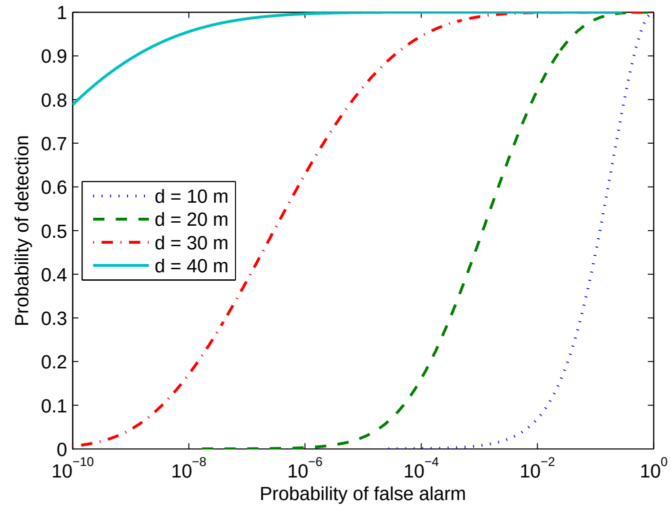
Fig. 4. Configuration of multiple receivers. With this configuration, checking position solution against known PMU locations can effectively detect all spoofing attaks (threat models [S1]–[S3]).

are deployed in a substation with a distance of 20 to 50 meters between two neighboring receivers. If no receivers are spoofed, all receivers yield the same clock bias. If a fraction of the receivers are spoofed by a spoofer, the victim receivers yield a different clock bias than the clock bias seen by the innocent receivers. If all receivers are spoofed by the same spoofer, although they generate the same clock bias, their position solutions are the same because the position solution is controlled by the spoofer and does not depend on the receiver's location. In this case, the spoofing attack can also be detected. The only way to spoof multiple receivers without being detected is to employ multiple spoofers, each of which has to fine-tune the transmit power so as to spoof just one receiver, and the spoofers should be synchronized to ensure the clock biases output by all receivers are the same. This spoofing attack is too complicated and too costly to be practical.

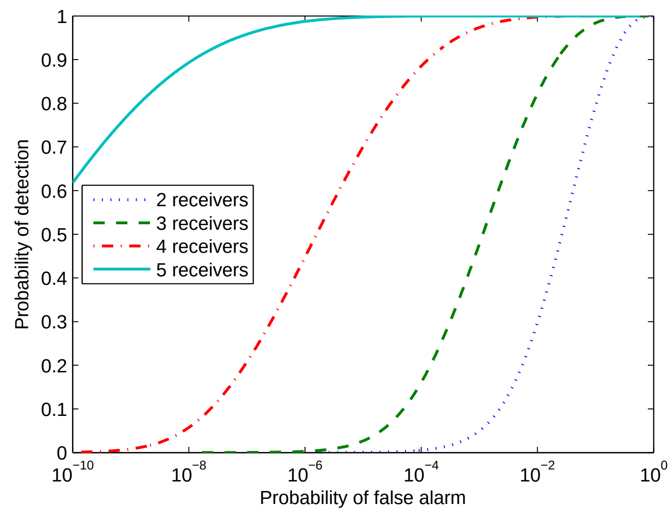
Swaszek and Hartnett [29] have analyzed the performance of this spoofing-detection method. Assume the m receivers are spaced evenly around a circle with a radius r. Let $d = 2r\sin(\pi/m)$ be the distance between two neighboring receiver. The spoofing detection performance depends on the parameters m, d, and σ, the standard deviation of positioning errors. We generate Fig. 5 (a) and (b) to show the receiver operating characteristic curves for different spacing and different number of receivers, respectively. It can be seen that increasing space and increasing number of receivers can improve spoofing detection performance.

[C8] Check time solution against learnt statistics of receiver clocks

Spoofing attacks and receiver errors are rare events. Based on this fact, we can design an algorithm to learn the stochastic behavior of receiver clocks [39]. When spoofing attacks (threat models [S1]–[S3]) and receiver errors occur (threat model [E]), the time solution is unlikely to be consistent with the learnt statistics of receiver clocks. Due to the stochastic volatility of receiver clocks, this countermeasure is considered auxiliary in our architecture.



(a) Different spacing, $m = 3$ receivers.



(b) Fixed spacing ($d = 20$ m), different number of receivers.

Fig. 5. Spoofing detection performance of countermeasure [C7] ($\sigma = 5$ m).

V. Comparison and Implementation Consideration

Table I summarizes the effectiveness of the countermeasures described above. For each threat model, markers $*$, $\circ$, or $\cdot$ denote if a certain countermeasure is effective, auxiliary, or ineffective, respectively.

The table shows that our multi-layered multi-receiver approach provides at least two effective countermeasures against each threat. Taking auxiliary countermeasures into account, at least three countermeasures are available against each threat. The redundancy in countermeasures guarantees highly reliable GPS-based timing even if one countermeasure fails.

Countermeasures [C1]–[C4] in the signal conditioning layer and the tracking loop layer require modification of current GPS time reference receivers used in PMUs. In particular, [C2] and [C4] require output of samples from digital baseband. Thus, these countermeasures are unlikely to be widely implemented in the near future. Since countermeasures [C5]–[C8] utilize

TABLE I
EFFECTIVENESS OF COUNTERMEASURES AGAINST THREAT MODELS

	[J]	[S1]	[S2]	[S3]	[E]
[C1]	·	∘	∘	∘	·
[C2]‡	·	∗	∗	·	·
[C3]§	∗	·	·	·	·
[C4]†	∗	∘	∘	∘	∘
[C5]‡	∘	∗	·	·	∗
[C6]‡§	·	∗	∘	∘	∗
[C7]†§	·	∗	∗	∗	∗
[C8]	·	∘	∘	∘	∘

Effectiveness of a countermeasure against a threat model:
∗ effective
∘ auxiliary
· ineffective

Requirements for a countermeasure:
† multiple networked receivers in vicinity
‡ multiple networked receivers at dispersed locations
§ static receivers

the output available in current GPS time reference receivers, they can be implemented in current power girds with minimal modification. As can be seen from Table I, countermeasures [C5]–[C8] still provide redundant protection against spoofing attacks and receiver errors.

VI. CONCLUDING REMARKS

This paper has presented a reliable and robust GPS-based timing mechanism supporting power system applications such as the PMU. We have designed a multi-layered multi-receiver architecture that incorporates eight countermeasures in all layers of receiver signal and data processing. Most of the countermeasures have fully exploited the static and networked nature of time reference receivers. We have defined five threat models, and qualitatively analyzed the effectiveness of each countermeasure against each threat model. The analysis has demonstrated that the redundant, independent but complementary countermeasures provide high reliability and robustness.

Accurate timing is a critical element for many economic activities around the world, including not only power grids but also communication systems and financial networks. All these systems rely on static, networked GPS time reference receivers. Our multi-layered multi-receiver architecture, although developed in the context of power systems, is also applicable to other systems.

ACKNOWLEDGMENT

This work was supported in part by the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) under US Department of Energy Award DE- OE0000097.

The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

REFERENCES

[1] R. E. Wilson, "Uses of precise time and frequency in power systems," *Proceedings of the IEEE*, vol. 79, no. 7, pp. 1009–1018, 1991.

[2] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, 2005.

[3] T. L. Baldwin, L. Mili, J. Boisen, M. B., and R. Adapa, "Power system observability with minimal phasor measurement placement," *IEEE Transactions on Power Systems*, vol. 8, no. 2, pp. 707–715, 1993.

[4] C. Martinez, M. Parashar, J. Dyer, and J. Coroas, "Phasor data requirements for real time wide-area monitoring, control and protection applications," Consortium for Electric Reliability Technology Solutions, Tech. Rep., Jan. 2005. [Online]. Available: http://www.phasor-rtdms.com/downloads/research/PhasorDataRequirements-WhitePaper012605.pdf

[5] R. F. Nuqui, "State estimation and voltage security monitoring using synchronized phasor measurements," Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2001.

[6] A. G. Phadke, "Synchronized phasor measurements: A historical overview," in *Proceedings of the 2002 IEEE/PES Transmission and Distribution Conference and Exhibition: Asia Pacific*, vol. 1, 2002, pp. 476–479.

[7] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and J. Kintner, Paul M., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008)*, Savannah, GA, Sep. 2008, pp. 2314–2325.

[8] S. Pullen, G. X. Gao, C. Tedeschi, and J. Warburton, "The impact of uninformed RF interference on GBAS and potential mitigations," in *Proceedings of the 2012 International Technical Meeting of the Institute of Navigation (ION ITM 2012)*, Newport Beach, CA, Jan. 2012, pp. 780–789.

[9] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. Raleigh, NC: ACM, 2012, pp. 450–461.

[10] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 34, pp. 146–153, 2012.

[11] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domínguez-García, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.

[12] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Going up against time: The power grid's vulnerability to GPS spoofing attacks," *GPS World*, Aug. 2012.

[13] L. Heng, G. X. Gao, T. Walter, and P. Enge, "GPS signal-in-space integrity performance evolution in the last decade: Data mining 400,000,000 navigation messages from a global network of 400 receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 4, pp. 2932–2946, Oct. 2012.

[14] J. M. Dow, R. E. Neilan, and C. Rizos, "The International GNSS Service in a changing landscape of global navigation satellite systems," *Journal of Geodesy*, vol. 83, pp. 689–689, 2009.

[15] L. Heng, G. X. Gao, T. Walter, and P. Enge, "Automated verification of potential GPS signal-in-space anomalies using ground observation data," in *Proceedings of the 2012 IEEE/ION Position Location and Navigation Symposium (IEEE/ION PLANS 2012)*, Myrtle Beach, SC, Apr. 2012, pp. 1111–1118.

[16] P. D. Groves and D. C. Long, "Adaptive tightly-coupled, a low cost alternative anti-jam INS/GPS integration technique," in *Proceedings of the 2003 International Technical Meeting of the Institute of Navigation (ION ITM 2003)*, Anaheim, CA, Jan. 2003, pp. 429–440.

[17] 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, OR, Sep. 2011, pp. 436–446.

[18] D. De Lorenzo, J. Gautier, J. Rife, P. Enge, and D. Akos, "Adaptive array processing for GPS interference rejection," in *Proceedings of the*

18th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2005), Long Beach, CA, Sep. 2005, pp. 618–627.
[19] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS anti-spoofing 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, TN, Sep. 2012, pp. 1233–1243.
[20] L. Heng, T. Walter, P. Enge, and G. X. Gao, "Overcoming RFI with high mask angle antennas and multiple GNSS constellations," in *Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, Sep. 2013, pp. 3433–3442.
[21] G. X. Gao, L. Heng, A. Hornbostel, H. Denks, M. Meurer, T. Walter, and P. Enge, "DME/TACAN interference mitigation for GNSS: Algorithms and flight test results," *GPS Solutions*, vol. 17, no. 4, pp. 561–573, Oct. 2013.
[22] 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, OR, Sep. 2011, pp. 1888–1896.
[23] 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, TN, Sep. 2012, pp. 2878–2884.
[24] F. Dovis, X. Chen, A. Cavaleri, K. Ali, and M. Pini, "Detection of spoofing threats by means of signal parameters estimation," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, Sep. 2011, pp. 416–421.
[25] P. Misra, E. Bayliss, R. LaFrey, M. Pratt, and R. Muchnik, "Receiver autonomous integrity monitoring (RAIM) of GPS and GLONASS," *NAVIGATION*, vol. 40, no. 1, pp. 87–104, 1993.
[26] J. Blanch, T. Walter, and P. Enge, "RAIM with optimal integrity and continuity allocations under multiple failures," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 46, no. 3, pp. 1235–1247, 2010.
[27] P. Enge, T. Walter, S. Pullen, C. Kee, Y.-C. Chao, and Y.-J. Tsai, "Wide area augmentation of the Global Positioning System," *Proceedings of the IEEE*, vol. 84, no. 8, pp. 1063–1088, 1996.
[28] P. Enge, "Local area augmentation of GPS for the precision approach of aircraft," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 111–132, Jan. 1999.
[29] P. F. Swaszek and R. J. Hartnett, "Spoof detection using multiple COTS receivers in safety critical applications," in *Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, Sep. 2013.
[30] 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, OR, Sep. 2003, pp. 1543–1552.
[31] S. Lo, D. D. Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," *Inside GNSS*, Sep. 2009.
[32] GPS Wing, *Interface Specification IS-GPS-200E*, Jun. 2010.
[33] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA: Ganga-Jamuna Press, 2006.
[34] 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.
[35] 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*, to appear.
[36] L. Heng, D. B. Work, and G. X. Gao, "Cooperative GNSS authentication: Reliability from unreliable peers," *Inside GNSS*, vol. 8, no. 5, pp. 70–75, Sep. 2013.
[37] A. Soloviev and J. Dickman, "Collaborative GNSS signal processing," in *Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, Sep. 2013.
[38] M. Lashley, D. Bevly, and J. Hung, "Performance analysis of vector tracking algorithms for weak GPS signals in high dynamics," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 4, pp. 661–673, Aug. 2009.
[39] K. Wang and M. Rothacher, "Stochastic modeling of high-stability ground clocks in GPS analysis," *Journal of Geodesy*, vol. 87, no. 5, pp. 427–437, 2013.