Short Paper: Detection of GPS Spoofing Attacks in Power Grids

Der-Yeuan Yu[†], Aanjhan Ranganathan[†], Thomas Locher[‡], Srdjan Capkun[†], David Basin[†]

[†]Department of Computer Science
ETH Zurich, Switzerland
{dyu,raanjhan,capkuns,basin}@inf.ethz.ch

[‡]ABB Corporate Research
Switzerland
thomas.locher@ch.abb.com

ABSTRACT

Power companies are deploying a multitude of sensors to monitor the energy grid. Measurements at different locations should be aligned in time to obtain the global state of the grid, and the industry therefore uses GPS as a common clock source. However, these sensors are exposed to GPS time spoofing attacks that cause misaligned aggregated measurements, leading to inaccurate monitoring that affects power stability and line fault contingencies. In this paper, we analyze the resilience of phasor measurement sensors, which record voltages and currents, to GPS spoofing performed by an adversary external to the system. We propose a solution that leverages the characteristics of multiple sensors in the power grid to limit the feasibility of such attacks. In order to increase the robustness of wide-area power grid monitoring, we evaluate mechanisms that allow collaboration among GPS receivers to detect spoofing attacks. We apply multilateration techniques to allow a set of GPS receivers to locate a false GPS signal source. Using simulations, we show that receivers sharing a local clock can locate nearby spoofing adversaries with sufficient confidence.

Categories and Subject Descriptors

C.2.1 [**Computer Systems Organization**]: Computer-Communication Networks—*Network Architecture and Design*

Keywords

GPS spoofing; clock synchronization; power grids

1. INTRODUCTION

The power industry is deploying sensor networks in the power grid for maintenance and monitoring purposes. The state-of-the-art system, known as a wide-area monitoring system (WAMS), is an infrastructure that uses modern sensors such as phasor measurement units (PMUs) to accurately measure power lines at different locations. Obtaining knowledge of an accurate state of the power grid requires that sensor data from PMUs is timestamped with respect to the same time reference. This implies that PMUs across the grid have synchronized clocks when timestamping their measurements. Currently, this is achieved by having PMUs synchronize to GPS time through built-in GPS modules. However, the lack of authentication in civilian GPS messages exposes the system to GPS clock spoofing attacks that could lead to inaccurate power state estimation.

In this paper, we consider the problem of GPS spoofing in power grids. We show that given their fixed deployment locations, PMUs may detect spoofing attacks by verifying their locations and checking clock offsets with other neighboring PMUs. These checks constrain the adversary's freedom of choosing where and when spoofed signals should be sent. Given sufficiently many GPS receivers, we show that the adversary cannot spoof their clocks without violating some constraints and thereby being detected by the system. Although similar mechanisms have been proposed to detect GPS spoofing [3,7,9], verification that leverages multiple receivers with different synchronization settings in the power grid has not yet been addressed. Additionally, our system enables PMUs to use multilateration to calculate the adversary's position.

Our contributions in this paper are the following. First, we define the GPS clock spoofing problem in the context of power grid infrastructures that consist of multiple spatially distributed PMUs. Second, we derive constraints imposed on the adversary to successfully execute a spoofing attack without being detected. Finally, we use existing multilateration methods to allow PMUs to locate the spoofer. In contrast to previous work, our solution considers a mixed set of receivers, which may or may not have synchronized clocks, to detect spoofing attacks by verifying the calculated location and time information. We show that, for example, spoofing can be detected with at least 5 synchronized receivers or at least 6 non-synchronized receivers.

2. BACKGROUND AND MOTIVATION

We introduce the power grid wide-area monitoring system and its reliance on GPS to motivate the problem.

2.1 Wide-Area Monitoring Systems

A WAMS [20] consists of PMUs that are installed at electrical substations to measure circuit quantities of power lines, as shown in Figure 1. An important requirement while aggregating PMU measurements from different substations is the *time alignment* of data, which implies that

WiSec'14, July 23–25, 2014, Oxford, UK.

ACM 978-1-4503-2972-9/14/07 ...$15.00.
http://dx.doi.org/10.1145/2627393.2627398.

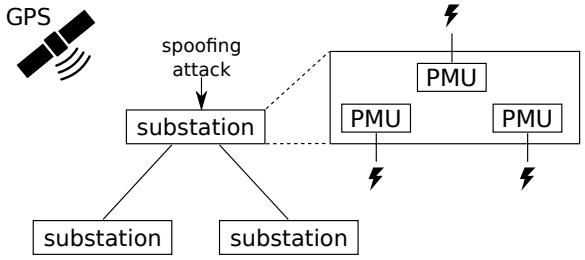

Figure 1: Illustration of PMUs installed in substations across a power grid to measure power lines. Spoofing attacks can occur in a substation that offsets the clocks of nearby PMUs.

all the PMUs should synchronize to a common time source to make synchronized measurements. The IEEE C37.118 standard governing PMU specifications defines the maximally tolerated clock synchronization error between any two measurements from different PMUs to be 31.8 or 26.5 microseconds for 50 or 60 Hertz systems, respectively [1]. As a possible solution, the precise time protocol (PTP) defined by IEEE 1588 [15] can be implemented to synchronize numerous nearby devices to a central clock with microsecond to sub-microsecond accuracy. However, for a power grid deployed on a nationwide scale, PTP is infeasible due to its dependence on specialized switches. As a more scalable alternative, modern PMUs mostly resort to GPS-based solutions [13]. The use of GPS for clock synchronization therefore exposes PMUs to intentional GPS spoofing attacks.

2.2 GPS Clock Synchronization and Spoofing

GPS satellites orbit the Earth and broadcast their orbit information and time. A GPS receiver receives messages from the satellites and calculates its own location and clock offset relative to the time of GPS satellites by solving a set of time-of-arrival (TOA) equations. PMUs installed across the power grid leverage clock synchronization in GPS to timestamp measurements with respect to the same time reference, referred to as GPS time.

The adversary can spoof civilian GPS messages since they are not authenticated. As a result, receivers may calculate incorrect locations or clock offsets, as shown by Shepard et al. [13]. GPS simulators are already available in the open market and allow an adversary to easily launch GPS spoofing attacks. Furthermore, these simulators are also capable of spoofing messages of other navigation systems like GLONASS.

Incorrect timestamping of phasor measurement data impacts the reliability of applications such as distance line protection and voltage stability monitoring [8]. Existing work has investigated the impact of incorrect timestamps on various power protection and monitoring mechanisms that use PMU measurements. Jiang et al. [9] demonstrate the feasibility of GPS spoofing attacks on single PMUs, and show that spoofing the GPS receiver clocks on the PMUs can cause erroneous estimates of the actual power load and trigger false warnings of power instability. Zhang et al. [18] have also investigated the impact of spoofed GPS timestamps on voltage stability monitoring. Moreover, they show that *line fault location*—an application that identifies the location of a power line failure, such as a short circuit on the transmission line—can be misled by up to 180 km if the system is subject to a GPS spoofing attack that shifts the clock by as little as 2.8 milliseconds. Motivated by the potential impact of GPS spoofing, we analyze the GPS spoofing problem and propose a solution that leverages the specific characteristics of GPS use in the power grid.

3. PROBLEM FORMULATION

We approach the problem of GPS spoofing on PMUs in electrical substations by first defining the system and adversarial models.

3.1 System Model

We assume that each PMU has its own GPS antenna, and all GPS antennas are spatially distributed along the rooftop of the substation perimeter, which is typically around 50 to 100 meters wide. The system can therefore be abstractly viewed as a set of n_r GPS receivers $\mathcal{R} = \{R_1, ..., R_{n_r}\}$. Since a PMU is normally installed in a fixed position within a substation, we can assume that a GPS receiver R_i knows its physical location ℓ_i. This can be achieved by the administrator giving the location information to the GPS module, which is supported by existing GPS receivers, during initial PMU deployment. These devices communicate over an existing network to transmit measurements. We denote the set of n_s GPS satellites orbiting Earth by $\mathcal{S} = \{S_1, ..., S_{n_s}\}$. At a predefined time, satellite S_j broadcasts its location in space, denoted by ℓ_j^s, and the corresponding GPS time, denoted by t_j^s, at which the message is sent.

3.2 Adversarial Model

We consider an adversary that has complete knowledge of the physical location of all the GPS receivers in $\mathcal{R}$. The adversary can place multiple antennas at arbitrary locations to send out fake GPS signals and trick PMUs into synchronizing their clocks incorrectly. When the adversary is sending spoofed signals to impersonate an authentic satellite S_j, we use S_j^a to denote the satellite that is emulated. The entire set of emulated satellites is denoted by $\mathcal{S}^a$. For a fake GPS signal from each emulated satellite S_j^a, the adversary now has the following variables to assign values for a successful clock desynchronization: the claimed trajectory of the emulated satellite, and the corresponding true location of the antenna and transmit time of a fake GPS message.

We also assume that the spoofed signals are received by all GPS receivers near the targeted substation. Otherwise, if the adversary can send different signals to each GPS receiver (e.g., using directional antennas), each receiver can be independently spoofed to an arbitrary location and time without violating constraints between the receivers [14]. In addition, we focus our discussion on civilian GPS signals, which do not implement authentication, since modern PMUs produced by manufacturers without military affiliation do not have access to military GPS signals.

3.3 Objectives

Under the system and adversarial models, our goal is to analyze the security of clock synchronization of GPS-enabled PMUs across the power grid in the presence of spoofing attacks, and determine ways to synchronize PMU clocks such that they are accurate with respect to the error bound tolerated by standards [1]. Concretely, we aim at analyzing the

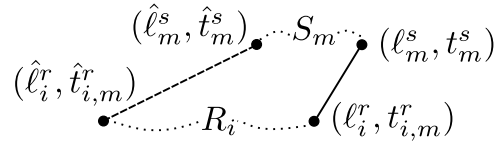

Figure 2: The receiver perceives the TOA equation as marked by the dotted line, while the true TOA equation is marked by the solid line.

feasibility of GPS spoofing attacks in the power grid and propose countermeasures to detect or prevent them.

4. DETECTION OF SPOOFING ATTACKS

We now describe the verification that can be performed by multiple GPS receivers in collaboration and the resulting constraints on undetectable spoofing attacks.

4.1 Formulation of GPS Spoofing

We begin by summarizing the adversary's variables for each emulated satellite S^a_m and each victim receiver R_i to successfully mount a spoofing attack. First, the adversary may arbitrarily announce its orbit information and thereby claim to be at location $\hat{\ell}^a_m$ at time $\hat{t}^a_m$. Second, the adversary chooses the true location ℓ^a_m to place the spoofing antenna and the true time t^a_m when the signal is sent, where t^a_m is related to $\hat{t}^a_m$ by a clock delay δ^a_m: $\hat{t}^a_m = t^a_m + \delta^a_m$. Finally, for each victim receiver R_i receiving the satellite signal, the adversary spoofs it to the location $\hat{\ell}_i$ and incurs a clock offset of $\hat{\delta}^r_{i,m}$. The local timestamp therefore becomes $\hat{t}^r_{i,m} = t^r_{i,m} + \hat{\delta}^r_{i,m}$. Note that the clock offset $\hat{\delta}^r_{i,m}$ is specific to each satellite-receiver pair. Table 1 summarizes the notations used throughout this paper.

The true TOA equation of the adversary's GPS satellite signal at the victim's GPS receiver can be derived as

$$c\left(t^r_{i,m} - t^a_m\right) = \left|\ell^r_i - \ell^a_m\right|, \tag{1}$$

where c is the speed of the medium. The clock synchronization of the receiver is based on the received GPS message and its perceived reception time,

$$c\left(\hat{t}^r_{i,m} - \hat{t}^a_m\right) = \left|\hat{\ell}^r_i - \hat{\ell}^a_m\right|, \tag{2}$$

where the left-hand side is commonly referred to as the *pseudorange* between receiver R_i and satellite S^a_m. Figure 2 illustrates the relationship between the two TOA equations.

The adversary relates its claimed/true satellite information and the desired locations and clock offsets to which a receiver would be spoofed to solve for the variables. All variables can be related by taking the difference between Equation (1) and Equation (2), resulting in

$$\left|\ell^r_i - \ell^a_m\right| + c\left(\hat{\delta}^r_{i,m} - \delta^a_m\right) = \left|\hat{\ell}^r_i - \hat{\ell}^a_m\right|, \tag{3}$$

The adversary's goal is therefore to solve for the variable sets marked in Table 1 such that Equation (3) is satisfied for each satellite-receiver pair.

4.2 Verification by Receivers

Different types of verification can be implemented across the GPS receivers to place constraints on the adversary's variables and thereby limit the feasibility of spoofing attacks.

	Emulated satellite S^a_m	
	ℓ_m, t_m	Location and time of authentic satellite
Set 1	ℓ^a_m, t^a_m	True location and time
Set 2	$\hat{\ell}^a_m, \hat{t}^a_m$	Claimed location and time
	Receiver R_i when receiving messages from S^a_m	
	$\ell^r_i, t^r_{i,m}$	True location and time upon reception
Set 3	$\hat{\ell}^r_i$	Calculated location
	$\hat{t}^r_{i,m}$	Reception time recorded by local clock
Set 4	$\hat{\delta}^r_{i,m}$	Calculated clock offset

Table 1: Notations used in this paper and the variable sets that the adversary can influence

We assume that the adversary sends spoofed signals of n_a of satellites. Out of the given n_r victim receivers, we define n_{rc} as the number of receivers that share a local clock.

Message Content Verification. When spoofing civilian GPS messages, the adversary may freely select Variable Set 2 since there is no message authentication. However, the power company may obtain an authentic copy of the data by setting up a GPS receiver at a remote location to receive signals from authentic satellites. Receivers can therefore compare messages from the adversary with the authentic copy, imposing the following constraint on the adversary:

$$\hat{\ell}^a_m = \ell_m \text{ and } \hat{t}^a_m = t_m.$$

Receiver Location Verification. Given that PMUs are installed in fixed and known locations in the substation, GPS receivers can leverage this knowledge to remove the adversary's freedom on Variable Set 3. The adversary must therefore send signals that do not affect the calculated locations of the receivers:

$$\forall R_i \in \mathcal{R}^a_m, \quad \left|\hat{\ell}^r_i - \ell^r_i\right| < \varepsilon_g.$$

The choice of ε_g depends the accuracy of the GPS receiver when localizing in a setting without GPS spoofing. Based on studies of localization errors of modern GPS receivers [16], ε_g can be approximately 10 meters or assigned based on the specification of individual GPS receivers.

Single Receiver Clock Offset Verification. Given that GPS satellites themselves are tightly synchronized, the difference between a receiver's clock and that of a satellite should be similar across different satellites:

$$\forall S_m, S_n \in \mathcal{S}^a, \forall R_i \in \mathcal{R}^a_m, \quad \left|\hat{\delta}^r_{i,m} - \hat{\delta}^r_{i,n}\right| < \varepsilon_t. \tag{4}$$

Similar to the tolerated location difference, the tolerated clock error ε_t can be defined based on the specification of the GPS receiver and is typically around 100 nanoseconds [11].

Grouped Receivers Clock Offset Verification. Recall that in Section 2.1, clock synchronization protocols such as PTP cannot be scaled to synchronize devices throughout a wide area that is the power grid. They are still useful, however, within a local substation. As a result, a set $\mathcal{R}_{\text{sync}}$ of GPS receivers in the same substation and synchronized using PTP may compare their clock offsets with each other. This leads to another constraint:

$$\forall S_m, S_n \in \mathcal{S}^a, \forall R_i, R_j \in \mathcal{R}^a_m \bigcap \mathcal{R}_{\text{sync}}, \left|\hat{\delta}^r_{i,m} - \hat{\delta}^r_{j,n}\right| < \varepsilon_{\text{sync}}. \tag{5}$$

Given the two variants of clock offset verification, Equation (5) implies that only 1 free variable can be assigned by the adversary as the only clock offset for the synchronized receivers. For non-synchronized receivers, the adversary is still constrained by Equation (4) for every receiver, implying that there are $n_r - n_{rc}$ clock offsets for the adversary to assign. It therefore follows that the adversary may specify $n_r - n_{rc} + 1$ separate clock offsets in Variable Set 4.

Finally, in our adversary model, the adversary can freely place the antennas and transmit signals at desired times. As a result, for Variable Set 1, the adversary can freely choose the true location (3 dimensions) and time (1 dimension) of each emulated satellite, amounting to $4n_a$ variables.

In summary, the adversary has to solve for $4n_a + n_r - n_{rc} + 1$ variables, which are subject to $n_r n_a$ instances of Equation (3), each representing the TOA relationship between an emulated satellite and a victim receiver. The variables become overdetermined if there are more equations than variables:

$$n_r n_a > 4n_a + n_r - n_{rc} + 1. \tag{6}$$

This restricts the adversary to at most one single solution for every variable. The single solution is the trivial one, where $\hat{\ell}^a_m = \ell^a_m$ and $\hat{t}^a_m = t^a_m$, that is, the correct location and time of the satellites. If no error is tolerated in the verification process by the receivers, the adversary must transmit messages from the authentic satellite location and time as claimed in the message to prevent being detected. In this case, the adversary is essentially behaving honestly, and spoofing is not possible. As an example, if the adversary sends spoofed signals of four emulated satellites to five synchronized GPS receivers placed at different locations, then Inequality (6) is satisfied, and therefore spoofing can be detected. Based on the selection of the thresholds ε_g, ε_t, and $\varepsilon_{\text{sync}}$, however, the adversary may assign the variables to be numerically close to the theoretical solution and still affect the clock offsets of the receivers. It is therefore important to choose tight thresholds values such that spoofing attacks are infeasible due to the tightened constraints.

5. LOCALIZATION OF THE ADVERSARY

In this section, we evaluate the use of multiple GPS receivers to estimate the true location of the source of a received GPS message using multilateration techniques [12].

5.1 Multilateration

We now describe a technique that allows a set of receivers sharing a local clock to locate the source of a GPS message. Recall that PMUs are installed in fixed locations within electrical substations, and therefore such a setup is practical to realize. Combined with the knowledge of their positions, a group of GPS receivers can infer the true position of an incoming GPS signal using time-difference-of-arrival (TDOA) equations. This mechanism, referred to as multilateration, can be used to verify the location claimed in the GPS message and to locate a possible spoofing adversary.

Let $\mathcal{R}$ be a set of receivers that share a common local clock, and S^a_m be the adversary's fake satellites. Each receiver $R_i \in \mathcal{R}$ may construct the following TOA relationship with the signal source using Equation (1).

$$|\ell^a_m - \ell^r_i| = c\left[\left(\hat{t}^r_{i,m} - \hat{\delta}^r_{i,m}\right) - t^a_m\right]. \tag{7}$$

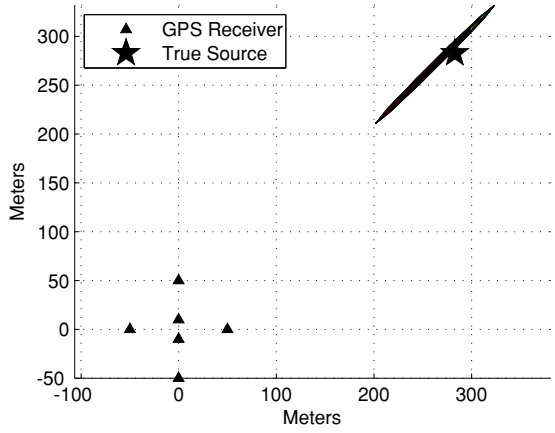

Figure 3: Locating the adversary roughly 400 meters away. The ellipse represents a 80% confidence region around the estimated location.

Taking the difference between Equation (7) for receivers R_i and R_j, we can obtain the following TDOA relationship between the two with respect to the same GPS message:

$$|\ell^a_m - \ell^r_i| - |\ell^a_m - \ell^r_j| = c\left(\hat{t}^r_{i,m} - \hat{t}^r_{j,m}\right) = c\Delta^m_{ij}, \tag{8}$$

where the time difference is represented as $\Delta^m_{ij} = \hat{t}^r_{i,m} - \hat{t}^r_{j,m}$.

The GPS message's source location ℓ^a_m computed by the receivers via Equation (8) describes a hyperboloid in 3D space. Based on multiple sets of TDOA equations between different pairs of receivers in $\mathcal{R}$, the GPS source location can be solved as the intersection of a set of hyperboloids, each corresponding to one TDOA equation between a pair of receivers. Since a minimum of 4 hyperboloids are required to generate a unique solution, this method works if there are at least 5 receivers in $\mathcal{R}$ that share a local clock.

This multilateration approach allows the receivers to verify a received GPS message's true source location, which can be compared with its claimed location in the message or used to determine the location of a spoofing GPS signal source in the event of a spoofing attack.

Obtaining the source location by solving the set of TDOA equations is non-trivial. This is due to the non-linearity of Equation (8) for every receiver pair and real-world errors such as those from multipath effects in wireless communication. Moreover, the system of equations becomes overdetermined when there are more than 5 receivers in $\mathcal{R}$, which should be taken into account when dealing with, for example, a large substation that contains many PMUs. Solutions, such as those provided by Chan and Ho [4] or Dogancay [5], already exist and can be readily adopted to obtain estimates of the source location.

5.2 Evaluation

In order to evaluate the localization method using an actual implementation, two types of information are needed: (1) the locations, ℓ^r_i, of the GPS receivers; (2) the times, $\hat{t}^r_{i,m}$, when GPS messages are received. While the former is known during deployment, the latter requires that GPS receivers record the time when each individual satellite message is received. Currently, however, commercially off-the-shelf GPS receivers do not output such information. We consider the construction of specialized GPS receivers out

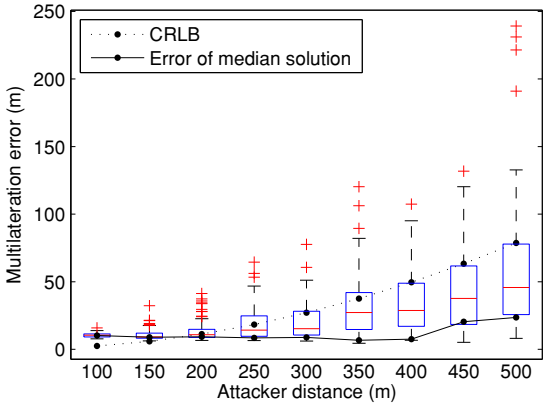

Figure 4: Box plot of multilateration errors using the solution by Chan and Ho [4], compared to the errors of the median of multiple runs (taken separately for each axis) and the theoretical CRLB for one single run.

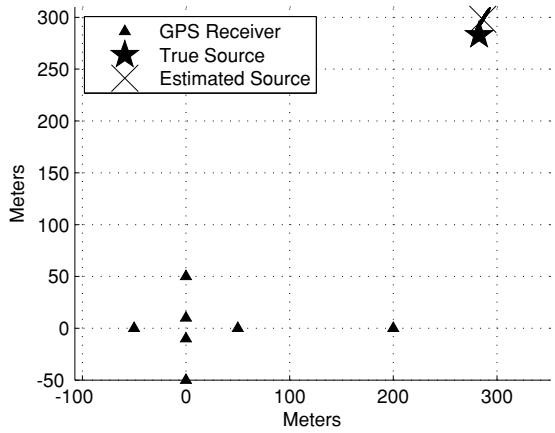

Figure 5: Signal source estimation improves when an additional GPS receiver is positioned far away from the original set.

of this paper's scope and so use simulations to generate the time differences when evaluating our approach.

We perform simulations to verify the use of signal source localization on a GPS receiver system with sufficient receivers (> 5) for multilateration. Our simulation consists of a set of 6 GPS receivers $\mathcal{R} = \{R_1, ..., R_6\}$, dispersed across a 100 m $\times$ 100 m $\times$ 20 m rectangular prism, which is realistic for an electrical substation. All GPS receivers synchronize their clocks to a local time source, each with an error as a random variable $\varepsilon_{\text{sync}}$. A fake GPS signal source S^a is modeled as a signal source $400\,m$ away from the center of the GPS receivers. In reality, this is a plausible placement because the signal source could be, for example, a GPS simulator mounted in the adversary's vehicle that is close to the electrical substation. The distance between receiver R_i and the signal source is $d_i = |\ell_i^r - \ell^a|$.

The TDOA localization method mentioned in Section 5 takes two inputs: (1) the locations of the GPS receivers, which is given based on our setup; (2) the difference of signal reception time between two receivers, which we generate in the simulation due to the lack of hardware support.

The time difference Δ_{ij} between two receivers R_i and R_j that receive the same signal is $\Delta_{ij} = c^{-1}|d_i - d_j| + \varepsilon_{\text{sync}}$, where $\varepsilon_{\text{sync}}$ is independently sampled for each time difference. Equation (8) for the receiver pair R_i and R_j becomes

$$|\ell^a - \ell_i^r| - |\ell^a - \ell_j^r| = |d_i - d_j| + c^{-1}e.$$

We simulate the time difference between receiver pairs (R_1, R_2), (R_1, R_3), (R_1, R_4), (R_1, R_5), and (R_1, R_6), which results in a set of 5 TDOA equations.

The adversary's location can subsequently be solved by intersecting the hyperboloids described by the TDOA equations, and we use the maximum likelihood estimator by Chan and Ho [4]. We also model the real-world inaccuracies of clock synchronization protocols using $\varepsilon_{\text{sync}}$ in Equation (5). In our simulation, $\varepsilon_{\text{sync}}$ is assumed to be a normal random variable with a standard deviation of 1 nanosecond, which is a realistic accuracy for state-of-the-art clock synchronization protocols among devices in a local network [11].

Figure 3 illustrates our simulated environment setup and compares the estimated adversary location to the ground truth. As observed, the location of a real-world adversary sending spoofed signals to an electrical substation from a distance of 400 meters can be estimated.

We also evaluate the errors of locating signal sources in different distances, defined as the distance between the estimated position and the true position, which is theoretically lower bounded by the Cramér-Rao lower bound (CRLB) [4]. Figure 4 is a comparison among the average errors of 100 trials, the CRLB, and the error of the median of the solutions. It shows that taking the median over multiple executions gives a superior accuracy over the CRLB of a single-iteration solution, and can be an option for GPS receivers to track the adversary over a longer period of time.

Figure 4 also shows that when the adversary is farther away from the GPS receivers, the approximation error increases. However, we observe that the direction from the receivers to the spoofed signal source can still be determined, as previously depicted by the narrow covariance ellipse in Figure 3. Furthermore, the accuracy can be further improved if other distant GPS receivers participate in solving the TDOA equations. Figure 5 illustrates the improved accuracy of multilateration by placing an additional GPS receiver farther away, around 200 m, from the original set of PMUs but still synchronized to the same local clock. In reality, if the adversary's antenna is far away from the substation, then it is reasonable to assume that GPS receivers in PMUs in other substations or in nearby transmission towers would also receive the signal and assist in multilateration.

6. RELATED WORK

In order to synchronize clocks across PMUs installed in a nationwide scale without requiring specialized hardware for networked time protocols, the industry often relies on GPS for clock synchronization. This has been shown by Shepard et al. [13] to be vulnerable to GPS spoofing. In our work, we propose mechanisms to increase its robustness against such malicious attacks. Jiang et al. [9] analyze how GPS spoofing can be performed on a single PMU as well as the impact on voltage stability monitoring and propose various detection techniques. Our contributions differ from theirs by analyzing the problem when multiple PMUs are deployed and how the adversary can be located.

In existing work on spoofing detection, Garofalo et al. [6] propose verifying GPS signal strengths to detect spoofing and to synchronize with other redundant clocks in a network via NTP protocols. Zhang et al. [19] propose a method of detecting clock synchronization attacks by monitoring the standard deviation of the differences in the signal-to-noise ratio from two GPS receiving antennas. Jafarnia-Jahromi et al. [7] provide an comprehensive overview of various ways single GPS receivers can use to detect spoofing. On the theory side, Tippenhauer et al. [14] investigate formulations of the GPS spoofing problem. Our work focuses on formulating the GPS problem by considering victim receivers with and without clock synchronization and their effects on reducing the feasibility of an undetectable spoofing attack.

For locating a signal source, Bhatti et al. [2] investigate possibilities of locating GPS interference signal sources in an urban setup, which assumes a 2D environment and close proximity between the source and receiver network. Strategies of placing GPS receivers to reduce the errors of multilateration has also been analyzed [17]. Various emitter localization methods based on multilateration have been proposed and compared in the past [4, 10]. A closed-form and efficient estimator that is adopted in this paper is introduced by Chan and Ho [4], which employs a maximum likelihood estimator to approximate the solution for TDOA equations. We apply this to a 3D substation setup to demonstrate the feasibility of locating the adversary.

7. CONCLUSION

In this paper, we explored the security of GPS-based clock synchronization against spoofing attacks for phasor measurement units in power grids. The solution may also be applied to other stationary sensor networks. Receivers collaborating to verify the information from GPS navigation messages may detect spoofing attacks. Existing multilateration techniques can also be applied to locate an adversary with sufficient accuracy. We showed that deploying sufficiently many receivers increases the difficulty and risk for the adversary. For these mechanisms to work, GPS receivers should record the reception time of each individual GPS message. Future GPS receivers that make such information available for analysis would improve their robustness against spoofing attacks.

8. ACKNOWLEDGMENTS

We are grateful for the feedback provided by the anonymous reviewers as well as the comments from Yongdae Kim, Sebastian Obermeier, Joel Reardon, and Michael Wahler.

9. REFERENCES

[1] IEEE Standard for Synchrophasors for Power Systems. *IEEE Std C37.118.1-2011*, 2011.

[2] J. Bhatti, T. Humphreys, and B. Ledvina. Development and Demonstration of a TDOA-based GNSS Interference Signal Localization System. In *Position Location and Navigation Symposium, IEEE/ION*, 2012.

[3] J. V. Carroll. Vulnerability Assessment of the US Transportation Infrastructure that Relies on the Global Positioning System. *Journal of Navigation*, 2003.

[4] Y. Chan and K. Ho. A Simple and Efficient Estimator for Hyperbolic Location. *IEEE Trans. Signal Processing*, 1994.

[5] K. Dogancay. Emitter Localization Using Clustering-based Bearing Association. *IEEE Trans. Aerospace and Electronic Systems*, 2005.

[6] A. Garofalo, C. Sarno, L. Coppolino, and S. D'Antonio. A GPS Spoofing Resilient WAMS for Smart Grid. In *Dependable Computing*, Lecture Notes in Computer Science. 2013.

[7] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Int'l Journal of Navigation and Observation*, 2012.

[8] J.-A. Jiang, J.-Z. Yang, Y.-H. Lin, C.-W. Liu, and J.-C. Ma. An Adaptive PMU Based Fault Detection/Location Technique for Transmission Lines. I. Theory and Algorithms. *IEEE Trans. Power Delivery*, 2000.

[9] X. Jiang, J. Zhang, B. Harding, J. Makela, and A. Dominguez-Garcia. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *IEEE Trans. Power Systems*, 2013.

[10] G. Mao, B. Fidan, and B. D. Anderson. Wireless Sensor Network Localization Techniques. *Computer Networks*, 2007.

[11] P. Moreira, J. Serrano, T. Wlostowski, P. Loschmidt, and G. Gaderer. White Rabbit: Sub-nanosecond Timing Distribution over Ethernet. In *Int'l Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, 2009.

[12] R. Schmidt. A New Approach to Geometry of Range Difference Location. *IEEE Trans. Aerospace and Electronic Systems*, 1972.

[13] D. P. Shepard, T. E. Humphreys, and A. A. Fansler. Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. *Int'l Journal of Critical Infrastructure Protection*, 2012.

[14] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the Requirements for Successful GPS Spoofing Attacks. In *ACM Conference on Computer and Communications Security*, 2011.

[15] A. Vallat and D. Schneuwly. Clock Synchronization in Telecommunications via PTP (IEEE 1588). In *IEEE Int'l Frequency Control Symposium*, 2007.

[16] M. G. Wing, A. Eklund, and L. D. Kellogg. Consumer-grade Global Positioning System (GPS) Accuracy and Reliability. *Journal of Forestry*, 2005.

[17] B. Yang. Different Sensor Placement Strategies for TDOA Based Localization. In *IEEE Int'l Conference on Acoustics, Speech and Signal Processing*, 2007.

[18] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li. Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Trans. Smart Grid*, 2013.

[19] Z. Zhang, M. Trinkle, A. Dimitrovski, and H. Li. Combating Time Synchronization Attack: A Cross Layer Defense Mechanism. In *ACM/IEEE Int'l Conference on Cyber-Physical Systems*, 2013.

[20] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson. Design Aspects for Wide-Area Monitoring and Control Systems. *Proc. IEEE*, 2005.