Evaluation of the Detection and Mitigation of Time Synchronization Attacks on the Global Positioning System

Ali Khalajmehrabadi
Department of Electrical and Computer Engineering
University of Texas at San Antonio
San Antonio, Texas, USA
ali.khalajmehrabadi@utsa.edu

Nikolaos Gatsis
Department of Electrical and Computer Engineering
University of Texas at San Antonio
San Antonio, Texas, USA
nikolaos.gatsis@utsa.edu

David Akopian
Department of Electrical and Computer Engineering
University of Texas at San Antonio
San Antonio, Texas, USA
david.akopian@utsa.edu

***Abstract*—This paper provides an evaluation of the proposed Time Synchronization Attack Rejection and Mitigation (TSARM) technique. The evaluation platform includes a real GPS spoofing mechanism available in TEXBAT and applied on the raw GNSS measurements obtained from a commercial GPS receiver. The key signatures to observe are the deviations on the clock bias and drift of the receiver under spoofed and normal conditions. The numerical evaluation substantiates the strengths of TSARM and renders great insight to its practicality in mitigating the effects of a real spoofer.** [1]

***Index Terms*—Global Navigation Satellite System, Spoofing Detection, Optimization**

I. Introduction

Despite the widespread utilization of the civilian Global Navigation Satellite System (GNSS) in infrastructures and user navigation, GNSS lacks any mechanism to protect itself from unintentional malfunctions and intentional attacks [1], [2]. Primary protection comes at the Receiver Autonomous Integrity Monitoring (RAIM) level, which indicates the inconsistencies in the residuals of the navigation equation [3], [4]. However, recent concerns on the vulnerability of the GNSS to sophisticated attacks have been rising [5].

The vulnerability of the GNSS comes from the fact that public civilian GNSS channels are unencrypted. A typical spoofer may employ different mechanisms to attack these channels and mislead the victim receiver: 1) Jamming: the spoofer (also called jammer) sends high power signals to the victim receiver so that it fails to track the authentic GNSS signal. This way, the normal operation of the receiver is halted and the user is stranded [6]–[9]. 2) Synthetic signal spoofing: the spoofer transmits fake GNSS signals with manipulated navigation messages [10]. 3) Record-and-Replay: this is the most sophisticated spoofing mechanism in which the spoofer records the authentic GNSS signal, manipulates the signal properties and transmits them to the victim receiver. The manipulation of the signals may include delay and retransmit of the authentic signal or manipulation of the navigation data [8], [11].

Spoofing on the GNSS may mislead the position, velocity and timing of the receiver. Our main focus in this paper is the attack on timing, called Time Synchronization Attack (TSA). TSAs are usually applied on static receivers which in fact utilize GNSS for their timing synchronization applications. Global Positioning System (GPS) is a well-known GNSS system. Two infrastructures that rely on GPS for their timing applications include power distribution systems and cellular towers [12]. Power systems use Phasor Measurement Units (PMU) to monitor the soundness of the distribution system. To address the impact of malicious attacks on Phase Measurement Unit (PMU) data, the Electric Power Research Institute published a technical report that recognizes the vulnerability of PMUs to GPS spoofing under its scenario WAMPAC.12: GPS Time Signal Compromise. These attacks introduce erroneous time stamps which are eventually equivalent to inducing wrong phase angle in the PMU measurements.

This work introduces the evaluation of a novel spoofing detection and mitigation for static GPS receivers, called Time Synchronization Attack Rejection and Mitigation (TSARM) [13]. The basis of this work is performed in navigation domain of the GPS receiver and hence, manipulation with baseband signal processing domain is not needed. This technique is easily integrable with the current off-the-shelf GPS devices. Using the measured pseudorange and pseudorange rates in the victim receiver and considering the

[1] This work was supported by National Science Foundation under grant No. ECCS-1719043

978-1-5386-1647-5/18/$31.00 ©2018 IEEE

practical constraints of a real spoofer, our technique estimates the spoofer anomaly behavior and corrects the measurements of the victim receiver.

In what follows, we first discuss the evaluation platform in Section II and then elaborate the spoofing detection and mitigation approach in Section III. Section IV shows the numerical results of the technique followed by conclusion in Section V.

II. Evaluation Platform

A real spoofing mechanism has been provided by Texas Spoofing Battery database (TEXBAT). The database contains the clean raw GPS measurements along with spoofed measurement under different spoofing scenarios. The spoofer is a National Instrument zero-delay security code estimation and replay (SCER) attack for a static receiver.

Our interest is on a timing attack with a 10-db power advantage over the authentic signal ensemble. The victim GPS receiver is a Google Nexus 9 tablet which has been equipped with the GPS chipset that provides raw GNSS measurements. An Android application processes these raw signal measurements and generates navigation measurements. The spoofing data on the pseudorange and pseudorange rate has been obtained by subtracting clean raw GPS measurement from their under-attack equivalents. Then, this spoofing data is mounted on the real raw navigation measurements obtained from Nexus 9 receiver. Our technique receives navigation measurements and performs the spoofing mitigation by correcting the psedorange and pseudorange rates. The corrected clock bias and clock drift is the output of the spoofing detection and correction block.

III. Spoofing Detection and Mitigation Approach

In this work, we specifically model the spoofing attacks. This model is quite general and encompasses the effect of various spoofing attacks on pseudorange and pseudorange rates on the victim receivers measurements considering the spoofers constraints

$$\begin{aligned} \rho_s[l] &= \rho[l] + s_\rho[l] \\ \dot{\rho}_s[l] &= \dot{\rho}[l] + s_{\dot{\rho}}[l] \end{aligned} \tag{1}$$

where s_ρ and $s_{\dot{\rho}}$ are the spoofing perturbations on pseudoranges and pseudorange rates, respectively; and ρ_s and $\dot{\rho}_s$ are respectively the spoofed pseudorange and pseudorange rates.

Considering that the attacks do not alter the position or velocity, but only the clock bias and clock drift, we introduce the state vector containing the clock bias and clock drift as

$$\underbrace{\begin{pmatrix} cb_{\mathrm{u}}[l+1] \\ c\dot{b}_{\mathrm{u}}[l+1] \end{pmatrix}}_{\mathbf{x}_{l+1}} = \underbrace{\begin{pmatrix} 1 & \Delta t \\ 0 & 1 \end{pmatrix}}_{\mathbf{F}} \underbrace{\begin{pmatrix} cb_{\mathrm{u}}[l] \\ c\dot{b}_{\mathrm{u}}[l] \end{pmatrix}}_{\mathbf{x}_l} + \underbrace{\begin{pmatrix} cs_b[l] \\ cs_{\dot{b}}[l] \end{pmatrix}}_{\mathbf{s}_l} + \underbrace{\begin{pmatrix} cv_b[l] \\ cv_{\dot{b}}[l] \end{pmatrix}}_{\mathbf{v}_l} \tag{2}$$

The measurement model contains the pseudorange and pseudorange rates as:

$$\underbrace{\begin{pmatrix} \boldsymbol{\rho}[l] \\ \dot{\boldsymbol{\rho}}[l] \end{pmatrix}}_{\mathbf{y}_l} = \underbrace{\begin{pmatrix} \mathbf{1}_{N\times 1} & \mathbf{0}_{N\times 1} \\ \mathbf{0}_{N\times 1} & \mathbf{1}_{N\times 1} \end{pmatrix}}_{\mathbf{H}} \underbrace{\begin{pmatrix} cb_{\mathrm{u}}[l] \\ c\dot{b}_{\mathrm{u}}[l] \end{pmatrix}}_{\mathbf{x}_l} + \underbrace{\begin{pmatrix} \|\mathbf{p}_1[l] - \mathbf{p}_{\mathrm{u}}[l]\| \\ \vdots \\ \|\mathbf{p}_N[l] - \mathbf{p}_{\mathrm{u}}[l]\| \\ (\mathbf{v}_1[l] - \mathbf{v}_{\mathrm{u}}[l])^T \cdot \frac{\mathbf{p}_1[l] - \mathbf{p}_{\mathrm{u}}[l]}{\|\mathbf{p}_1[l] - \mathbf{p}_{\mathrm{u}}[l]\|} \\ \vdots \\ (\mathbf{v}_N[l] - \mathbf{v}_{\mathrm{u}}[l])^T \cdot \frac{\mathbf{p}_N[l] - \mathbf{p}_{\mathrm{u}}[l]}{\|\mathbf{p}_N[l] - \mathbf{p}_{\mathrm{u}}[l]\|} \end{pmatrix} - \begin{pmatrix} cb_1[l] \\ \vdots \\ cb_N[l] \\ c\dot{b}_1[l] \\ \vdots \\ c\dot{b}_N[l] \end{pmatrix}}_{\mathbf{c}_l} + \underbrace{\begin{pmatrix} w_{\boldsymbol{\rho}_1}[l] \\ \vdots \\ w_{\boldsymbol{\rho}_N}[l] \\ w_{\dot{\boldsymbol{\rho}}_1}[l] \\ \vdots \\ w_{\dot{\boldsymbol{\rho}}_N}[l] \end{pmatrix}}_{\boldsymbol{w}_l} . \tag{3}$$

where $\boldsymbol{\rho}[l] = [\rho_1[l], \ldots, \rho_N[l]]^T$ and $\dot{\boldsymbol{\rho}}[l] = [\dot{\rho}_1[l], \ldots, \dot{\rho}_N[l]]^T$. Let $l = k, \ldots, k+L-1$ defines the time index within the observation window of length L, where k is the running time index. The solution to the dynamical model of (2) and (3) is obtained through stacking L measurements and forming the following optimization problem:

$$\begin{aligned} (\hat{\mathbf{x}}, \hat{\mathbf{s}}) = \underset{\mathbf{x},\mathbf{s}}{\operatorname{argmin}} \Bigg\{ & \frac{1}{2} \sum_{l=k}^{k+L-1} \|\mathbf{y}_l - \mathbf{H}\mathbf{x}_l - \mathbf{c}_l\|^2_{\mathbf{R}_l^{-1}} \\ & + \frac{1}{2} \sum_{l=k}^{k+L-1} \|\mathbf{x}_{l+1} - \mathbf{F}\mathbf{x}_l - \mathbf{s}_l\|^2_{\mathbf{Q}_l^{-1}} + \sum_{l=k}^{k+L-1} \lambda \|\mathbf{D}\mathbf{s}_l\|_1 \Bigg\} \end{aligned} \tag{4}$$

. The first term is the weighted residuals in the measurement equation, and the second term is the weighted residuals of the state equation. The last regularization term promotes sparsity over the total variation of the estimated attack. Here, λ is a tuning parameter, $\mathbf{Q}_l$ and $\mathbf{R}_l$ is respectively the clock covariance matrix and the measurement covariance matrix.

The correction method takes into account the previously mentioned effect and modifies the bias and drift by subtracting the cumulative outcome of the clock bias and drift attacks.

IV. Numerical Results

This section provides a numerical evaluation of TSARM over the TEXBAT spoofing procedure. The set of real GPS signals has been recorded with the Google Nexus 9 Tablet at the University of Texas at San Antonio on January, 30, 2018. The spoofing procedure has been extracted from the navigation measurements of the TEXBAT. The spoofing procedure is a TSA for a static receiver, in which the spoofing affects the timing solution (clock bias and drift) of the receiver. In what follows, the ground truth for timing is the solution of the Weighted Least Square (WLS) in normal operation.

Fig.1 shows the attack procedure on pseudorange and pseudorange rate obtained from TEXBAT for 11 channels. The attack starts before $t = 100\ s$, remains over $\sim 100\ s$ and stops before $t = 300\ s$. The corresponding attack on the doppler frequency decreases pseudorange rate for $\sim 26\ m/s$ and then decreases till vanishes.

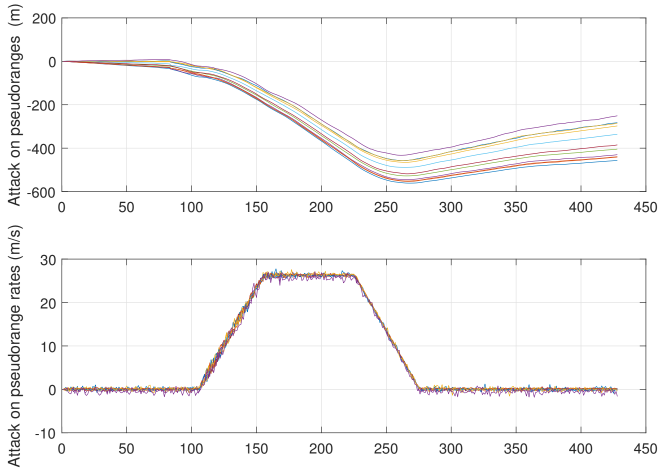

Fig. 1. Attack on pseudorange (top panel) and pseudorange rate (bottom panel) on 11 GPS channels. The local observation time is local.

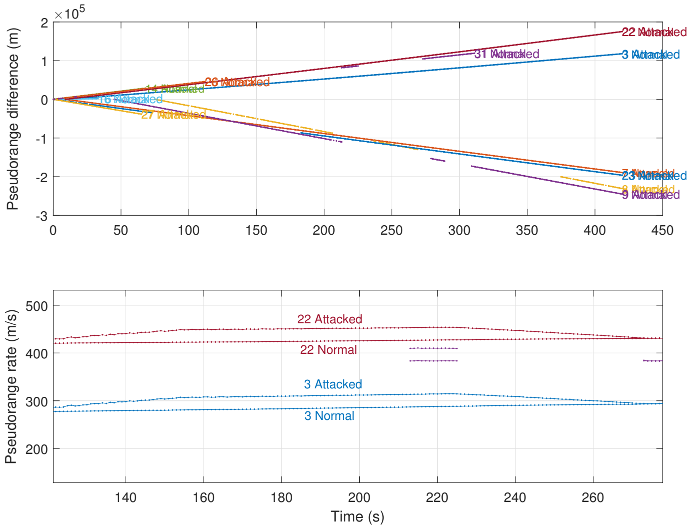

Fig. 2. Attack on pseudorange (top panel) and pseudorange rate (bottom panel) versus local observation time.

The normal and spoofed pseudorange change with respect to their initial value at $t = 0\ s$ is shown in Fig.2 for some of the visible satellites in the receiver's view. The bottom panel depicts the corresponding pseudorange rates under normal and attacked conditions. The tag at the end of each line indicates the satellite IDs and whether the pseudorange (or pseudorange rate) are in normal or attacked. The attack on the pseudorange rate is more visible due to the scale in the plot.

TSARM is implemented for an sliding window with $L = 50$ s with $T_{\text{lag}} = 10$ s. At initial values before $t = 120$ s, the attack has not started and the magnitude of the estimated attack is almost zero. Then, the attack starts gradually till it reaches a maximum level and then decreases. The procedure of sliding window is to correct the current clock bias and clock drift for all the times that have not been modified previously. Hence, at the first run, the estimates of the whole window are modified.

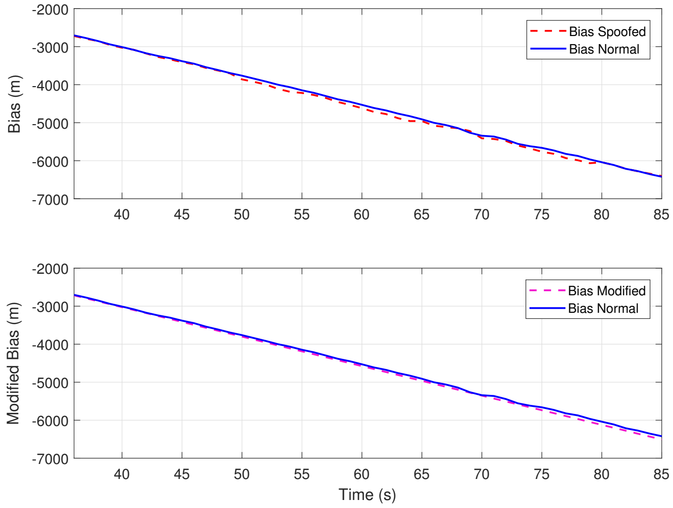

Fig. 3. Attacked clock bias (top panel) and modified clock bias (bottom panel) versus local observation time for $t = 35$ s through $t = 85$ s .

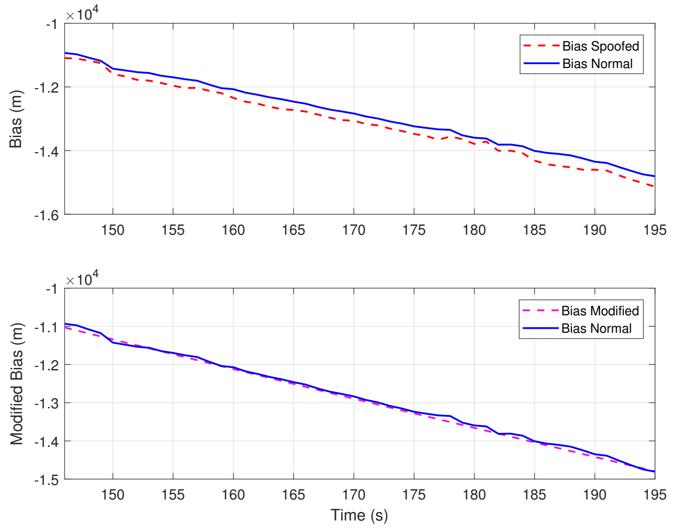

Fig. 4. Attacked clock bias (top panel) and modified clock bias (bottom panel) versus local observation time for $t = 145$ s through $t = 195$ s.

In Fig. 3, TSARM has been applied to correct the attack applied through TEXBAT. At initial times, small variations of the attack has been slightly modified. This variations occur $t = 145$ s through $t = 195$ s.

Fig. 4 shows the result of sliding window correction over the clock bias. As is obvious from the figure, the modification of the previous clock biases transforms the low TSARM detects the dynamic behavior of the spoofer, which facilitates the detection of attack through the total variation component in (4). The clock bias and drift have been modified for the previous time instants and need to be cleaned only for the last 10 seconds in the observation window. Here, TSARM is implemented for an sliding window with $L = 50$ s with $T_{\text{lag}} = 5$ s. The results show that the deviation imposed by the spoofer has been significantly decreased and the error lies in the standard margins defined by application.

V. Concluding Remarks

This work discussed an evaluation of time synchronization attack rejection and mitigation on devices that rely on GPS for time tagging their measurements. By direct modeling of the attack on the measurements, the attack mitigation technique is able to solve an optimization problem to estimate the attacks on the clock bias and clock drift. The spoofer manipulated clock bias and drift are corrected using the estimated attacks. The accuracy of this technique lies within the standardized accuracy in PMU and CDMA applications. The proposed method can be implemented for real-time operation.

Acknowledgment

The authors would like to thank the Radio Navigation Laboratory at the University of Texas at Austin for providing the navigation measurements of the TEXBAT database.

References

[1] I. Yaesh and U. Shaked, "Neuro-adaptive $h_{infinity}$ estimation and its application to improved tracking in GPS receivers," *IEEE Trans. Ind. Electron.*, vol. 56, no. 3, pp. 642–647, Mar. 2009.

[2] X. Li and Q. Xu, "A reliable fusion positioning strategy for land vehicles in GPS-denied environments based on low-cost sensors," *IEEE Trans. Ind. Electron.*, vol. 64, pp. 3205–3215, Apr. 2017.

[3] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "SPREE: A spoofing resistant GPS receiver," in *Proc. of the 22Nd Annual Int. Conf. on Mobile Comput. and Netw.*, 2016, pp. 348–360.

[4] P. Teunissen, "Quality control in integrated navigation systems," *IEEE Aeros. and Elect. Sys. Magazine*, vol. 5, pp. 35 – 41, July 1990.

[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. of the 21st Int. Tech. Meeting of the Sat. Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, Sept. 2008, pp. 2314–2325.

[6] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proc. of the ACM Conf. on Comput. and Commun. Security*, Oct. 2012, pp. 450–461.

[7] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful GPS spoofing attacks," in *Proc. of the 18th ACM Conf. on Comput. and Commun. Security*, Oct. 2011, pp. 75–86.

[8] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Computer Survey*, vol. 48, no. 4, pp. 64:1–64:31, May 2016.

[9] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. on Aeros. and Elect. Systems*, vol. PP, no. 99, pp. 1–1, 2017.

[10] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protect.*, vol. 5, pp. 146–153, Dec. 2012.

[11] P. Papadimitratos and A. Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures," in *Proc. of the IEEE Military Commun. Conf.*, San Diego, CA, USA, Nov. 2008, pp. 1–7.

[12] "Energy.gov, Office of Electricity Delivery & Energy Reliability," http://energy.gov/oe/services/technology-development/smart-grid, accessed: 2016-08-08.

[13] A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, "Real-time rejection and mitigation of time synchronization attacks on the global positioning system," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 8, pp. 6425–6435, Aug. 2018.