IEEE Open Journal of the Computer Society

Received 11 May 2023; accepted 16 May 2023. Date of publication 22 May 2023;
date of current version 8 June 2023. The review of this article was arranged by Associate Editor Zhaolong Ning.

Digital Object Identifier 10.1109/OJCS.2023.3278496

A Light-Weight Technique to Detect GPS Spoofing Using Attenuated Signal Envelopes

XIAO WEI[1], MUHAMMAD NAVEED AMAN[2] (Senior Member, IEEE), AND BIPLAB SIKDAR[1] (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583
[2]School of Computing, University of Nebraska-Lincoln, Lincoln, NE 68588 USA

CORRESPONDING AUTHOR: Muhammad Naveed Aman (e-mail: naveed.aman@unl.edu)

This work was supported by the Ministry of Education, Singapore under Grants A-0009040-00-00 and A-0009040-01-00.

ABSTRACT Global Positioning System (GPS) spoofing attacks have attracted more attention as one of the most effective GPS attacks. Since the signals from an authentic satellite and the spoofer undergo different attenuation, the captured envelope of fake GPS signals exhibits distinctive transmission characteristics due to short transmission paths. This can be utilized for GPS spoofing detection. The existing technique for GPS spoofing are either computationally too expensive, require specialize hardware/software updates, or are not accurate enough. To solve these issues, we propose a light-weight GPS spoofing detection method based on a dynamic threshold and captured signal envelope. We validate the proposed technique using experiments based on actual GPS signals and hardware. The relation between envelope characteristics and the distance between a GPS transmitter and receiver are revealed. Inspired by the uncovered relation, a threshold approach towards the detection of GPS spoofing is developed. The proposed approach features a dynamic threshold determined by the *dispersion value* of a signal envelope's variance instead of a fixed threshold to maximize detection performance in multiple attack scenarios. The results show that the proposed technique can effectively detect GPS spoofing attacks with better accuracy and lower computational complexity as compared to existing techniques.

INDEX TERMS Global positioning system, spoofing attacks, intrusion detection, signal evelope.

I. INTRODUCTION

The Global Positioning System (GPS) is widely used in navigation systems, communication systems, engineering surveys, Financial institutions, and critical infrastructures such as the power grid. It provides precise location and time information based on a satellite position in space and the signal propagation range. The signal transmission time is synchronized since atomic clocks are equipped on GPS satellites for time synchronizing. The satellite position is calculated by GPS ephemeris and almanac. A GPS civil receiver decodes the navigation data for GPS time and the satellite positions, and the propagation range is measured by a coarse/acquisition (C/A) code.

The generation and processing procedure of GPS civil signals is transparent and detailed in [1]. The C/A code of each satellite is public while the GPS ephemeris and almanac are open access and GPS signals are not encrypted. These cause the system is vulnerable to a spoofing attack. A GPS spoofing attack refers to an adversary gaining control over the calculated location and time of the victim receiver by broadcasting fake signals at GPS frequency. Todd Humphreys's team showed a successful spoofing attack on unmanned aircrafts [2] and surface vessels [3]. In their experiments, the fake signals are designed to be aligned with the authentic signals at first, the signal power of the fake signals is then increased to attract the victim receiver, once the receiver starts tracking the fake signal, the signal is designed to gradually deviate the receiver from its actual position. The authors in [4] show that a spoofing attack can be implemented by broadcasting fake signals through RF devices, which makes spoofing attacks easier. Fake GPS signals can be generated by software [5] for any target time and location. Spoofing attacks are discussed theoretically in [6] and [7]. Although [6] studied spoofing attacks based on ephemeris manipulation, [7] focuses on the

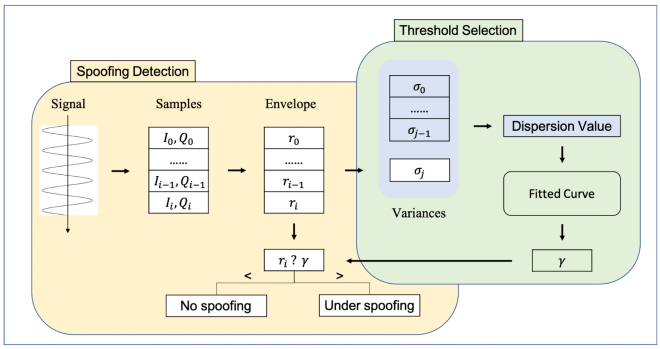


FIGURE 1. Processing procedures.

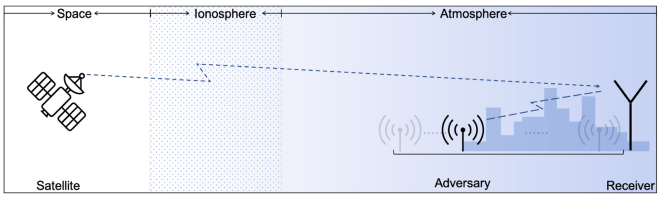


FIGURE 2. System model.

change of signal time. However, both works show the feasibility of spoofing a receiver's time while keeping the location in minor deviation.

Spoofing attacks can be catastrophic to systems that rely on GPS time or location. One such example is that of the modern power grids [8]. A clock offset of greater than 26.5 μs breaks the stability of the power grid and can cause a black-out. Similarly, GPS spoofing attacks can deceive navigation units of vehicles and mislead the vehicles to restricted areas [2]. In addition, GPS service has already penetrated into many aspect of our lives with the development of the Internet of things (IoT). For example, precision agriculture, intelligent transportation system, and commercial activities (e.g. shared bicycle, Pokemon GO) all depend on the GPS.

The importance and widespread applications of GPS make detection of GPS spoofing crucial. There are many existing works, we categorize them as techniques based on encryption and authentication; signal quality and signal processing based techniques; and assistance based techniques. Encryption methods [9], [10], [11], [12] insert special information into GPS signals while authentication methods [13], [14], [15], [16], [17] take advantage of the unpredictable nature of GPS signals. Although, Encryption- or authentication-based methods are more robust than others, their higher computational complexity and implementation requirements in terms of the design of the GPS scheme make them less feasible. Assistance based techniques such as using directional antennas to examine the signal of arrival [18], [19], [20], [21], [22] or using sensors and clocks to provide reference time [23], [24], [25] require additional hardware support. Morever, assistance based techniques rely on synchronized reference information and catch which not only results in a complex system but also increases the detection latency. Finally, there are techniques purely based on the received signals, including signal quality [26], [27], [28], [29] and signal processing methods [30], [31], [32], [33], [34]. More details about related works are in Section VI.

Targeting the effectiveness and timeliness of GPS spoofing detection, we work from the basic feature of communication transmission – signal attenuation. Authentic GPS signals are transmitted from the satellites in space and are reflected by the ionosphere, troposphere, and urban environments with dense buildings. Since authentic signals traverse significanlty longer distances as compared to fake signals, the envelope of authentic and fake signals differ significantly. In this article, we propose a distribution-based spoofing detection method and a dynamic threshold selection method to improve the overall performance. Our main contributions are as follows:

1) An analytical model for the distribution of a signal's envelope based on the distance between the transmitter and receiver.
2) A light-weight threshold technique based on the distribution of signal envelopes to detect GPS spoofing attacks.
3) A dynamic threshold selection mechanism based on the dispersion of variance of a signal's envelope.

The rest of this article is organized as follows. We first introduce the system model in Section II. In Section III, we describe the proposed technique and the experimental design is described in Section IV. The detection results are presented in Section V and the proposed *dispersion value*-based threshold selection mechanism is explained in Section V. Section V discusses the results and a comparison of the proposed detection method with related literature is presented in Section VI. In the end, we conclude the article in Section VII.

II. SYSTEM MODEL

We consider the system model shown in Fig. 2. GPS satellites orbit at 19300 km above the earth's surface while the receiver and adversary are located on the earth's surface. We consider the following two scenarios:

1) *Legitimate Scenario:* The GPS receiver tracks authentic GPS signals that are transmitted by GPS satellites in the space. Signals experience reflections within ionosphere and atmosphere before reaching a receiver. At the surface of earth, the average signal power is around -171 dBW and the signal to noise ratio is around 30 dB.
2) *Attack Scenario:* The GPS receiver tracks fake signals that are transmitted by an adversary. Fake signals are transmitted at a higher signal power to overlay the authentic ones. The adversary broadcasts fake signals by an antenna which is placed close to the victim receiver and keeps a relatively stable distance to maintain a continuous and stable attack [3].

III. PROPOSED SPOOFING DETECTION TECHNIQUE

Denoting the transmitter and receiver by *Tx* and *Rx*, respectively, the signal received by the *Rx* can be modeled as

follows [35]:

$$y(t) = \sum_{n=1}^{N} x_n(t) \tag{1}$$

$$= \sum_{n=1}^{N} (x_{n,i}(t) + jx_{n,j}(t))e^{j2\pi f_c t} + \eta(t), \tag{2}$$

where $x_{n,i}(t)$ and $x_{n,j}(t)$ are the in-phase and quadrature components of $x_n(t)$, respectively. $\eta(t)$ is the additive white Gaussian noise and N is the total number of symbols. Let $I(t)$ and $Q(t)$ be the in-phase and quadrature components of $y(t)$, we get

$$I(t) = r(t)\cos(2\pi f_c t + \theta(t)) + \eta_i(t), \tag{3}$$

$$Q(t) = r(t)\sin(2\pi f_c t + \theta(t)) + \eta_j(t), \tag{4}$$

where $r(t)$ and $\theta(t)$ are the envelope and phase of the received signal, $\eta_i(t)$ and $\eta_j(t)$ are the in-phase and quadrature components of signal noise $\eta(t)$. The white Gaussian noise can be ignored for signal envelope calculation since it is independent of authentic and fake GPS signals. As the proposed technique is based on the signal envelope, with out loss of generality, the received signal envelope is given as follows:

$$r(t) = \sqrt{I(t)^2 + Q(t)^2}. \tag{5}$$

Considering a Rayleigh distributed channel, the mean and variance of the received signal envelope will vary with the distance (d_i) between the *Tx* and *Rx* as follows:

$$\mathbb{E}[R] = \sqrt{\frac{\pi}{2}}\sigma_R = \frac{\sqrt{\pi d_i^{-\alpha}}}{2}. \tag{6}$$

$$Var(R) = \frac{4-\pi}{2}\sigma_R^2 = \frac{4-\pi}{2d_i^{\alpha}}. \tag{7}$$

Thus, the probability density functions for a spoofed signal envelope and an authentic signal envelope will be significantly different given that the GPS satellites are 19300 km away from the earth's surface while the adversary cannot be too far from the receiver due to the capability of attack devices [1]. Accordingly, the probability of missed detection (P_{MD}), probability of false alarm (P_{FA}), and probability of detection (P_D) for attack scenarios that have different distances between *Tx* and *Rx* can be calculated as follows:

$$P_{MD} = P_{d_i}[R < \gamma] = \int_{\infty}^{\gamma} f_A(r)dr, \tag{8}$$

$$P_{FA} = P_{d_0}[R > \gamma] = 1 - \int_{\infty}^{\gamma} f_L(r)dr, \tag{9}$$

$$P_D = P_{d_i}[R > \gamma] = 1 - \int_{\infty}^{\gamma} f_A(r)dr, \tag{10}$$

where γ is the detection threshold, d_i is the distance between the adversary's antenna and the *Tx*, and d_0 the distance between the GPS satellites and the *Tx*. Moreover, $f_L(r)$ and $f_A(r)$ represent the pdf of the envelope $r(t)$ for legitimate signals and spoofed signals, respectively. The pdf of the envelope of a signal can be considered rayleigh distributed or normally distributed [36].

A. RAYLEIGH DISTRIBUTED SIGNAL ENVELOPE

A Rayleigh distribution is characterized by the following pdf:

$$f_R(r) = \frac{r}{\sigma_R^2} e^{-\frac{r^2}{2\sigma_R^2}}, r \geq 0, \tag{11}$$

where, the scale parameter σ_R is related to d_i, the distance between *Tx* and *Rx* [37]. An attack with larger d_i leads to greater $\sigma_{R,i}$ and vice versa, i.e., the pdf of the envelope will vary according to the distance between a transmitter and receiver. Using this insight, the pdfs of the envelope under attack with the attacker located at $d_i \in \{0.2, 0.5, 1, 5\}$ m and the pdf under the legitmate scenario, i.e., $d_0 = 19300$ km are plotted in Fig. 3(a). we observe different pdf curves for different d_is.

B. NORMALLY DISTRIBUTED ENVELOPE

If the envelope of a received signal is assumed to be normally distributed then the pdf is as follows:

$$f_N(r) = \frac{1}{\sigma_N\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{r-\mu}{\sigma_N}\right)^2} \tag{12}$$

where μ is the mean of envelope, and σ_N^2 is the variance of envelope given by (6) and (7), respectively. Then, the variance of the envelope can be re-written as:

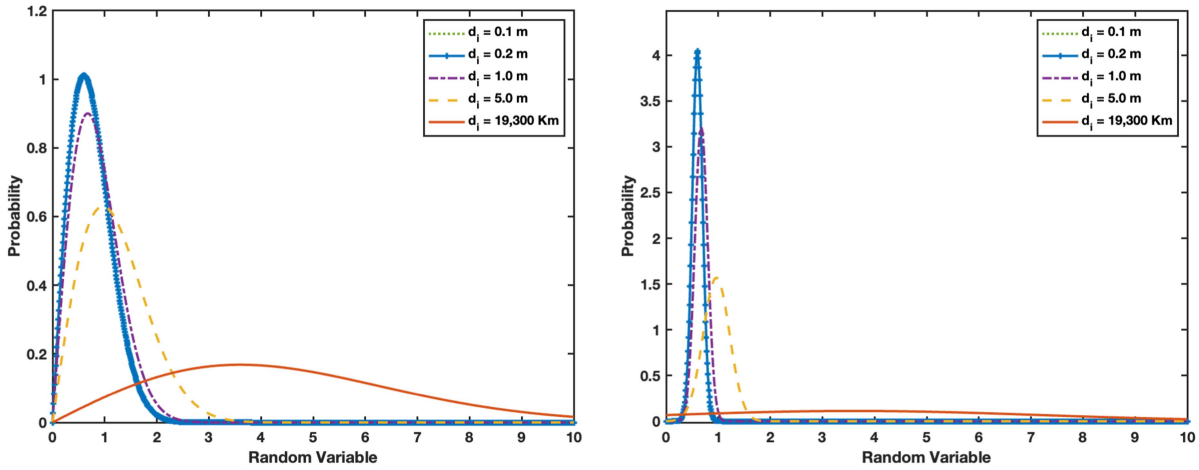
$$Var(R) = \frac{4-\pi}{\pi}\mathbb{E}(R)^2 \tag{13}$$

Thus, the mean and variance of the envelope in (12) will vary according to the distance of the attacker from the *Rx*. The pdf curves for $d_0 = 19300$ km and $d_i = 0.2$ m, 0.5 m, 1 m, 5 m are shown in Fig. 3(b). We observe that as d_i changes the mean and variance of the pdfs also change.

IV. EXPERIMENT DESIGN

We conducted experiments to capture authentic GPS signals and also generated fake signals to be transmitted by an adversary. The experiment illustration is shown in Fig. 4. The victim receiver side consists of a computer, NI USRP device and a GPS antenna. The computer controls the USRP-2943R to capture the signals at GPS civil frequency 1575.42 MHz with the GPS antenna. The adversry consists of a laptop, BladeRF and an antenna. The laptop controls the BladeRF to broadcast the generated fake GPS signals.

The fake GPS signals were generated by the open source software GPS-SIM-SDR [5]. The spoofing position is set to be a route in China while the receiver is actually located at a fix position in Singapore. The GPS time is also spoofed to an early time. The BladeRF board is configured to set the transmit frequency at 1575.42 MHz, sampling rate at 2.5 MHz, and the transmit gain at 73 dB. The USRP is configured to set the receiver frequency at 1575.42 MHz, sampling rate at 16 MHz,



(a) Rayleigh distributed. (b) Normally distributed.

FIGURE 3. Envelope probability density function.

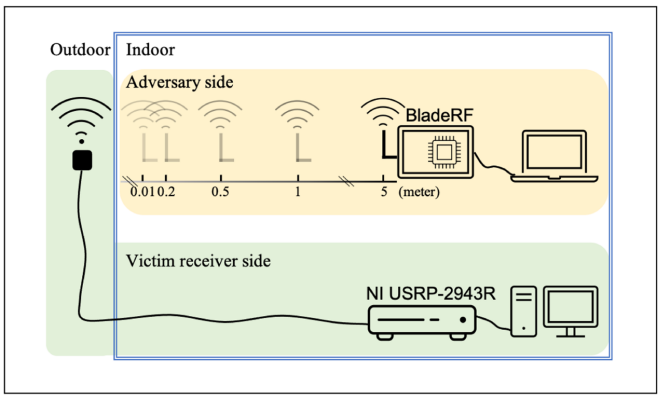


FIGURE 4. Experiment illustration.

(a) Without Spoofing attack (b) With Spoofing attack

FIGURE 5. Illustration of the spoofing attack.

and the receive gain at 25 dB. A series of spoofing attacks are conducted by placing the adversary antenna at 0.01 m, 0.2 m, 0.5 m, 1 m, and 5 m away from the receiver's antenna.

In the experiment, a phone with the 'GPS test' and 'Baidu Map' applications installed was used to verify the attack. GPS test shows the visible satellite, their signal strength and the

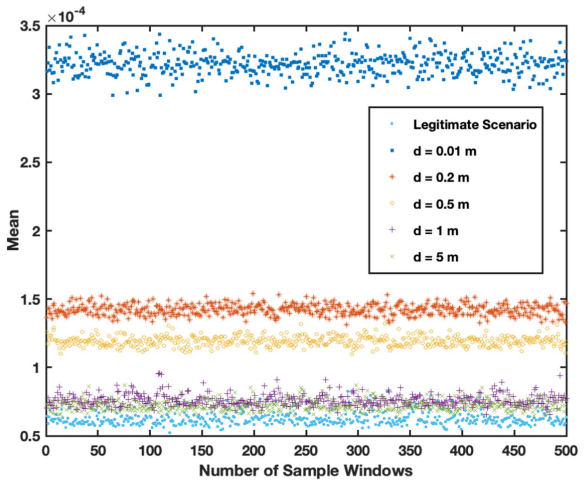


FIGURE 6. Mean of envelope samples (WinSize = 500).

GPS time, while the Baidu Map shows the position. As shown in Fig. 5(a), without the spoofing attack, the signal to noise ratio (SNR) of different satellites varies, the calculated time coincides with the actual time, and the calculated location is at the National University of Singapore (NUS) campus in Singapore. Fig. 5(b) shows the results when there is a spoofing attack at 5 m, the SNR of different satellites are similar and above 30, the calculated time is the spoofed time, and the calculated location is at China. This shows that our experiment design can successfully generate spoofed signals for actual android applications. Thus, the results presented in this paper are representative of actual GPS spoofing attacks.

The signal's envelope is calculated by (5) from the I & Q samples. A 500 window size was used for the mean of envelope calculation. Fig. 6 shows the mean value of 500 windows observed for attacks at different distances. The average value of envelope means are 3.441×10^{-4}, 1.423×10^{-4}, 1.194×10^{-4}, 7.592×10^{-5}, 7.151×10^{-5} for attacks

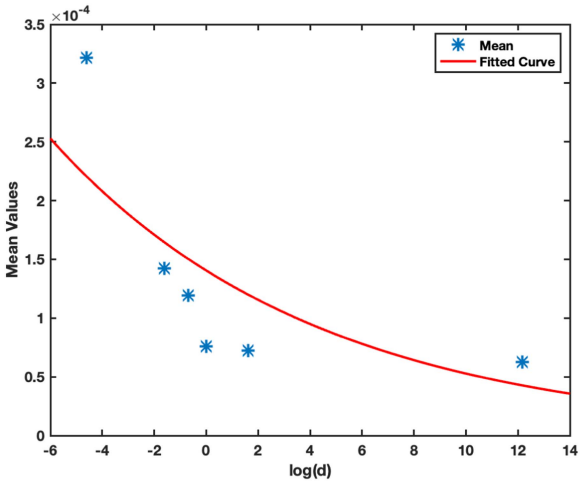


FIGURE 7. The trend between mean of a signal's envelope and distance.

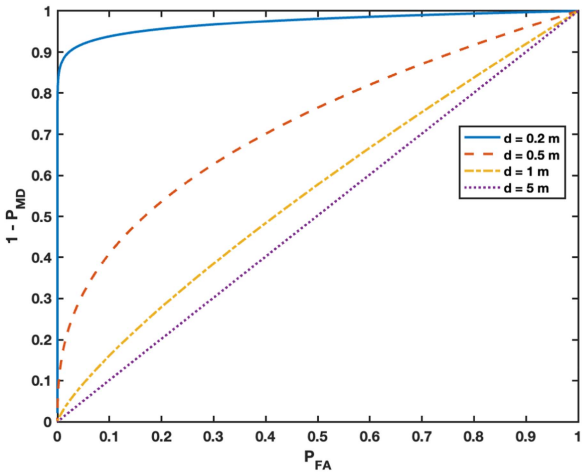


FIGURE 8. ROC under Rayleigh distribution.

at 0.01 m, 0.2 m, 0.5 m, 1 m, and 5 m, respectively. The envelope mean for authentic signals is 6.248×10^{-5}. We fitted the average envelope mean value over a window with 500 samples with

$$\tilde{r} = ae^{bl} \tag{14}$$

in Fig. 7, where a $= 1.405 \times 10^{-4}$, b $= 9.795 \times 10^{-2}$. We observe that the average value of the mean of a signal's envelope decreases exponentially with increasing the distance between the receiver's and an attacker's antenna

V. RESULTS

In this section, we evaluate the performance of the proposed spoofing detection mechanism. Considering the Rayleigh distribution for the signal envelope, the miss classification probabilities can be described by:

$$P_{MD} = 1 - e^{\frac{-\gamma^2}{2\sigma_R{}^2}} = 1 - e^{-\gamma^2 d_i^{\alpha}}, \tag{15}$$

$$P_{FA} = e^{\frac{-\gamma^2}{2\sigma_R{}^2}} = e^{-\gamma^2 d_0^{\alpha}}, \tag{16}$$

$$P_D = e^{\frac{-\gamma^2}{2\sigma_R{}^2}} = e^{-\gamma^2 d_i^{\alpha}}. \tag{17}$$

Fig. 8 shows receiver operating characteristic (ROC) curves for the different d_i values. we observe that the area under the ROC curve increases as d_i reduces. The changes of P_D, P_{MD}, and P_{FA} over various thresholds are plotted in Fig. 9. As d_0 is constant, we only get one curve for P_{FA}. However, P_D and P_{MD} curves vary according to the distance between attacker and Rx. We observe that a threshold between 1 and 2 with a $d_i > 0.2$ m leads to better results.

Assuming the signal envelope to be distributed as a normal distribution, Fig. 10 shows the variance directly calculated from the signal's envelope and the average of the variance of 500 samples over various distances d_i. We observe that for each d_i, the variance directly calculated from the signal's envelope is approximately the same for the average variance calculate over a window of samples. Thus, we do not need

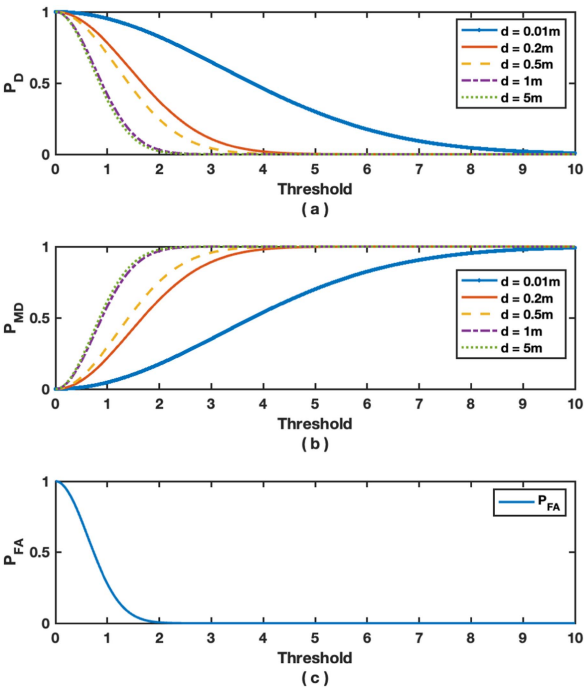


FIGURE 9. Detection probabilities over thresholds based on Rayleigh distribution for different attacks (a) P_D, (b) P_{MD}, (c) P_{FA}.

to applying averaging. The ROC for the proposed scheme is shown in Fig. 11. The miss classification rates are shown in Fig. 12 and given as follows:

$$P_{MD} = \frac{1}{2}\left[1 + erf\left(\frac{\gamma - \mu_i}{\sigma_i\sqrt{2}}\right)\right] = \frac{1}{2}\left[1 + erf\left(d_i^{\frac{\alpha}{2}}(\gamma - \mu_i)\right)\right], \tag{18}$$

$$P_{FA} = \frac{1}{2}\left[1 - erf\left(\frac{\gamma - \mu_0}{\sigma_0\sqrt{2}}\right)\right] = \frac{1}{2}\left[1 - erf\left(d_0^{\frac{\alpha}{2}}(\gamma - \mu_0)\right)\right], \tag{19}$$

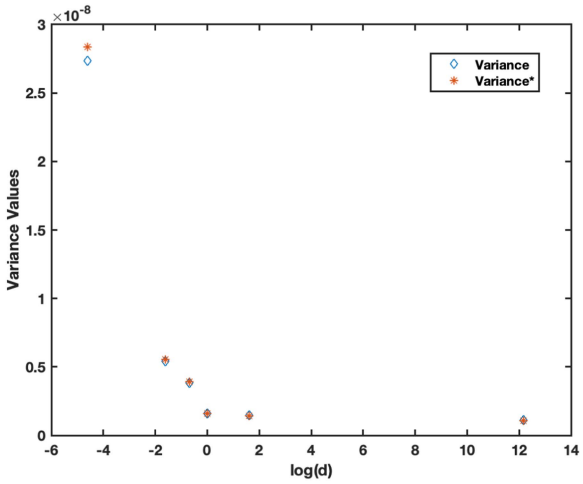


FIGURE 10. The comparison of Variance and Variance*.

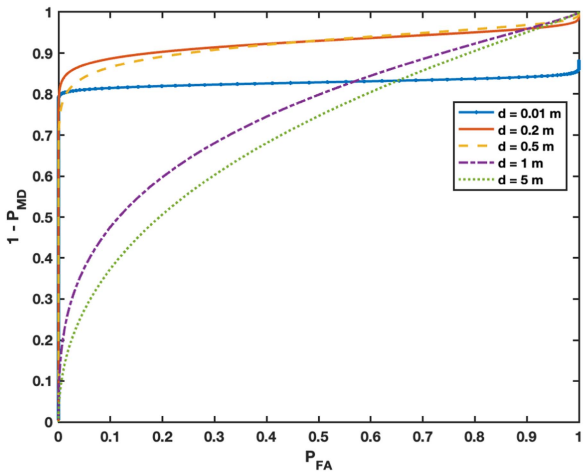


FIGURE 11. ROC under normal distribution.

$$P_D = \frac{1}{2}\left[1 - erf\left(\frac{\gamma - \mu_i}{\sigma_i\sqrt{2}}\right)\right] = \frac{1}{2}\left[1 - erf\left(d_i^{\frac{\alpha}{2}}(\gamma - \mu_i)\right)\right]. \tag{20}$$

where $erf^{-1}(z)$ is the inverse error function and can be extended by the Maclaurin series [38]. We observe that the optimal value for threshold is $\gamma > 0.5$.

Figs. 9 and 12 show that the performance of detecting spoofed signals depends on the threshold γ. Thus, to obtain a balanced performance criterion, we define a new metric Ω, the effective detection rate, taking into account P_{MD} and P_{FA} as follows:

$$\Omega = 1 - \lambda_{MD}P_{MD} - \lambda_{FA}P_{FA}, \tag{21}$$

with

$$\lambda_{MD} + \lambda_{FA} = 1 \tag{22}$$

where λ_{MD} and λ_{FA} are weights defining the importance of P_{MD} and P_{FA}, respectively. As a higher P_{MD} is typically more harmful, we chose $\lambda_{MD} = 0.7$, $\lambda_{FA} = 0.3$, for a $P_{FA} < 0.8$. The corresponding plots for Ω versus threshold values are

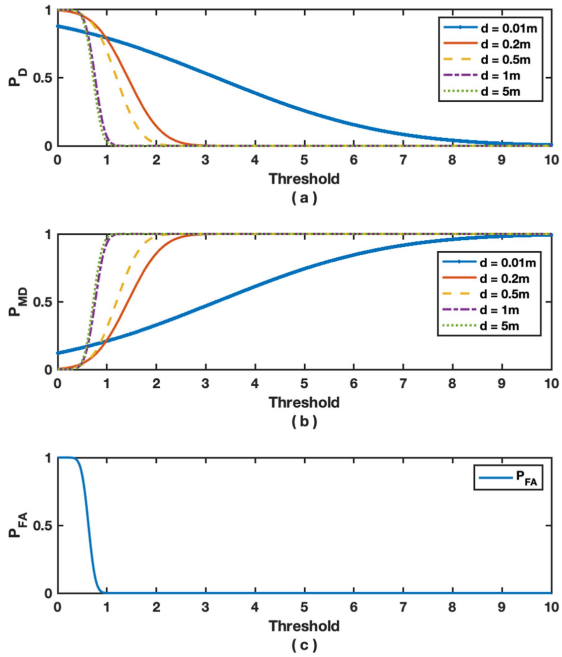
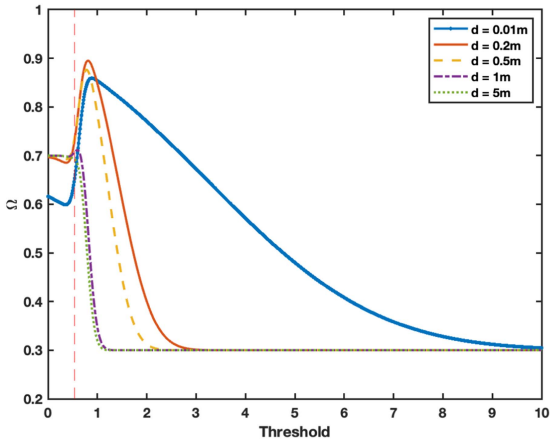


FIGURE 12. Detection probabilities over thresholds based on Normal distribution for different attacks: (a) P_D, (b) P_{MD}, and (c) P_{FA}.

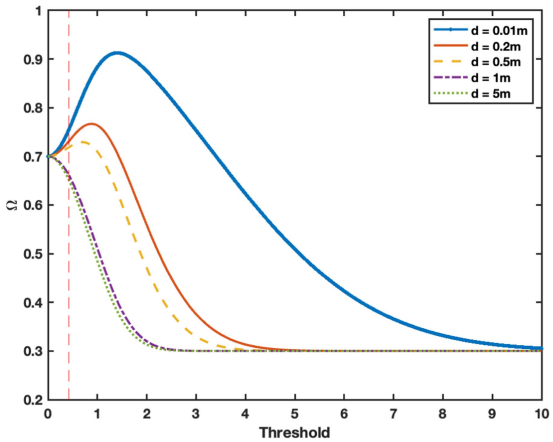
shown in Fig. 13. For $P_{FA} > 0.8$, we observe that in Fig. 13(a) the minimum required threshold value is $\gamma > 0.54$ while that for Fig. 13(b) the minimum required threshold value is $\gamma > 0.42$. Similarly, as d_i increases the peak of the curves moves to the right, i.e., the optimal threshold value increases. Thus, the upper bound on γ is defined by the curve corresponding to $d_i = 0.01$ m. This shows the acceptable range for γ is [0.54 0.89] and [0.42 1.40] after taking the signal envelope as Rayleigh distributed and normally distributed, respectively.

The value of the performance criterion after assuming the signal envelope as a Rayleigh or Normal distribution for different d_is is given in Tables 1(a) and (b), respectively. We observe that the best value of Ω is obtained using a threshold value which depends on d_i. Therefore, using a fixed threshold to detect attacks in different scenarios may not lead to the best performance, i.e., the threshold needs to be adjusted according the the attacker distance from the *Rx*.

The I & Q samples of signals captured from attacks at various distances are shown in Fig. 16. This shows that the variance of the envelope of received signals may not be a good predictor as the variance between attacks from $d_i > 0.2$ m does not have clear boundaries. This is also obvious from Fig. 15(a). To maximize the performance of the proposed technique in detecting attacks from different distances, we analyzed the dispersion of the received signals to devise an optimal threshold value in Fig. 15(b). The dispersion value is defined as the distance between the confidence bounds of variances. As shown in Fig. 14, the variance of attacks at closer distances is scattered over a larger area. We fitted



(a) Rayleigh distributed envelope.



(b) Normally distributed envelope.

FIGURE 13. Ω versus Threshold.

the variance using an exponential curve with 95% confidence bounds. The distances between the confidence bounds are marked in Fig. 14. In order to have a clear view on all scenarios, the variance of attacks at 1 m, 5 m, and legitimate scenario are drawn separately. We observe that the *dispersion value* drops from 7.7056×10^{-9} to 6.4072×10^{-10} when increasing the attacking distance from 1 m to 5 m, while the legitimate scenario value is 5.4716×10^{-10}. Fig. 15(b) shows that the *dispersion value* decreases when the attacker moves away from the *Rx*. We define the optimal threshold that leads to a best performance as γ^*. For this purpose we fit a curve as follows:

$$\gamma = a d_v^b + c \tag{23}$$

where γ is the threshold, d_v is the *dispersion value*, and a, b, c are the coefficients. Note that the coefficients are dynamically renewed according to the distance of the attacker from the receiver.

In Fig. 17, the *optimal thresholds* are plotted against the *dispersion values*. The fitted curve is generated by (23) with 95% confidence. For detection based on Rayleigh distribution

TABLE 1. Performance Under Different Thresholds

(a) Rayleigh Distribution

Threshold	Distance				
	0.01m	0.2m	0.5m	1m	5m
1.40	**0.9124**	0.7071	0.6275	0.4035	0.3824
0.88	0.8630	**0.7669**	0.7221	0.5463	0.5217
0.69	0.8211	0.7593	**0.7292**	0.6001	0.5803
0.42	0.7547	0.7308	0.7186	**0.6613**	0.6517
0.42	0.7547	0.7308	0.7186	0.6613	**0.6517**

(b) Normal Distribution

Threshold	Distance				
	0.01m	0.2m	0.5m	1m	5m
0.89	**0.8591**	0.8835	0.8470	0.4428	0.3847
0.81	0.8525	**0.8949**	0.8737	0.5483	0.4763
0.78	0.8444	0.8926	**0.8763**	0.5888	0.5166
0.59	0.6958	0.7702	0.7729	**0.7112**	0.6851
0.54	0.6530	0.7316	0.7365	0.7072	**0.6929**

in Fig. 17, the resulting coefficients are $a = 1.29 \times 10^3$, $b = 1.982 \times 10^{-4}$, and $c = -1.289 \times 10^3$, and the fitted curve is

$$\hat{\gamma_R} = 1290\, d^{0.0001982} - 1289 \tag{24}$$

For detection based on normal distribution in Fig. 17(a), the resulting coefficients are $a = 94.41$, $b = 0.001306$, and $c = -93.45$, and the fitted curve is

$$\hat{\gamma_R} = 94.41\, d^{0.001306} - 93.45 \tag{25}$$

Fig. 18 shows the value of Ω plotted against the `log` of d_i for the optimal threshold and fitted threshold. We observe that the performance of the fitted threshold values is approximately the same as the optimal threshold values. We also present the plot for the worst performance generated using the lower bound of the threshold range, i.e., $\gamma = 0.54$ and $\gamma = 0.42$ for the Rayleigh distributed and Normally distributed signal envelope, respectively.

To summarize these results, Table 2 presents the comparison of the fitted threshold performance with the optimal threshold and worst threshold performance. We observe that the fitted thresholds have significant performance gains while the performance loss is not significant. We summarise the performance of spoofing detection using the optimal threshold and the dynamic threshold obtained after curve fitting in Table 3 to compare the proposed scheme using a Rayleigh distribution method and Normal distribution method. We observe that overall using the Normal distribution to characterize the received signal envelope results in better performance. Moreover, the performance of using the optimal threshold and dynamic threshold is approximately the same. However, the Rayleigh distribution method is more suitable for situations where the attacker is extremely close to the receiver.

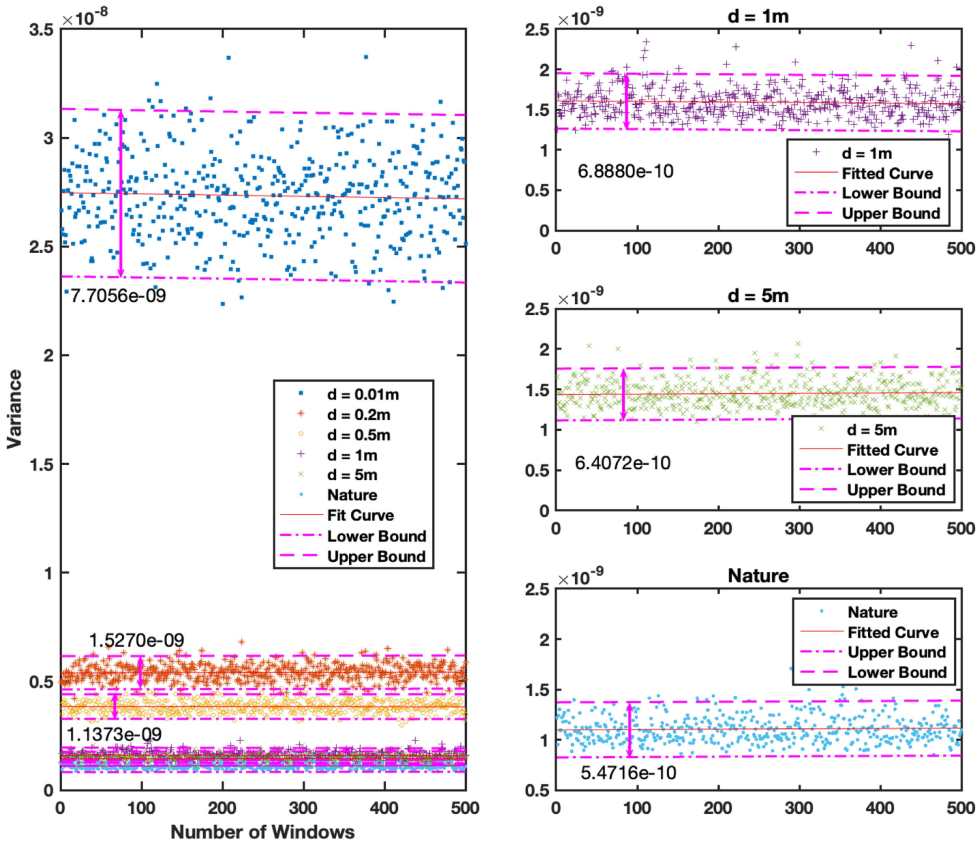


FIGURE 14. The range between confidence bounds which fit the variance of the signal's envelope for attacks.

TABLE 2. Comparison of Performance Under Selected Thresholds

(a) Rayleigh Distribution

Difference \ Distance	0.01m ($\gamma = 1.13$)	0.2m ($\gamma = 0.72$)	0.5m ($\gamma = 0.64$)	1m ($\gamma = 0.52$)	5m ($\gamma = 0.50$)
Improvement over worst case	0.1453	0.0544	0.1014	0.2388	0.2511
Deterioration from best case	0.0124	0.0055	0.0004	0.0191	0.0182

(b) Normal Distribution

Difference \ Distance	0.01m ($\gamma = 0.93$)	0.2m ($\gamma = 0.73$)	0.5m ($\gamma = 0.69$)	1m ($\gamma = 0.63$)	5m ($\gamma = 0.62$)
Improvement over worst case	0.2051	0.1451	0.1141	0.2650	0.2892
Deterioration from best case	0.0010	0.0181	0.0256	0.0033	0.0190

TABLE 3. The Performance When Respectively Applying Optimal and Selected Thresholds to Their Corresponding Attack Scenarios

Threshold Type	Distribution Type	Distance 0.01m	0.2m	0.5m	1m	5m
Optimal Threshold	Rayleigh	0.9124	0.7669	0.7292	0.6613	0.6517
	Normal	0.8591	0.8949	0.8763	0.7111	0.6929
Dynamic Threshold	Rayleigh	0.9000	0.7614	0.7288	0.6423	0.6335
	Normal	0.8581	0.8767	0.8506	0.8762	0.7078

TABLE 4. Summary of Existing GPS Spoofing Detection Techniques

Requirements	Complexity	Timeliness	Update	Data Source	Technique
Wesson et al. [34]	Med	High	Firmware	Signals	Hypothesis testing
Wang et al. [26]	Low	Med	Firmware	Signals	STL discriminator
Manesh et al. [39]	Med	LOW	Firmware	Signals	Neural network
Mina et al. [40]	Med	Med	Firmware	Signals	Network of multi-receivers
Kang et al. [19]	Med	High	Hardware	Signals	Direction-of-arrival
Shafiee et al. [41]	Med	Med	Firmware	Signals	Neural network
Schmidt et al. [30]	High	Med	Firmware	Signals	LASSO
Arafin et al. [42]	Low	High	Firmware	Hardware oscillators	Frequency drift and offset
Bhamidipati et al. [18]	Med	High	Hardware	Signals	Pseudorange residuals
Sabouri et al. [43]	High	Low	Firmware	Power grid	Neural network
Xie et al. [44]	Low	Low	Firmware	Power grid	Quasi-dynamic state estimation
Prandhan et al. [45]	Low	Low	Firmware	Power grid	Hypothesis testing
Proposed	Low	High	Firmware	Signals	Distribution of signal envelope

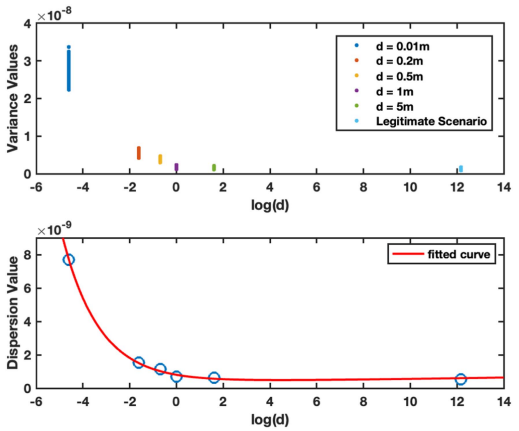


FIGURE 15. (a) variance of signal envelopes, and (b) dispersion of variance.

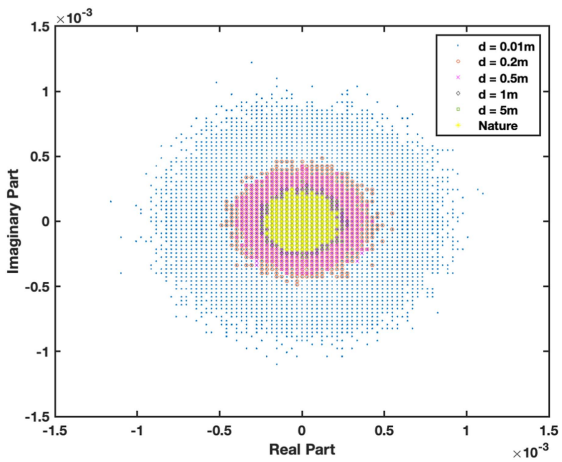
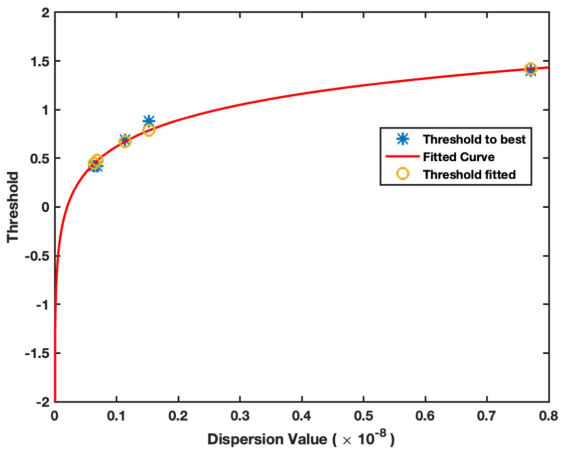
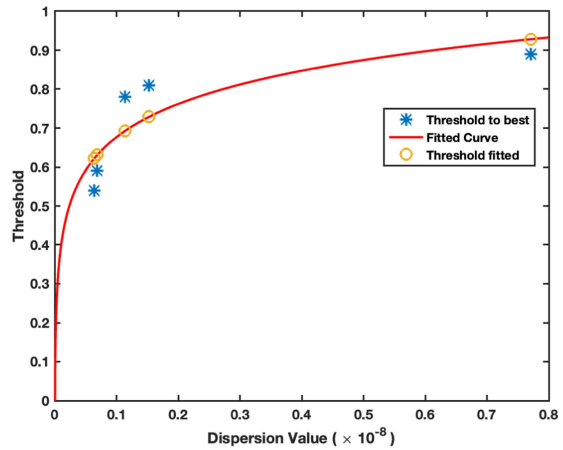


FIGURE 16. I & Q samples of the captured signals.



(a) Rayleigh distribution.



(b) Normal distribution.

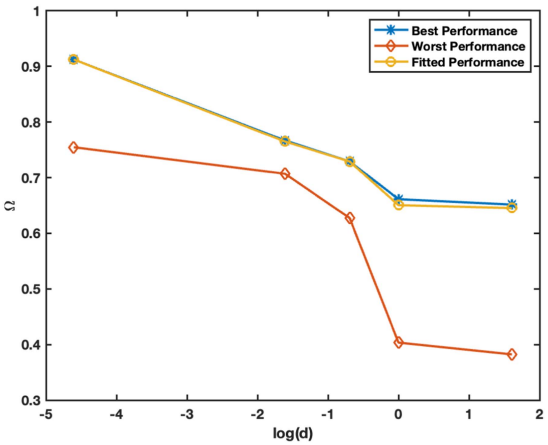
FIGURE 17. The dispersion value and its corresponding thresholds.

VI. COMPARISON WITH EXISTING TECHNIQUES

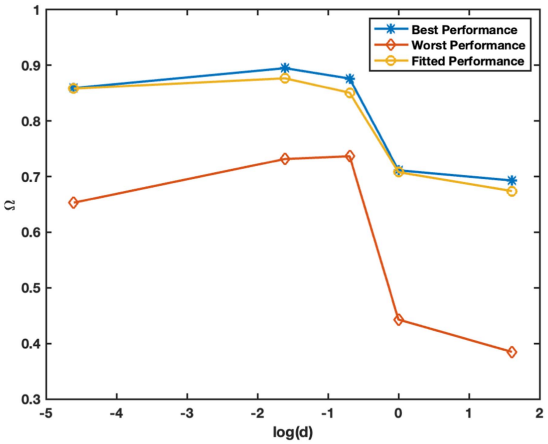
In this section, we compare the proposed detection methods with the existing works.

A. GENERAL COMPARISON

Table 4 lists measurements on the related works in terms of complexity, efficiency, update requirement, data source, and the technique basis. In Table 4, there are two works [19]



(a) Rayleigh Distribution



(b) Normal Distribution

FIGURE 18. Performance of the proposed technique under different thresholds.

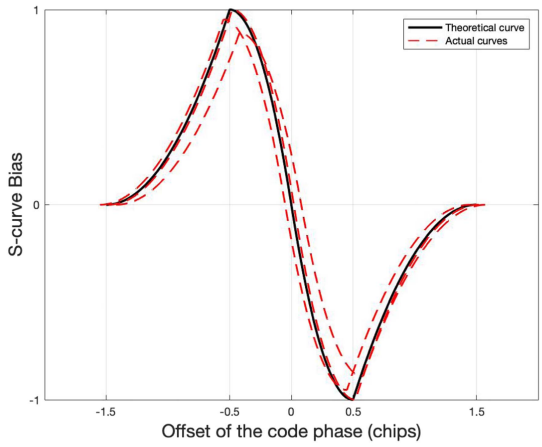


FIGURE 19. S-curve vs the offset of code phase when applying $(I_E^2 + Q_E^2) - (I_L^2 + Q_L^2)$ as CLD.

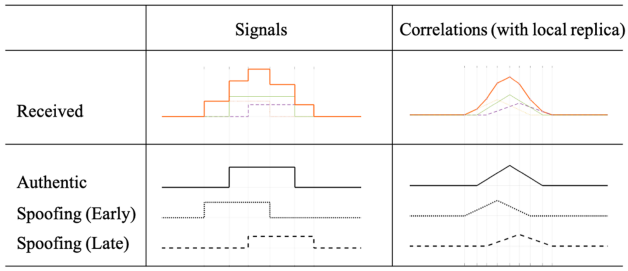


FIGURE 20. Basis of the technique proposed in [30].

TABLE 5. Comparison of Detection Probability

	0.01m	0.2m	0.5m	1m	5m
Wang et al. [8]	0.73	0.58	0.57	0.55	0.68
Schmidt et al. [13]	0.76	0.74	0.67	0.69	0.61
Proposed	0.94	0.88	0.86	0.79	0.79

and [18] the require hardware updates which are difficult to implement. [19] detects spoofing by monitoring the direction of arrival using one direction antenna. While [18] employs distributed multiple directional antennas to analyse the different pseudo-range residuals to estimate the spoofed time error. Other detection methods require firmware updates. Among these, there are four works [42], [43], [44], [45] based on the data from power grids. [42] uses the inherent hardware oscillator in power grids as the frequency state reference and does spoofing detection by monitoring the state changes. [43] uses the rotor angles of generator buses of power grids as features to train a Neural network. [44] uses multiple features of power grids, such as bus voltage magnitudes, phase angles, and generator speed, to estimate a quasi-dynamic estimation for spoofing classification. Similarly, [45] employs rotor angle, rotor speed, and internal voltage to do a generalized likelihood ratio-based hypotheses classification. These power grids data based techniques and [40] are less efficient in terms of processing, since they need to wait for the information from other sources. Although [40] does not use additional antennas or data from power grids, it collects GPS signals from multiple receivers and uses the extracted P(Y) signal to form a network for spoofing detection. Only [26], [30], [34], [39], [41] are based on solely the received GPS signals. However, [39], [41] build neural network models for signal processing. Although they are accurate in predicting spoofing, they require extra resources for data collection and training to generate a fitted model. [34] proposed a method based on sensing the distortion of signal correlation peaks and power. To further evaluate the proposed technique, we compare it with the works in [26] and [30], both papers are based on the correlation process during tracking signals. The technique in [26] detects spoofing by monitoring the first-order derivation of the S-curve Bias (SCB). In [26], the non-coherent discriminator, $(I_E^2 + Q_E^2) - (I_L^2 + Q_L^2)$, are considered as the code loop discriminator (CLD) in the tracking loop, and the

TABLE 6. Comparison of Proposed Technique's Computational Complexity With Existing Techniques

Technique	Parameters	Computational Complexity
Wang et al. [26]	Trace length: n, formula size: m	$O(n \times m)$
Arafin et al. [42]	Number of signal samples: n	$O(n\log n)$
Xie et al. [44]	Number of state variables: n	$O(n^3)$
Prandhan et al. [45]	Number of state variables: n	$O(n^2)$ to (n^4)
Proposed Technique	Number of samples: n	$O(n)$

output of CLD are collected as an S-curve. As shown in Fig. 19, theoretically, when the local replica is promptly aligned with the incoming signal (offset of code phase is zero), the value of the S-curve is zero. Due to the noise and distortion by front-end processing, the offset of code phase usually are not at zero for zero value S-curve. [26] invites this offset deviation as SCB. As mentioned in [26], the SCBs fluctuate around zero without spoofing attack while they fluctuate falling or increasing significantly with a spoofing attack. Hence, a proper threshold is expected to include the first-order derivation of SCBs without spoofing and exclude that with spoofing.

The technique in [30] discriminates the correlation peaks based on least absolute shrinkage and selection operator (LASSO). The incoming signals are multiplied with the local replicas for code phase selection. As shown in Fig. 20, there is only one peak when authentic signal correlate with local replicas. However, the received signal are a combination of authentic signal and signals from multipath or spoofing which leads the correlation result with many peaks, as shown by the orange curve. This correlation result can be broke down to the summation of correlation of authentic signals in different delay. To calculate the optimal combination of authentic correlation results, [30] uses LASSO to solve the convex optimization problem. The output are coefficients of each early or late authentic signal replica. In the legitimate scenario, the coefficients of authentic signal replicas are significantly smaller than the coefficient of authentic signal, since multipath signals usually experience more attenuation. In the attack scenario, the coefficients that correspond to spoofing signals are noticeably greater than the coefficients that correspond to multipath signals, since the spoofing signal will be transmitted at higher power to get tracked by a victim receiver. Hence, as proposed by [30], the spoofing attack can be detected by monitoring the ratio of coefficients.

B. MISCLASSIFICATIONS

For comparison, we consider the worst case in our result where the P_{FA} is around 70%. When applying the SCB method [26] to our data set, $1.1 \times 10^{-}3$ is used as the detection threshold for $P_{FA} \approx 70\%$. When applying the LASSO method [30] to our data set, the threshold is 0.73. Other settings are same with [26] and [30]. The detection results are listed in Table 5. The proposed method outperforms the others in all attacking scenarios. Moreover, the detection methods in [26] and [30] make use of the correlator output of the tracking loop while the proposed method does not have this requirement. This leads to significant reduction of the detection time in the proposed technique.

C. COMPUTATIONAL COMPLEXITY

The proposed technique is based on comparing the variance of the signal envelope against a threshold. Therefore, the only thing that needs to be computed to detect spoofing is the variance of the signal envelope. Many algorithms for calculating the variance for a set of samples with size n have a worst case running time of $O(n)$ [46]. As the computational complexity of comparing two values is given by $O(1)$; Thus, the proposed technique's computational complexity can be given by $O(n+1) = O(n)$. Table 6 presents a comparison of the proposed technique with those techniques in Table 4 that have a low computational complexity. We observe that the proposed technique clearly outperforms the existing light-weight techniques for spoofing detection.

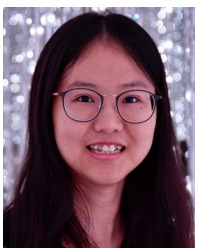
VII. CONCLUSION

This paper presented a light-weight technique for detecting GPS spoofing attacks. The proposed technique is based on an analytical model of the distribution of a signal's envelope. The variance of the received signal's envelope is shown to be significantly different for an attack and legitimate scenarios. Thus, the proposed technique uses a threshold for the variance of samples in a signal envelope. We also observed that the threshold for variance is sensitive to the distance of an attacker. Therefore, we presented a technique to dynamically select the threshold based on the dispersion value of the variance. Experiments on actual hardware show the effectiveness of the proposed technique. We observe that the proposed technique can detect GPS spoofing with probability of detection greater than 90%.

REFERENCES

[1] K. Borre and D. Akos, "A software-defined GPS and Galileo receiver: Single-frequency approach," in *Proc. 18th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2005, pp. 1632–1637.
[2] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.
[3] J. Bhatti and T. E. Humphreys, "Covert control of surface vessels via counterfeit civil GPS signals," *J. Inst. Navig.*, vol. 64, pp. 51–66, 2017.
[4] L. Huang and Q. Yang, "GPS spoofing: Low-cost GPS simulator," presented at DEFCON 23, 2015. [Online]. Available: https://infocondb.org/con/def-con/def-con-23/lowcost-gps-simulator-gps-spoofing-by-sdr
[5] T. Ebinuma, "Software-defined GPS signal simulator," [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[6] X. Jiang et al., "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.
[7] X. Wei and B. Sikdar, "Impact of GPS time spoofing attacks on cyber physical systems," in *Proc. IEEE Int. Conf. Ind. Technol.*, 2019, pp. 1155–1160.
[8] 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. Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.
[9] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. 16th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2003, pp. 1543–1552.
[10] O. Pozzobon, L. Canzian, M. Danieletto, and A. Dalla Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *Proc. IEEE 5th ESA Workshop Satell. Navigation Technol. Eur. Workshop GNSS Signals Signal Process.*, 2010, pp. 1–6.
[11] O. Pozzobon, "Keeping the spoofs out: Signal authentication services for future GNSS," *Inside GNSS*, vol. 6, no. 3, pp. 48–55, 2011.
[12] M. N. Aman, K. C. Chua, and B. Sikdar, "Physically secure mutual authentication for IoT," in *Proc. IEEE Conf. Dependable Secure Comput.*, 2017, pp. 310–317.
[13] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 469–475, Feb. 2019.
[14] J. M. Anderson et al., "Chips-message robust authentication (Chimera) for GPS civilian signals," in *Proc. 30th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2017, pp. 2388–2416.
[15] L. Heng, D. Chou, and G. X. Gao, "Cooperative GPS signal authentication from unreliable peers," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2014, pp. 2801–2809.
[16] 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 Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2013.
[17] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, J. Inst. Navigation*, vol. 59, no. 3, pp. 177–193, 2012.
[18] S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "GPS spoofing detection and mitigation in PMUs using distributed multiple directional antennas," in *Proc. IEEE Int. Conf. Commun.*, 2019, pp. 1–7.
[19] C. H. Kang, S. Y. Kim, and C. G. Park, "Adaptive complex-EKF-based DOA estimation for GPS spoofing detection," *IET Signal Process.*, vol. 12, no. 2, pp. 174–181, 2017.
[20] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2014, pp. 2233–2242.
[21] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigation*2012, pp. 3007–3016.
[22] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proc. Int. Tech. Meeting Inst. Navigation*, 2009, pp. 124–130.
[23] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *Proc. IEEE Int. Conf. Localization GNSS*, 2015, pp. 1–6.
[24] Y. Bardout, "Authentication of GNSS position: An assessment of spoofing detection methods," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2011, pp. 436–446.
[25] N. A. White, P. S. Maybeck, and S. L. DeVilbiss, "Detection of interference/jamming and spoofing in a DGPS-aided inertial system," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 34, no. 4, pp. 1208–1217, Oct. 1998.
[26] W. Wang, N. Li, R. Wu, and P. Closas, "Detection of induced GNSS spoofing using S-curve-bias," *Sensors*, vol. 19, no. 4, 2019, Art. no. 922.
[27] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation: J. Inst. Navigation*, vol. 59, no. 4, pp. 281–290, 2012.
[28] P. Vahid, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N0 estimates," in *Proc. 25th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2012, pp. 2878–2884.
[29] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2011, pp. 1888–1896.
[30] E. Schmidt, N. Gatsis, and D. Akopian, "A GPS spoofing detection and classification correlator-based technique using the LASSO," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 6, pp. 4224–4237, Dec. 2020.
[31] B. Xu, Q. Jia, and L.-T. Hsu, "Vector tracking loop-based GNSS NLOS detection and correction: Algorithm design and performance analysis," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 7, pp. 4604–4619, Jul. 2020.
[32] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigation*2011, pp. 2646–2656.
[33] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019.
[34] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.
[35] M. N. Aman and B. Sikdar, "Distinguishing between channel errors and collisions in IEEE 802.11," in *Proc. 46th Annu. Conf. Inf. Sci. Syst.*, 2012, pp. 1–6.
[36] R. G. Gallager, *Principles of Digital Communication*, 1st ed. New York, NY, USA: Cambridge Univ. Press, 2008.
[37] M. N. Aman, W. K. Chan, and B. Sikdar, "Collision detection in IEEE 802.11 networks by error vector magnitude analysis," in *Proc. IEEE Glob. Commun. Conf.*, 2012, pp. 5218–5223.
[38] J. Stewart, *Calculus: Concepts and Contexts*. Belmont, CA, USA: Cengage Learning, 2009.
[39] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *Proc. IEEE 16th Annu. Consum. Commun. Netw. Conf.*, 2019, pp. 1–6.
[40] T. Y. Mina, S. Bhamidipati, and G. X. Gao, "GPS spoofing detection for the power grid network using a multireceiver hierarchical framework architecture," *Navigation J. Inst. Navigation*, vol. 66, no. 4, pp. 857–875, 2019.
[41] E. Shafiee, M. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *J. Navig*, vol. 71, no. 1, pp. 169–188, 2018.
[42] M. T. Arafin, D. Anand, and G. Qu, "A low-cost gps spoofing detector design for Internet of Things (IoT) applications," in *Proc. Great Lakes Symp.*, 2017, pp. 161–166.
[43] M. Sabouri, S. Siamak, M. Dehghani, M. Mohammadi, and M. H. Asemani, "Intelligent GPS spoofing attack detection in power grids," in *Proc. IEEE 11th Smart Grid Conf.*, 2020, pp. 1–6.
[44] J. Xie and A. S. Meliopoulos, "Sensitive detection of GPS spoofing attack in phasor measurement units via quasi-dynamic state estimation," *Computer*, vol. 53, no. 5, pp. 63–72, May 2020.
[45] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2016, pp. 391–395.
[46] C. Chen, "Welford algorithm for updating variance," May 9, 2023. [Online]. Available: https://changyaochen.github.io/welford/



XIAO WEI received the B.Eng. degree in network engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2013, and the M.Sc. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2016, where she is currently working toward the Ph.D. degree. Her research interests include GPS spoofing, radio-frequency cyber attacks, and cyber physical systems.

MUHAMMAD NAVEED AMAN (Senior Member, IEEE) received the B.Sc. degree in computer systems engineering from KPK UET, Peshawar, Pakistan, the M.Sc. degree in computer engineering from the Center for Advanced Studies in Engineering, Islamabad, Pakistan, the M.Engg. degree in industrial and management engineering and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2006, 2008, and 2012, respectively. He is currently an Assistant Professor with the University of Nebraska-Lincoln, Lincoln, Nebraska. His research interests include IoT and network security, hardware systems security and privacy, wireless and mobile networks, and stochastic modelling.

BIPLAB SIKDAR (Senior Member, IEEE) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the Faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include wireless network, security for IoT, and cyber physical systems.