GPS Signal Authentication From Cooperative Peers

Liang Heng, *Member, IEEE*, Daniel B. Work, *Member, IEEE*, and Grace Xingxin Gao, *Member, IEEE*

***Abstract*—Secure reliable position information is indispensable for many transportation systems and services, such as traffic monitoring, fleet management, electronic toll collection, route guidance, vehicle telematics, and emergency response. Unfortunately, civil Global Positioning System (GPS) signals are vulnerable to spoofing attacks. This paper introduces a signal authentication architecture based on a network of cooperative GPS receivers. A receiver in the network correlates its received military P(Y) signal with those received by other receivers (hereinafter referred to as cross-check receivers) to detect spoofing attacks. This paper describes three candidate structures to implement this architecture and evaluates spoofing detection performance through theoretical analyses and field experiments. We show that the spoofing detection performance improves exponentially with increasing number of cross-check receivers. Even if the cross-check receivers are low cost, unreliable, and in challenging environment, cooperative authentication can match, if not outperform, a single high-quality reliable reference receiver in terms of spoofing detection performance.**

***Index Terms*—Authentication, cooperative, global navigation satellite systems, Global Positioning System (GPS), reliability, security, spoofing detection.**

I. Introduction

LOCATION awareness is crucial to many transportation systems and services, including traffic monitoring, fleet management, electronic toll collection, route guidance, vehicle telematics, and emergency response [1]–[3]. The Global Positioning System (GPS) technology has been transforming the transportation landscape by allowing agencies to effectively monitor and manage transportation assets. In the area of road traffic monitoring, GPS data have significantly improved our ability to monitor traffic conditions in real time [4], [5]. Unlike dedicated traffic monitoring sensors installed in the pavement or along the roadside, GPS data can be collected very cheaply from personal navigation devices, GPS-equipped smartphones, and from fleet vehicle monitoring systems. This has also introduced a new market based on buying large volumes of GPS data, processing it into useful traffic information, and, finally, selling the processed information for display on online maps or in navigation applications [6]. In addition to traffic monitoring, toll collection is also adopting GPS technology and benefits from GPS data. A notable example is the Toll Collect Project, which has operated in Germany since 2005 [7], [8]. Using GPS to identify when a vehicle is on a tolled road, this system outperforms traditional toll gates in terms of wide-area coverage and flexible toll fee calculation [9].

Ever-growing adoption of GPS technology and dependence on GPS data call for techniques capable to authenticate GPS signals to provide secure reliable location information. Unfortunately, security was not an initial design consideration for civil use of GPS [10]. The power of GPS signals received on the Earth is as low as 10^{-16} W, even below the thermal noise floor [11]. The civil signals are unencrypted, with their structures explicitly described in publicly available documents [12]. As a result, civil GPS receivers are vulnerable to attacks such as jamming, meaconing, and spoofing [13]–[17].

Jamming is the intentional broadcast of a high-power interfering signal at the GPS frequency in order to deny GPS receivers within a certain area access to the GPS signals. Hence, jamming is disruptive but usually detected by the receiver whenever it stops tracking satellites.

Meaconing, as a kind of replay attack, is the recording and rebroadcast of GPS signals that overpower the authentic signals. A meaconing attack that replays the whole GPS spectrum can even fool a military receiver. However, an inherent limitation of meaconing is that the position calculated by a compromised receiver is equal to the position of the attacker's antenna used to record the GPS signals. Hence, meaconing can expose the attacker's position, and manipulation of the position solution is subject to the physical maneuverability of the attacker's antenna.

Spoofing is a much more sophisticated and dangerous attack than jamming or meaconing. A spoofer synthesizes and broadcasts counterfeit GPS signals in order to manipulate a target receiver's reported position or time, or both [13], [18]. In comparison with jamming and meaconing, spoofing poses a greater security risk because it is covert and it can manipulate a target receiver's output at the attacker's will. There has been an experiment showing that a spoofer can mislead a GPS-directed semiautonomous vehicle without trigging any alarms [19].

An even more troublesome scenario is self-spoofing. For example, a GPS data vendor may mix authentic GPS data with faked data and profit from selling such a kind of mixed data. A driver may spoof the GPS receiver in his vehicle's monitoring system in order to avoid paying a toll. In this paper, we aim at techniques that do not only protect receivers from being spoofed but also protect a third party from counterfeit GPS data.

Manuscript received April 22, 2014; revised September 6, 2014; accepted November 12, 2014. Date of publication December 18, 2014; date of current version July 31, 2015. The Associate Editor for this paper was J. V. Krogmeier.

L. Heng and G. X. Gao are with the Department of Aerospace Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA (e-mail: heng@illinois.edu; gracegao@illinois.edu).

D. B. Work is with the Department of Civil and Environmental Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA (e-mail: dbwork@illinois.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2014.2372000

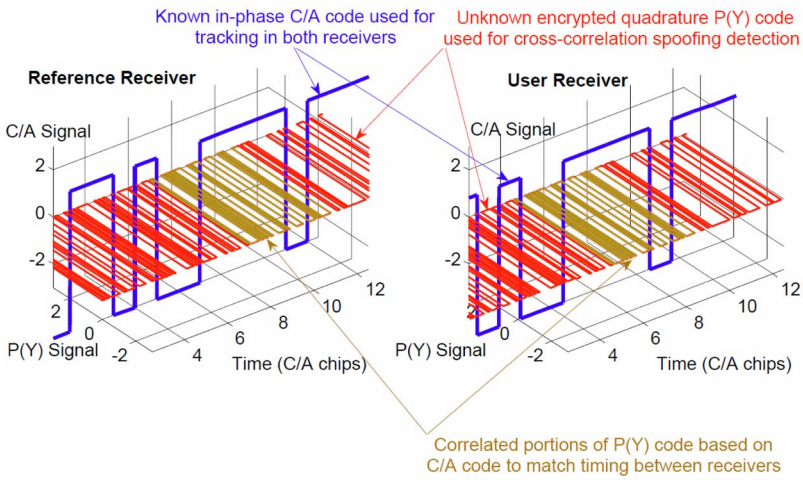


Fig. 1. Principle of cross-correlation spoofing detection (adapted from [29, Fig. 1]). The publicly known C/A signal and the encrypted P(Y) signal are modulated onto the GPS L1 carrier in-phase and quadrature, respectively [11]. Each receiver tracks the C/A code and uses its phase and timing relationships to the P(Y) code to take a snippet of the same part of the P(Y) code. A high correlation will appear if the two snippets contain the same P(Y) code.

A. GPS Spoofing Countermeasures

So far, a variety of methods have been proposed to harden civil GPS receivers against spoofing attacks. These methods can be generally categorized into three groups: external assistance, signal statistics, and cryptographic authentication. The first group performs consistency checks against metrics external to the GPS subsystem, such as the information from inertial sensors, odometers, cellular networks, and high-stability clocks [20], [21]. The second group performs statistical tests on features inherent in GPS signals, including angle of arrival [22], [23], signal quality [24], signal power [25], [26], and multipath [27]. The third group relies on unpredictable cryptographic information carried by GPS signals [10], [28]–[30]. Unlike the first group of methods, cryptographic methods do not require any additional hardware, which can be a hurdle to mass-market GPS applications that are sensitive to cost, weight, and/or size. In comparison with the second group, cryptographic methods enable a receiver to differentiate authentic signals from counterfeit signals with higher confidence and robustness, particularly when the receiver is moving so that the statistics of authentic signals can be highly unstable.

Three types of cryptographic spoofing countermeasures have been explored in recent literature. The first option, known as navigation message authentication (NMA), inserts public-key digital signature into the navigation message [28], [30]–[32]. Another strategy is to interleave spread spectrum security codes (SSSCs) with normal civil GPS spreading codes so that parts of spreading sequences are periodically unpredictable [28], [33]. Both NMA and SSSC require significant modifications to the legacy GPS signal structure. They are unlikely to be implemented in the coming decade due to the static nature of GPS interface specification (IS) and long deployment cycles. The third approach relies on codeless cross correlation of unpredictable encrypted military P(Y) code between two civil GPS receivers [10], [29], [34], [35]. Without any modification to the GPS IS, this approach is practical today. Furthermore, the cross-correlation method can easily enable a third party, such as a traffic data vendor or a Location Assurance Provider [36], to ensure that an asserted position is *bona fide*.

The cross-correlation spoofing detection method borrows the idea from the dual-frequency GPS codeless receiver, which correlates the L1 and L2 P(Y) codes in order to find the differential delay between the phases of two codes [37]. As shown in Fig. 1, this method correlates a snippet of L1 signal from the receivers to be authenticated (hereafter referred to as "user receivers") with a snippet from the reference receiver. Both snippets are known to contain the same part of the military P(Y) codes broadcast by a GPS satellite visible to both receivers. Although the P(Y) code is encrypted and thus unknown, and although its received versions are noisy and may be distorted by a narrowband radio-frequency front end [29], when conducting cross correlation, the P(Y) code components in the two snippets are sufficiently similar to create a high correlation peak if neither the user receiver nor the reference receiver is spoofed. However, if the reference receiver is also spoofed, particularly by the same spoofer to the user receiver, the authentication result will be incorrect.

Previous papers [10], [29] have analyzed the performance of the cross-correlation spoofing detection method using one reliable reference receiver. In addition, they proposed employing a few dedicated reference stations to provide GPS signal authentication service for a wide area. Despite the strong merits, such a client–server authentication service has some limitations. First and foremost, it requires considerable investment into the setup of reference stations, not to mention the maintenance cost. Second, since fixed reference stations can be located, they are vulnerable to organized targeted jamming and spoofing attacks, and loss of a majority of the reference stations may paralyze the authentication service.

B. Authentication From Multiple Cooperative Peers

In this paper, we extend the dual-receiver P(Y)-code correlation method to a network of receivers and present a GPS signal authentication architecture in an *ad hoc* cooperative manner. The fundamental difference from the client–server approach [10], [29] is that our architecture relies on multiple voluntary peers (hereinafter referred to as "ad hoc cross-check receivers"

or simply "cross-check receivers") as references. The cross-check receivers can be mobile, low quality, unreliable, and even spoofed. The authentication process consists of two steps: *pairwise check* and *decision aggregation*. In the pairwise check, the P(Y) signal received by a user receiver is correlated with that received by each cross-check receiver. Each such correlation provides a decision as to the authenticity of the signal received by the user receiver. In decision aggregation, the pairwise decisions are aggregated to determine if the user receiver is spoofed.

The cooperative manner is superior to the client–server manner in terms of cost, user capacity, and robustness, due to unlimited geographically dispersed low-cost ad hoc cross-check receivers. However, one should be aware that an ad hoc cross-check receiver is less reliable than a dedicated reference receiver. First, a mass-market GPS receiver, particularly one embedded in a smartphone, may not be as good as a dedicated geodetic-grade receiver in terms of the antenna and the signal conditioning circuit. Second, a cross-check receiver may intentionally be malicious so that it provides no or even negative contribution to the final authentication result. Third, a cross-check receiver can be also spoofed, and sometimes, a user receiver and a cross-check receiver may be spoofed by the same spoofer if they are not sufficiently far apart. We shall further show in this paper that our proposed architecture is actually robust against these potential issues because the spoofing detection performance improves exponentially with increasing number of cross-check receivers.

C. Organization of the Remainder of This Paper

Section II describes three candidate structures to implement our proposed cooperative authentication architecture and compares their advantages and disadvantages. Section III presents a probabilistic analysis of authentication performance under the assumption that cross-check receivers can be spoofed or malicious with certain probabilities. Section IV validates the theoretical conclusions through a few numerical examples. Section V shows field experiment results on pairwise check performance. Finally, Section VI concludes this paper.

II. Authentication System Structures

There are multiple approaches to implementing our proposed cooperative authentication system. These approaches differ from one another mainly in where correlations are computed. One approach is to distribute correlation computation to cross-check receivers. Another option is to compute all the correlations in a centralized way, either by the user receiver itself or by a third party, which wants to ensure the validity of the position and clock reported by the user receiver. Here, we present three candidate structures and qualitatively discuss their tradeoffs between authentication delay, cost, CPU time, and robustness.

This paper considers two purposes of GPS signal authentication: spoofing detection and position assertion verification. The first purpose is concerned with the scenario that a user receiver wants to check the authenticity of its received signals. Since a successful spoofing attack usually needs to synthesize the GPS signals of all the satellites in view [13], [18], checking the authenticity of the signal from one satellite suffices to detect a spoofing attack. To this end, the user receiver and all cross-check receivers only need to collect a snippet of quadrature-phase baseband signal for one GPS satellite visible to all of them. The second purpose is concerned with the scenario that a third party (e.g., a fleet manager) checks whether a position asserted by a user receiver is authentic or not. To enable position assertion verification, the user receiver must report a snippet that contains the complex baseband signal (both in-phase and quadrature). Then, the third party can track multiple satellites from the snippet and calculate the position solution, which ought to match the asserted position. In addition, the third party can extract the quadrature-phase baseband signal for a GPS satellite from the snippet and correlate it with the quadrature-phase baseband snippets from cross-check receivers. The correlation results are used to determine the authenticity of the user reported snippet. All the following three candidate structures will achieve the first purpose, whereas only the last one is designed to support the second purpose.

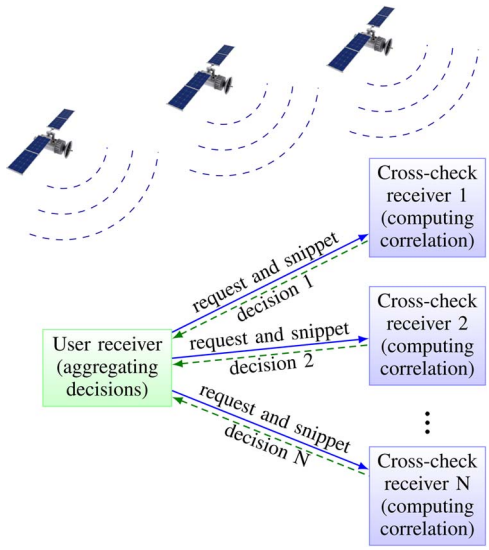


Fig. 2. First candidate structure of authentication system. Each cross-check receiver computes the correlation between its own snippet and the one from the user receiver and decides whether the signal received by the user receiver is authentic or not. The user receiver collects the decisions from all cross-check receivers and, finally, determines the authenticity of its received signal by an appropriate statistical measure.

A. Candidate Structure 1: Correlation Computed by Cross-Check Receivers

Fig. 2 illustrates the first candidate structure, in which correlation computation is distributed to cross-check receivers. The procedure is explained in detail in Table I. When a user receiver wants to know whether its received signal is authentic or not, it finds N peers as cross-check references. The user receiver and all cross-check receivers agree to collect a snippet of quadrature-phase baseband signal for one GPS satellite at a time in the immediate future. The user receiver sends its snippet to the reference receivers via secure channels. Then, each reference receiver correlates its own snippet with the one from the user receiver and decides if the signal received by the user receiver is authentic or not. Finally, the user receiver aggregates the decisions from the N reference receivers and determines the

TABLE I
PROCEDURE OF THE AUTHENTICATION SYSTEM ILLUSTRATED IN FIG. 2

Steps	Actions
1	User receiver sends out authentication requests with its rough location.
2	Available receivers within an appropriate area respond to requests.
3	User receiver chooses N cross-check receivers and a common-view GPS satellite. User receiver and cross-check receivers agree on a time t in the immediate future.
4	User receiver and cross-check receivers collect snippets of quadrature-phase baseband signal from the GPS satellite at the time t.
5	User receiver sends its snippet to the N cross-check receivers.
6	Each cross-check receiver correlates its snippet with user receiver's, and replies to the user receiver with a decision "authentic" or "spoofed."
7	User receiver determines the authenticity of its received signal by aggregating all these decisions.

authenticity of its received signal by an appropriate statistical measure. Since snippets of GPS signals have to be transported over a communication network, a security protocol, such as Transport Layer Security and Internet Protocol Security [38], should be used to avoid man-in-the-middle attacks.

The authentication process can be performed in near real time, and the time delay mainly depends on data collection, communication, and computation. According to Psiaki *et al.* [29], a snippet of approximately 1 s is generally needed for reliable spoofing detection. A narrow-band GPS front end usually has a bandwidth of 2.4 MHz, and 1-s 1-bit quadrature-phase samples yield 2.4 Mb of data. For current 3G/4G cellular networks, it typically takes 1 s or less to transfer one snippet. The time of computation depends, but a rule of thumb is that a receiver must have the capability of processing 1-s data within 1 s. Since the time for sending and responding requests and aggregating decisions is usually negligible, the authentication process can take as short as $2 + N$ seconds: 1 s for collecting snippets, N seconds for transferring the user receiver's snippet to N cross-check receivers, and 1 s for computing the correlations. It is worth nothing that our cooperative authentication does not require highly reliable spoofing detection for each cross-check receiver and thus allows a much shorter snippet to be collected. Therefore, a delay of $2 + N$ seconds is a conservative estimate. In addition, if the user receiver can upload its snippet to a cloud service for file sharing, from which the cross-check receivers can download the snippet simultaneously, then the authentication delay can be shortened to 4 s: 1 s for collecting snippets, 1 s for uploading, 1 s for downloading, and 1 s for computing the correlations.

An obvious advantage of this structure is no requirement of external support (assuming that a file-sharing cloud is not used). However, unlike the other three candidate structures to be described, this structure requires each cross-check receiver to compute a correlation using its own computation power. The CPU time consumption is generally acceptable because one cross-check receiver only computes one correlation (compared with the second structure where the user receiver needs to compute N correlations). In practice, the cross-check receivers with more spare CPU time will more likely respond to the authentication request.

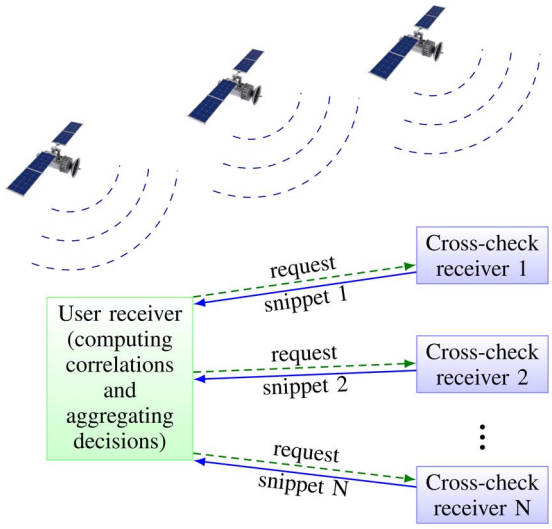


Fig. 3. Second candidate structure of authentication system. All cross-check receivers send their collected snippets to the user receiver. The user receiver computes correlations and determines the authenticity of its received signal.

As mentioned in Section I-B, an issue with cooperative authentication is that there may exist some spam receivers being deliberately malicious (or playfully mischievous). In this structure, a malicious cross-check receiver may reply to the user receiver with a random decision independent of the correlation or, even worse, a decision always opposite to the correct decision based on the correlation. In Section III, we shall show that the performance deterioration due to malicious cross-check receivers can be compensated by more cross-check receivers.

B. Candidate Structure 2: Correlation Computed by the User Receiver

Fig. 3 illustrates the second candidate structure, in which correlation computation is centralized to the user receiver. The major difference from the first candidate structure is that, after the user receiver and cross-check receivers collect snippets, the cross-check receivers send their snippets to the user receiver. The user receiver computes N correlations, based upon which it determines whether its received signal is authentic or not.

In this structure, the user receiver has to receive N snippets and then compute N correlations. If we still assume that it takes 1 s to transfer a snippet or to compute a correlation, the whole authentication process will take $1 + 2N$ seconds, a much longer delay in comparison with the first and second candidate structures.

The biggest advantage of this structure is that the user receiver can operate in a status close to radio silence because it does not send its snippet to any cross-check receiver or third party. Therefore, this structure is suitable for scenarios such as an on-duty drone authenticating its received GPS signals.

Another advantage with this structure is its better resistance to malicious cross-check receivers because the only way to disturb the authentication process is to send a random irrelevant snippet. In Section III, we shall show that such kind of

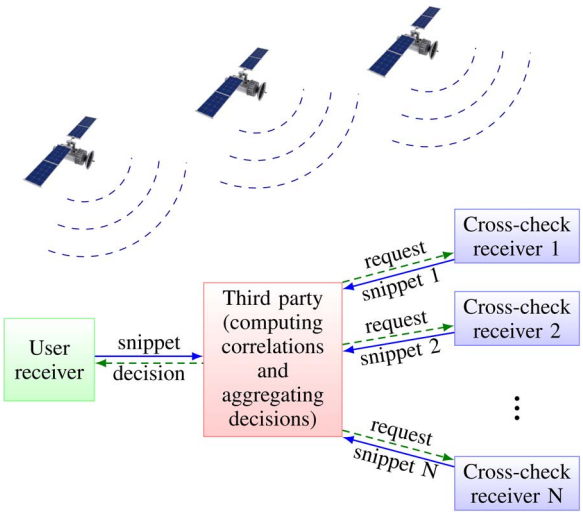


Fig. 4. Third candidate structure of authentication system. A trusted third party wants to ensure the correctness of the position and time reported by a user receiver. Then, the user receiver and cross-check receivers collect snippets and upload them to the third party, which computes the correlations and determines the authenticity of the position and time reported by the user receiver.

disturbance causes less performance deterioration than a cross-check receiver that always provides the incorrect decision.

For commercial applications, this structure saves the CPU time of cross-check receivers. Thus, more receivers are willing to respond to the authentication request.

C. Candidate Structure 3: Correlation Computed by a Third Party

Fig. 4 illustrates the third candidate structure, in which a trusted third party is in charge of collecting snippets, computing correlations, and aggregating decisions. Unlike the first and second structures, in addition to letting the user receiver know whether its received GPS signal is authentic or not, this structure enables a third party (which is usually an administrator or an overseer of a number of user receivers) to check whether a position (or time, or both) asserted by a user receiver is authentic or not.

This structure also allows for a much faster authentication process because all receivers can send snippets to the third party simultaneously. The third party has a much higher computing power than mobile devices so that the time for computing correlations is negligible. If we still assume that the snippet is 1-s long, the whole authentication process can take as little as 2 s: 1 s for collecting snippets and 1 s for transferring the snippets to the third party via 3G/4G cellular networks.

Similar to the second structure, this structure has a good resistance against malicious cross-check receivers.

D. Comparison of the Three Structures

Table II compares the advantages and disadvantages of the three candidate structures. It can be seen that an external support, such as a third party in charge of the whole authentication process or a cloud for computing correlations, can greatly reduce authentication delay and offload the intensive computations. In addition, an external support can help find cross-check receivers by maintaining a continuously updated database of available receivers. An external support can also help mitigate the negative effect due to malicious cross-check receivers by maintaining a database of historical performance of cross-check receivers. Therefore, for most commercial GPS authentication systems, the third structure should be used to exploit the benefit from an external support. Nevertheless, for scenarios where an external support is impossible or undesirable, the first and second structures still have their merits.

TABLE II
COMPARISON OF THE THREE CANDIDATE STRUCTURES

Candidate Structure	1	2	3
External support required	no	no	yes
Authentication delay (seconds)†	$2+N$‡	$1+2N$	2
User receiver CPU time	tiny	huge	no
Cross-check receiver CPU time	huge	no	no
User receiver sends snippet out	yes	no	yes
Cross-check receiver sends snippet out	no	yes	yes
Allow a third party to verify user receiver's assertion	no	no	yes

† Assume that it takes one second for a receiver to transfer a snippet or to compute a correlation, and it takes negligible time for a third party to compute a correlation.

‡ Four seconds if a file-sharing service is used for cross-check receivers to download a snippet simultaneously.

III. Analysis of Authentication Performance

Authentication is essentially a statistical hypothesis test; thus, it has a probability of making two types of errors: false alarm and missed detection. This section is devoted to a rigorous analysis of the probability of the two types of errors in cooperative authentication.

A. Assumptions and Notations

In order to simplify the analysis, we assume that all ad hoc cross-check receivers have the same spoofing detection performance, namely, the same probability of false alarm and the same probability of missed detection. A cross-check receiver can be malicious with a certain probability. Additionally, a cross-check receiver can be spoofed with a certain probability, and the spoofer can be the same as or different from the spoofer, which is attacking the user receiver. The list below summarizes the notations used throughout this paper.

- A — Final authentication result from aggregating all A_i, $i=1,\ldots,N$.
- A_i — Pairwise check decision using the ith cross-check receiver, $i=1,\ldots,N$: $A_i=0$ "authentic," and $A_i=1$ "spoofed."
- α — Equal to $\text{Prob}(A_i=1|S=0)$, for all $i=1,\ldots,N$, probability of false alarm using an unspoofed nonmalicious cross-check receiver.
- β — Equal to $\text{Prob}(A_i=0|S=1)$, for all $i=1,\ldots,N$, probability of missed detection using an unspoofed nonmalicious cross-check receiver.
- C — Pairwise check test statistic.

$F(x;n,p)$	Cumulative distribution function (CDF) of a binomial random variable X with parameters n and p.
H_0	Null hypothesis that a user receiver's snippet and a cross-check receiver's snippet contain the same P(Y) code.
H_1	Alternative hypothesis that a user receiver's snippet and a cross-check receiver's snippet contain different P(Y) codes.
N	Number of cross-check receivers.
$\mathcal{N}(\mu,\sigma^2)$	Normal distribution with mean μ and variance σ^2.
P_{FA}	Equal to $\mathrm{Prob}(A=1\|S=0)$, probability of false alarm of the final authentication result.
P_{MD}	Equal to $\mathrm{Prob}(A=0\|S=1)$, probability of missed detection of the final authentication result.
P_D	Equal to $1-P_{\mathrm{MD}}$, probability of detection, also referred to as detection power.
P_{SS}	Probability of 1) a cross-check receiver being spoofed by the same spoofer that is attacking the user receiver and 2) a cross-check receiver being malicious such that its pairwise check decision is always opposite to the correct decision based on the correlation.
P_{SD}	Probability of 1) a cross-check receiver being spoofed by a different spoofer from the spoofer that is attacking the user receiver and 2) a cross-check receiver being malicious such that its pairwise check decision is based on the correlation involving a random irrelevant snippet.
S	True status of user receiver: $S=0$ "authentic," and $S=1$ "spoofed."
X	Decision aggregation test statistic, equal to $\sum_{i=1}^{N} A_i$, number of "spoofed" decisions.
ξ	Decision aggregation spoofing detection threshold. The user receiver is determined to be "authentic" if $X<\xi$ and to be "spoofed" if $X\geq\xi$.
ζ	Pairwise check decision threshold. If $C\geq\zeta$, then H_0 will be accepted; otherwise, H_1 will be accepted.

B. Signal Model and Performance of Pairwise Check

Here, let Receiver 1 be a user receiver and Receiver 2 be an ad hoc cross-check receiver. Suppose that both receivers track the GPS L1 signal with perfect carrier and symbol timing recovery. The quadrature-phase baseband signals that contain the L1 P(Y) code are given by

$$s_1[t]=\Lambda_1 p_1[t]+n_1[t] \quad (1)$$
$$s_2[t]=\Lambda_2 p_2[t]+n_2[t] \quad (2)$$

where $t\in\{1,2,\ldots,T\}$ is the index of a total of T samples, Λ_1 and Λ_2 are the received P(Y) code amplitudes (after distortion and attenuation) for the two receivers, $p_1[t]$ and $p_2[t]=\pm1$ denote the unknown P(Y) code sequences, and $n_1[t]\sim\mathcal{N}(0,\sigma_1^2)$ and $n_2[t]\sim\mathcal{N}(0,\sigma_2^2)$ account for receiver noises and other irrelevant GPS signals. The spoofing detection is based on the test statistic

$$C=\frac{1}{T}\sum_{t=1}^{T}s_1[t]s_2[t]. \quad (3)$$

Define $c[t]=s_1[t]s_2[t]$ for all $t\in\{1,2,\ldots,T\}$. Under the hypothesis H_0 that both receivers receive the same P(Y) code, i.e., $p_1[t]=p_2[t]$ for all t, the expectation and variance of $c[t]$ are given by

$$\begin{aligned}E(c[t])&=E\left((\Lambda_1p_1[t]+n_1[t])(\Lambda_2p_2[t]+n_2[t])\right)\\&=\Lambda_1\Lambda_2 \quad (4)\\ \mathrm{Var}(c[t])&=E\left((\Lambda_1p_1[t]+n_1[t])^2(\Lambda_2p_2[t]+n_2[t])^2\right)\\&\quad-(E(c[t]))^2,\\&=\Lambda_1^2\sigma_2^2+\Lambda_2^2\sigma_1^2+\sigma_1^2\sigma_2^2. \quad (5)\end{aligned}$$

By the central limit theorem (CLT), for a very large T, we have

$$C_{H_0}\sim\mathcal{N}\left(\mu_{H_0},\sigma_{H_0}^2\right)=\mathcal{N}\left(\Lambda_1\Lambda_2,\frac{\Lambda_1^2\sigma_2^2+\Lambda_2^2\sigma_1^2+\sigma_1^2\sigma_2^2}{T}\right). \quad (6)$$

Under the hypothesis H_1 that the two receivers receive different P(Y) codes, let us assume that $p_1[t]$ is independent from $p_2[t]$ for all t. Then, the expectation and variance of $c[t]$ are given by

$$E(c[t])=E\left((\Lambda_1p_1[t]+n_1[t])(\Lambda_2p_2[t]+n_2[t])\right)=0 \quad (7)$$

$$\begin{aligned}\mathrm{Var}(c[t])&=E\left((\Lambda_1p_1[t]+n_1[t])^2(\Lambda_2p_2[t]+n_2[t])^2\right)\\&\quad-(E(c[t]))^2\\&=\left(\Lambda_1^2+\sigma_1^2\right)\left(\Lambda_2^2+\sigma_2^2\right). \quad (8)\end{aligned}$$

By CLT, for a very large T, we have

$$C_{H_1}\sim\mathcal{N}\left(\mu_{H_1},\sigma_{H_1}^2\right)=\mathcal{N}\left(0,\frac{\left(\Lambda_1^2+\sigma_1^2\right)\left(\Lambda_2^2+\sigma_2^2\right)}{T}\right). \quad (9)$$

The signal-to-noise ratio (SNR) for the received signals is given by $\gamma_1=\Lambda_1^2/\sigma_1^2$ and $\gamma_2=\Lambda_2^2/\sigma_2^2$. Normalizing (1) by σ_1 and (2) by σ_2 and considering the fact that $\gamma_1\ll1$ and $\gamma_2\ll1$, we can finally simplify (6) and (9) into

$$C_{H_0}\sim\mathcal{N}\left(\sqrt{\gamma_1\gamma_2},\frac{\gamma_1+\gamma_2+1}{T}\right)\approx\mathcal{N}\left(\sqrt{\gamma_1\gamma_2},1/T\right) \quad (10)$$

$$C_{H_1}\sim\mathcal{N}\left(0,\frac{(1+\gamma_1)(1+\gamma_2)}{T}\right)\approx\mathcal{N}\left(0,1/T\right). \quad (11)$$

Given a pairwise check decision threshold ζ, if $C\geq\zeta$, then the null hypothesis H_0 will be accepted; otherwise, the alternative hypothesis H_1 will be accepted. Thus, the probability of false alarm α and the probability of missed detection β are given by

$$\alpha=Q\left((\sqrt{\gamma_1\gamma_2}-\zeta)\sqrt{T}\right) \quad (12)$$

$$\beta=Q(\zeta\sqrt{T}) \quad (13)$$

where the Q-function $Q(x)=(2\pi)^{-1/2}\int_x^\infty\exp(-u^2/2)du$ is the tail probability of the standard normal distribution. Fig. 5 shows the receiver operating characteristic (ROC) curves [39] under the following settings:

- user receiver carrier-to-noise ratio (C/N_0): fixed to 38 dB;
- cross-check receiver C/N_0: varying from 36 to 41 dB;
- noise equivalent bandwidth: 2.4 MHz;
- number of samples in a snippet, i.e., T: 2.4×10^6.

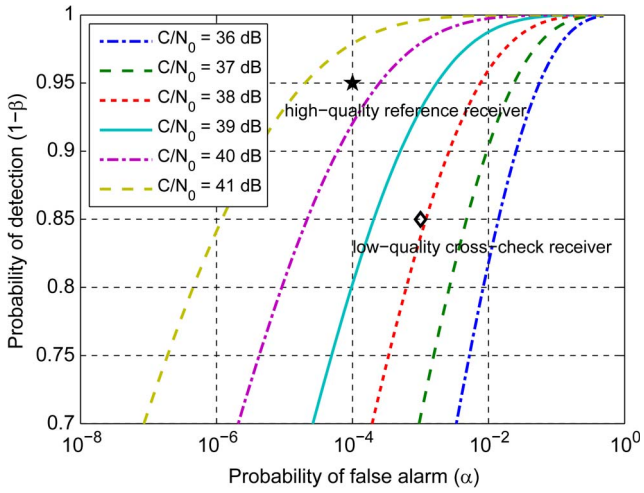


Fig. 5. ROC curve of pairwise check. The user receiver is assumed to have a carrier-to-noise ratio (C/N_0) of 38 dB, whereas the C/N_0 of the cross-check receiver varies from 36 to 41 dB. In the numerical examples (see Section IV), we select $\alpha = 0.001$ and $\beta = 0.15$ (corresponding to $C/N_0 \approx 38.1$ dB) as the typical performance of a low-quality cross-check receiver and $\alpha = 0.0001$ and $\beta = 0.05$ (corresponding to $C/N_0 \approx 40.4$ dB) as the typical performance of a high-quality reference receiver.

An ROC curve connects $(\alpha, 1-\beta)$ pairs for different thresholds ζ. In general, the closer a ROC curve is to the top left corner (which represents an ideal spoofing detector that detects all spoofing attacks without issuing any false alarms), the better the pairwise check performance is.

The Chernoff bound of Q-function is $Q(x) \leq (1/2)\exp(-x^2/2)$ for all $x > 0$. When the threshold ζ is chosen properly, i.e., $0 < \zeta < \sqrt{\gamma_1\gamma_2}$, increasing T decreases both α and β exponentially, as shown by

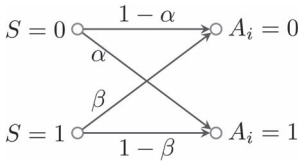
$$\alpha \leq \frac{1}{2}\exp\left(-(\sqrt{\gamma_1\gamma_2} - \zeta)^2 T\right) \tag{14}$$

$$\beta \leq \frac{1}{2}\exp(-\zeta^2 T). \tag{15}$$

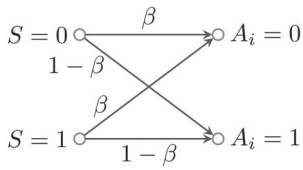
The preceding upper bounds on spoofing detection errors are based on a single pairwise check. For N cross-check receivers, the total number of samples increases to NT. Therefore, we can conjecture that the probabilities of false alarm and missed detection will both decrease exponentially with the increase in N. In the following two subsections, we show that this conjecture is true, although the cross-check receivers can be spoofed or malicious.

C. Channel Models

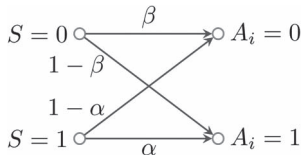
Since both S and A_i are binary, spoofing detection can be considered as an asymmetric communication channel. When the ith cross-check receiver is not spoofed or malicious, the channel model is simply given by



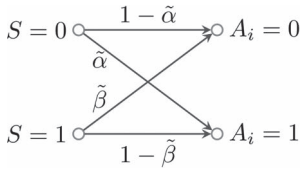
When the ith cross-check receiver is spoofed by a different spoofer to the user receiver or the cross-check receiver behaves in a malicious manner such that its authentication decision is based on the correlation involving a random irrelevant snippet, the snippets from two receivers do not match whether the user receiver is spoofed or not. Therefore, the channel model is given by



When the ith cross-check receiver is spoofed by the same spoofer to the user receiver or the cross-check receiver purposely responds with an authentication decision always opposite to the correct decision based on the correlation, the channel becomes



Among the preceding three channel models, the first occurs with a probability $1 - P_{\rm SD} - P_{\rm SS}$, the second occurs with a probability $P_{\rm SD}$, and the third occurs with a probability $P_{\rm SS}$. Therefore, the aggregated channel is given by



where

$$\tilde{\alpha} = (1 - P_{\rm SS} - P_{\rm SD})\alpha + (P_{\rm SS} + P_{\rm SD})(1 - \beta) \tag{16}$$

$$\tilde{\beta} = (1 - P_{\rm SS})\beta + (P_{\rm SS})(1 - \alpha). \tag{17}$$

D. Final Authentication Performance After Aggregating Decisions

Let $X = \sum_{i=1}^{N} A_i$ and ξ be a preset threshold, where ξ is an integer such that $0 \leq \xi \leq N$. The user receiver is determined to be authentic if $X < \xi$ and to be spoofed if $X \geq \xi$. Thus, we have

$$\begin{aligned} P_{\rm FA} &= {\rm Prob}(A = 1 | S = 0) = {\rm Prob}(X \geq \xi | S = 0) \\ &= \sum_{m=\xi}^{N} \binom{N}{m} \tilde{\alpha}^m (1 - \tilde{\alpha})^{N-m} \end{aligned} \tag{18}$$

$$\begin{aligned} P_D &= {\rm Prob}(A = 1 | S = 1) = {\rm Prob}(X \geq \xi | S = 1) \\ &= \sum_{m=\xi}^{N} \binom{N}{m} (1 - \tilde{\beta})^m \tilde{\beta}^{N-m}. \end{aligned} \tag{19}$$

Clearly, a greater ξ leads to lower $P_{\rm FA}$ but higher $P_{\rm MD}$, whereas a less ξ leads to lower $P_{\rm MD}$ but higher $P_{\rm FA}$. In practice, ξ should be properly chosen to balance $P_{\rm FA}$ and $P_{\rm MD}$.

Equations (16)–(19) show that P_{SD} only affects P_{FA}, whereas P_{SS} affects both P_{FA} and P_D. Therefore, we can expect that P_{SS} deteriorates performance more significantly than P_{SD} does.

The CDF of a binomial random variable Y with parameters n and p can be expressed as

$$F(y;n,p)=\sum_{m=0}^{\lfloor y\rfloor}\binom{n}{m}p^m(1-p)^{n-m} \tag{20}$$

where $\lfloor y\rfloor$ is the greatest integer less than or equal to y. When $y\le np$, by Hoeffding's inequality [40], an upper bound is given by

$$F(y;n,p)\le \exp\left(-2\frac{(np-y)^2}{n}\right). \tag{21}$$

Rewrite (18) and (19) as $P_{\mathrm{FA}}=F(N-\xi;N,1-\tilde{\alpha})$ and $P_{\mathrm{MD}}=1-P_D=F(\xi-1;N,1-\tilde{\beta})$. Considering a threshold selection strategy $\xi=\kappa N$ such that

$$N\tilde{\alpha}\le\xi=\kappa N\le N(1-\tilde{\beta}) \tag{22}$$

we have

$$\begin{aligned}P_{\mathrm{FA}}&\le \exp\left(-2\frac{(\xi-\tilde{\alpha}N)^2}{N}\right)\\&=\exp\left(-2N(\kappa-\tilde{\alpha})^2\right)\end{aligned} \tag{23}$$

$$\begin{aligned}P_{\mathrm{MD}}&\le F(\xi;N,1-\tilde{\beta})\le \exp\left(-2\frac{\left(N(1-\tilde{\beta})-\xi\right)^2}{N}\right)\\&=\exp\left(-2N(1-\tilde{\beta}-\kappa)^2\right).\end{aligned} \tag{24}$$

It can be seen that both P_{FA} and P_{MD} decrease exponentially with the increase in N. The parameter κ determines how fast P_{FA} and P_{MD} shrink. A larger κ hastens exponential decay of P_{FA}, whereas a smaller κ hastens exponential decay of P_{MD}.

In addition, (22) implies a fundamental requirement, i.e.,

$$\tilde{\alpha}+\tilde{\beta}<1 \tag{25}$$

unless the requirement was met, increasing N would not improve authentication performance.

E. Impact of Spoofed or Malicious Cross-Check Receivers

In (23) and (24), if we choose $\kappa=(1/2)(1+\tilde{\alpha}-\tilde{\beta})$, both P_{FA} and P_{MD} decrease at the same rate, on the order of $\exp(-N(1-\tilde{\alpha}-\tilde{\beta})^2)$. Therefore, the parameter $\lambda=1-\tilde{\alpha}-\tilde{\beta}$ is a *figure of merit* characterizing how fast the final authentication performance improves with an increasing N. By (16) and (17), we have

$$\begin{aligned}\lambda&=1-\tilde{\alpha}-\tilde{\beta}\\&=(1-\alpha-\beta)(1-2P_{\mathrm{SS}}-P_{\mathrm{SD}})\end{aligned} \tag{26}$$

which indicates that the factor $1-2P_{\mathrm{SS}}-P_{\mathrm{SD}}$ is the penalty for the unreliability of ad hoc cross-check receivers.

Equation (26) shows that P_{SS} causes twice as great performance deterioration as P_{SD} does. P_{SS} is the probability of two events: 1) a cross-check receiver being spoofed by the same spoofer that is attacking the user receiver and 2) a cross-check receiver being malicious such that its authentication decision is always opposite to the correct decision based on the correlation. In practice, it is recommended to choose a cross-check receiver at least hundreds of meters away from the user receiver in order to reduce the probability of Event 1. Event 2 can only happen in Candidate Structure 1; thus, P_{SS} can be assumed to be zero for Candidate Structure 2 to Candidate Structure 4. Furthermore, if information about the historical performance of cross-check receivers is available, some iterative learning algorithms [41] can be used to identify malicious cross-check receivers and preclude their negative impacts.

IV. Numerical Examples

The previous section has shown an exponential decay of P_{FA} and P_{MD} with increasing number of cross-check receivers. Furthermore, (26) shows that the performance deterioration due to P_{SS} is twice as great as that due to P_{SD}. These theoretical conclusions are based on the upper bounds given by (23) and (24). This section presents several numerical results computed using (18) and (19) for the purpose of validating the theoretical conclusions.

According to Fig. 5, we assume the following performance of the pairwise check throughout this section:

- $\alpha=0.001$ and $\beta=0.15$ (corresponding to $C/N_0\approx$ 38.1 dB) for a reliable low-quality cross-check receiver;
- $\alpha=0.0001$ and $\beta=0.05$ (corresponding to $C/N_0\approx$ 40.4 dB) for a reliable high-quality reference receiver.

A. ROC Curves

By (18) and (19), for fixed $\tilde{\alpha}$, $\tilde{\beta}$, and N, the final authentication performance varies at various threshold settings of ξ. Since $X=\sum_{i=1}^{N}A_i$ is always an integer between 0 and N, varying ξ results in $N+1$ discrete pairs of P_{FA} and P_D. Therefore, an ROC curve is a piecewise linear curve connecting the $N+1$ points.

Fig. 6 shows the ROC curves for two cases: all cross-check receivers are reliable ($P_{\mathrm{SS}}=P_{\mathrm{SD}}=0$) and cross-check receivers can be spoofed or malicious with probabilities $P_{\mathrm{SS}}=0.1$ and $P_{\mathrm{SD}}=0.1$. It can be seen that increasing number of cross-check receivers always improves performance. When cross-check receivers are unreliable with such a large probability, four unreliable cross-check receivers are sufficient to match the performance of a single reliable low-quality cross-check receiver ($P_{\mathrm{FA}}=0.001$ and $P_{\mathrm{MD}}=0.15$), and seven can match a single reliable high-quality reference receiver ($P_{\mathrm{FA}}=0.0001$ and $P_{\mathrm{MD}}=0.05$).

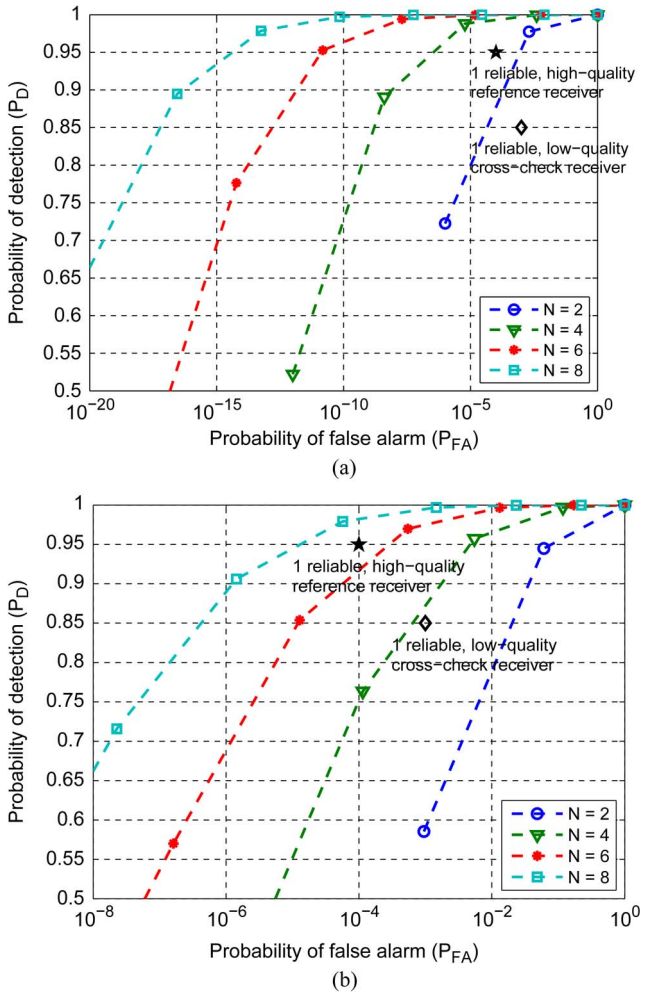


Fig. 6. ROC curves for reliable and unreliable cross-check receivers ($\alpha = 0.001$ and $\beta = 0.15$). (a) Cross-check receivers are all reliable ($P_{\rm SS} = P_{\rm SD} = 0$). Multiple cross-check receivers always outperform a single low-quality one. Three unreliable low-quality cross-check receivers are at par with a single reliable high-quality reference receiver. (b) Cross-check receivers are unreliable ($P_{\rm SS} = P_{\rm SD} = 0.1$, very conservative assumption). Four unreliable low-quality cross-check receivers match a single reliable low-quality cross-check receiver, and seven match a single reliable high-quality reference receiver.

B. Exponential Decay of $P_{\rm FA}$ and $P_{\rm MD}$ With Increasing N

Figs. 7 and 8 show probability of missed detection and probability of false alarm, both as functions of number of cross-check receivers, respectively. Four cases are considered in the figures: $P_{\rm SS} = P_{\rm SD} = 0$; $P_{\rm SS} = 0.05$ and $P_{\rm SD} = 0.1$; $P_{\rm SS} = P_{\rm SD} = 0.1$; and $P_{\rm SS} = 0.15$ and $P_{\rm SD} = 0$. Please note that the latter three cases satisfy $2P_{\rm SS} + P_{\rm SD} = 0.3$. By (26), it is expected that they will lead to very similar performance.

In Fig. 7, for a given N, we adjust ξ to achieve $P_{\rm FA} = 0.001$ and plot the corresponding $P_{\rm MD}$. As previously discussed, varying ξ can only give $N + 1$ discrete pairs of $P_{\rm FA}$ and P_D. Therefore, we obtain $P_{\rm MD}$ at $P_{\rm FA} = 0.001$ by a piecewise liner interpolation of these pairs. In Fig. 8, we obtain $P_{\rm FA}$ at $P_{\rm MD} = 0.15$ for various N in the same manner.

It is shown in Fig. 7 that, for a constant $P_{\rm FA}$, $P_{\rm MD}$ decreases exponentially with increasing number of cross-check receivers. A similar behavior of $P_{\rm FA}$ for a constant $P_{\rm MD}$ is also shown in Fig. 8. In addition, both figures clearly demonstrate that

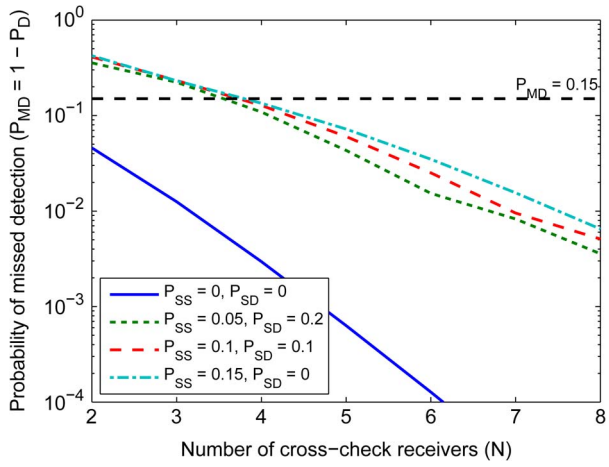


Fig. 7. Probability of missed detection ($P_{\rm MD}$) as a function of number of cross-check receivers (N) for a fixed $P_{\rm FA} = 0.001$ under four reliability assumptions. $P_{\rm MD}$ decreases exponentially with increasing N. The three cases $P_{\rm SS} = 0.05$ and $P_{\rm SD} = 0.1$, $P_{\rm SS} = P_{\rm SD} = 0.1$, and $P_{\rm SS} = 0.15$ and $P_{\rm SD} = 0$ lead to similar performance because they all satisfy $2P_{\rm SS} + P_{\rm SD} = 0.3$.

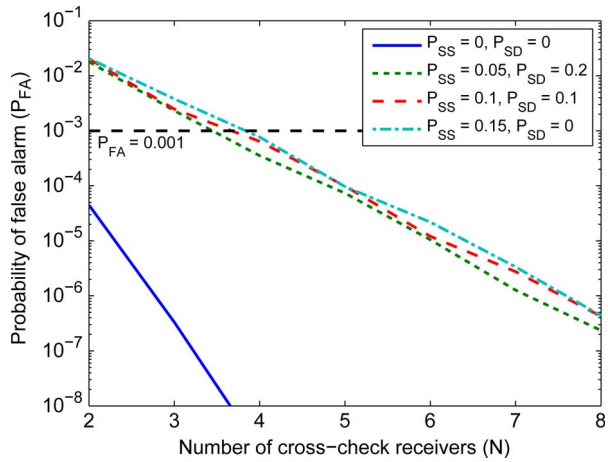


Fig. 8. Probability of false alarm ($P_{\rm FA}$) as a function of number of cross-check receivers (N) for a fixed $P_{\rm MD} = 0.15$ under four reliability assumptions. $P_{\rm FA}$ decreases exponentially with increasing N. The three cases $P_{\rm SS} = 0.05$ and $P_{\rm SD} = 0.1$, $P_{\rm SS} = P_{\rm SD} = 0.1$, and $P_{\rm SS} = 0.15$ and $P_{\rm SD} = 0$ lead to similar performance because they all satisfy $2P_{\rm SS} + P_{\rm SD} = 0.3$.

$P_{\rm SS}$ deteriorates performance twice as significantly as $P_{\rm SD}$ does. This confirms our theoretical conclusions in the previous section. Additionally, the figures show that, even if 15%–25% of the cross-check receivers are unreliable (a very conservative assumption, with different combinations of $P_{\rm SS}$ and $P_{\rm SD}$), four cross-check receivers suffice to provide as low $P_{\rm FA}$ and $P_{\rm MD}$ as a single reliable cross-check receiver.

V. Experiments

Here, we conduct field experiments to evaluate authentication performance in real environments. Since Sections III and IV have analyzed and demonstrated the performance of decision aggregation, this section focuses on pairwise check.

In the experiments, we employ multiple SiGe GN3S samplers and portable antennas to collect raw intermediate frequency samples of GPS signals. The SiGe front end is a thumb-sized USB device designed for low-cost software-defined GPS and

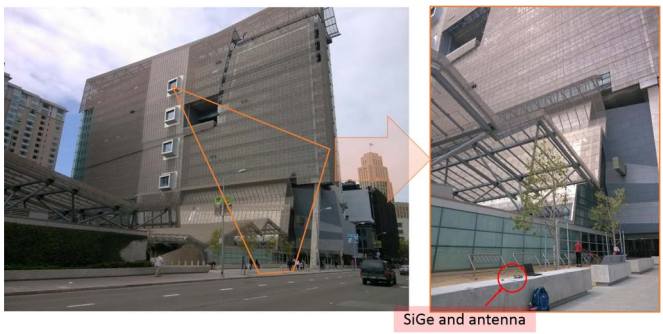


Fig. 9. Experiment 1: a SiGe receiver was in an urban canyon in San Francisco, CA. The receiver was able to acquire only three satellites. Fortunately, the three satellites were visible to the other SiGe receiver in Urbana, IL.

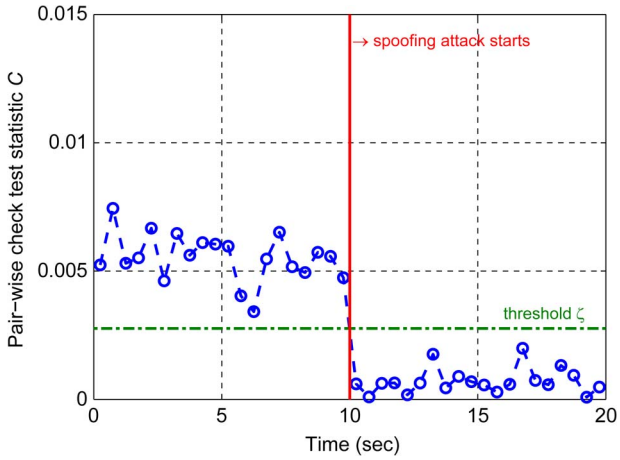


Fig. 10. Experiment 1 (3000 km apart, one receiver in urban canyon): pairwise check test statistic over time. Each snippet is 0.5-s long ($T = 2.046 \times 10^6$). Spoofing signal is injected from 10 s, with the counterfeit C/A code phase moving away from the authentic C/A code phase at a rate of 0.5 chips per second.

Galileo receivers. It has a sampling frequency from 4 to 16 MHz and a quantization resolution of 2 bits (four levels). The data are postprocessed using our developed software receiver, which is modified from [42]. Snippets of P(Y) codes are extracted from the tracking loops and then used to compute correlations.

The experiments are conducted in different spatial conditions (urban canyon and open space) and different transport modes (static and moving) with different distances between receivers. In comparison with the experiments in [29], which used static high-quality front ends and antennas, our experiments can better evaluate the authentication performance for real applications, particularly the GPS receivers in mobile devices and on vehicles.

A. Experiment 1: 3000 km Apart, One Receiver in Urban Canyon

The first data set was collected on March 27, 2014. As shown in Fig. 9, one SiGe receiver was in an urban canyon in San Francisco, CA, with open sky to the south east. The other receiver was in Urbana, IL, with a clear view of the sky. Two receivers were approximately 3000 km apart. Both receivers were static. The San Francisco receiver experienced severe signal blockage and multipath and was able to track only three satellites with a low SNR. Fortunately, the Urbana receiver was able to track the three satellites; thus, the pairwise check was possible.

We performed cross correlation of the P(Y) snippets generated from the data set. Each snippet is 0.5-s long. At a sampling frequency of 4.092 MHz, a snippet contains $T = 2.046 \times 10^6$ samples. The snippets are normalized, i.e., the snippets have a zero mean and are scaled such that $\sigma_1^2 = \sigma_2^2 = 1$. The correlation shows that $\Lambda_1\Lambda_2 \approx 0.00553$. According to (12) and (13), we chose the threshold $\zeta = 0.00553/2 \approx 0.00276$ so that we have the same probabilities of false alarm and missed detection, i.e., $\alpha = \beta$.

We injected spoof signal into the raw data from the San Francisco receiver starting from 10 s. The spoofing signal was initially synchronized to the authentic signal so that the receiver could lock on to both authentic and counterfeit C/A codes. Then, the counterfeit C/A code phase moved away from the authentic C/A code phase at a rate of 0.5 chips per second. The receiver tracking loop was dragged by the spoofing signal because the spoofing signal was slightly stronger than the authentic signal.

Fig. 10 shows the pairwise check test statistic C, as defined in (3), before and under the spoofing attack. The test statistic C is above the threshold ζ until the attack starts. As soon as the attack starts, C quickly drops below ζ. Due to the relatively low SNR, at some epochs, C is very close to the threshold, with the potential to cause false alarms or missed detection if the threshold was not properly chosen.

This experiment shows that it is possible to use a receiver in urban canyon environments for cooperative authentication, as long as the receivers are able to track at least one satellite. However, the performance deterioration due to a low SNR should be compensated by using more cross-check receivers, as discussed in Sections III and IV.

B. Experiment 2: 22 km Apart, One Moving Receiver

The second data set was collected on April 3, 2014. One SiGe receiver was on a car moving at roughly 45 mi/h in Rantoul, IL. The other receiver was in Urbana, IL. Two receivers were approximately 22 km apart. Both receivers had a clear view of the sky. Ten satellites were visible to each receivers, and eight of them were tracked by both receivers.

We performed similar cross correlation as done in Experiment 1. Because the data were collected at a different sampling frequency, i.e., 5.456 MHz, a 0.5-s snippet contains $T = 2.728 \times 10^6$ samples. The snippets are normalized. The correlation shows that the estimate of $\Lambda_1\Lambda_2 \approx 0.01295$, and we chose the threshold $\zeta = 0.01295/2 \approx 0.00648$.

We injected spoof signal into the raw data from the Rantoul receiver in the same way as Experiment 1. The only difference is that the counterfeit C/A code phase moved away from the authentic C/A code phase at a lower rate, i.e., 0.375 chips per second.

Fig. 11 shows the pairwise check test statistic C before and under the spoofing attack. In comparison with Experiment 1, C drops slower when the attack starts. This is because the counterfeit C/A code phase moved away from the authentic

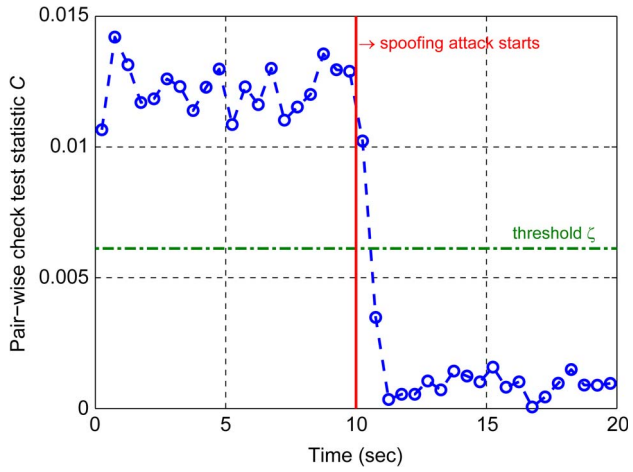


Fig. 11. Experiment 2 (22 km apart, one moving receiver): pairwise check test statistic over time. Each snippet is 0.5-s long ($T = 2.728 \times 10^6$). Spoofing signal is injected from 10 s, with the counterfeit C/A code phase moving away from the authentic C/A code phase at a rate of 0.375 chips per second.

C/A code phase at a lower rate in this experiment. Due to the relatively high SNR, apart from the transit period, C is distinctly above ζ before the attack and below ζ after the attack. In comparison with Experiment 1, this experiment shows that pairwise check performance is sensitive to spatial conditions (e.g., urban canyon or open space) and insensitive to transport modes (e.g., static or moving). This observation agrees with (12) and (13), which show that SNR significantly affects pairwise check performance.

VI. Conclusion

This paper has presented a GPS signal authentication architecture that relies on a network of cooperative low-cost receivers. In our architecture, the encrypted military GPS signals are sampled by a user receiver and several ad hoc cross-check receivers at the same time. The samples from the user receiver and each cross-check receiver are cross correlated in order to detect spoofing attacks. The spoofing detection results from all cross-check receivers are aggregated to reach the final decision of the authenticity of the signal received by the user receiver. This paper has described and compared three candidate structures to implement this concept.

Furthermore, this paper has validated the concept through a theoretical analysis and several numerical examples. We have assumed that the cross-check receivers can be spoofed or malicious with certain probabilities. The analysis and numerical examples have shown that the spoofing detection performance improves exponentially with increasing number of cross-check receivers. Additionally, we have conducted two field experiments to evaluate pairwise check performance in different spatial conditions (urban canyon and open space) and different transport modes (static and moving). The experiments shows that SNR is the major factor affecting pairwise check performance. A powerful aspect of these results is that, even if the cross-check receivers are low cost, unreliable, and in challenging environments, a modest number of such receivers will match, if not outperform, a single high-quality reliable reference receiver in terms of spoofing detection performance.

References

[1] C. R. Drane and C. Rizos, *Positioning Systems in Intelligent Transportation Systems*. Norwood, MA, USA: Artech House, 1998.
[2] G. Mintsis, S. Basbas, P. Papaioannou, C. Taxiltaris, and I. Tziavos, "Applications of GPS technology in the land transportation system," *Eur. J. Oper. Res.*, vol. 152, no. 2, pp. 399–409, Jan. 2004.
[3] S. T. S. Thong, C. T. Han, and T. A. Rahman, "Intelligent fleet management system with concurrent GPS & GSM real-time positioning technology," in *Proc. 7th Int. Conf. ITST*, Jun. 2007, pp. 1–6.
[4] B. Hoh *et al.*, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proc. 6th Int. Conf. MobiSys, Appl. Serv.*, 2008, pp. 15–28.
[5] J. C. Herrera *et al.*, "Evaluation of traffic data obtained via GPS-enabled mobile phones: The mobile century field experiment," *Transp. Res. C, Emerging Technol.*, vol. 18, no. 4, pp. 568–583, Aug. 2010.
[6] INRIX, INRIX Triples Real-Time Traffic Flow Coverage in North America to Over 160 000 Miles, Kirkland, WA, USA. [Online]. Available: http://www.inrix.com/pressrelease.asp?ID=68
[7] F. Bolte, "Fee collection for heavy goods vehicles on German motorways," in *Proc. IEE Semin. Road User Charging*, Mar. 2003, pp. 10/0–10/7.
[8] D. Salos, A. Martineau, C. Macabiau, B. Bonhoure, and D. Kubrak, "Receiver autonomous integrity monitoring of GNSS signals for electronic toll collection," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 94–103, Feb. 2014.
[9] W.-H. Lee, S.-S. Tseng, and C.-H. Wang, "Design and implementation of electronic toll collection system based on vehicle positioning system techniques," *Comput. Commun.*, vol. 31, no. 12, pp. 2925–2933, Jul. 2008.
[10] S. Lo, D. D. Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," *Inside GNSS*, vol. 4, no. 5, pp. 30–39, Sep./Oct. 2009.
[11] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2006.
[12] *Interface Specification IS-GPS-200E*, GPS Wing, Los Angeles, CA, USA, Jun. 2010.
[13] T. E. Humphreys *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meet. Satell. Div. ION GNSS*, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.
[14] S. Pullen, G. X. Gao, C. Tedeschi, and J. Warburton, "The impact of uninformed RF interference on GBAS and potential mitigations," in *Proc. ION ITM*, Newport Beach, CA, USA, Jan. 2012, pp. 780–789.
[15] GPS World, Massive GPS Jamming Attack by North Korea, May 2012. [Online]. Available: http://gpsworld.com/massive-gps-jamming-attack-by-north-korea
[16] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proc. ACM Conf. CCS*, 2012, pp. 450–461.
[17] Wall Street Journal, GPS Spoofing Threat Grows, Feb. 2013. [Online]. Available: http://blogs.wsj.com/tech-europe/2013/02/19/gps-spoofing-threat-grows
[18] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domínguez-García, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.
[19] UT News, UT Austin Researchers Successfully Spoof an $80 Million Yacht at Sea, Jul. 2013. [Online]. Available: http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea
[20] J. Krumm and K. Hinckley, "The NearMe wireless proximity server," in *UbiComp 2004: Ubiquitous Computing*, vol. 3205, N. Davies, E. Mynatt, and I. Siio, Eds. Berlin, Germany: Springer-Verlag, 2004, ser. Lecture Notes in Computer Science, pp. 283–300.
[21] Y. Bardout, "Authentication of GNSS position: An assessment of spoofing detection methods," in *Proc. 24th Int. Tech. Meet. Satell. Div. ION GNSS*, Portland, OR, USA, Sep. 2011, pp. 436–446.
[22] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proc. 25th Int. Tech. Meet. Satell. Div. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 1233–1243.
[23] D. Borio, "Panova tests and their application to GNSS spoofing detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 381–394, Jan. 2013.
[24] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proc. 24th Int. Tech. Meet. Satell. Div. ION GNSS*, Portland, OR, USA, Sep. 2011, pp. 1888–1896.
[25] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via Automatic Gain Control (AGC)," *NAVIGATION*, vol. 59, no. 4, pp. 281–290, 2012.

[26] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/No estimates," in *Proc. 25th Int. Tech. Meet. Satell. Div. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 2878–2884.
[27] F. Dovis, X. Chen, A. Cavaleri, K. Ali, and M. Pini, "Detection of spoofing threats by means of signal parameters estimation," in *Proc. 24th Int. Tech. Meet. Satell. Div. ION GNSS*, Portland, OR, USA, Sep. 2011, pp. 416–421.
[28] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proc. 16th Int. Tech. Meet. Satell. Div. ION GPS/GNSS*, Portland, OR, USA, Sep. 2003, pp. 1543–1552.
[29] 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.
[30] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION*, vol. 59, no. 3, pp. 177–193, 2012.
[31] C. J. Wullems, "A spoofing detection method for civilian L1 GPS and the E1-B Galileo safety of life service," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 4, pp. 2849–2864, Oct. 2012.
[32] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.
[33] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proc. 6th Int. Conf. IH*, Toronto, ON, Canada, 2004, pp. 239–252.
[34] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. 18th Int. Tech. Meet. Satell. Div. ION GNSS*, Long Beach, CA, USA, Sep. 2005, pp. 1285–1290.
[35] B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, and J. A. Bhatti, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proc. 25th Int. Tech. Meet. Satell. Div. ION GNSS*, Nashville, TN, USA, Sep. 2012, pp. 1–10.
[36] C. Harpes, B. Jager, and B. Gent, "Secure localisation with location assurance provider," in *Proc. ENC—GNSS*, Savannah, GA, USA, 2009.
[37] K. T. Woo, "Optimum semicodeless carrier-phase tracking of L2," *NAVIGATION*, vol. 47, no. 2, pp. 82–99, 2000.
[38] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.
[39] J. A. Swets, *Signal Detection Theory and ROC Analysis in Psychology and Diagnostics: Collected Papers*. Mahwah, NJ, USA: Lawrence Erlbaum Associates, 1996.
[40] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Amer. Stat. Assoc.*, vol. 58, no. 301, pp. 13–30, Mar. 1963.
[41] D. R. Karger, S. Oh, and D. Shah, "Iterative learning for reliable crowdsourcing systems," in *Proc. Adv. Neural Inf. Process. Syst.*, J. Shawe-Taylor, R. Zemel, P. Bartlett, F. Pereira, and K. Weinberger, Eds., 2011, vol. 24, pp. 1953–1961.
[42] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*. Berlin, Germany: Springer-Verlag, 2007.

Liang Heng (M'13) received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, in 2006 and 2008, respectively, and the Ph.D. degree from Stanford University, Stanford, CA, USA, in 2012, all in electrical engineering.

He is a Postdoctoral Research Associate with the Department of Aerospace Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, USA. His research interests are cooperative navigation and satellite navigation.

Dr. Heng is a member of The Institute of Navigation.

Daniel B. Work (M'14) received the B.Sc. degree from Ohio State University, Columbus, OH, USA, in 2006 and the M.Sc. and Ph.D. degrees from University of California, Berkeley, CA, USA, in 2007 and 2010, respectively, all in civil engineering.

He is an Assistant Professor in the Department of Civil and Environmental Engineering and the Coordinated Science Laboratory with University of Illinois at Urbana-Champaign, Urbana, IL, USA. His research interests are in control, estimation, and optimization of cyberphysical systems; mobile sensing; and inverse modeling and data assimilation applied to problems in civil and environmental engineering.

Prof. Work has received a number of awards, including the 2011 IEEE Intelligent Transportation Systems Society Best Dissertation Award.

Grace Xingxin Gao (M'12) received the B.S. degree in mechanical engineering and the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2001 and 2003, respectively, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, USA, in 2008.

She is an Assistant Professor with the Department of Aerospace Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, USA. Before joining University of Illinois at Urbana-Champaign in 2012, she was a Research Associate with Stanford University.

Prof. Gao has received a number of awards, including the RTCA William E. Jackson Award, The Institute of Navigation Early Achievement Award, 50 GNSS Leaders to Watch by GPS World Magazine, and multiple best presentation awards at ION GNSS conferences.