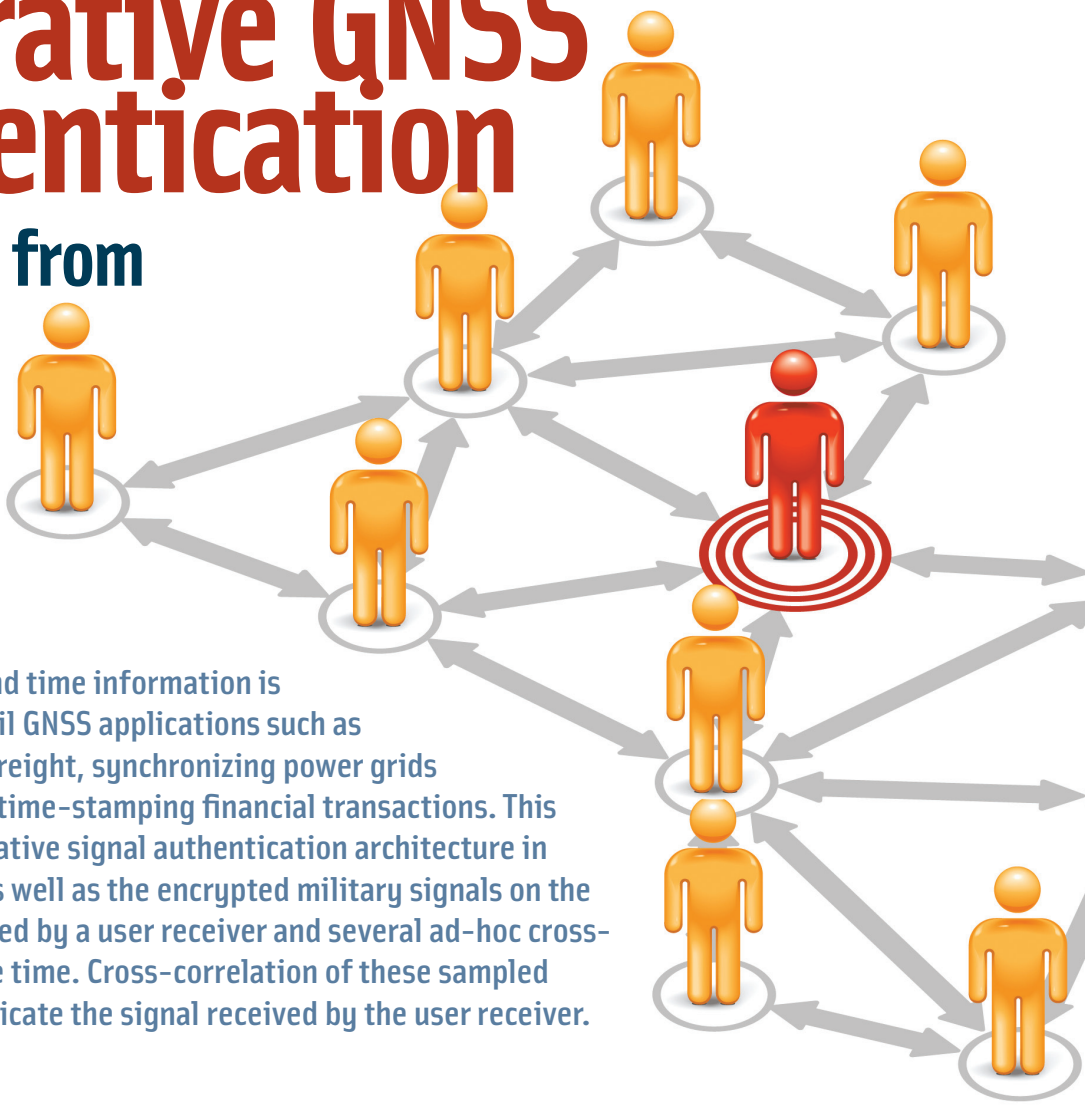
Cooperative GNSS Authentication

Reliability from Unreliable Peers



Secure, reliable position and time information is indispensable for many civil GNSS applications such as guiding aircraft, tracking freight, synchronizing power grids and cellular networks, and time-stamping financial transactions. This article introduces a cooperative signal authentication architecture in which civil GNSS signals, as well as the encrypted military signals on the same frequency, are sampled by a user receiver and several ad-hoc cross-check receivers at the same time. Cross-correlation of these sampled signals are used to authenticate the signal received by the user receiver.

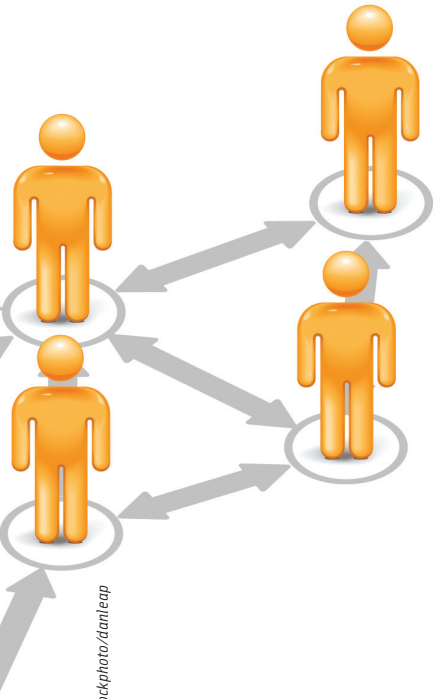
LIANG HENG, DANIEL B. WORK, AND GRACE XINGXIN GAO
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

During the past two decades, the Global Positioning System, together with other GNSSs, has become an essential element of the global information infrastructure, with myriad applications in almost every facets of modern businesses and lifestyles, including communication, energy distribution, finance and insurance, and transportation. Ever-growing dependence on GNSS creates strong incentives to attack civil GNSS, for either an illegitimate advantage or a terrorism purpose.

Unfortunately, security is not a built-in feature of GNSS open service. It has been known that low-received-power, unencrypted civil signals are vulnerable to jamming and spoofing attacks. Jamming is the intentional broadcast of a high-power "blocking" signal at the GNSS frequency. Hence, jamming is disruptive but usually detected by the receiver whenever it stops tracking satellites.

Unlike jamming, spoofing is a much more sophisticated attack. A spoofer intentionally broadcasts a counterfeit GNSS signal that overpowers the authentic signal so as to manipulate a victim receiver's reported position, time, or both. Spoofing poses a greater security risk because it is deceptive and usually undetected by a Standard Positioning Service (SPS) receiver.

So far, a variety of methods have been proposed to harden civil GNSS receivers against spoofing attacks. These defensive 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 GNSS subsystem, such as the information from inertial sensors, odometers, cellular networks, and high-stability clocks. The second group performs statistical tests on features inherent in GNSS signals, including angle of arrival, signal quality, signal power, and multipath. The third group relies on cryptographic, unpredictable



© iStockphoto/danleap

information carried by GNSS signals. The Additional Resources section near the end of this article provides a list of some of the key papers and articles describing these various types of spoofing defenses.

Unlike the first group of methods, cryptographic methods need no additional hardware. In comparison to the second group, cryptographic methods enable users to differentiate authentic signals from counterfeit signals with higher confidence, especially in a complex environment where the statistics of authentic signals can be highly unstable.

Three types of cryptographic spoofing defense have appeared in recent literature. The first option, known as navigation message authentication (NMA), inserts public-key digital signatures into the navigation message. Another strategy is to interleave spread-spectrum security codes (SSSC) with normal civil GPS spreading codes so that parts of spreading sequences are periodically unpredictable.

Both NMA and SSSC require significant modifications to the legacy GPS signal structure. Consequently, 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. With little or even no modification to the GPS IS and the hardware of current GPS receivers, this approach is not only promising but also practical *today*. However, this approach in a centralized client-server approach requires dedicated reference stations at secure locations, which implies a considerable setup and maintenance cost.

The cooperative approach is superior to the centralized client–server approach in terms of cost, availability, user capacity, and robustness.

This article will show that cross-correlation-based spoofing detection can be performed in a cooperative manner that incorporates information from other nearby GNSS receivers, without the requirement of high-quality, secure dedicated reference stations. The reliability arises from assistance provided by low-cost and even "unreliable" peers, which are voluntary but can be spoofed or dishonest.

Signal Authentication from Cooperative Peers

The cross-correlation spoofing detection 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. The spoofing detection basically correlates a snapshot of L1 signal from the receiver to be authenticated (hereinafter referred to as the "user receiver") with a snapshot from the cross-check reference receiver; both snapshots are known to contain the same part of P(Y) code.

Although the P(Y) code is known by neither receiver and although its received version is noisy and may be distorted by a narrow-band RF front-end, a high correlation peak can still appear if neither receiver is spoofed or if both receivers are spoofed by the same spoofer. A low correlation peak appears when one of the receivers is spoofed and the other is not, or when both receivers are spoofed by different spoofers who counterfeit different P(Y) codes.

The signal authentication architecture proposed by S. Lo *et alia* and M. L. Psiaki *et alia* is in a centralized client-server approach, where each user receiver is served by a single dedicated reference receiver.

This architecture has several disadvantages. First and foremost, it requires considerable investment in the reference stations, not to mention the maintenance cost. Second, because a small number of reference stations is preferred due to cost considerations, the limited number of reference stations further limits the availability and robustness of the service, and also limits user capacity. Third, a limited number of reference stations at known locations are vulnerable to organized, targeted jamming and spoofing attacks, and loss of a majority of the reference stations could paralyze the authentication service.

Realizing these disadvantages, in this article we propose a GNSS signal authentication architecture in an ad hoc, cooperative approach. The fundamental difference from the centralized client-server approach is that our architecture uses multiple voluntary peers (hereinafter referred to as "ad-hoc cross-check receivers" or simply "cross-check receivers") as references.

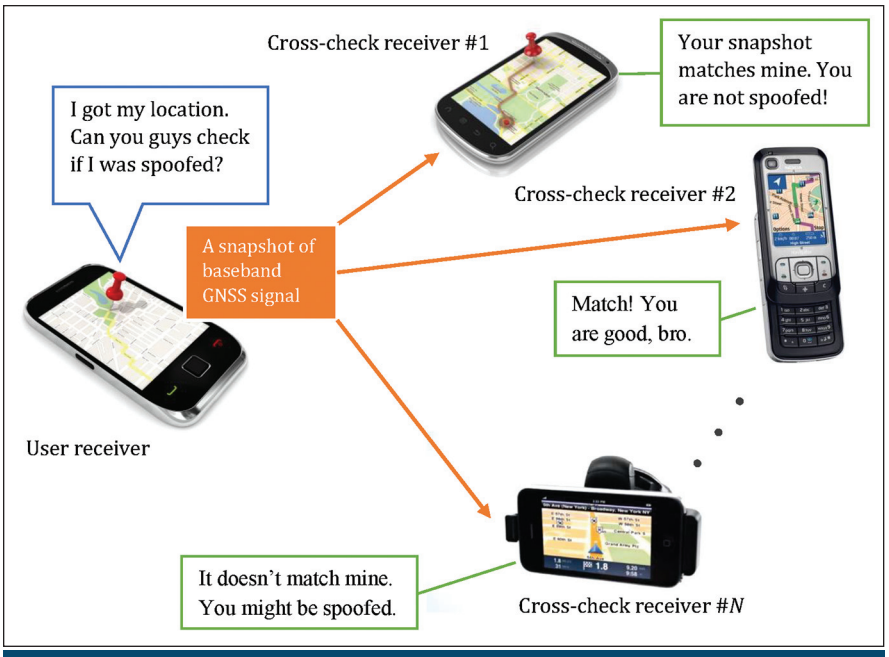


FIGURE 1 Cross-correlation spoofing detection in a cooperative approach. The signal received by the user receiver is checked against those received by multiple ad-hoc cross-check receivers. In this approach, each cross-check receiver computes the correlation between its own snapshot and the one from the user receiver. Note that the correlations can also be computed by the user receiver itself, a cloud service, or a third party.

Steps	Actions
1	User receiver sends out authentication requests with its location.
2	Available receivers within an appropriate area (neither too close to nor too far from the user receiver) respond to requests.
3	User receiver randomly chooses a number of receivers, and sends out a GPS time in the immediate future.
4	User receiver and cross-check receivers collect samples of baseband GNSS signal at the GPS time.
5	User receiver sends its samples to all cross-check receivers.
6	Each cross-check receiver correlates its samples with user receiver's, and replies to the user receiver with a decision "authentic" or "unauthentic."
7	User receiver determines the authenticity of its received signal by aggregating all these decisions.

TABLE 1 Procedure of the authentication system illustrated in Figure 1, where correlations are computed by ad-hoc cross-check receivers in a distributed approach

In our proposed authentication architecture, the signal received by the user receiver is checked against that received by each cross-check receiver. Each such check provides a "decision" as to the authenticity of the signal received by the user receiver, and an aggregation of these decisions leads to the final decision regarding the reliability or authenticity of the GNSS position.

The cooperative approach is superior to the centralized client-server approach in terms of cost, availability, user capacity, and robustness. However, one should be aware that each ad-hoc cross-check receiver is less reliable than a dedicated reference receiver. First, a mass-market GNSS receiver, especially 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 be "dishonest" so that its authentication decision is falsified, even always opposite to the honest decision. Besides, a cross-check receiver can also be spoofed, and sometimes may be spoofed by the same spoofer if it is not sufficiently distant from the user receiver.

We shall further show in this article that our proposed approach is actually robust against these factors. In fact, the spoofing detection performance improves exponentially with the number of cross-check receivers involved in an authentication solution.

Candidate Structure of Authentication System

There are several approaches for implementing our proposed authentication system. These differ from one another mainly in where correlations are computed.

One approach is to distribute correlation computation to either cross-check receivers or a cloud service. Another option is to compute all the correlations in a centralized way, either by the user receiver itself or by a third party, which requires authentic position and/or clock information of the user receiver.

This section will present a candidate structure in which cross-check receivers compute the correlations. This structure is attractive because of its good privacy protection: the cross-check receivers need not release their collected snapshots of GNSS signals to anybody.

Figure 1 depicts a scenario of this structure, and the whole procedure is explained in detail in **Table 1**. In Figure 1, a user receiver wants to know whether its received signal is authentic or not; so, it randomly chooses N peers as cross-check references. The user receiver and all cross-check receivers agree to collect a snapshot of baseband GPS signal at a GPS time in the immediate future. The user receiver sends its snapshot to the reference receivers via secure channels. Then each reference receiver correlates its own snapshot with the one from the user receiver, and decides if the signal received by the user receiver is authentic or not. The user receiver collects the decisions from all three reference receivers, and finally determines the authenticity of its received signal by an appropriate statistical measure. Because snapshots of GNSS signals have to be transported over a communication network, a security protocol, such as transport layer security (TLS) or IPsec, is 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 M. L. Psiaki *et alia*,

S	Actual status of user receiver: S=0 unspoofed, and S=1 spoofed.
N	Number of cross-check receivers.
A_i	Authentication result using the ith cross-check receiver, i=1...N: A_i=0 "authentic", and A_i=1 "unauthentic."
A	Final authentication result from aggregating all A_i, i=1...N.
α	Equal to Prob(A_i=1|S=0), for all i=1,...,N, probability of false alarm using one unspoofed cross-check receiver.
β	Equal to Prob(A_i=0|S=1), for all i=1,...,N, probability of missed detection using one unspoofed cross-check receiver.
P_{FA}	Equal to Prob(A=1|S=0), probability of false alarm of the final authentication result.
P_{MD}	Equal to Prob(A=0|S=1), probability of missed detection of the final authentication result.
P_D	Equal to 1-P_{MD}, probability of detection, also referred to as detection power.
P_{SS}	Probability of (a) cross-check receiver being spoofed by the same spoofer as the user receiver and (b) a cross-check receiver being dishonest such that its authentication decision is always opposite.
P_{SD}	Probability of a cross-check receiver being spoofed by a different spoofer than the user receiver.

TABLE 2 List of terms and notations used in analysis of spoofing detection methods

a snapshot of approximately one second is generally needed for reliable spoofing detection. A narrow-band GNSS front-end usually has a bandwidth of 2.4 megahertz, and one-second one-bit quadrature-phase samples yield 2.4 megabits of data. Current 3G/4G cellular networks typically take one second or less to upload or download the data. The time of computation depends, but a rule of thumb is that a receiver must have the capability of processing one-second data within one second. Because the time required for sending/responding to requests and aggregating decisions is usually negligible, the authentication process can take as short as four seconds.

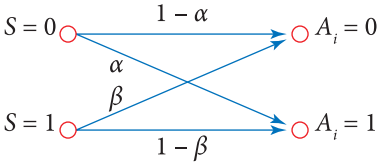
It is worth nothing that our cooperative authentication does not require highly reliable spoofing detection for each cross-check receiver and thus allows a much shorter snapshot to be collected. Therefore, four seconds is a very conservative estimate.

Analysis of Spoofing Detection Performance

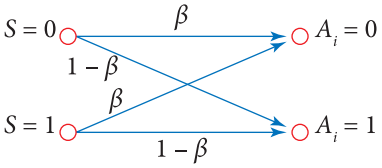
Essentially a statistical hypothesis test, any spoofing detection has a probability of making two types of errors: false alarm and missed detection. This section is devoted to a rigorous analysis of the probability of these two types of errors in cooperative authentication.

Assumptions and Notations. In order to simply the analysis, we assume that all ad-hoc cross-check receivers have the same detection performance, namely, the same probability of false alarm and the same probability of missed detection. 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 of the user receiver. Table 2 summarizes the notations used throughout this article.

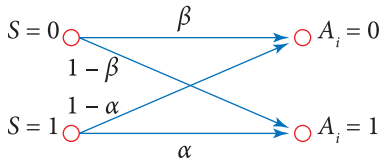
Channel Models. Since both S and A_i are binary, spoofing detection can be considered as an asymmetric communication channel. When the ith cross-check receiver is not spoofed, the channel model is simply given by the following.



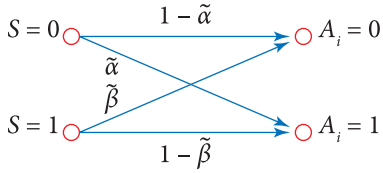
When the ith cross-check receiver is spoofed by a different spoofer than the user receiver, the snapshots from two receivers do not match whether the user receiver is spoofed or not. Therefore, the channel model is given by the following.



When the ith cross-check receiver is spoofed by the same spoofer as the user receiver or the cross-check receiver purposely lies with opposite authentication results, the channel becomes the following.



Among the three preceding channel models, the second occurs with a probability P_{SD}, and the third occurs with a probability P_{SS}. Therefore, the aggregated channel is given by the following,



where

$$\tilde{\alpha}=(1-P_{SS}-P_{SD})\alpha+(P_{SS}+P_{SD})(1-\beta),$$
$$\tilde{\beta}=(1-P_{SS})\beta+P_{SS}(1-\alpha).$$

Spoofing Detection Performance. Let $X=\sum_{i=1}^{N}A_i$ and t be a threshold. The final authentication result will be "authentic" if $X<t$ and "unauthentic" if $X\geq t$. Thus, we have

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

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

From the four preceding equations, we can see that P_{SD} only affects P_{FA}, while P_{SS} affects both P_{FA} and P_D. Because P_{SS} deteriorates performance more significantly than P_{SD}, in practice it is wise to choose cross-check receivers far from the user receiver in order to reduce P_{SS}.

Numerical Examples. We assume that $\alpha=0.001$ and $\beta=0.15$ for the following reason. M. L. Psiaki *et alia* have shown that for a narrow-band GNSS receiver with an ideal ADC, a 0.4-second correlation interval leads to a detection power $P_D\geq 0.95$ when $P_{FA}=0.0001$ and $C/N_0\geq 40$ dB-Hz. This is equivalent to $\alpha=0.0001$ and $\beta=0.05$. In cooperative authentication, ad-hoc cross-check receivers may be of low cost and low quality. Therefore, $\alpha=0.001$ and $\beta=0.15$ represent a reasonable and very conser-

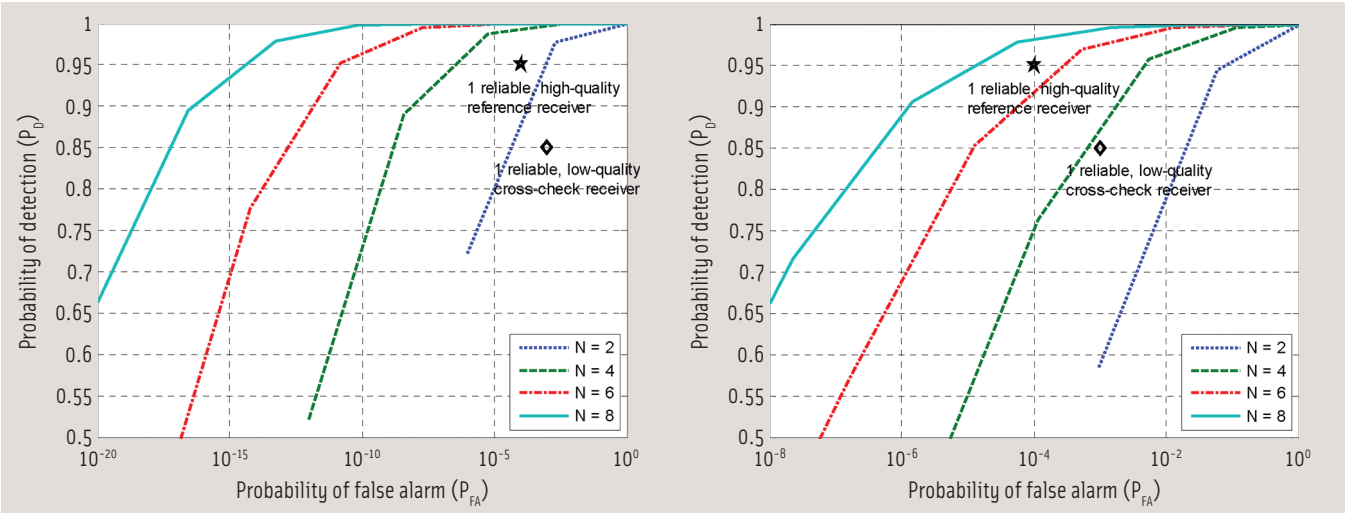


FIGURE 2 Receiver operating characteristic (ROC) curves for reliable and unreliable cross-check receivers (α = 0.001 and β = 0.15). Panel A (left): Cross-check receivers are all reliable ($P_{SS} = P_{SD} = 0$). Multiple cross-check receivers always outperform a single low-quality one. Three unreliable, low-quality cross-check receivers are on a par with a single reliable, high-quality reference receiver. Panel B (right): Cross-check receivers are unreliable ($P_{SS} = P_{SD}$ = 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.

vative assumption.

Figure 2 shows the receiver operating characteristic (ROC) curves for two cases: all cross-check receivers are reliable ($P_{SS} = P_{SD} = 0$); cross-check receivers can be spoofed or dishonest with probabilities P_{SS} = 0.1 and P_{SD} = 0.1. Figure 2 shows that increasing the number of cross-check receivers always improves performance.

It can be seen that when cross-check receivers are spoofed with such large probabilities, four unreliable cross-check receivers are sufficient to match the performance of a single reliable, low-quality cross-check receiver, and seven can match a single reliable, high-quality reference receiver.

Figure 3 and **Figure 4** show probability of missed detection and probability of false alarm, both as functions of the number of cross-check receivers. Four cases are considered in the figures: $P_{SS} = P_{SD} = 0$, $P_{SS} = 0.02$ and $P_{SD} = 0.18$, $P_{SS} = P_{SD} = 0.1$, $P_{SS} = 0.18$ and $P_{SD} = 0.02$.

From Figure 3 we can see that for a constant P_{FA}, P_{MD} decreases approximately exponentially with the number of cross-check receivers. Figure 4 shows a similar behavior. Even though the probability $P_{SS} = P_{SD} = 0.2$ is overly conservative, a modest number of cross-check receivers provides a sufficiently low probability of

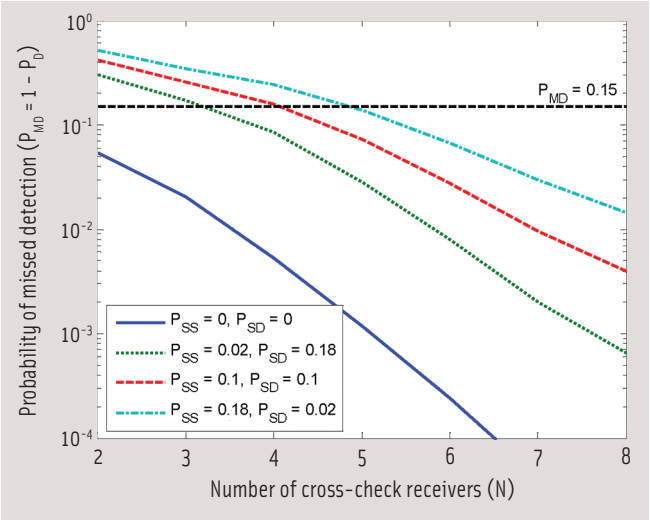


FIGURE 3 Probability of missed detection as a function of number of cross-check receivers for four reliability assumptions ($P_{FA} = \alpha$ = 0.001 and β = 0.15). Even if we assume 20 percent of the cross-check receivers are spoofed (a very conservative assumption, with different combinations of receivers spoofed by the same or different spoofers), a modest number of cross-check receivers provides a sufficiently low probability of missed detection.

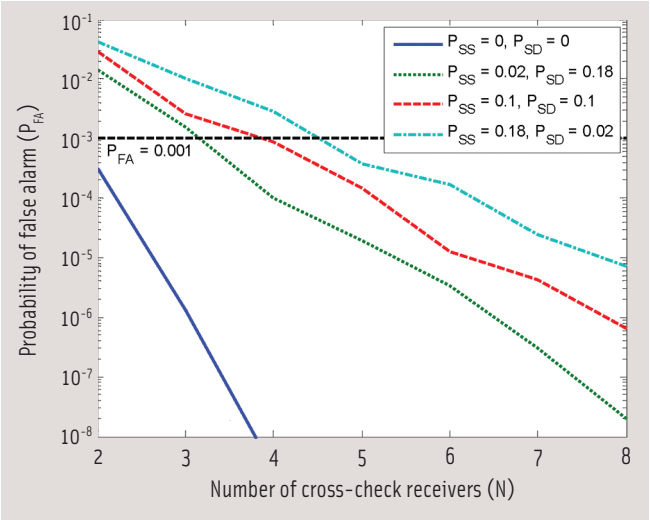


FIGURE 4 Probability of false alarm as a function of number of cross-check receivers under four reliability assumptions (α = 0.001 and $P_{MD} = \beta$ = 0.15). Even if we assume 20 percent of the cross-check receivers are spoofed (a very conservative assumption, with different combinations of receivers spoofed by the same or different spoofers), a modest number of cross-check receivers provides a sufficiently low probability of false alarm.

missed detection and false alarm.

Additionally, as foreseen in the previous section, P_{SS} deteriorates performance more significantly than P_{SD}.

Concluding Remarks

Secure, reliable position and time information is vital for many critical civil GNSS applications. This article has presented a signal authentication architecture that relies on a network of cooperative, low-cost receivers.

The civil GNSS signals, together with the encrypted military signals on the same frequency, 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. The spoofing detection results from all cross-check receivers are aggregated to reach a final decision regarding the authenticity of the signal received by the user receiver.

This article has validated the concept through a theoretical analysis. We have assumed the cross-check receivers can be spoofed or dishonest. The analysis and numerical examples have shown that the spoofing detection performance improves exponentially with the number of cross-check receivers.

A surprising and powerful aspect of the results is that with a modest number of cross-check receivers, each single cross-check receiver does not have to be high-quality, highly reliable, or highly robust to spoofing attacks.

Additional Resources

[1] Akos, D. M., "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)", *NAVIGATION, Journal of The Institute of Navigation,* Vol. 59, No. 4, Winter 2012, pp. 281–290

[2] Bardout, Y., "Authentication of GNSS Position: An Assessment of Spoofing Detection Methods," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, Oregon, September 2011, pp. 436–446

[3] Daneshmand, S., and A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, Tennessee, September 2012, pp. 1233–1243

[4] Dehghanian, V., and J. Nielsen, and G. Lachapelle, "GNSS Spoofing Detection Based on Receiver C/No Estimates," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012),* Nashville, Tennessee, September 2012, pp. 2878–2884

[5] Dovis, F., and X. Chen, A. Cavaleri, K. Ali, and M. Pini "Detection of Spoofing Threats by Means of Signal Parameters Estimation," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, Oregon, September 2011, pp. 416–421

[6] Humphreys, T. E., and B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008),* Savannah, GA, Sep 2008, pp. 2314–2325.

[7] Lo, S., and D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication: A Secure Civil GNSS for Today," *Inside GNSS,* September/October 2009

[8] Pini, M., and M. Fantino, A. Cavaleri, S. Ugazio, and L. Lo Presti, "Signal Quality Monitoring Applied to Spoofing Detection," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, OR, Sep 2011, pp. 1888–1896

[9] Psiaki, M. L. , and B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," to appear in *IEEE Transactions on Aerospace and Electronic Systems.*

[10] Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003),* Portland, Oregon, September 2003, pp. 1543–1552

[11] Wesson, K., and M. Rothlisberger and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation,* Vol 59, Num 3, 2012, pp 177–193

Authors

Liang Heng is a postdoctoral research associate in the Department of Aerospace Engineering, University of Illinois at Urbana-Champaign. He received the B.S. and M.S. degrees from Tsinghua University, China in 2006 and 2008, and the Ph.D. degree from Stanford University in 2012, each in Electrical Engineering. His research interests are cooperative navigation and satellite navigation. He is a member of the Institute of Electrical and Electronics Engineer (IEEE) and the Institute of Navigation (ION).

Daniel B. Work is an assistant professor in the Department of Civil and Environmental Engineering, University of Illinois at Urbana-Champaign. Prof. Work earned his bachelor of science degree (2006) from the Ohio State University, and a master of science (2007) and Ph.D. (2010) from the University of California, Berkeley, each in civil engineering. Dr. Work has research interests in control, estimation, and optimization of cyber physical systems, mobile sensing, and inverse modeling and data assimilation, applied to problems in civil and environmental engineering.

Grace Xingxin Gao is an assistant professor in the Aerospace Engineering Department at University of Illinois at Urbana-Champaign. She received her B.S. degree in Mechanical Engineering in 2001 and her M.S. degree in Electrical Engineering in 2003, both at Tsinghua University, China. She obtained her Ph.D. degree in Electrical Engineering at Stanford University in 2008. Before joining Illinois at Urbana-Champaign as an assistant professor in 2012, Prof. Gao was a research associate at Stanford University. Prof. Gao has won a number of awards, including RTCA William E. Jackson Award, Institute of Navigation Early Achievement Award, 50 GNSS Leaders to Watch by GPS World Magazine, and multiple best presentation awards at ION GNSS conferences. IG