A Probabilistic Framework for Global Navigation Satellite System Signal Timing Assurance

Kyle D. Wesson and Brian L. Evans
Department of Electrical and
Computer Engineering
The University of Texas at Austin
Email: kyle.wesson@utexas.edu, bevans@ece.utexas.edu

Todd E. Humphreys
Department of Aerospace Engineering and
Engineering Mechanics
The University of Texas at Austin
Email: todd.humphreys@mail.utexas.edu

***Abstract*—Global Navigation Satellite System (GNSS) signals serve as a worldwide timing reference in numerous technological sectors. Yet GNSS receivers are vulnerable to so-called spoofing attacks that can manipulate the time reference. We illustrate the need for a probabilistic security model in the context of authenticating a timing signal as opposed to the traditionally non-probabilistic security models of message authentication and cryptography. Our primary contribution is establishing the necessary conditions for timing assurance in the context of security-enhanced GNSS signals. In addition, we formulate a probabilistic framework for timing assurance that combines cryptography and statistical signal processing across multiple network layers.**

I. Introduction

Global Navigation Satellite System (GNSS) signals provide a global time reference that synchronizes telecommunication networks, power grids, and air traffic. The security of GNSS broadcasts is a concern because attackers can transmit counterfeit, or spoofed, signals that can deceive victim receivers into reporting an incorrect position, velocity, or time solution [1]. Spoofing attacks can impede handoff between cell phone base stations, cause power outages, or crash unmanned aerial vehicles [2]–[4]. To defend against spoofing, GNSS receivers seek to authenticate GNSS signals—that is, to verify that the received signals (1) originated from the declared satellite transmitter, and (2) arrived without delay [5], [6].

GNSS timing assurance, the topic of this paper, and message authentication, which ensures data security [7], can be distinguished by their security models. Message authentication is predicated on the computational infeasibility of finding weaknesses in the underlying cryptographic functions or discovering the private signing key—tasks whose probability of success is vanishingly small [8]. By contrast, the intrinsic security of timing assurance is weaker and demands a probabilistic security model because the information of interest is conveyed through the signal timing in addition to the modulated data [5], [9]. Thus, even without reading or altering the modulated data, malefactors can manipulate the information content of a timing signal simply by delaying the signal itself.

GNSS anti-spoofing techniques are categorized as either cryptographic methods that employ secure keys [5], [10], [11] or as non-cryptographic methods that are designed to be sensitive to certain GNSS signal statistics [12], [13]. To date, there is no encompassing framework that addresses the probabilistic nature of each technique or offers an expedient way to combine multiple techniques for a probabilistic security analysis.

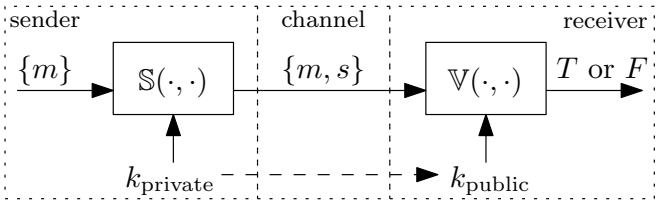

Fig. 1. Diagram illustrating the public-key digital signature system. The verification algorithm $\mathbb{V}(\cdot)$ asserts if the message-signature pair $\{m, s\}$ is authentic: the holder of k_{private} generated $\{m, s\}$ exactly.

Our primary contribution is establishing necessary conditions for timing authentication of security-enhanced (i.e., cryptographic) GNSS signals under a probabilistic framework that combines cryptographic and statistical signal processing. We then show how statistics meeting these necessary conditions can be coupled with non-cryptographic statistics in a generalized probabilistic framework.

II. Data Message Authentication

Data message authentication is predicated on the computational infeasibility of (1) performing a brute-force search for the secret signing key, or of (2) reversing one-way hash functions. The probability of success of either task even under the most optimistic assumptions—the fastest supercomputers running the most advanced cryptanalysis techniques—is so vanishingly small that standards bodies assume near-absolute security of data authentication techniques over periods of years. The National Institute of Standards and Technology considers standardized data authentication techniques with an underlying cryptographic secret key strength of 112 bits secure through the year 2030 [14].

Public-key digital signature algorithms are often employed to achieve data message authentication (e.g., signing emails with the Digital Signature Algorithm). Here, a cryptographic signature algorithm $\mathbb{S}$ generates a message signature s based on the input message m and a secret cryptographic key k_{private}: $\mathbb{S}(k_{\text{private}}, m) = s$. Application of a cryptographic verification

Preprint of the 2013 Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, Nov. 3-6, 2013

algorithm $\mathbb{V}$ to the message-signature pair $\{m, s\}$ with a corresponding cryptographic public key k_{public} derived from k_{private} results in a Boolean: $\mathbb{V}(k_{\text{public}}, \{m, s\}) = T$ or F. If true, the result confirms that the owner of k_{private} generated $\{m, s\}$ and that $\{m, s\}$ arrived without modification. The public-key digital signature model is illustrated in Figure 1.

We assume that s is unpredictable prior to reception, because so far as it is known, the tasks of either (1) recovering k_{private} from any number of signed messages or from k_{public}, or (2) predicting s based on m or k_{public} are computationally infeasible. These tasks are difficult to talk about in probabilistic terms. Instead, the assumption is based on the mathematics of the underlying cryptographic functions and the scrutiny of security experts worldwide that has yet to reveal a weakness in the approach.

In data message authentication, the result of $\mathbb{V}$ is a sufficient statistic; no other metric is assumed to offer any additional information about the authenticity of the message-signature pair. By analogy with other detection tests described later, one can consider this statistic in the context of a hypothesis test: $\mathbb{V}$ is tested against a threshold to determine the difference between the null hypothesis H_0 (no spoofing) and the alternate hypothesis H_1 (spoofing). The probability of detection $P_{D,\mathbb{V}}$ of an attack against a cryptographic message authentication system, either an attack that modifies $\{m, s\}$ or forges s, is effectively perfect (i.e., $P_{D,\mathbb{V}} = 1$). The probability of false alarm $P_{F,\mathbb{V}} = 0$.

Given the near certainty with which the technique guarantees data message authentication, it may be surprising that data message techniques alone are insufficient to authenticate timing signals. In the next section, two types of attacks against security-enhanced GNSS signals will illustrate why *signal* authentication requires both data message and timing authentication. Data message authentication is a necessary, but not sufficient, component of comprehensive signal authentication. The latter requires components that span the sub-physical to presentation layer.

III. Security-Enhanced Signals

Below the physical layer, in what might be called the signal definition layer, security-enhanced (i.e., signed) GNSS signals must be specified to include *a priori* unpredictable data, referred to as a security code, that can be validated only after broadcast. Define the security code $w = \{m, s\}$, and let it modulate a typical spread-spectrum timing signal modeled at the output of a receiver after demodulation and sampling [5]:

$$Y_k = w_k c_k \cos(\omega_{IF} t_k) + N_k \tag{1a}$$

$$= w_k s_k + N_k \tag{1b}$$

Here, at sample index k, w_k is a security code with chip length T_w, c_k is a spreading code with chip length T_c, ω_{IF} is the downmixed carrier frequency, and N_k is additive white Gaussian noise samples. Note that $s_k \equiv c_k \cos(\omega_{IF} t_k)$ is deterministic.

The defining feature of w_k is that some or all of its symbols are unpredictable to an attacker prior to broadcast but can be validated after [5]. The message-signature pair generated via a public-key digital signature technique confers both features, although other techniques could be employed instead (e.g., symmetric-key encryption). The security code enables two critical components in support of signal authentication: (1) data message authentication and (2) hypothesis testing for security code estimation and replay attacks.

IV. Attacking Security Enhanced Signals

Security-enhanced signals force an attacker to either record and re-broadcast the entire signal or to estimate w_k on-the-fly.

A. Record and Playback Attack

In a record and playback attack, the attacker records the entire radio-frequency spectrum containing the security-coded signal and replays it at a later time. For a single signal, the combination of the authentic and recorded signal can be modeled as

$$Y_k = \alpha w_{k-d} s_{k-d} + N_{a,k} + w_k s_k + N_k \tag{2}$$

Here, $N_{a,k}$ is the noise introduced by the attacker, $d > 0$ is the number of samples of delay introduced between the recording and playback of the signal, and α is the attacker's amplitude advantage factor.

B. Security Code Estimation and Replay Attack

A security code estimation and replay (SCER) attack affords an attacker significantly greater flexibility than under a record and playback attack but also requires significantly more effort [10]. In a SCER attack, an attacker attempts to estimate w_k on-the-fly and broadcast a signal with correct security code estimate:

$$Y_k = \alpha \hat{w}_{k-d} s_{k-d} + w_k s_k + N_k \tag{3}$$

Here, $\hat{w}_{k-d}$ is the attacker's estimate of the security code and the other quantities are as before. The better the estimate of $\hat{w}_{k-d}$, the greater the likelihood the SCER attack is successful. The delay d is the sum of the processing/transmission delay and the estimation/control delay. The former does not enhance $\hat{w}_{k-d}$, while the latter is a spoofer-controlled choice to allow it more time to form $\hat{w}_{k-d}$.

C. Insufficiency of Data Message Authentication

Consider applying the data message authentication technique of Sec. II to the attack modeled in Eq. 2. For a very strong α (i.e., $\alpha \gg 1$), the spoofed signals overpower the authentic signals. In turn, the GNSS receiver would authenticate the signal: w_{k-d} would pass $\mathbb{V}$ because it was generated from k_{private}. Note that $\mathbb{V}$ cannot identify d. The result is a successful attack that modifies the victim receiver's time estimate by d. The SCER attack proceeds similarly, but its success depends on the accuracy of $\hat{w}_{k-d}$. Clearly, signal authentication requires verifying the consistency of the incoming signal timing (i.e., timing of the spreading and

security code) with the receiver's own time estimate. While $\mathbb{V}$ is effective for source authentication, it does not offer timing authentication.

The presence of noise N_k in Eq. 1 causes additional difficulties for $\mathbb{V}$. Strong noise can cause bit errors, despite application of error correction techniques [15], which results in $\mathbb{V}$ = 0. Bit errors occur at a known rate under H_0. The probability of a false alarm when verifying $\{m, s\}$ of length $N_{\{m,s\}}$ is $P_{F,\mathbb{V}} = 1-(1-p_e)^{N_{\{m,s\}}}$ where p_e is the probability that a single bit is decoded incorrectly.

To reduce the false alarm rate of message authentication in the presence of noise, it is appropriate to consider the statistic $B = \overline{\mathbb{V}} \wedge E$ where E represents the output of an error detection routine (i.e., $E = 1$ for no errors detected). If B asserts under H_1, then an attack is detected: $\mathbb{V} = 0$ and $E = 1$. If B remains low under H_0, then either verification passes or errors were detected in the bit stream. If B asserts under H_0, then there was a false alarm.

The probability of false alarm $P_{F,B}$ is the probability that the error detection routine failed to detect errors when errors were present. For modernized GNSS signals, this is a very low probability because both error correction and error detection are applied. Note that error correction and detection only applies to low-rate security codes (e.g., at the bit-level) and not high-rate security codes (e.g., embedded in the security code) [10]. For the latter, $\mathbb{V}$ is considered alone. Finally, note that cryptographic operations occur at the presentation layer as defined by the Open Systems Interconnection model [16].

The remaining sections describe the necessary elements for signal authentication, including timing consistency and SCER detectors at the physical layer, and illustrate why the intrinsic security model of signal authentication demands a probabilistic framework compared to pure data authentication.

V. Timing Consistency Check

A critical component of signal authentication is verifying that the incoming signal timing is consistent with the receiver's time estimate. The timing consistency check is a hypothesis test at the physical layer on the difference between the received and predicted code phase of the spreading code c_k [5].

Let $\tilde{\tau}_{k_m}$ be the measured code phase of the arrival time of a feature of the incoming signal, and let $\bar{\tau}_{k_m} = \mathbb{E}[\tau_{k_m}|\underline{\mathbf{Y}}^{k_{m-1}}]$ be the predicted code phase given all measurements $\underline{\mathbf{Y}}^{k_{m-1}}$ where $\underline{\mathbf{Y}}^{k_{m-1}} \equiv [Y_1, Y_2, \ldots, Y_{k_{m-1}}]^T$. Here, m represents the index corresponding to the measurement whose measurement interval spans from $t_{k_{m-1}}$ to t_{k_m}. The hypothesis test is

$$\nu_{k_m} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma_\nu \tag{4}$$

Here, $\nu_{k_m} = \tilde{\tau}_{k_m} - \bar{\tau}_{k_m}$ is the innovation, or difference, between the measured $\tilde{\tau}_{k_m}$ and predicted code phase $\bar{\tau}_{k_m}$. The time-varying value of γ_ν depends on a pre-set false alarm probability $P_{F,\nu}$ and on the innovation's conditional distribution, $p_{\nu_{k_m}|\underline{\mathbf{Y}}^{k_{m-1}}}(\xi|\underline{\mathbf{Y}}^{k_{m-1}})$, which is derived from $p(\tilde{\tau}_{k_m} - \tau_{k_m})$ and $p_{\tau_k,\underline{\mathbf{Y}}^{k_{m-1}}}(\xi|\underline{\mathbf{Y}}^{k_{m-1}})$. Typically, the distributions are assumed to be Gaussian. The threshold is the value of γ_ν for which

$$P_{F,\nu} = \int_{\gamma_\nu}^{\infty} p_{\nu_{k_m}|\underline{\mathbf{Y}}^{k_{m-1}}}(\xi|\underline{\mathbf{Y}}^{k_{m-1}})d\xi \tag{5}$$

The timing hypothesis test depends critically on the accuracy of the receiver's internal oscillator because the latter provides a reference for measuring the promptness of the incoming signal. Thus, somewhat counterintuitively, the receiver must already have an accurate estimate of time, and know its estimate to be accurate, if it is to validate the promptness of an incoming timing signal. Note that timing consistency alone cannot detect spoofing attacks in cases where the spoofed signal's delay remains below γ_ν. Thus, timing consistency is necessary but not sufficient for timing authentication of security-enhanced GNSS signals; it must be combined with other tests to ensure a high probability of spoofing detection.

VI. SCER Detector

The SCER detector is a hypothesis test at the physical layer to detect if the security code arrived intact and promptly. This test takes the form of a correlation between the incoming signal and a locally-generated signal replica that measures the promptness and accuracy of the incoming signal relative to the receiver's local clock. The full derivation and performance evaluation of the SCER detector is in [10]; a summary is offered here.

Let $\boldsymbol{s} = [s_{l_m}, s_{l_m+1}, \ldots, s_{l_m+N-1}]^T$ be a realization of the vector of N security-code chip-level statistics for start index l_m. Here, each element of $\boldsymbol{s}$ is a weighted correlation of the received signal Y_k with the code-carrier replica s_k and a locally-generated copy of the lth security code. The weighting function emphasizes more heavily the samples of the security code that immediately follow a security code chip boundary, because this is the time when the spoofer's estimate $\hat{w}_{k-d}$ is most uncertain and, thus, the authentic and spoofed signals are most easily distinguishable. After some manipulations on $\boldsymbol{s}$ to form $L(\boldsymbol{s})$, the detection test takes the form:

$$L(\boldsymbol{s}) \underset{H_0}{\overset{H_1}{\gtrless}} \gamma_L \tag{6}$$

The distribution of $L(\boldsymbol{s})$, $p_{L|H_j}(\xi|H_j)$ for $j = 0, 1$, is distributed as a non-central chi-square distribution with N degrees of freedom and non-centrality parameter λ_j. Given $p_{L|H_j}(\xi|H_j)$ for $j = 0, 1$, the threshold γ_L can be chosen to satisfy a pre-determined probability of false alarm $P_{F,L}$ by solving for γ_L in

$$P_{F,L} = \int_{\gamma_L}^{\infty} p_{L|H_0}(\xi|H_0)d\xi \tag{7}$$

A corresponding probability of detection $P_{D,L}$ is

$$P_{D,L} = \int_{\gamma_L}^{\infty} p_{L|H_1}(\xi|H_1)d\xi \tag{8}$$

One assumptions of the SCER detector is that the spoofed signals power advantage is no more than 4 dB greater than the authentic signals. This leads to the next necessary component of security-enhanced GNSS signal authentication.

VII. Total In-Band Power Monitor

During a spoofing attack against a security-enhanced GNSS signal, an admixture of authentic and spoofed signals are present (c.f., Eqs. 2 and 3), which will increase the measured in-band signal power P_T. The purpose of this detector is to monitor the nominal in-band power levels and detect when additional power is present due to spoofed signals, thereby limiting the power advantage of the spoofer.

Consider the following hypothesis pair, which models P_T as measured by a defender's front-end:

$$H_0 : P_T = P_A + N_0 B, \tag{9a}$$
$$H_1 : P_T = P_A + P_S + N_0 B \tag{9b}$$

Here, $P_A = \sum_i P_{A,i}$ is the total received signal power from each authentic signal $P_{A,i}$, $P_S = \sum_i P_{S,i}$ is the total received signal power from each spoofed signal $P_{S,i}$, N_0 is the one-sided noise power density at the low-noise amplifier (LNA), and B is the one-sided LNA filter bandwidth.

A spoofer seeking to maximize the likelihood of a successful attack will set its power advantage factor $\eta \equiv P_S/P_A > 1$ since higher values of η reduce the defender's probability of detecting a spoofing attack (c.f., [10], Sec. IV.B). Applying this notation to the hypothesis pair in Eq. 9 yields

$$H_0 : P_T = P_A + N_0 B, \tag{10a}$$
$$H_1 : P_T = P_A(1+\eta) + N_0 B \tag{10b}$$

Given the densities $p_{P_T|H_j}(\xi|H_j)$ for $j = 0, 1$, an optimal detection test exists:

$$P_T \underset{H_0}{\overset{H_1}{\gtrless}} \gamma_{P_T} \tag{11}$$

The threshold γ_{P_T} corresponding to a specific probability of false alarm P_{F,P_T} can be computed:

$$P_{F,P_T} = \int_{\gamma_{P_T}}^{\infty} p_{P_T|H_0}(\xi|H_0) d\xi \tag{12}$$

A corresponding probability of detection P_{D,P_T} is

$$P_{D,P_T} = \int_{\gamma_{P_T}}^{\infty} p_{P_T|H_1}(\xi|H_1) d\xi \tag{13}$$

In practice, computing analytical forms of $p_{P_T|H_j}(\xi|H_j)$ for $j = 0, 1$ for the detection test of Eq. 11 is intractable because η has no determinable distribution and N_0 can vary widely depending on the number and time-varying magnitudes of natural and man-made interference sources that contribute to T_I. Given these difficulties, a more modest goal for the in-band signal power test is sought.

Because the SCER detector assumes that $\eta \leq \eta_{\max}$, the modest goal of the operational in-band signal power detection test is to limit $\eta \leq \eta_{\max}$ so that values of $\eta > \eta_{\max}$ result in the measured P_T exceeding γ_{P_T} for an acceptable P_{F,P_T}. A value of γ_{P_T} that meets these goals can be derived based on historical atmospheric data from [17]. In addition, so-called personal privacy devices (i.e., jammers) are becoming increasingly prevalent. Statistics of these devices in [18] can further help set γ_{P_T}.

VIII. Probabilistic Framework

In the case of data message authentication, only the measurement $z = \mathbb{V}$ was necessary to determine the authenticity of $\{m, s\}$. In the case of signal authentication, the timing consistency, SCER, and in-band power detector and error correction are required to authenticate the GNSS signal. Under the probabilistic framework for cryptographic GNSS signal authentication, the measurement incorporates all of the statistics:

$$\boldsymbol{z} = [\overline{\mathbb{V}} \wedge E, \nu, L, P_T]^T \tag{14}$$

Given $\boldsymbol{z}$, one can consider the joint probability distribution $p_{\boldsymbol{z}|H_j}(\boldsymbol{\xi}|H_j)$ for $j = 0, 1$ and form the appropriate tests based on the density function. In this case, the system-wide probability of false alarm P_F is

$$P_F = \int_{\gamma}^{\infty} p_{\boldsymbol{z}|H_0}(\boldsymbol{\xi}|H_0) d\boldsymbol{\xi} \tag{15}$$

for a given γ. A corresponding system-wide probability of detection P_D is

$$P_D = \int_{\gamma}^{\infty} p_{\boldsymbol{z}|H_1}(\boldsymbol{\xi}|H_1) d\boldsymbol{\xi} \tag{16}$$

The probabilistic framework for signal authentication offered here illustrates how the intrinsic security of signal authentication is much weaker than that of data message authentication. The security depends on multiple detection tests at several network layers (i.e., sub-physical, physical, and presentation layers) each with their own probabilities of detection and false alarm. Furthermore, the system-wide P_D and P_F are set subject to a security risk assessment unique to individual users and scenarios.

A. Combination with Non-Cryptographic Techniques

The statistics that represent the necessary conditions for security-enhanced GNSS signal authentication can be readily coupled with other non-cryptographic statistics in a generalization probabilistic framework. Non-cryptographic techniques have been proposed that examine incoming signal statistics of Y_k for distortions that are present during a spoofing attack [12]. One example is the complex early-minus-late tap difference D. To combine this statistic with the cryptographic statistics in Eq. 14, D is simply appended to $\boldsymbol{z}$:

$$\boldsymbol{z} = [\overline{\mathbb{V}} \wedge E, \nu, L, P_T, D]^T \tag{17}$$

Then, a new characterization of $p_{\boldsymbol{z}|H_j}(\boldsymbol{\xi}|H_j)$ can be computed either analytically or empirically.

B. Characterizing the Joint Probability Distribution

The success of this probabilistic approach to GNSS signal authentication hinges on the correct characterization of $p_{\boldsymbol{z}|H_j}(\boldsymbol{\xi}|H_j)$. Thus far, only two hypotheses were considered: the null hypothesis of no spoofing, and the alternative hypothesis of spoofing. In practice, additional hypotheses need to be tested. For example, multipath causes statistical variations similar to spoofing [19]. If the spoofing and multipath hypothesis are indistinguishable then a high false alarm rate exists

[12]; hence, a multipath hypothesis is necessary to reduce false alarm rates between spoofing and multipath. Thus, three hypothesis will each need to be characterized.

Characterizing $p_{\boldsymbol{z}|H_0}(\boldsymbol{\xi}|H_0)$ under the null hypothesis H_0 is amenable to an analytical solution assuming the thermal noise N_k takes on a Gaussian distribution. Characterizing $p_{\boldsymbol{z}|H_1}(\boldsymbol{\xi}|H_1)$ under the multipath hypothesis H_1 is suited to a combined analytical and empirical approach. Multipath can be modeled analytically [20] but the combinations of real-world recordings with a theoretical analysis will offer a better characterization of $p_{\boldsymbol{z}|H_1}(\boldsymbol{\xi}|H_1)$ than analysis alone. Finally, characterizing $p_{\boldsymbol{z}|H_2}(\boldsymbol{\xi}|H_2)$ under the spoofing hypothesis H_2 is only possible empirically, and even then, only partially. The number of spoofing attack vectors is enormous; only a subset can be considered. Empirical analysis will leverage the Texas Spoofing Test Battery [21]. This collection of recorded spoofing scenarios is available for evaluating civil Global Positioning System signal authentication techniques and offers a wide-range of potential spoofing attacks with which to generate $p_{\boldsymbol{z}|H_2}(\boldsymbol{\xi}|H_2)$.

IX. Conclusion and Future Work

This paper has illustrated why data message authentication techniques alone are not sufficient for timing assurance in the context of a security-enhanced Global Navigation Satellite System (GNSS) signal. Instead, a probabilistic framework that combines cryptography and signal processing detection tests at multiple network layers is necessary to capture the subtleties and the weaker intrinsic security of signal authentication. Future work will characterize the joint distribution $p_{\boldsymbol{z}|H_j}(\boldsymbol{\xi}|H_j)$ under M-ary hypothesis testing for a combined cryptographic and non-cryptographic anti-spoofing approach.

Acknowledgments

The authors thank the members of The University of Texas at Austin Radionavigation Laboratory and the Embedded Signal Processing Laboratory. K. Wesson was supported by the Department of Defense through the National Defense Science and Engineering Graduate Fellowship.

References

[1] T. E. Humphreys, 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 ION GNSS Meeting*. Savannah, GA: Institute of Navigation, 2008.

[2] D. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[3] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proceedings of the ION GNSS Meeting*. Nashville, TN: Institute of Navigation, 2012.

[4] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[5] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[6] M. Luk, A. Perrig, and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication," in *Proceedings of Fourth ACM workshop on security of ad hoc and sensor networks*, Alexandria, VA, October 2006, pp. 147–156.

[7] NIST, "Digital signature standard," National Institute of Standards and Technology, FIPS PUB 186-3, June 2009.

[8] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.

[9] P. Papadimitratos and A. Jovanovic, "Protection and fundamental vulnerability of GNSS," in *IEEE Int. Workshop on Satellite and Space Communications*, 2008, pp. 167–171.

[10] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2011, to be published; available at http://radionavlab.ae.utexas.edu/detstrat.

[11] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, 2013, to be published; available at http://web.mae.cornell.edu/psiaki/.

[12] K. Wesson, D. Shepard, J. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[13] P. Y. Montgomergy, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the ION ITM*, Anaheim, CA, Jan. 2009.

[14] NIST, "Recommendation for key management—Part I: General (revised)," National Institute of Standards and Technology, SP 800-57, March 2007.

[15] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Wiley, 2005.

[16] H. Zimmerman, "OSI reference model—the ISO model of architecture for open systems interconnection," *IEEE Transactions on Communications*, vol. COM-28, no. 4, pp. 425–432, April 1980.

[17] G. Nita, D. Gary, L. Lanzerotti, and D. Thomson, "The peak flux distribution of solar radio bursts," *The Astrophysical Journal*, vol. 570, p. 423, 2002.

[18] R. Mitch, R. Dougherty, M. Psiaki, S. Powell, B. O'Hanlon, J. Bhatti, and T. Humphreys, "Signal characteristics of civil GPS jammers," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2011.

[19] R. D. J. van Nee, "Spread-spectrum code and carrier synchronization errors caused by multipath and interference," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 29, no. 4, pp. 1359–1365, Oct. 1993.

[20] P. Closas, C. Fernandez-Prades, and J. A. Fernandez-Rubino, "A Bayesian approach to multipath mitigation in GNSS receivers," *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 4, pp. 695–706, Aug. 2009.

[21] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proceedings of the ION GNSS Meeting*. Nashville, Tennessee: Institute of Navigation, 2012.