Detection Strategy for Cryptographic GNSS Anti-Spoofing

Todd E. Humphreys

Abstract—**A strategy is presented for detecting spoofing attacks against cryptographically-secured Global Navigation Satellite System (GNSS) signals. The strategy is applicable both to military Global Positioning System signals and to proposed security-enhanced civil GNSS signals, whose trustworthiness is increasingly an issue of national security. The detection strategy takes the form of a hypothesis test that accounts for the statistical profile of a replay-type spoofing attack. A performance and robustness evaluation demonstrates that the detection test is both powerful and tolerant of some uncertainty in the threat model. The test is validated by experiments conducted on a spoofing testbed.**

Keywords: Cryptographic anti-spoofing, GNSS security, GNSS spoofing detection, GNSS authentication.

I. Introduction

Spoofing is no longer a concern only for military Global Positioning System (GPS) users. Spoofing attacks, in which counterfeit GPS signals are generated for the purpose of manipulating a target receiver's reported position and time, have been demonstrated with low-cost commercial equipment against a wide variety of civil GPS receivers [1], [2]. The growing dependence of critical civil infrastructure on GPS—for transportation, communication, energy distribution, and banking and finance—makes civil GPS spoofing not only an economic and safety threat but also a matter of national security [3]–[5].

Military GPS signals have long been protected against spoofing by a cryptographic anti-spoofing technique whereby a binary chipping sequence that is only predictable to authorized users modulates the GPS carrier [6]. A growing literature recommends similar techniques be applied to protect civil GPS signals [7], [8] and other Global Navigation Satellite System (GNSS) signals [9], [10]. As opposed to anti-spoofing techniques that depend on accurate inertial measurements [11] or multiple antennas [12], cryptographic spoofing defenses are attractive because they can be implemented without additional hardware. Navigation message authentication (NMA), the insertion of a public-key digital signature into the low-rate (e.g., 50 Hz) civil navigation message stream, is viewed as a practical near-term approach to securing civil GNSS signals [7]–[9], [13], [14].

For cryptographic techniques to be effective against GNSS spoofing, a proper detection test must be implemented within each secured receiver. What little has been written on this subject in the open literature has observed that spoofing can be detected as a drop in the correlation power over an encrypted interval [7]. But this simple detection technique is far from optimal against an attack in which the spoofer attempts to estimate, manipulate, and replay a cryptographically-secured GNSS signal in real-time. It is especially ineffective for NMA-secured signals, which manifest no detectable drop in the standard correlation power under a replay attack. What is needed is an open and thorough statistical treatment of the spoofing detection problem for cryptographically-secured GNSS signals.

This paper makes three principal contributions. First, it develops a model for sophisticated replay-type spoofing attacks against security-enhanced GNSS signals. Second, it derives a unified near-optimal detection strategy for such attacks. The strategy is applicable to both low-rate cryptographic techniques such as NMA and high-rate techniques such as legacy military GPS Y-code encryption. Third, this paper demonstrates that with a proper detection test NMA is effective for anti-spoofing. This result, which has not been previously established in the open literature, is significant given the immediate need for a practical defense against civil GNSS spoofing.

II. Generalized Model for Security-Enhanced GNSS Signals

Consider the following model for the digital signal exiting the radio frequency (RF) front end of a GNSS receiver:

$$Y_k = w_k c_k \cos(2\pi f_{IF} t_k + \theta_k) + N_k \tag{1}$$

Here, at sample index k, w_k is a ±1-valued security code with chip length T_w, c_k is a known ±1-valued spreading (ranging) code with chip length T_c, t_k is receiver time, f_{IF} is the intermediate value of the downmixed carrier frequency, θ_k is the beat carrier phase, and N_k is a sequence of independent, identically distributed zero-mean Gaussian noise samples with variance σ^2 that model the effects of thermal noise and interfering signals. The variance σ^2 and the unity signal amplitude imply a carrier-to-noise ratio

$$C/N_0 = \frac{1}{4\sigma^2 T_s} \tag{2}$$

where T_s is the sampling interval.

This model considers only a single GNSS signal corresponding to a unique combination of spreading code and carrier frequency. A single-signal model is appropriate because although a spoofer may generate counterfeit replicas of an entire ensemble of GNSS signals, the spoofing detection

Author's address: Department of Aerospace Engineering, The University of Texas at Austin, Austin TX, 78712, Email: (todd.humphreys@mail.utexas.edu).

problem can be treated at the level of individual signals within the ensemble.

The spoofing detection problem involves two agents: the spoofer and the receiver it is targeting. The latter is simultaneously attempting to defend itself by detecting the spoofing attack. Hereafter, these two agents will be referred to as the spoofer and the defender.

For convenience, both the spoofer and defender will be assumed to have ideal clocks and to sample incoming signals simultaneously with sampling interval T_s. Thus, t_k will refer hereafter to true time at sample index k within both the spoofer and defender. The assumptions of ideal time and simultaneous sampling simplify the detection analysis without significantly altering the underlying statistics so long as the spoofer's front end bandwidth is at least as wide as the defender's.

The model in (1) differs from traditional sampled GNSS signal models (e.g., those presented in [15]) in two ways. First, the signal and noise have been normalized so that the modeled signal amplitude is unity. This normalization has no effect on C/N_0 but simplifies the notation of the detection problem. Second, the security code w_k has been substituted in place of the usual ± 1-valued navigation data sequence d_k. In fact, w_k subsumes rather than replaces d_k: w_k is a generalization of a binary modulating sequence carrying encryption or authentication codes that may be modulated by d_k or may be embedded within d_k.

The security code w_k can be classified as high rate or low rate by comparing its chip interval T_w to the coherent accumulation interval $T_a : 1 \leq T_a \leq 20$ ms typically applied in GNSS receivers. For a high-rate code $T_w \ll T_a$ whereas for a low-rate code $T_w \approx T_a$. The following specific examples will help clarify the definition of w_k.

1) Let (1) model a downmixed version of the GPS L1 or L2 P(Y) code signal. In this case, the security code is given by $w_k = d_k \tilde{W}_k$, where d_k is the legacy GPS navigation data and $\tilde{W}_k$ is the GPS W code, unpredictable to unauthorized users, which modulates the P code (represented in this case by c_k) to form the Y code [16]. The security code in this case can be classified as high-rate because the chip length T_w is the same as the chip length of the W code, or approximately 2 μs, which is much shorter than typical values of T_a.
2) Let (1) model a downmixed version of the modernized GPS L2 CM code signal. In this case, $w_k = d_k$, where d_k carries civil navigation (CNAV) formatted navigation data, which, as presently defined, are highly predictable but could be modified to include periodic unpredictable authentication messages, as proposed in [7], [8]. Insertion of periodic unpredictable authentication messages (e.g., digital signatures) into the GPS CNAV data stream is an example implementation of NMA. The security code in this case can be classified as low-rate because the chip length T_w is the same as the underlying navigation data stream before application of forward error correction, or $T_w = 40$ ms, which is close to typical values of T_a.

Encryption codes such as the GPS W code serve a dual purpose: they both authenticate and deny unauthorized access to the signals they encrypt. Authentication codes, on the other hand, are single-purpose: they assure the user that the signals they modulate originate with the expected GNSS but they do not deny signal access. Accordingly, the authentication codes proposed for civil GNSS in [7]–[9] modulate the underlying signals only intermittently and would not prevent a receiver that ignores them from tracking the signals they modulate.

Whether it represents an encryption or authentication code, the crucial feature of the security code w_k in the context of spoofing detection is that it contains segments of chips that can be modeled as perfectly random, and therefore unpredictable, from the point of view of a would-be spoofer.

III. Security Code Estimation and Replay Attack

A. Overview

The unpredictability of the security code is an obstacle for a would-be spoofer. A simple spoofing technique such as discussed in [1] relies on the known signal structure of the GPS L1 C/A signal and the near-perfect predictability of its navigation data stream. However, if a GNSS signal is security enhanced so that segments of its spreading code or navigation data are unpredictable, then the spoofer in [1] cannot perfectly match its counterfeit signals chip-for-chip to the authentic signals. The same holds true for any other spoofing technique except for zero-delay meaconing, which is the recording and instantaneous playback of an entire block of RF spectrum containing an ensemble of GNSS signals [3], [8]. Meaconing is, however, a strongly constrained type of spoofing: the constituent GNSS signals in a meaconer's transmitted ensemble cannot be manipulated independently but instead must all be delayed equivalently. In view of this, a would-be spoofer has an incentive to seek a more flexible technique.

A spoofer could, of course, ignore the broadcast security codes altogether, filling in dummy values for w_k, but such a scheme is easily detected. In an attack against a GNSS signal modulated by a low-rate security code such as proposed in [8], [9], the dummy w_k values would fail the cryptographic validation test. Against a high-rate security code, the dummy w_k values would yield zero average power when correlated with the true w_k sequence [7], [9].

A strategy more flexible than meaconing and more effective than dummy-value-filling is for the spoofer to estimate the security code w_k as best it can in real time for each GNSS signal it intends to spoof. In this scheme, as the spoofer obtains an estimate of each successive security chip, it immediately injects this estimate into a signal replica generator primed with up-to-date spreading code and carrier replicas. This is the security code estimation and replay (SCER) attack. The resulting signal, as it exists within the spoofer before scaling, up-mixing, and rebroadcast, is modeled as

$$\hat{y}_k = \hat{w}_k c(\hat{\tau}_k) \cos(2\pi f_{IF} t_k + \hat{\theta}_k) \tag{3}$$

where $\hat{w}_k$ is the security code estimate, $c(\hat{\tau}_k)$ is the known spreading code evaluated at the code offset estimate $\hat{\tau}_k$, $\hat{\theta}_k$ is the beat carrier phase estimate, and t_k is time, all evaluated at sample index k.

For received signals with moderate to high C/N_0, the code offset and phase estimates $\hat{\tau}_k$ and $\hat{\theta}_k$ produced by the spoofer's code and carrier tracking loops will be close to the true quantities. In any case, assuming $\hat{\tau}_k = \tau_k$ and $\hat{\theta}_k = \theta_k$ only favors the spoofer in the detection problem, which is consistent with a pessimistic defensive model. Accordingly, let the spoofing signal model be rewritten as

$$\hat{y}_k = \hat{w}_k c_k \cos(2\pi f_{IF} t_k + \theta_k) = \hat{w}_k s_k \tag{4}$$

where c_k and θ_k are as in (1) and $s_k \triangleq c_k \cos(2\pi f_{IF} t_k + \theta_k)$ has been introduced as an abbreviation.

It will be useful to distinguish SCER attack variations in terms of latency and w-code estimation strategy.

B. Latency

For a single GNSS signal corresponding to a particular satellite, the combined SCER-spoofing and authentic received signals can be modeled as

$$Y_k = \alpha \hat{w}_{k-d} s_{k-d} + w_k s_k + N_k \tag{5}$$

The first term on the right hand side of (5) represents the spoofing signal, with $\alpha \geq 1$ being the spoofing signal's amplitude advantage factor and $\hat{w}_{k-d}$ being the security code estimate arriving with a delay of d samples relative to the authentic security code w_k. The second and third terms on the right-hand side of (5) represent the authentic signal and receiver noise, as described previously.

The delay d can be modeled as the sum $d = p + e$ of a processing and transmission delay p and an estimation and control delay e. The former represents the required signal processing and propagation time and does not contribute to better estimates of the security code chips. The latter represents an additional delay imposed by the spoofer to improve its estimate of the security code chip values and to control the relative phasing of the spoofing signals so as to impose spoofer-defined position and timing offsets on the defender.

Consistent with a pessimistic model, in this paper p is assumed to be zero and the spoofer's estimate $\hat{w}_{k+d}$, which arrives at the defender's RF front end at time t_{k+d}, is assumed to enjoy the benefit of all data in the authentic security code w_k up to time t_{k+d}. Clearly, a spoofer with zero processing and transmission delay is not realistic; nonetheless, the $d = e$ assumption provides a useful limiting case against which spoofing detection strategies can be benchmarked.

1) Zero-Latency SCER Attack: In the zero-latency SCER attack, the spoofer is assumed to rebroadcast a counterfeit signal that is initially exactly aligned with its authentic signal counterpart in the defender's RF front end. Thus, $d = 0$ in (5) and the security code estimate $\hat{w}_k$ that arrives at time t_k is based on data in w_k up to t_k.

2) Non-Zero-Latency SCER Attack: In the non-zero-latency SCER attack, the spoofer is assumed to rebroadcast a counterfeit signal that arrives at the defender's RF front end with a delay of $d > 0$ samples ($dT_s > 0$ seconds) relative to the authentic signal. Any significant total delay dT_s in the spoofer's counterfeit signal would be immediately obvious to a defender that has been continuously tracking the authentic signal since before the beginning of the spoofing attack [5], [9]. Therefore, the spoofer's strategy in the non-zero-latency SCER attack will be to break this continuity by jamming or blocking the authentic signals for a interval of time before initiating the spoofing attack, thus widening the defender's timing uncertainty, or "window of acceptance" [7], [8], [17]. The required duration of this signal-denial interval depends on the desired delay dT_s and on the assumed stability of the defender's clock (for stationary defenders). As an example, for the low-cost temperature-compensated crystal oscillators typical in commercial GNSS equipment, in-the-field stability is approximately one part in 10^7. Thus, to widen the defender's time uncertainty beyond one GPS W-code chip length ($T_w \approx 2$ μs) would require approximately 20 seconds of jamming or blockage.

When the total delay is greater than or equal to the security code chip length (i.e., $dT_s \geq T_w$), then analysis of the non-zero-latency SCER attack becomes similar to analysis of so-called Z-tracking used in survey- and science-grade GPS receivers [16].

C. Security Code Estimation

Consider the signal model of (1) from the perspective of a spoofer attempting to estimate the value of each chip in the security code w_k. Let the variance of the spoofer's independent Gaussian noise samples N_k be σ_s^2. In keeping with a model that favors the spoofer, assume that the spoofer has perfect knowledge of the signal structure and can generate a local replica s_k that is perfectly code- and carrier-phase aligned with the code and carrier product of the received signal. Under these conditions, which describe ideal coherent detection, the optimal security code chip estimator structure is a matched filter [18], [19]. Let $W_l \in \{-1, 1\}$ represent the value of lth security code chip and let k_l represent the index of the first sample within the lth chip. Then the output of the matched filter after the first n samples within the lth chip have been processed is

$$Z_l(n) = \frac{2}{n} \sum_{k=k_l}^{k_l+n-1} Y_k s_k \tag{6}$$

for $n = 1, 2, ..., \lfloor T_w/T_s \rfloor$. Due to the linearity of the matched filter operation, $Z_l(n)$ is Gaussian distributed with mean $E[Z_l(n)] = W_l$ and variance $\sigma_Z^2(n) = 2\sigma_s^2/n$. The matched filter output $Z_l(n)$ can therefore be modeled as

$$Z_l(n) = W_l + N_l(n), \quad N_l(n) \sim \mathcal{N}\left(0, \sigma_Z^2(n)\right) \tag{7}$$

In this statistical model, the effect of the double-frequency term created by the product $Y_k s_k$ is assumed to be negligible, which favors the spoofer in the detection problem.

Another way of viewing $Z_l(n)$ is as a sufficient statistic for estimating W_l. In other words, $Z_l(n)$ summarizes the information in $\{Y_k : k_l \leq k < k_l + n\}$ that is relevant to estimating W_l [20]. Given the first n samples in W_l, the optimal estimate of W_l is a function of $Z_l(n)$ that depends on the chosen optimality criterion. Three well-established criteria will be considered: maximum likelihood (ML), maximum a posteriori (MAP), and minimum mean square error (MMSE)

[21]. Estimates based on these criteria can be related to $Z_l(n)$ as shown in Fig. 1.

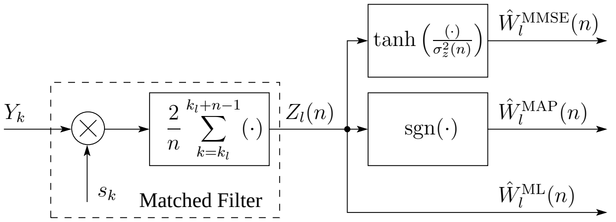
Y_k
$\frac{2}{n}\sum_{k=k_l}^{k_l+n-1}(\cdot)$
s_k
Matched Filter
$Z_l(n)$
$\tanh\left(\frac{(\cdot)}{\sigma_z^2(n)}\right)$
$\hat{W}_l^{\mathrm{MMSE}}(n)$
$\mathrm{sgn}(\cdot)$
$\hat{W}_l^{\mathrm{MAP}}(n)$
$\hat{W}_l^{\mathrm{ML}}(n)$

Fig. 1. Estimator structure for the minimum mean square error (MMSE), maximum a posteriori (MAP), and maximum likelihood (ML) estimates of the lth security code chip W_l. All estimates are based on the sufficient statistic $Z_l(n)$.

1) Maximum Likelihood Estimate of W_l: The ML estimate $\hat{W}_l^{\mathrm{ML}}(n)$ is the value of W_l that makes $Z_l(n)$ appear most likely; that is, it maximizes the probability distribution of $Z_l(n)$ conditioned on W_l:

$$\hat{W}_l^{\mathrm{ML}}(n) = \arg\max_{W_l} p\left(Z_l(n)|W_l\right) \tag{8}$$

The distribution $p\left(Z_l(n)|W_l\right) = \mathcal{N}(Z_l(n); W_l, \sigma_Z^2(n))$ is maximized by choosing $\hat{W}_l^{\mathrm{ML}}(n) = Z_l(n)$, where $\mathcal{N}(x; \mu, \sigma^2)$ denotes the functional form of a Gaussian distribution with independent variable x, mean μ, and variance σ^2. Note that because the ML estimate operates without any prior constraint on the value of W_l, $\hat{W}_l^{\mathrm{ML}}(n)$ can take on any real value. It will be shown later on that the ML estimate's inability to incorporate the constraint $W_l \in \{-1, 1\}$ makes it typically the weakest of the three estimates in terms of minimizing the probability of detection.

The mean and variance of $\hat{W}_l^{\mathrm{ML}}(n)$ are the same as those given previously for $Z_l(n)$. Also useful for later computations will be the second moment

$$E[(\hat{W}_l^{\mathrm{ML}}(n))^2] = 1 + \sigma_Z^2(n) \tag{9}$$

2) Maximum A Posteriori Estimate of W_l: The MAP estimate $\hat{W}_l^{\mathrm{MAP}}(n)$ is the value of W_l that maximizes the *a posteriori* distribution of W_l conditioned on $Z_l(n)$:

$$\begin{aligned}\hat{W}_l^{\mathrm{MAP}}(n) &= \arg\max_{W_l} p\left(W_l|Z_l(n)\right) \\ &= \arg\max_{W_l} \left[p\left(Z_l(n)|W_l\right)p(W_l)\right]\end{aligned} \tag{10}$$

Assuming the security code chip values come from a binary symmetric source, the *a priori* distribution $p(W_l)$ can be written

$$p(W_l) = \tfrac{1}{2}\delta(W_l + 1) + \tfrac{1}{2}\delta(W_l - 1) \tag{11}$$

where $\delta(x)$ is the Dirac delta function. As opposed to the ML estimate, the MAP estimate, by way of the prior distribution $p(W_l)$, enforces the constraint $W_l \in \{-1, 1\}$. Given that $p(W_l)$ is only nonzero at discrete values of W_l, it is convenient to express $\hat{W}_l^{\mathrm{MAP}}(n)$ in terms of a probability mass function:

$$\hat{W}_l^{\mathrm{MAP}}(n) = \arg\max_{W_l \in \{-1,1\}} P\left(W_l|Z_l(n)\right) \tag{12}$$

This rule is equivalent to choosing $\hat{W}_l^{\mathrm{MAP}}(n) = \mathrm{sgn}(Z_l(n))$, by which one can see that the MAP criterion leads to a "hard" decision about the value of W_l. It will be shown later on that in many cases the MAP estimate is the spoofer's best choice for minimizing the probability of detection.

Note that due to the $\mathrm{sgn}(\cdot)$ nonlinearity, the statistics of $\hat{W}_l^{\mathrm{MAP}}(n)$ are not Gaussian. $\hat{W}_l^{\mathrm{MAP}}(n)$ can be modeled as

$$\hat{W}_l^{\mathrm{MAP}}(n) = \begin{cases} W_l & \text{w.p.} \quad 1 - p_e(n) \\ -W_l & \text{w.p.} \quad p_e(n) \end{cases} \tag{13}$$

where $p_e(n) = \frac{1}{2}\mathrm{erfc}\left(\sqrt{n}/2\sigma_s\right)$ is the error probability and $\mathrm{erfc}(\cdot)$ is the complementary error function. From this, one can obtain the mean and second moment of $\hat{W}_l^{\mathrm{MAP}}(n)$ as

$$E[\hat{W}_l^{\mathrm{MAP}}(n)] = W_l(1 - 2p_e(n)) \tag{14}$$

$$E[(\hat{W}_l^{\mathrm{MAP}}(n))^2] = 1 \tag{15}$$

3) Minimum Mean Square Error Estimate of W_l: The MMSE estimate $\hat{W}_l^{\mathrm{MMSE}}(n)$ is chosen to minimize the mean square error conditioned on $Z_l(n)$:

$$\hat{W}_l^{\mathrm{MMSE}}(n) = \arg\min_{\hat{W}_l} E\left[(\hat{W}_l - W_l)^2|Z_l(n)\right] \tag{16}$$

The solution to (16) is the conditional mean $E[W_l|Z_l(n)]$, which can be expressed as

$$\begin{aligned}E[W_l|Z_l(n)] =& P(W_l = 1|Z_l(n)) - P(W_l = -1|Z_l(n)) \\ =& 2P(W_l = 1|Z_l(n)) - 1 \\ =& \tanh\left(Z_l(n)/\sigma_Z^2(n)\right)\end{aligned}$$

where use has been made of the constraint

$$P(W_l = -1|Z_l(n)) = 1 - P(W_l = 1|Z_l(n))$$

and the fact that

$$P(W_l = 1|Z_l(n) = z) = \frac{1}{1 + e^{-2z/\sigma_Z^2(n)}}$$

Like the MAP estimator, the MMSE estimator incorporates the prior constraint $W_l \in \{-1, 1\}$; however the $\tanh(\cdot)$ nonlinearity allows $\hat{W}_l^{\mathrm{MMSE}}(n)$ to take on any real value in the domain $(-1, 1)$. One can show that the MMSE estimate minimizes the reduction in C/N_0 seen by the defender when $dT_s = T_w$. The proof of this is similar to the proof given in [16] that the $\tanh(\cdot)$ nonlinearity minimizes the squaring loss in so-called Z-tracking receivers. Hence, one might expect the MMSE estimate to be the most effective of the three methods considered for minimizing the probability of detection. However, it will be shown later on that this is not the case for all values of T_w.

As for $\hat{W}_l^{\mathrm{MAP}}(n)$, the MMSE estimator's nonlinearity causes the statistics of $\hat{W}_l^{\mathrm{MMSE}}(n)$ to be non-Gaussian, with mean and second moment given by

$$E[\hat{W}_l^{\mathrm{MMSE}}(n)] = \int_{-\infty}^{\infty} \tanh\left(\frac{z}{\sigma_Z^2(n)}\right)\mathcal{N}\left(z; W_l, \sigma_Z^2(n)\right)dz \tag{17}$$

$$E[(\hat{W}_l^{\mathrm{MMSE}}(n))^2] = \int_{-\infty}^{\infty} \tanh^2\left(\frac{z}{\sigma_Z^2(n)}\right)\mathcal{N}\left(z; W_l, \sigma_Z^2(n)\right)dz \tag{18}$$

It should be noted that, due to the summation in (6), $\hat{W}_l^{\mathrm{MMSE}}(n)$ is correlated along the index n. The same holds true for $\hat{W}_l^{\mathrm{ML}}(n)$ and $\hat{W}_l^{\mathrm{MAP}}(n)$.

IV. A Single-Chip Detection Statistic

The SCER-spoofing detection problem is best treated as a hypothesis test wherein one decides between the null hypothesis H_0 (no SCER attack underway) and the alternative hypothesis H_1 (SCER attack underway). A decision between the two hypotheses is based on samples Y_k from the GNSS RF front end taken over some range of k. To simplify the analysis, it is convenient to first consider a hypothesis test involving samples Y_k taken over the interval spanned by a single security code chip. Accordingly, this section develops a detection statistic S_l corresponding to the lth security code chip. The next section synthesizes a full detection statistic from a set of N single-chip statistics.

A. Single-Chip Hypothesis Test

Consider the following hypothesis pair, which models the samples Y_k output by the defender's RF front end during the interval spanned by the lth security code chip. The model is based on the received signal model in (1) and the spoofing signal model in (4):

$$H_0 : Y_k = W_l s_k + N_k, \tag{19a}$$

$$H_1 : Y_k = g\left[\alpha \hat{W}_l(n_{lk}) s_k + N_k\right] \tag{19b}$$

Here, $k = k_l, k_l+1, ..., k_l+M-1$, where M is the number of samples in the lth security code chip (M is approximated as constant from chip to chip). Under hypothesis H_0, the received signal is an authentic GNSS signal with security code chip value W_l and independent noise samples distributed as $N_k \sim \mathcal{N}(0, \sigma_r^2)$, where σ_r^2 corresponds to $(C/N_0)_r$, the authentic signal's C/N_0 as seen by the defender, with σ_r^2 related to $(C/N_0)_r$ as in (2). Under hypothesis H_1, the received signal is a spoofer-generated counterfeit signal modulated by an estimate $\hat{W}_l(n_{lk})$ of the lth security code chip. The type of the estimate, whether ML, MAP, or MMSE, will be specified as necessary. The index n_{lk} represents the number of samples that contribute to the spoofer's estimate of W_l, just as does the index n in (6); n_{lk} can be expressed in terms of the index of the first sample within the lth chip, k_l, and the spoofer's presumed estimation delay d:

$$n_{lk} = \min(k + d - k_l + 1, M) \tag{20}$$

Note that this expression for n_{lk} assumes that the spoofer's estimate of W_l is based on at least one sample, since when $k = k_l$ and $d = 0$, $n_{lk} = 1$. This assumption is consistent with the zero-latency SCER attack model introduced previously, which contemplates a spoofer with zero processing and transmission delay. The $\min(\cdot)$ function is required in (20) because no estimate of W_l can benefit from more than the total number of samples within the interval spanned by W_l. The following subsections define the coefficients α and g.

1) The Amplitude Factor α: For simplicity, the received signal under H_0 is modeled as having unity amplitude. As a consequence, the authentic received signal power averaged over the lth security code chip is

$$P_a = \frac{1}{M} \sum_{k=k_l}^{k_l+M-1} W_l^2 s_k^2 \approx \frac{1}{2}$$

Ignoring for now the gain factor g, the average received signal power over the same interval for the H_1 hypothesis is

$$P_s = \frac{1}{M} \sum_{k=k_l}^{k_l+M-1} \alpha^2 E[\hat{W}_l^2(n_{lk})] s_k^2$$

In the computation of P_s, $\hat{W}_l(n_{lk})$ is treated as a random variable whose mean square value $E[\hat{W}_l^2(n_{lk})]$ will be unity for the MAP estimator [Eq. (15)] but will deviate from unity for the ML and MMSE estimators [Eqs. (9) and (18)], with the greatest deviation at small values of n_{lk}. Thus, without compensation, the ML or MMSE estimators would result in the spoofing signal having an implicit power advantage or disadvantage compared to the authentic signal. For comparison of different spoofing techniques, it is convenient to explicitly model the spoofer's power advantage by defining the factor $\eta \triangleq P_s/P_a$. The power advantage is enforced by defining the amplitude factor α such that $\alpha^2 \triangleq \eta / P_{\hat{W}_l}$, with

$$P_{\hat{W}_l} = \frac{1}{M} \sum_{k=k_l}^{k_l+M-1} E[\hat{W}_l^2(n_{lk})]$$

By setting $\eta = 1$, one can model a SCER attack in which the spoofing and authentic signals have equivalent power, and by setting $\eta > 1$, one can model a situation in which the received spoofing signal is more powerful than the received authentic signal. A later section will analyze the tradeoffs involved, from the spoofer's perspective, in setting the value of η.

2) The Automatic Gain Control Factor g: To minimize distortion losses in the analog-to-digital conversion process, multibit-quantizing GNSS RF front ends route signals through an automatic gain controller (AGC) before quantization [15]. The AGC has the effect of maintaining the power level constant in the output sample train Y_k. In the model given by (19), this constant power level is assumed to be equal to $1/2 + \sigma_r^2$, which is the power in Y_k under the H_0. Thus, the AGC factor g under H_0 is assumed to be unity. Under H_1, the AGC factor becomes $g = (1/2 + \sigma_r^2)(\eta/2 + \sigma_r^2)^{-1}$ so that the power in Y_k under H_1 is also $1/2 + \sigma_r^2$. Hence, if $\eta > 1$, then $g < 1$. Inclusion of g in the hypothesis test model is necessary to properly account for the effect that increasing η has on the noise sample variance.

3) Remarks: The hypothesis test model in (19) invokes a significant assumption; namely, that under a spoofing attack only the counterfeit signal is present. This assumption is valid in cases where the spoofer blocks or otherwise nulls the authentic signals before transmitting its counterfeit replicas, which it can do in any one of the following ways: (1) injecting the spoofing signal directly into the defender's RF input, bypassing the antenna, (2) covering the defender's antenna with material that blocks RF energy at GNSS frequencies and transmitting its counterfeit signals beneath this cover, (3) transmitting at such a high spoofing power factor (e.g., $\eta > 3$) that the authentic signal is effectively eliminated by the automatic gain control in the defender's RF front end, or (4) intentionally transmitting a signal that nulls the authentic signal at the location of the defender's antenna, as described in [1].

The assumption is not valid, however, during the initial stage of an over-the-air, unobstructed, low-power, non-nulling attack, which may prove to be a common attack mode. In this case, an admixture of the counterfeit and authentic signals is received, with the authentic signal weaker than the spoofing signal but not entirely negligible during the initial stage of the attack when the signals are approximately code-phase aligned. At this stage a so-called vestigial signal spoofing defense such as discussed in [22] is a useful complement to a cryptographic defense. As the attack proceeds and the authentic and counterfeit correlation peaks separate, the model for H_1 in (19) becomes valid.

Neglecting the vestige of the authentic signal under H_1 favors the defender in the spoofing detection problem, which is an exception to the pessimistic defensive model generally adopted in this paper in which simplifying assumptions tend to favor the spoofer. But adequately modeling the envelope of interaction between the two signals would complicate the hypothesis model, and would, in all likelihood, demonstrate what might be expected: spoofing detection based on security codes is least powerful when the spoofing and authentic signals are approximately aligned and are similar in magnitude. Moreover, consideration of the centimeter-level accuracy required and experience with the spoofing testbed discussed in [23] suggests that it is difficult to generate spoofing signals that are carrier-phase aligned with their authentic counterparts from the perspective of the defender's RF front end. If the spoofer fails to achieve this alignment to within 1/6 of a carrier cycle (about 3 cm at the GPS L1 frequency) then the model in (19) becomes approximately valid because the in-phase vestige of the authentic signal is suppressed by more than 3 dB. In any case, the experimental results in Sec. VIII will demonstrate that the hypothesis model remains useful despite significant interaction between the authentic and spoofing signals under H_1.

B. An Optimal Single-Chip Statistic

Referring to the model in (19), let $\boldsymbol{Y}_l = [Y_{k_l}, Y_{k_l+1}, ..., Y_{k_l+M-1}]^T$ be a vector of samples taken over the lth security code chip. The optimum procedure for deciding between H_0 and H_1 compares a threshold value against the so-called likelihood ratio, or the ratio of the distribution of $\boldsymbol{Y}_l$ under H_1 to the distribution of $\boldsymbol{Y}_l$ under H_0, written as [19]

$$\Lambda(\boldsymbol{y}_l) = \frac{p_{\boldsymbol{Y}_l|H_1}(\boldsymbol{y}_l|H_1)}{p_{\boldsymbol{Y}_l|H_0}(\boldsymbol{y}_l|H_0)} \tag{21}$$

If $\hat{W}_l(n_{lk}) = \hat{W}_l^{\mathrm{ML}}(n_{lk})$, then $\boldsymbol{Y}_l$ is distributed as a Gaussian random vector under both the H_0 and H_1 hypotheses. On the other hand, if $\hat{W}_l(n_{lk}) = \hat{W}_l^{\mathrm{MMSE}}(n_{lk})$ or if $\hat{W}_l(n_{lk}) = \hat{W}_l^{\mathrm{MAP}}(n_{lk})$, then the the H_0 distribution of $\boldsymbol{Y}_l$ remains Gaussian but the H_1 distribution is non-Gaussian. Nonetheless, it can be shown that the Gaussian noise samples N_k cause the H_1 distribution of $\boldsymbol{Y}_l$ to be approximately Gaussian even for MMSE and MAP estimation under the following conditions: (1) the spoofing power factor η remains below about 3, and (2) the ratio of the defender's sample noise to the spoofer's sample noise σ_r^2/σ_s^2 is greater than about 0.8. Under these conditions the variance of the noise samples N_k is large relative to the variance of the signal term $\alpha\hat{W}_l(n_{lk})s_k$, and thus the statistics of Y_k are dominated by the Gaussian statistics of N_k. If condition (1) above is violated then the spoofer will be vulnerable to detection by an in-band power test, as will be discussed further in Section VI; if condition (2) is violated then the spoofer's estimate $\hat{W}_l(n_{lk})$ will be so inaccurate that the spoofer will be easily detected even if the detector structure assumes Y_k is Gaussian.

Given the above considerations, $\boldsymbol{Y}_l$ can be safely approximated as a Gaussian random vector under both H_0 and H_1 and for all security chip estimation strategies. With this approximation the log of the likelihood function in (21) reduces to a difference between two quadratic forms. Let the mean and covariance of $\boldsymbol{Y}_l$ under H_j be denoted as $\boldsymbol{\mu}_{lj}$ and $K_{lj},\ j = 0, 1$. Then the log likelihood ratio test can be written

$$\begin{aligned}\tilde{S}_l(\boldsymbol{y}_l) \triangleq \log\Lambda(\boldsymbol{y}_l) =& (\boldsymbol{y}_l - \boldsymbol{\mu}_{l0})^T K_{l0}^{-1}(\boldsymbol{y}_l - \boldsymbol{\mu}_{l0}) \\ &- (\boldsymbol{y}_l - \boldsymbol{\mu}_{l1})^T K_{l1}^{-1}(\boldsymbol{y}_l - \boldsymbol{\mu}_{l1}) \underset{H_0}{\overset{H_1}{\gtrless}} \tilde{\gamma}_l\end{aligned} \tag{22}$$

which is interpreted as "choose H_1 if the detection statistic $\tilde{S}_l(\boldsymbol{y}_l)$ exceeds the threshold $\tilde{\gamma}_l$; otherwise choose H_0." Here, $\boldsymbol{y}_l = [y_{k_l}, y_{k_l+1}, ..., y_{k_l+M-1}]^T$ is a realization of the observation vector $\boldsymbol{Y}_l$ containing a particular set of observed samples. When viewed as a random variable, $\tilde{S}_l(\boldsymbol{y}_l)$ is written $\tilde{S}_l(\boldsymbol{Y}_l)$. Given the probability distribution of $\tilde{S}_l(\boldsymbol{Y}_l)$ under H_0 and under H_1, the threshold $\tilde{\gamma}_l$ can be chosen to satisfy a pre-determined probability of false alarm P_F from which a corresponding probability of detection P_D can be calculated. It should be noted that, for a single-chip hypothesis test, P_D will be unacceptably low; hundreds of chip-level detection statistics must be combined to increase P_D beyond a satisfactory value, as discussed in the next section.

In the form shown in (22), the single-chip decision problem is equivalent to the general Gaussian problem treated in [20]. In the general case for which $\boldsymbol{\mu}_{l0} \neq \boldsymbol{\mu}_{l1}$ and $K_{l0} \neq K_{l1}$, expressions for the H_0 and H_1 distributions of $\tilde{S}_l(\boldsymbol{Y}_l)$ are not easily derived. Special cases of the problem lead to a simplification of (22). For example, when $\boldsymbol{\mu}_{l0} = \boldsymbol{\mu}_{l1}$ as is approximately true when $\hat{W}_l(n) = \hat{W}_l^{\mathrm{ML}}(n)$, then (22) can be expressed as a single quadratic form. But even in this case the distributions of $\tilde{S}_l(\boldsymbol{Y}_l)$ under H_0 and H_1 are cumbersome owing to the unequal variances of successive samples under H_1. This is true even though K_{l1} can be diagonalized by an orthogonal transformation of $\boldsymbol{Y}_l$.

C. A Sub-Optimal Single-Chip Statistic

To obtain tractable expressions for the detection statistic distributions, consider a simplification of (22). This simplification favors the spoofer by making the detection test sub-optimal; nonetheless, as will be shown later on, the simplified test will remain sufficiently powerful for good detection performance. As mentioned in Section III-C, the MMSE and MAP estimates of W_l incorporate the constraint $W_l \in \{-1, 1\}$ in their *a priori* distributions whereas the ML estimate does not. Consequently, it can be shown that the MAP and MMSE estimates tend to yield a lower probability of detection than the ML estimate under optimal detection conditions, which suggests that a spoofing defense should focus on the MAP and MMSE estimates. When these estimation strategies are assumed, one finds that the sensitivity of the test in (22) is driven primarily by the difference in the means $\boldsymbol{\mu}_{l0} - \boldsymbol{\mu}_{l1}$ as opposed to the difference in the covariance matrices $K_{l0} - K_{l1}$. The latter difference is small because both K_{l0} and K_{l1} are dominated by the statistics of the independent noise samples N_k under the two conditions mentioned above. Given this, it is reasonable to assume $K_{l1} \approx K_{l0} = \sigma_r^2 I_{M\times M}$. With this approximation the detection test in (22) can be rewritten as

$$\begin{aligned}\tilde{S}_l(\boldsymbol{y}_l) =& \frac{1}{\sigma_r^2}(\boldsymbol{y}_l - \boldsymbol{\mu}_{l0})^T(\boldsymbol{y}_l - \boldsymbol{\mu}_{l0}) \\ &- \frac{1}{\sigma_r^2}(\boldsymbol{y}_l - \boldsymbol{\mu}_{l1})^T(\boldsymbol{y}_l - \boldsymbol{\mu}_{l1}) \underset{H_0}{\overset{H_1}{\gtrless}} \tilde{\gamma}_l\end{aligned}$$

Multiplying by σ_r^2, canceling terms, rearranging, and absorbing constants into a new threshold γ_l yields a simplified single-chip detection test:

$$S_l(\boldsymbol{y}_l) = \boldsymbol{y}_l^T(\boldsymbol{\mu}_{l1} - \boldsymbol{\mu}_{l0}) \underset{H_0}{\overset{H_1}{\gtrless}} \gamma_l \tag{23}$$

Recognizing that

$$\boldsymbol{\mu}_{l0} = W_l[s_{k_l}, s_{k_l+1}, ..., s_{k_l+M-1}]^T$$

and that

$$\begin{aligned}\boldsymbol{\mu}_{l1} = g\alpha\big[&E[\hat{W}_l(n_{lk_l})]s_{k_l}, E[\hat{W}_l(n_{l(k_l+1)})]s_{k_l+1}, \\ &..., E[\hat{W}_l(n_{l(k_l+M-1)})]s_{k_l+M-1}\big]^T\end{aligned}$$

the detection statistic $S_l(\boldsymbol{y}_l)$ can be expressed as the sum

$$S_l(\boldsymbol{y}_l) = \sum_{k=k_l}^{k_l+M-1} y_k \beta(n_{lk}) W_l s_k \tag{24}$$

where $\beta(n) = g\alpha E[\hat{W}_l(n)]/W_l - 1$, or more properly its absolute value, plays the role of a weighting function in the correlation of the received samples y_k with W_l and s_k. Note that $\beta(n)$ depends on η, σ_s, d, and the assumed security code chip estimation strategy; thus, it changes according to the threat model. As can be seen in Fig. 2, for a zero-delay SCER attack $\beta(n)$, tends to weight most heavily the samples that immediately follow a chip transition in the security code sequence. This makes intuitive sense: the spoofing and authentic signals are most easily distinguished immediately following a security chip transition when the spoofer's estimate of W_l is least certain. As more time elapses the spoofer's estimate of W_l improves until the spoofing and authentic signals become practically indistinguishable. The tapering profile of $\beta(n)$ also implies that for low-rate security codes with long T_w it is not usually necessary to correlate against all M samples within a security code chip; instead, for computational savings, the correlation can be limited to a suitable $\bar{M} < M$ samples.

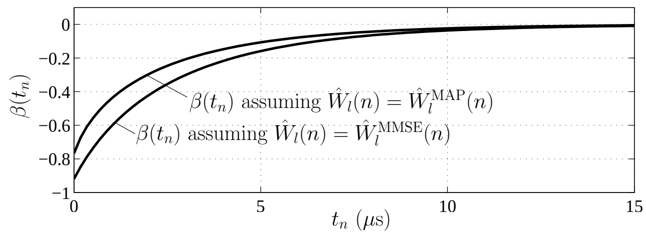

Fig. 2. Profiles of $\beta(t_n) = \beta(nT_s)$ for two different threat models of a SCER attack, both of which assume $\eta = 1$, $d = 0$, and a spoofer $C/N_0 = 54$ dB-Hz.

It should be emphasized that S_l is not a particularly sensitive statistic for detecting a SCER attack when $\hat{W}_l(n) = \hat{W}_l^{\mathrm{ML}}(n)$ because in this case $\boldsymbol{\mu}_{l0} \approx \boldsymbol{\mu}_{l1}$. Nonetheless, the ML estimates of W_l are so noisy to begin with that a detector based on S_l demonstrates good performance against ML SCER attacks, as will be shown later on. Against the stronger MAP and MMSE SCER attacks, S_l is near the optimal detection statistic, as it must be for good performance.

D. Details on Calculating S_l

As shown in (24), the statistic S_l is formed by a weighted correlation of the received signal y_k with a code and carrier replica s_k and a local copy of the lth security code chip W_l. Such calculations assume that the defender can generate s_k, which implies tight tracking of the incoming spreading code and carrier phase (conditions of ideal coherent detection), and that it can generate W_l, which implies either prior knowledge of the security code or the ability to reconstruct the security code after some delay.

In private-key spreading code authentication schemes such as the civil level-3 technique introduced in [7] and military GPS Y- and M-code security, receivers store secure keys that allow them to generate W_l as needed. In public-key authentication schemes with a low-rate security code, such as NMA [7]–[9], the long security code chip intervals allow the receiver to obtain a highly accurate estimate of W_l, the authenticity of which is subsequently verified by a public-key validation function. If validated, the receiver's estimated W_l values are considered true and the corresponding statistics S_l are generated by operations on buffered data; if invalidated, the receiver reports a spoofing attack [8]. In public-key authentication schemes with a high-rate security code such as the level-2 technique proposed in [7], the key required to generate unpredictable sequences of W_l is revealed in the navigation message moments after each unpredictable sequence is received [7], [9]. Thus, after receipt and cryptographic validation of the key, W_l is reconstructed and the statistic S_l is generated by operations on buffered data.

E. Statistics of S_l

Because $\boldsymbol{Y}_l$ can be approximated as a Gaussian random vector under the two conditions discussed in Section IV-B, and because the detection statistic S_l is a linear transformation of $\boldsymbol{Y}_l$, it follows that S_l is approximately Gaussian distributed under both H_0 and H_1. Let the mean and variance of S_l under H_j be denoted as $\mu_{S_l j}$ and $\sigma^2_{S_l j}$, $j = 0, 1$. It can be shown that the following expressions for these quantities are valid for all threat models:

$$\mu_{S_l 0} = \frac{1}{2} \sum_{k=k_l}^{k_l+M-1} \beta(n_{lk}) \tag{25}$$

$$\sigma^2_{S_l 0} = \frac{\sigma_r^2}{2} \sum_{k=k_l}^{k_l+M-1} \beta^2(n_{lk}) \tag{26}$$

$$\mu_{S_l 1} = \frac{g\alpha W_l}{2} \sum_{k=k_l}^{k_l+M-1} \beta(n_{lk}) E[\hat{W}_l(n_{lk})] \tag{27}$$

$$\begin{aligned} \sigma^2_{S_l 1} =& g^2 \sigma^2_{S_l 0} - \mu^2_{S_l 1} \\ &+ \frac{g^2\alpha^2}{4} \sum_{k=k_l}^{k_l+M-1} \sum_{j=j_l}^{j_l+M-1} \beta(n_{lk})\beta(n_{lj}) q(l, n_{lk}, n_{lj}) \end{aligned} \tag{28}$$

Here, j_l, like k_l, is the index of the first sample in the lth security code chip. The expressions for $E[\hat{W}_l(n_{lk})]$ required in (27) were given in Section III-C for the various security code estimation strategies. The function $q(l, n, m) \triangleq E[\hat{W}_l(n)\hat{W}_l(m)]$ is the correlation between two spoofer-generated estimates of W_l, one estimate based on n samples and the other on m samples. If one assumes that $\hat{W}_l(n) = \hat{W}_l^{\mathrm{ML}}(n)$ then $q(l, n, m)$ is equivalent to

$$q(l, n, m) = 1 + \frac{2\sigma_s^2 \min(n, m)}{nm} \tag{29}$$

which lends itself to easy computation. On the other hand, if one assumes $\hat{W}_l(n) = \hat{W}_l^{\mathrm{MAP}}(n)$ or $\hat{W}_l(n) = \hat{W}_l^{\mathrm{MMSE}}(n)$, then a closed-form expression for $q(l, n, m)$ does not appear obtainable. However, recognizing that $\hat{W}_l^{\mathrm{MAP}}(n)$ and $\hat{W}_l^{\mathrm{MMSE}}(n)$ are simply nonlinear functions of the matched filter output $Z_l(n)$, one can define the bivariate Gaussian random variable $\boldsymbol{Z_l} = [Z_l(n), Z_l(m)]^T$ and express $q(l, n, m)$ directly in terms of the density $p_{Z_l(n),Z_l(m)}(\xi_n, \xi_m) = \mathcal{N}([\xi_n, \xi_m]^T; \bar{\boldsymbol{Z}}_{\boldsymbol{l}}, P)$:

$$q(l, n, m) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(\xi_n, \xi_m) p_{Z_l(n),Z_l(m)}(\xi_n, \xi_m) d\xi_n d\xi_m \tag{30}$$

If $\hat{W}_l(n) = \hat{W}_l^{\mathrm{MAP}}(n)$, then $f(\xi_n, \xi_m) = \mathrm{sgn}(\xi_{\mathrm{n}})\mathrm{sgn}(\xi_{\mathrm{m}})$; if $\hat{W}_l(n) = \hat{W}_l^{\mathrm{MMSE}}(n)$, then
$f(\xi_n, \xi_m) = \tanh(\xi_n/\sigma^2_{Z_l}(n)) \tanh(\xi_m/\sigma^2_{Z_l}(m))$. The mean of $\boldsymbol{Z}_l$ is $\bar{\boldsymbol{Z}}_l = [W_l, W_l]^T$ and the (i, j)th element of its 2×2 covariance matrix is $P(i, j) = 2\sigma_s^2 \min(i, j)/ij$.

Equation (30) can be numerically integrated to produce $q(l, n, m)$. In general, $Z_l(n)$ and $Z_l(m)$ are highly correlated and the density $p_{Z_l(n),Z_l(m)}(\xi_n, \xi_m)$ is concentrated within an elongated ellipse rotated approximately 45 degrees from the horizontal axis in the ξ_n, ξ_m plane. A more compact range of integration and better numerical properties result by introducing the coordinate transform $\boldsymbol{U}_l = R^{-T}\boldsymbol{Z}_l$ where $R^T R = P$ is the Cholesky factorization of P [24]. Also, as might be expected by reference to the specific case in (29), $q(l, n, m)$ is insensitive to the value of $W_l \in \{-1, 1\}$; thus, $q(l, n, m)$ can be written with only two arguments as $q(n, m) = q(m, n)$, where the last equality recognizes the commutativity of n and m. Although in a real-time application it would not be practical to numerically integrate (30) at all the values of n_{lk} and n_{lj} required in (28), one could tabulate $q(n, m)$ for expected values of σ_s and calculate (28) via table lookup.

V. Detection of a SCER Attack

A. Full Detection Statistic

Under any practical SCER attack detection scenario the probability of detection associated with a single-chip detection statistic will be unacceptably low. A more powerful detection statistic can be synthesized from a set of single-chip statistics. Recognizing that the single-chip statistics $\{S_l : l = 1, 2, ...\}$ are approximately Gaussian distributed and, due to the independence of W_l and W_k for $l \neq k$, independent from one another, the full detection problem reduces to a case of the general Gaussian problem treated in [20]. Let $\boldsymbol{S} = [S_{l_m}, S_{l_m+1}, ..., S_{l_m+N-1}]^T$ be a vector of N chip-level statistics S_l for some start index l_m. Assume that over a block of N chips the spoofer's security code estimation strategy does not change and that σ_r and σ_s remain approximately constant. Then the elements of $\boldsymbol{S}$ will be statistically uniform and each element's mean and variance under H_j can be denoted simply as $\mu_j = \mu_{S_l j}$ and $\sigma_j^2 = \sigma^2_{S_l j}$, $j = 0, 1$. The detection problem then reduces to a test of the form

$$(\boldsymbol{s} - \boldsymbol{\mu}_0)^T K_0^{-1}(\boldsymbol{s} - \boldsymbol{\mu}_0) - (\boldsymbol{s} - \boldsymbol{\mu}_1)^T K_1^{-1}(\boldsymbol{s} - \boldsymbol{\mu}_1) \underset{H_0}{\overset{H_1}{\gtrless}} \gamma^*$$

where $\boldsymbol{\mu}_0 = \mu_0 \boldsymbol{1}_N$, $\boldsymbol{\mu}_1 = \mu_1 \boldsymbol{1}_N$, $K_0 = \sigma_0^2 I_{N\times N}$, and $K_1 = \sigma_1^2 I_{N\times N}$, with $\boldsymbol{1}_N$ representing the $N \times 1$ vector of ones and $I_{N\times N}$ representing the $N \times N$ identity matrix. The vector $\boldsymbol{s} = [s_{l_m}, s_{l_m+1}, ..., s_{l_m+N-1}]^T$ is a realization of the observation vector $\boldsymbol{S}$ containing a particular set of observed single-chip detection statistics. Taking advantage of the regular structure of K_0 and K_1, the test can be rewritten as

$$a\boldsymbol{s}^T\boldsymbol{s} + \boldsymbol{s}^T\boldsymbol{b} + c \underset{H_0}{\overset{H_1}{\gtrless}} \gamma^*$$

where

$$a = \frac{1}{\sigma_0^2} - \frac{1}{\sigma_1^2}, \qquad \boldsymbol{b} = b\boldsymbol{1}_N = 2\left(\frac{1}{\sigma_1^2}\boldsymbol{\mu}_1 - \frac{1}{\sigma_0^2}\boldsymbol{\mu}_0\right)$$

and c is a scalar constant independent of $\boldsymbol{s}$. Completing the square and absorbing constants into a new threshold γ, the test is further reduced to

$$L(\tilde{\boldsymbol{s}}) = a\tilde{\boldsymbol{s}}^T\tilde{\boldsymbol{s}} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma \tag{31}$$

where $\tilde{\boldsymbol{s}} = \boldsymbol{s} + \boldsymbol{b}/2a$. The quantity $L(\tilde{\boldsymbol{s}})$ is the full SCER attack detection statistic, which, when viewed as a random variable, is written $L(\tilde{\boldsymbol{S}})$. By the form of (31) one can recognize the distribution of $L(\tilde{\boldsymbol{S}})$ as:

$$p_{L|H_j}(\xi|H_j) = \frac{1}{|a|\sigma_j^2}\chi_N^2\left(\frac{\xi}{a\sigma_j^2}; \lambda_j\right), \quad j = 0, 1 \tag{32}$$

where

$$\lambda_j = \sum_{i=1}^{N} \left(\frac{\mu_j + b/2a}{\sigma_j} \right)^2, \quad j = 0, 1$$

and where $\chi_N^2(\xi;\lambda)$ is the functional form of a noncentral chi-square distribution with N degrees of freedom and noncentrality parameter λ.

B. Calculation of γ and P_D

Given $p_{L|H_0}(\xi|H_0)$, the threshold γ can be chosen to satisfy a pre-determined probability of false alarm P_F by solving for γ in

$$P_F = \int_{\gamma}^{\infty} p_{L|H_0}(\xi|H_0) d\xi$$

A corresponding probability of detection P_D is calculated as

$$P_D = \int_{\gamma}^{\infty} p_{L|H_1}(\xi|H_1) d\xi$$

Care should be taken to properly treat for the case $a \leq 0$, which occurs in rare cases when η is large and σ_s is small.

In an operational spoofing detection system, P_F will be set to a fixed value (e.g., 10^{-4}) and γ will be re-calculated as necessary under conditions of changing μ_0 and σ_0. Likewise, P_D, which varies with μ_1 and σ_1, can be re-calculated with each N-length batch of S_l processed to provide a real-time measure of the power of each detection test. Reference [8] discusses the use of P_D in a real-time signal authentication strategy.

C. Detector Performance

The performance of the SCER attack detection test proposed in the foregoing sections can be evaluated in terms of the so-called receiver operating characteristic (ROC), which gives P_D as a function of P_F [19]. This section presents ROCs for representative attack scenarios against high-rate and low-rate security codes. Each ROC has been generated on the basis of the statistical model for S_l given in Section IV-E, which has been cross-checked against extensive Monte-Carlo-type numerical simulations, and on the the statistical model for $L(\tilde{\boldsymbol{S}})$ given in Section V-A.

In all cases considered in this section the C/N_0 of the authentic signal as tracked by the spoofer, denoted $(C/N_0)_s$ and related to σ_s by (2), is assumed to be 54 dB-Hz. This is approximately the strongest C/N_0 that can be expected for terrestrial GNSS reception without resorting to a directional antenna or special cooling of the antenna amplifier [25]. The assumed C/N_0 of the authentic signal as tracked by the defender, $(C/N_0)_r$, is 48 dB-Hz. The particular $(C/N_0)_r$ and $(C/N_0)_s$ values chosen here, while somewhat arbitrary, are meant to represent a challenging detection scenario in which the spoofer is nominally assumed to have a 6 dB signal strength advantage compared with the defender. Also, in all cases considered in this section the assumed threat model has been exactly matched to the actual attack parameters. In other words, the detection test correctly models the spoofer's security code chip estimation strategy, whether ML, MAP, or MMSE, and correctly models the values of η, σ_s, σ_r, and d. Imperfectly matched detection models will be treated in the next two sections.

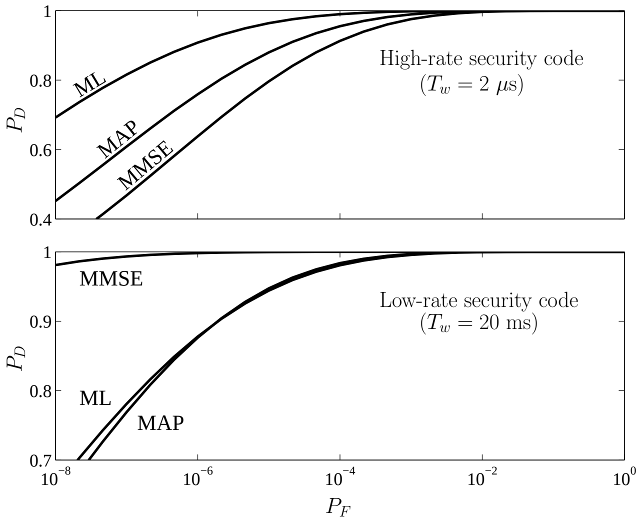

Fig. 3. ROCs for the ML, MAP, and MMSE security code estimation strategies under the following scenario: $(C/N_0)_s = 54$ dB-Hz, $(C/N_0)_r = 48$ dB-Hz, $\eta = 1$, $d = 0$, $N = 400$. Top panel: High-rate security code with $T_w = 2$ μs. Bottom panel: Low-rate security code with $T_w = 20$ ms.

The top panel of Fig. 3 shows ROCs for a zero-latency SCER attack against a high-rate security code ($T_w = 2$ μs). The detection test is based on a set of $N = 400$ single-chip observations S_l, which, at $T_w = 2$ μs, would allow a test to be run every 800 μs. For all tests the power factor $\eta = 1$, which means that the spoofing signal is matched in power to the authentic signal and that no security code estimation strategy has a hidden power advantage over the others. The need to perform an equal-power comparison among security code estimation strategies is the reason why the spoofing attack must be modeled in such a way that η can be set directly. It is clear from the plots in the top panel that MMSE is the spoofer's most potent security code estimation strategy under this scenario. Even still, and despite the spoofer's 6-dB C/N_0 advantage, the detection test against MMSE maintains $P_D > 0.9$ at $P_F = 10^{-4}$. For greater P_D, the number N of participating S_l can be increased.

The attack scenario for the bottom panel of Fig. 3 is the same as for the top panel except that a low-rate security code is assumed, such as would be the case in a system protected by NMA. Again, the detection test is based on a set of $N = 400$ single-chip statistics S_l, which implies that, at $T_w = 20$ ms, each test would require an interval of 8 seconds. In fact, for a practical application of NMA the interval between tests will be longer than this because, to preserve backward compatibility, only short segments of the navigation message can be encrypted [8]. MAP and ML are the spoofer's most potent estimation strategies under this scenario, while the MMSE strategy is the most easily detected.

Focusing on the MMSE and MAP estimation strategies, for which the detection test is nearly optimal, consider that Fig. 3 reveals two somewhat surprising results. First, there is a stark difference between the MMSE and the MAP strategies for the low-rate security code case (lower panel). Second, whereas MMSE is more easily detected than MAP for the low-rate code, the opposite is true for the high-rate code. Figure 4 helps explain these results. For the same scenario parameters that apply to the lower panel of Fig. 3, it shows 20 simulated time histories of security code chip estimates $\hat{W}_l^{\mathrm{MMSE}}$ (top panel) and $\hat{W}_l^{\mathrm{MAP}}$ (bottom panel) over the first 20 μs after the beginning of a unity-valued security code chip. The nearly vertical lines in the lower panel of Fig. 4 result from transitions between ±1-valued MAP estimates. Eventually, as more samples are received, all the simulated MAP estimates settle to unity. The same is true for the MMSE estimates only in a limiting sense: substantial deviations from unity are present even after 10 μs. The MAP estimates have an advantage for low-rate codes (long T_w) because after a sufficient time elapses the estimates of W_l become nearly certain and it becomes optimal in the sense of reducing P_D to enforce the $W_l \in \{-1, 1\}$ *a priori* constraint. On the other hand, for high-rate codes such as one having $T_w = 2$ μs, the W_l estimates remain so uncertain over the entire length of the chip that the MMSE strategy, which minimizes the mean square error, performs better in the sense of reducing P_D. The transition value of T_w at which the MMSE and MAP strategies are equally potent in terms of reducing P_D depends on the values of $(C/N_0)_s$ and $(C/N_0)_r$; for the parameters that apply to Fig. 3, the transition occurs at $T_w = 4$ μs.

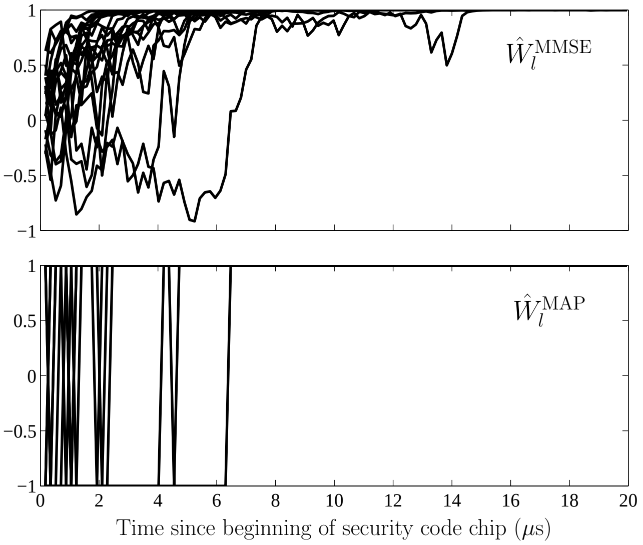

Fig. 4. Simulated time histories of security code chip estimates $\hat{W}_l^{\mathrm{MMSE}}$ (top panel) and $\hat{W}_l^{\mathrm{MAP}}$ (bottom panel) over the first 20 μs after the beginning of a security code chip. Scenario parameters are identical to those for the bottom panel of Fig. 3. MMSE and MAP chip estimates are based on the same simulated matched filter output Z_l.

One might also wonder how changes in the parameters σ_r, σ_s, η, and d affect detector performance. The issues of detector sensitivity to parameter variations and detector robustness to parameter uncertainty will be treated in the next section.

VI. Detector Robustness

The SCER attack detection test proposed in this paper assumes that the parameters σ_r, σ_s, η, and d are known to the defender, along with the spoofer's security code estimation strategy, whether ML, MAP, or MMSE. But of course the defender cannot be expected to know for certain the spoofer's estimation strategy or the exact signal parameters. One approach to dealing with this uncertainty, referred to as robust detection, is to demonstrate that a detection test which assumes a particular threat model is still able to maintain good performance even when the actual threat deviates from the assumed model, so long as the deviation is confined to a reasonable neighborhood about the assumed threat model [19]. Adopting this approach, the present section will focus on the parameters σ_r, σ_s, η, and d. Section VII will treat uncertainty in the spoofer's security code estimation strategy.

A. Variation and Uncertainty in σ_r and σ_s

Consider first the parameters σ_r and σ_s [correspondingly, $(C/N_0)_s$ and $(C/N_0)_r$]. For convenience, let the spoofer's C/N_0 advantage over the defending receiver be denoted $\Delta(C/N_0)_{sr} \triangleq (C/N_0)_s - (C/N_0)_r$. As $\Delta(C/N_0)_{sr}$ increases, a spoofing attack becomes more potent because the spoofer's W_l estimates are more accurate and the defender is less able to distinguish the detection statistic $L(\tilde{s})$ from noise. In recognition of this, the goal of cryptographic anti-spoofing should not be to prevent a successful attack at all cost, but to make one difficult. In this paper's view, if the spoofer is forced to employ a specialized high-gain antenna to carry out a successful attack, then the cryptographic anti-spoofing system has met its goal. Accordingly, this paper will assume that $\sigma_s^2 \geq \sigma_r^2/2$, which implies $\Delta(C/N_0)_{sr} \leq 3$ dB. This is consistent with a spoofing model in which the defender and spoofer are close to one another and both employ commercially-available antennas with a wide field of view. The up-to-3-dB advantage recognizes that the spoofer's active antenna may have a somewhat better noise figure than the defender's or the spoofer may be slightly better positioned for signal reception, but it is assumed that the spoofer does not employ a highly directional antenna or special cooling of the antenna amplifier.

In the absence of spoofing or other interference, the defender can be expected to maintain an estimate of $(C/N_0)_r$ from which σ_r can be calculated via (2). Preliminarily, assume that an accurate estimate is available and consider only the effect of variation in $(C/N_0)_r$ on P_D. Figure 5 shows how worst-case P_D varies with $(C/N_0)_r$ on the range $40 \leq (C/N_0)_r \leq 51$ dB-Hz, which spans typical values of $(C/N_0)_r$, assuming a zero-latency SCER attack and $\Delta(C/N_0)_{sr} \leq 3$ dB.

The rightmost trace corresponds to a high-rate code with $N = 400$ chip-level observations and assumes the MMSE estimation strategy, which is the spoofer's most potent in this case. P_D drops precipitously as $(C/N_0)_r$ falls below about 46 dB-Hz because the increasing variance of the single-chip statistics S_l prevents the defender from reliably distinguishing H_0 from H_1. Increasing N from 400 to 1000 (center trace) maintains P_D above 0.9 over the full range of $(C/N_0)_r$ considered. A trace corresponding to a low-rate security code, which never drops significantly below $P_D = 1$ over the range considered, is also shown in the plot along the $P_D = 1$ line. The low-rate code performs better for equivalent N than the high-rate code because the former has the advantage that each S_l is based on a longer correlation with the incoming samples. It bears remembering, however, that the high-rate code allows a much shorter time between detection tests.

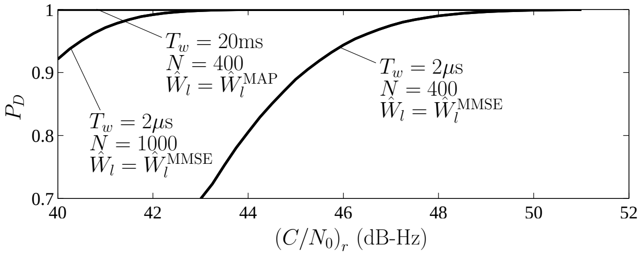

Fig. 5. Worst-case P_D as a function of $(C/N_0)_r$ assuming $\Delta(C/N_0)_{sr} \leq 3$ dB, $\eta = 1$, and $d = 0$.

Now consider uncertainty in σ_r [correspondingly, $(C/N_0)_r$]. For each successive detection test, the defender will typically employ an estimate of σ_r obtained during the previous test period. Due to satellite or vehicle dynamics, the previously-obtained estimate may be inaccurate by the time it is applied. It is also possible that the spoofer could intentionally manipulate the defender's estimate of σ_r by, for example, applying a low level of jamming as a prelude to a spoofing attack. If the jamming continues at the same level during the spoofing attack, then there will be no mismatch between the actual value of σ_r and the value that the defender assumes in its detection test, and the degradation in P_D will be as shown in Fig. 5 provided that, despite the jamming, $\Delta(C/N_0)_{sr} \leq 3$ dB. If instead the spoofer switches off the low-level jamming just as it begins a spoofing attack, then the actual σ_r will be smaller than the value assumed in the detection test.

Of course, the spoofer cannot apply an arbitrary level of jamming if it wishes to avoid detection. Reference [23] shows that, within a spectral band about a GNSS center frequency, any increase in the total received power beyond 1.5 dB above the quiescent in-band power has a less than 1 in 3000 chance of being naturally caused by solar effects during solar maximum. The likelihood falls to 1 in 8000 when averaged over the full 11-year solar cycle. Other causes of elevated in-band power such as the daily variation in number and type of overhead GNSS satellites or an increase in antenna temperature due to antenna mispointing would lead to an in-band power increase well below the 1.5 dB level. If one assumes that the power of the particular GNSS signal under test is small compared to the total in-band power, then it follows that the spoofer can only artificially reduce $(C/N_0)_r$ by up to 1.5 dB without detection.

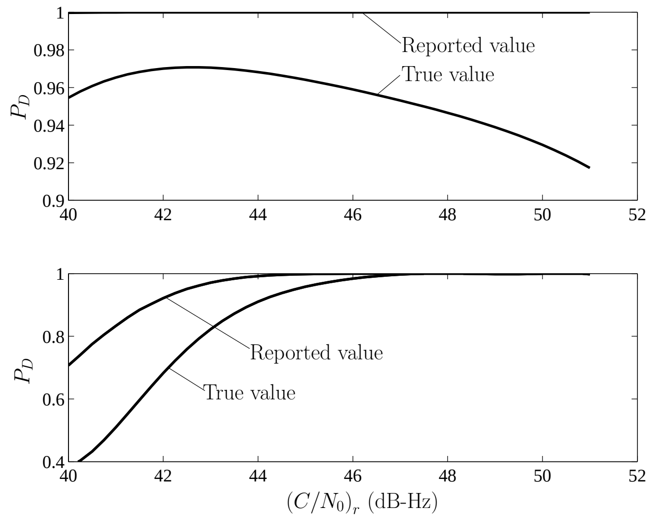

Fig. 6. Worst-case P_D as a function of $(C/N_0)_r$ assuming $d = 0$, $\Delta(C/N_0)_{sr} \leq 3$ dB, $\eta = 1$, and $P_F = 10^{-4}$. It is further assumed that the threat model underestimates $(C/N_0)_r$ by 2 dB (i.e., $(C/N_0)_{rTM} = (C/N_0)_r - 2$ dB-Hz). Top panel: Detector-reported and actual P_D for a low-rate security code with $T_w = 20$ms, MAP, and $N = 400$. Bottom panel: Detector-reported and actual P_D for a high-rate security code with $T_w = 2$ μs, MMSE, and $N = 1000$.

Figure 6 considers a scenario in which the threat model's value of $(C/N_0)_r$, denoted $(C/N_0)_{rTM}$, is 2 dB below the actual value, or 0.5 dB beyond the 1.5-dB limit just mentioned. As before, $\Delta(C/N_0)_{sr} \leq 3$ dB and the true value of $(C/N_0)_r$ ranges from 40 to 51 dB-Hz. The threat model correctly assumes that the spoofer has an up-to 3-dB C/N_0 advantage [i.e., $(C/N_0)_{sTM} \leq (C/N_0)_{rTM} + 3$ dB-Hz] but underestimates $(C/N_0)_r$ by 2 dB [i.e., $(C/N_0)_{rTM} = (C/N_0)_r - 2$ dB-Hz]. The mismatch in assumed and actual $(C/N_0)_r$ and $(C/N_0)_s$ values leads the detection test to apply a slightly mismatched weighting sequence β and a threshold γ that is somewhat higher than the correct value for $P_F = 10^{-4}$. The result is that the true value of P_D is below the value reported by the detection test, as shown in Fig. 6. The true value is also below the P_D that would have resulted from a properly matched test (not shown in the figure). Nonetheless, for the low-rate security code (top panel) the true P_D is maintained above 0.9 over the range considered, and for the high-rate code (bottom panel), the number of observations N can be increased to 2000 to keep the true P_D above 0.9. Therefore, the SCER attack detector can maintain good performance despite a fairly substantial underestimate of $(C/N_0)_r$.

Now consider overestimation of $(C/N_0)_r$. Suppose that $(C/N_0)_r \leq (C/N_0)_{rTM} \leq (C/N_0)_r + 2$ dB-Hz. In this case (not shown) true P_D remains high but P_F rises from 10^{-4} to a maximum of 0.35 over the usual range $40 \leq (C/N_0)_r \leq 51$ dB-Hz for both low-rate and high-rate codes when other scenario parameters are held as in Fig. 6. Clearly, a significant overestimate of $(C/N_0)_r$ would cause the detector to issue false alarms at an unacceptable rate. Fortunately, the spoofer cannot induce the defender to overestimate $(C/N_0)_r$. Moreover, for static receivers the detector's estimate of $(C/N_0)_r$ will be quite accurate. However, for a receiver mounted on a dynamic platform navigating through a cluttered environment, periodic overestimation of $(C/N_0)_r$, and consequent elevation of P_F, appears unavoidable.

B. Variation and Uncertainty in η

The spoofer's choice of η will be unknown to the defender but can be bounded. Reference [23] shows that for reliable spoofing η must exceed unity. At the other extreme, to avoid detection by an in-band power test with a threshold of 1.5 dB, as discussed above, η must be less than about 3 [23]. Figure 7 shows the effect on P_D of varying η within the range $1 \leq \eta \leq 5$ for high- and low-rate codes in a typical scenario. As usual, it is assumed that $\Delta(C/N_0)_{sr} \leq 3$ dB. Traces in the figure correspond to $(C/N_0)_r = 40$ or 51 dB-Hz, the extreme values of the usual range considered for $(C/N_0)_r$.

It is clear from the two traces marked $\eta_{TM} = \eta$ that even when the threat model value of η, denoted η_{TM}, is matched to the true value, changes in η affect P_D. In the low-rate case (top panel), one can see that for $(C/N_0)_r = 40$ dB-Hz, P_D takes on a minimum value of 0.9 at $\eta = 3.2$. This is the worst degradation of the low-rate P_D that non-unity η causes over the range $40 \leq (C/N_0)_r \leq 51$ dB-Hz. For the high-rate case (bottom panel), P_D obtains its minimum out beyond the largest value of η considered in the plot. The traces marked $\eta_{TM} = 1.2$ show that even if the defender fixes η_{TM} at a constant value of 1.2, the penalty paid relative to the matched $\eta_{TM} = \eta$ case is small for $1 \leq \eta \leq 3$ at both the low and the high ends of the $(C/N_0)_r$ range considered. In other words, if $\eta_{TM} = 1.2$, then the detector is fairly robust to uncertainty in η so long as η satisfies $1 \leq \eta \leq 3$.

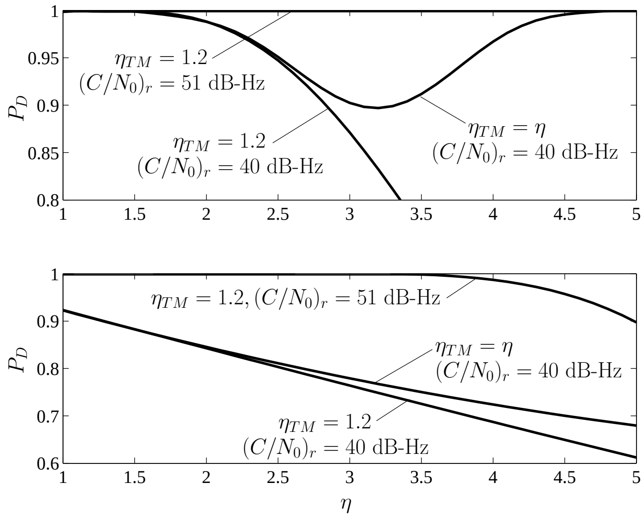

Fig. 7. Worst-case true P_D as a function of η assuming $d = 0$, $\Delta(C/N_0)_{sr} \leq 3$ dB, $N = 400$, and $P_F = 10^{-4}$. Top panel: Low-rate security code with $T_w =$ 20ms and $\hat{W}_l = \hat{W}_l^{\mathrm{MAP}}$. Bottom panel: High-rate security code with $T_w = 20$ μs and $\hat{W}_l = \hat{W}_l^{\mathrm{MMSE}}$.

It is worth emphasizing that the bound $\eta \leq 3$ and the 1.5-dB bound on the spoofer's ability to artificially reduce $(C/N_0)_r$ are only valid if the receiver's total in-band power is continuously monitored. This is the reason why the comprehensive signal authentication scheme advanced in [8] includes a jamming-to-noise meter on the RF front end.

C. Variation and Uncertainty in d

As with η, the spoofer's choice of delay d will be unknown to the defender but can be bounded. To prevent detection, the spoofer must maintain dT_s below the defender's timing uncertainty, or "window of acceptance" [7], [8], [17]. Reference [8] equates the width of the window of acceptance to the threshold γ_T of a timing offset hypothesis test. Thus, if $dT_s > \gamma_T$, an alarm will be triggered in the defender.

Figure 8 shows how P_D varies with dT_s for typical low- and high-rate scenarios when the threat model value of d, d_{TM}, is matched to the true value. As one might expect, P_D drops with increasing $dT_s \leq T_w$ because the spoofer's security code chip estimate accuracy improves with the longer minimum integration time. Note that P_D remains constant for $dT_s \geq T_w$, as evident in the high-rate plot, because the spoofer's security code chip estimates derive no additional benefit from delays exceeding T_w. Also note from Fig. 8 that the spoofer's most potent estimation strategy (MMSE for high-rate codes and MAP for low-rate codes) is more detectable for low-rate codes than for high-rate codes out to approximately $dT_s = 7$ μs. This agrees with the results shown in Fig. 3. In general, for a fixed number of security code chips N and small dT_s, spoofing detection is more powerful when dealing with low-rate codes than with high-rate codes because, while both the spoofer and the defender benefit from longer code chips, the defender benefits more.

To deal with uncertainty in dT_s, one can set $d_{TM}T_s = \min(\gamma_T, T_w)$, pessimistically assuming that the spoofer takes full advantage of the defender's timing uncertainty. If it is actually the case that $dT_s = d_{TM}T_s = \gamma_T$, then P_D varies with dT_s as shown in Fig. 8. If instead $dT_s < d_{TM}T_s$, then the true value of P_D in this mismatched case is no worse than the value of P_D shown in Fig. 8.

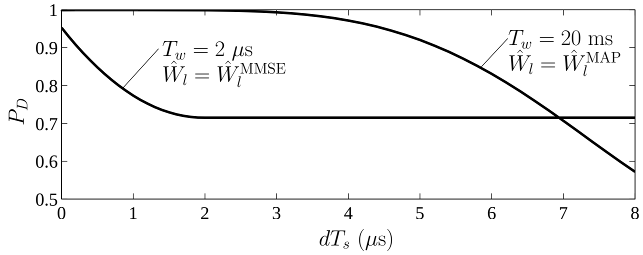

Fig. 8. Worst-case P_D as a function of dT_s assuming $d_{TM} = d$, $(C/N_0)_r = 46$ dB-Hz, $\Delta(C/N_0)_{sr} \leq 3$ dB, $N = 400$, $\eta = 1$, and $P_F = 10^{-4}$.

D. Discussion

The scenarios considered here highlight two advantages that high-rate security codes have over low-rate codes: (1) for the same number N of single-chip observations S_l, a high-rate code is able to perform a detection test within a much shorter time interval (e.g., 800 μs vs. 8 seconds for $N = 400$ and $T_w = 2$ μs vs. $T_w = 20$ ms), and (2) the benefit of the delay dT_s to the spoofer's security code estimates cannot exceed T_w; hence, a high rate security code strictly limits the extent to which P_D can be degraded by extending dT_s.

Nonetheless, low-rate security codes are useful for SCER attack detection. Reference [8] offers a practical low-rate security code implementation wherein batches of $N = 476$ unpredictable security code chips are periodically inserted into the navigation data stream—an instance of NMA. Figure

5 shows that with even fewer security code chips ($N = 400$), the low-rate code maintains P_D near 1 across the full range of $(C/N_0)_r$ in a zero-delay SCER attack, and Fig. 6 shows that the low-rate code is fairly robust in cases where $(C/N_0)_{rTM} < (C/N_0)_r$. Moreover, Fig. 8 makes it clear that, for the typical scenario considered, the low-rate security code maintains P_D above 0.9 out to a delay $dT_s = 5$ μs. Thus, one can claim that a low-rate strategy such as NMA is not only useful for message authentication, but also for authentication of the underlying signal in the sense that it is a powerful defense against a zero-delay SCER attack and remains strong against a non-zero-delay SCER attack for dT_s up to several μs. This result has not been previously established in the open literature.

VII. A Game-Theoretic Approach to Uncertainty in the Security Code Estimation Strategy

Each of the security code estimation strategies introduced in Section III-C is optimal for the criterion from which it is derived, whether ML, MAP, or MMSE. One might further conjecture that, for a given spoofing scenario, no other security code estimation strategy than one of these three would yield a smaller P_D in an optimal detection test or in the sub-optimal detection test proposed in this paper. Proof of this conjecture does not appear straightforward; however, it seems intuitively plausible and this paper will assume it to be true. A spoofer aiming to minimize P_D can therefore be expected to choose from among these three estimation criteria. Even still, from the defender's perspective, the spoofer's particular choice is uncertain. A sensible approach to dealing with this uncertainty would be for the receiver to apply three detection tests at each test interval, one tailored to each of the ML, MAP, and MMSE strategies. However, this "check all cases" approach is more computationally burdensome than performing a single test and is not always consistent with the Neyman-Pearson design criterion, which is to choose the decision rule that maximizes P_D for a fixed P_F [19]. A better approach is to treat estimation strategy uncertainty within the framework of game theory.

A. SCER Attack and Defense as a Two-Player Zero-Sum Game

A SCER attack and defense can be thought of as a two-player zero-sum (strictly competitive) game [26] in which the players—the spoofer and defender—choose from among the set {MAP, ML, MMSE} of pure strategies. The entries of the payoff matrix are the corresponding true values of P_D for the detection test proposed in this paper. As an example, consider the game in Table I, which corresponds to the scenario indicated in the caption. From this table, one can see that if the spoofer chooses the MAP security code estimation strategy and the defender implements a detection test that assumes MAP estimates, then $P_D = 0.85$. Among all matched strategies (spoofer and defender both choose the same strategy), MMSE is most effective for the spoofer in this scenario because it minimizes P_D along the upper left to lower right diagonal elements of the table. But the spoofer can do even better in terms of minimizing P_D if the defender fails to anticipate the spoofer's strategy. For example, if the spoofer chooses MMSE and the defender chooses ML, then, because the detection test is not properly matched to the threat, P_D drops to 0.64.

TABLE I
Scenario: $T_w = 2\ \mu$s, $dT_s = 0.2\ \mu$s, $N = 400$, $\eta = 1$, $(C/N_0)_r = 47$ dB-Hz, $(C/N_0)_s = 53$ dB-Hz, $P_F = 10^{-4}$

	Spoofer		
Defender	MAP	ML	MMSE
MAP	0.85	0.79	0.72
ML	0.83	0.82	0.64
MMSE	0.82	0.68	0.74

Assume for the moment that the defender and spoofer choose only one strategy at a time. Then standard reasoning from game theory applies to such spoofer-defender games. Define the defender's security level for a particular strategy as the smallest P_D for that strategy choice. For example, the security level for the defender's MAP strategy is 0.72. Likewise, from the spoofer's point of view a security level for a particular strategy can be defined as the maximum of all negative P_D values for that strategy, so that the spoofer's security level for MMSE is -0.64.

A reasonable approach to the game in Table I would be for each player to choose the strategy that maximizes the player's overall security level. Accordingly, the defender would choose MAP and the spoofer would choose MMSE. This strategy pair, written (MAP, MMSE), is said to be in equilibrium if it would not profit either player to unilaterally depart from it. One can see that (MAP, MMSE) is not, in fact, in equilibrium because, holding fixed the spoofer's choice of MMSE, the defender would do better by choosing MMSE.

An important result from game theory is that every two-person zero-sum game has an equilibrium point when randomized strategies are permitted; that is, when each player assigns a probability to each pure strategy and chooses according to this probability [26]. This result also applies in the context of a spoofing attack, although, for practical reasons, the spoofer and defender will probably adopt only pure strategies.

Some games in the present context do result in equilibrium even when the players are restricted to pure strategies. Consider the game in Table II, which corresponds to a low-rate security code in a challenging detection scenario.

TABLE II
Scenario: $T_w = 20$ ms, $dT_s = 2\ \mu$s, $N = 400$, $\eta = 1$, $(C/N_0)_r = 50$ dB-Hz, $(C/N_0)_s = 53$ dB-Hz, $P_F = 10^{-4}$

	Spoofer		
Defender	MAP	ML	MMSE
MAP	0.91	0.80	0.99
ML	0.01	0.99	0.02
MMSE	0.89	0.31	0.99

In this case, the strategy pair (MAP, MAP) is in equilibrium. Note also how poorly matched the ML detection test is against either the MAP or MMSE strategies. This is a common characteristic of low-rate codes.

B. Observations

Many games such as those in Tables I and II were analyzed for various spoofing scenarios. Observations resulting from this study can be summarized as follows.

1) Detection performance depends on what security code estimation strategy the spoofer chooses and what strategy the defender assumes. Two-person zero-sum game theory offers a framework for performance analysis in this context.
2) Not all spoofer-defender games result in equilibrium.
3) The ML detection test is poorly matched against either the MAP or MMSE strategies for low-rate codes.
4) It may be profitable for the defender to implement separate parallel detection tests tailored to each of the spoofer's possible strategies, but this is not always the case. For equivalent P_F, performing multiple detection tests can be worse for the defender than performing a single security-level-maximizing test.
5) It is both practical and rational in the current context for the spoofer to select a single strategy that will maximize its security level and for the defender to choose one or more detection tests depending on whether a single test or multiple tests maximizes the guaranteed minimum P_D. As a general rule, these goals lead the spoofer to choose MMSE for high-rate security codes and MAP for low-rate codes except when $\Delta(C/N_0)_{sr}$ is large, in which case it chooses ML for high-rate codes. For its part, the defender chooses MAP if limiting itself to a single strategy.

VIII. Experimental Results

An experimental testbed has been developed to evaluate the detection strategy proposed in this paper and other GNSS anti-spoofing techniques. The testbed consists of an advanced version of the real-time GPS L1 C/A spoofer originally presented in [1], a real-time software-defined GNSS receiver that plays the role of defender, and post-processing versions of both the spoofer and defender. This section presents a sample of test results; [23] gives a fuller description of the testbed and a more complete presentation of the experimental results.

For the results presented here, the testbed's post-processing spoofer was configured to mount a zero-delay SCER attack against the post-processing defender. The real-time spoofer and defender were not used because the latest version of the real-time spoofer at the time these experiments were conducted had a 2-ms processing delay, which prevents it from carrying out a true zero-latency attack. The attack was carried out as follows. The post-processing spoofer ingested authentic recorded GPS L1 C/A data and, treating the 20-ms navigation data bits as if they were unpredictable security code chips, generated current MAP estimates of each data bit as described in Section III-C. The spoofer then modulated each of 8 constituent spoofing signals in its output ensemble with the corresponding current navigation data bit estimates. The output data were subsequently combined at the sample level with the original authentic data to produce a data stream representing the composite spoofing and authentic signal ensembles. The post-processing defender ingested this combined data stream, tracked the signals present, and produced samples equivalent to the product $y_k s_k W_l$ in (24). These samples were weighted by an appropriate $\beta(n)$ to generate a sequence of chip-level statistics S_l. Batches of 400 S_l were combined as in (31) to generate a full detection statistic L every 8 seconds during the course of the experiment.

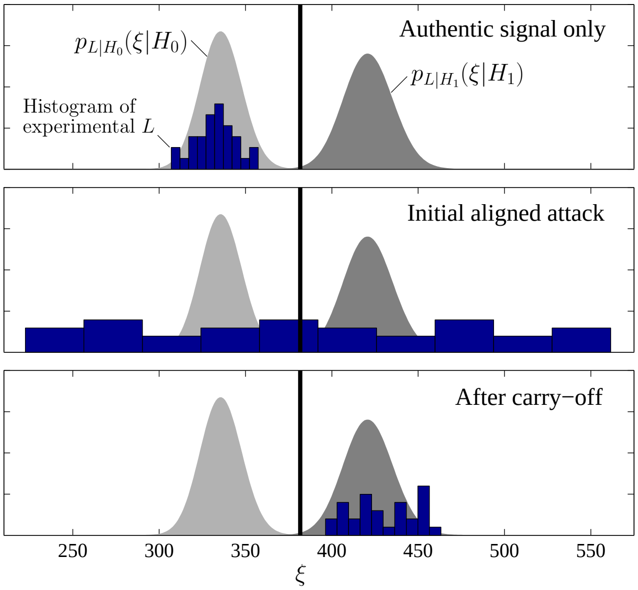

Fig. 9. Histograms of experimentally-generated detection statistics L (bar plots) compared with the detection threshold (thick vertical line) and the theoretical distributions $p_{L|H_j}(\xi|H_j)$, $j = 0, 1$ at various stages of a zero-delay SCER attack.

Figure 9 presents histograms of the experimentally-generated L for a particular GPS signal during three stages of the SCER attack. The top panel shows the attack prelude during which only the authentic signal was present. At this stage, the histogram of L values exhibits good correspondence with the theoretical null-hypothesis probability distribution $p_{L|H_0}(\xi|H_0)$, which is based on the value $(C/N_0)_r = 41$ dB-Hz that was measured by the defender. The alternative hypothesis distribution $p_{L|H_1}(\xi|H_1)$ corresponds to $(C/N_0)_s = 46$ dB-Hz, which was the spoofer's carrier to noise ratio for the same GPS signal during the attack. Thus, in this attack the spoofer's C/N_0 advantage over the defender was $\Delta(C/N_0)_{sr} = 5$ dB. The value of $(C/N_0)_s = 46$ dB-Hz in this experiment reflects the authentic signal's native C/N_0 in the original recorded data. The value of $(C/N_0)_r = 41$ dB-Hz reflects the authentic signal's C/N_0 value in the composite spoofing and authentic signal stream that was fed to the defender.

The center panel shows the situation during the initial stage of the attack when the authentic and spoofing signals were aligned to within a small fraction of the $\sim$ 1-μs spreading code chip interval. The counterfeit signal in this test was only slightly stronger (0.7 dB) than the authentic signal; as a result, there was strong interaction between the authentic and spoofing signals in the defender's complex-valued prompt correlator. The presence of code-phase-aligned and nearly equal-amplitude authentic and spoofing signals violates the either/or assumption of the hypothesis test model in (19). Despite this, the detection statistic exceeds the threshold more than half the time. However, instead of clustering within $p_{L|H_1}(\xi|H_1)$, the histogram spreads out. The spreading is driven by slow changes in the relative carrier phase of the authentic and spoofing signals.

After the spoofer has successfully carried off the defender's tracking points and the authentic and spoofed correlation peaks are separated by more than two spreading code chips, the model in in (19) again becomes valid. The bottom panel of Fig. 9 shows that at this stage the detection statistic clearly clusters beyond the detection threshold and roughly within the $p_{L|H_1}(\xi|H_1)$ distribution. It should be noted that in the experiment the post-carry-off C/N_0 value measured by the defender did not change significantly relative to the measured C/N_0 prior to the attack. Thus, a naive spoofing detection strategy that triggers on changes in C/N_0, or, equivalently, in the standard correlation power, would fail to detect this attack.

The results shown in Fig. 9 are representative of results from many similar experiments at various values of $(C/N_0)_r$ and $(C/N_0)_s$ that were conducted and which generally proved the utility of this paper's detection strategy [23]. The experiments also highlighted the variety of possible signal interactions during the initial stages of a spoofing attack, and underscored the sensitivity—previously discussed in Sec. VI-A—of the actual false alarm rate to overestimating $(C/N_0)_r$.

IX. Conclusions

A detection test has been developed for security code estimation and replay spoofing attacks against cryptographically-secured GNSS signals. The test is based on a model that captures the essential features of a replay-type spoofing attack. The test is nearly optimal for the spoofer's most potent security code estimation strategies and applies generally to low-rate security codes such as navigation message authentication and high-rate codes such as legacy GPS military encryption. A performance and robustness evaluation indicates that the detection test is able to maintain a high probability of false alarm despite some uncertainty in the spoofer's attack strategy and despite the spoofer's having a considerable carrier-to-noise ratio advantage, power advantage, and delay-improved security code estimates. Experimental tests on a spoofing testbed have validated the detector's statistical models in cases where only the authentic signal or a spoofing signal is present, and have shown that when both signals are present simultaneously the detector has a degraded but still useful sensitivity. Of immediate consequence, the results of this paper indicate that simple navigation message authentication would be an effective protection for civil GNSS signals against spoofing.

Acknowledgments

The author thanks Dr. Mark Psiaki and Dr. Todd Moon for informative discussions on detection theory, and Kyle Wesson for fruitful conversations on comprehensive anti-spoofing.

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] Anon., "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," John A. Volpe National Transportation Systems Center, Tech. Rep., 2001.

[4] ——, "Global positioning system impact to critical civil infrastructure (GICCI)," Mission Assurance Division, Naval Surface Warfare Center, Tech. Rep., 2009.

[5] U. Kroener and F. Dimc, "Hardening of civilian GNSS trackers," in *Proceedings of the 3rd GNSS Vulnerabilities and Solutions Conference*. Krk Island, Croatia: Royal Institute of Navigation, Sept. 2010.

[6] J. J. Spilker, Jr, *Global Positioning System: Theory and Applications*. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996, ch. 3: GPS Signal Structure and Theoretical Performance, pp. 57–119.

[7] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting*. Portland, Oregon: Institute of Navigation, 2003, pp. 1542–1552.

[8] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation*, 2011, submitted for review; available at http://radionavlab.ae.utexas.edu/nma.

[9] G. Hein, F. Kneissl, J.-A. Avila-Rodriguez, and S. Wallner, "Authenticating GNSS: Proofs against spoofs, Part 2," *Inside GNSS*, pp. 71–78, September/October 2007.

[10] O. Pozzobon, L. Canzian, M. Danieletto, and A. Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop on*, Dec. 2010, pp. 1 –6.

[11] N. White, P. Maybeck, and S. DeVilbiss, "Detection of interference/jamming and spoofing in a DGPS-aided inertial system," *Aerospace and Electronic Systems, IEEE Transactions on*, vol. 34, no. 4, pp. 1208–1217, 1998.

[12] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, April 2009.

[13] S. C. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts," in *Proceedings of the IEEE/ION PLANS Meeting*. Palm Springs, California: Institute of Navigation, 2010, pp. 708–717.

[14] K. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing: Securing the future of PNT," *Inside GNSS*, Jan. 2012.

[15] A. J. Van Dierendonck, *Global Positioning System: Theory and Applications*. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996, ch. 8: GPS Receivers, pp. 329–407.

[16] K. T. Woo, "Optimum semi-codeless carrier phase tracking of L2," *NAVIGATION, Journal of the Institute of Navigation*, vol. 47, no. 2, pp. 82 – 99, 2000.

[17] O. Pozzobon, C. Wullems, and M. Detratti, "Security considerations in the design of tamper resistant GNSS receivers," in *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop on*, dec. 2010, pp. 1 –5.

[18] M. K. Simon and M. Alouini, *Digital Communications over Fading Channels*. New York: Wiley, 2000.

[19] H. V. Poor, *An Introduction to Signal Detection and Estimation, 2nd Edition*. Springer, 1994.

[20] H. L. V. Trees, *Detection, Estimation, and Modulation Theory*. Wiley, 2001.

[21] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*. New York: John Wiley and Sons, 2001.

[22] 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.

[23] T. E. Humphreys, D. Shepard, and J. Bhatti, "A testbed for developing and evaluating GNSS signal authentication techniques," 2011, in preparation; available at http://radionavlab.ae.utexas.edu/testbed.

[24] T. K. Moon and W. C. Stirling, *Mathematical Methods and Algorithms for Signal Processing*. New Jersey: Prentice Hall, 2000.

[25] O. Montenbruck, A. Hauschild, and U. Hessels, “Characterization of GPS/GIOVE sensor stations in the CONGO network,” *GPS Solutions*, vol. 14, no. 3, pp. 193–205, 2011.

[26] R. D. Luce and H. Raiffa, *Games and Decisions: Introduction and Critical Survey*. Dover, 1989.