Autonomous Signal-Situational-Awareness in a Terrestrial Radionavigation System

Ronnie X.T. Kor[1], Peter A. Iannucci[1], and Todd E. Humphreys[1]

Abstract— **This paper aims to augment terrestrial radionavigation systems (TRNS) with autonomous signal-situational-awareness capability, allowing TRNS operators to detect spoofing and meaconing attacks within their systems. Such a capability is necessary to address a vulnerability to certain replay attacks that remains even when TRNS signals are secured by navigation message encryption and authentication. Two signal authentication techniques are developed to detect a weak spoofing signal in the presence of static and dynamic multipath. Both are shown to be effective in simulations of the varied operating environments that TRNS will encounter. With autonomous signal-situational-awareness, TRNS gain a defensive capability that GNSS cannot easily match: a comprehensive defense against most man-in-the-middle attacks on position, navigation, and timing services.**

I. Introduction

Global navigation satellite systems (GNSS) struggle to provide positioning, navigation, and timing (PNT) coverage in deep-urban and indoor environments. Current and upcoming terrestrial radionavigation systems (TRNS) like Locata [1] and NextNav [2] seek to extend PNT coverage by placing powerful ranging beacons throughout an urban environment. GNSS and TRNS face shared challenges in signal authentication and anti-spoofing that arise from fundamental properties of radio systems. Thus, the extensive scholarship on GNSS vulnerabilities [3], [4] largely applies to TRNS.

As recently outlined in [5], however, TRNS have unique security challenges: (1) the dynamic range of TRNS signal power is vastly wider than that of GNSS, allowing would-be spoofers access to high signal-to-noise ratio (SNR) signals and complicating spoofing mitigation based on simultaneous demodulation of spoofed and authentic waveforms [6]; (2) the angular distributions of spoofed, authentic, and multipath signals significantly overlap, rendering angle-of-arrival techniques based on multi-element antennas [7], [8] less effective; and (3) TRNS transmitters are physically accessible.

Nevertheless, TRNS also have inherent security advantages. Chief among these is that TRNS transmitters also function as receivers and can thus (1) accurately characterize the surrounding signal landscape's nominal statistics and thereafter (2) search for anomalies that reveal the presence of interfering signals. Current development of commercial TRNS clean-slate designs offers an opportunity to exploit this advantage of TRNS for enhanced security.

Related Work in Signal-Processing-Based Spoofing Detection Techniques: Several spoofing detection techniques proposed in the GNSS literature apply advanced signal processing algorithms to extract signal characteristics for source verification. Unlike other non-cryptographic spoofing defenses, these techniques can be readily implemented on existing GNSS receivers via a firmware upgrade. They can be divided into two classes, one that detects the inception of a spoofing attack, and another that performs a brute-force search for all signals in the landscape for post-inception detection.

Included in the first class are techniques that look for a sudden deviation in the received signal characteristics (carrier amplitude, beat carrier phase, code phase, carrier-to-noise density ratio, or received power) to detect the onset of a spoofing attack [9]–[11]. Also included are techniques based on Signal Quality Monitoring (SQM) that identify anomalous distortion in the complex correlation function [12], [13]. Multiple signal metrics can be derived by combining observations of both the received power and the correlation function distortion [14].

The second class of techniques performs a brute-force acquisition search for the presence of known signals using Complex Ambiguity Function (CAF) monitoring [15]. This approach avoids the problem of missed detection due to the transient nature of initial spoofing drag-off.

These techniques generally work for GNSS, as it has signal strength below the noise floor and a narrow dynamic range of signal power. In contrast, TRNS generally have high SNR—for quick acquisition in both dense-urban and indoor environments—and a wide signal power dynamic range. Analogous to variations in the received signal strength from low-elevation GNSS satellites in an urban environment, without detailed knowledge of its deep-fading channel model, a mobile receiver cannot straightforwardly predict the received signal strength of the authentic signal emanating from a particular TRNS beacon. Relatedly, when masquerading its signal as common multipath, a potential spoofer will have a wide margin to adjust its power in its attempt to overtake a victim receiver's tracking loops. In general, because TRNS operate in a quantitatively distinct regime of parameter space compared to GNSS (see [16, Subsec. 5.2.3]) it is challenging for mobile TRNS receivers to directly apply existing GNSS-targeted techniques for spoofing detection.

On the other hand, TRNS infrastructural monitors can fully exploit signal processing techniques for spoofing detection. Assuming that each has multiple correlators and secure clock synchronization [17], such monitors can narrowly char-

[1] R. Kor, P. Iannucci and T. Humphreys are with the Department of Aerospace Engineering and Engineering Mechanics, at The University of Texas at Austin, Austin, TX 78712 USA (e-mail: ronniekor@utexas.edu, peter.iannucci@austin.utexas.edu, todd.humphreys@utexas.edu).

acterize all signals in their nominal operating environments, after which signal anomalies in the surveilled landscape become apparent. This paper capitalizes on this feature of TRNS to propose two signal authentication techniques customized for TRNS monitors. It will be shown that a spoofing signal—even one with SNR below that of the authentic signal—can be detected despite the presence of static and dynamic multipath.

Related Work in TRNS Security: The present work complements the cryptographic security proposal presented in [5]. Briefly, [5] proposes a multi-tiered navigation message encryption (NME) + message authentication code (MAC)-based navigation message authentication (NMA) scheme. One can think of [5] as offering a basic level of navigation security via cryptographic methods. No TRNS should be fielded without such basic measures.

However, the techniques proposed in [5] are not sufficient to secure TRNS because the exposed spreading codes of a high-SNR TRNS signals makes them vulnerable to replication in a security code estimation and replay (SCER) [18] or meaconing attack. More generally, NME+NMA cannot fully protect TRNS against low-latency replay attacks. Even exotic signal-level security techniques like spreading code authentication (SCA) [19] or deterministic code-phase dithering [20] can be rendered ineffective by a spoofer's ability to access high-power authentic signals in a TRNS network.

Contributions: To address the gap in TRNS defenses against low-latency signal replay attacks, this paper proposes an autonomous signal-situational-awareness (SSA) overlay capability within a TRNS network. SSA is intended to augment basic TRNS cryptographic security. While some spoofers will remain undetectable, SSA gives TRNS operators a significantly improved chance of catching threats and alerting users without resorting to costly full-duplex techniques (those requiring bi-directional communication with users). Note that SSA is not possible for current GNSS space vehicles in medium Earth orbit, which can neither receive each other's signals nor detect low-power ground-based spoofers. This work seeks to place TRNS SSA on a solid theoretical and practical footing. First, signal authentication techniques for SSA are developed based on the prior work in [14] and [21]. Second, simulations with a theoretical model of multipath and spoofing signals are used to quantify the effectiveness of autonomous SSA under some of the myriad operating conditions encountered by generic TRNS.

II. Signal Authentication

This paper adopts a Bayesian binary hypothesis testing framework for distinguishing between the null hypothesis H_0 for the spoof-free case, and the alternate hypothesis H_1 for the spoofing case. The TRNS pre-correlation and post-correlation signal model for single-spoofer scenarios in a multipath environment, together with the probability distributions of signal components required to characterize the detection statistic, have been outlined in [16, Sec. 5.2]. This section develops the measurement models and formulates the detection statistics for signal authentication.

Consider a TRNS monitor receiving signals from a transmitting TRNS beacon at a standoff distance d, with its post-correlation output described by [16, Eq. 5.6]. There will typically be a significant number N_M of multipath components evident in the post-correlation function $\xi_k(\tau)$ ending at time $t_k = kT$, where T is the accumulation interval, but due to the quasi-static nature of the urban environment, the variation in $\xi_k(\tau)$ will be small over $(t_{k-1}, t_k]$, $\forall k$. These variations are caused by (1) thermal noise, (2) time-varying receiver non-idealities, and (3) urban environment movement. The first two factors are modeled by additive white Gaussian noise $r_N(t)$, whose contribution to $\xi_k(\tau)$ is detailed in [16, Sec. 5.2], while the third factor is modeled as a dynamic multipath component. Revisiting [16, Eq. 5.6], each multipath component can be further segregated into static $\xi_{M_s(k,i)}$ and dynamic $\xi_{M_d(k,i)}$ components:

$$\sum_{i=1}^{N_M} \xi_{M(k,i)}(\tau) = \sum_{i=1}^{N_M} \left[\xi_{M_s(k,i)}(\tau) + \xi_{M_d(k,i)}(\tau)\right] \qquad (1)$$

Let l be the number of signal taps sampling $\xi_k(\tau)$ across the lag window of interest, $\tau_w > 0$, with the centermost tap being aligned with $\tau = 0$, the location of the receiver's estimate of the authentic signal's correlation function peak, and the remaining taps being evenly spaced across τ_w. The uniform tap spacing is

$$\Delta\delta = \frac{\tau_w}{l-1}$$

and the vector of tap locations is

$$\boldsymbol{\delta} = \left[-\frac{\tau_w}{2}, -\frac{\tau_w}{2} + \Delta\delta, \cdots, \frac{\tau_w}{2} - \Delta\delta, \frac{\tau_w}{2}\right]^{\mathsf{T}} \in \mathbb{R}^l$$

with $\delta_i = -\frac{\tau_w}{2} + (i-1)\Delta\delta$ representing the ith tap location, $i = 1, \cdots, l$.

Being complex-valued, the post-correlation function can be viewed as having in-phase quadrature components: $\xi_k(\tau) = I_k(\tau) + jQ_k(\tau)$. Samples of $\xi_k(\tau)$ at the locations in $\boldsymbol{\delta}$ can be stacked into a single correlation measurement vector:

$$\boldsymbol{q}_k = \left[I_k(\delta_1), Q_k(\delta_1), \ldots, I_k(\delta_l), Q_k(\delta_l)\right]^{\mathsf{T}} \in \mathbb{R}^{2l} \qquad (2)$$

A hypothesis test for signal anomaly detection can be formulated in terms of the change in the distribution of $\boldsymbol{q}_k$ due to an additional signal component or components. Let $p_0(\boldsymbol{q}_k)$ and $p_1(\boldsymbol{q}_k)$ be the distribution of $\boldsymbol{q}_k$ under the null (H_0, no spoofing present) and alternate (H_1, spoofing present) hypotheses respectively.

The measurement $\boldsymbol{q}_k$ can be further dissected into its individual components:

$$H_0 : \boldsymbol{q}_k = \bar{\boldsymbol{q}} + \boldsymbol{w}_k \qquad (3a)$$

$$H_1 : \boldsymbol{q}_k = \bar{\boldsymbol{q}} + \boldsymbol{\mu}_k + \boldsymbol{w}_k \qquad (3b)$$

Here, $\bar{\boldsymbol{q}}$ is the mean of $\boldsymbol{q}_k$ under H_0, and $\boldsymbol{w}_k \sim \mathcal{N}(\boldsymbol{0}, P)$ is the measurement noise under both hypotheses, with $P = \mathbb{E}[(\boldsymbol{q}_k - \bar{\boldsymbol{q}})(\boldsymbol{q}_k - \bar{\boldsymbol{q}})^{\mathsf{T}}]$ being its covariance. P includes contributions due to dynamic multipath, thermal noise, and receiver non-idealities. Under H_1, there additionally enters a correlation distortion vector $\boldsymbol{\mu}_k$, which is a function of the false signal's code and carrier offsets $\Delta\tau_{Dk}$ and $\Delta\theta_{Dk}$ defined relative to the authentic signal's code and carrier phase. $\boldsymbol{\mu}_k$ will be further detailed in a later section. The amplitude of the false signal is given by $\epsilon_{Dk} > 0$. In the case of a successful detection, the false signal's amplitude and code and carrier offsets may also be estimated. For a false detection, estimates of these parameters are specious; typically, they match those of a strong dynamic multipath component.

The hypotheses H_0 and H_1 can be expressed in terms of probability distributions as follows, where $p_0(\boldsymbol{q}_k)$ is modeled as a Gaussian distribution with a mean of $\bar{\boldsymbol{q}}$ and covariance P, and $p_1(\boldsymbol{q}_k)$ has the same distribution but with an unknown deviation to the mean:

$$H_0 : \boldsymbol{q}_k \sim \mathcal{N}(\bar{\boldsymbol{q}}, P) \tag{4a}$$

$$H_1 : \boldsymbol{q}_k \sim \mathcal{N}(\bar{\boldsymbol{q}} + \boldsymbol{\mu}_k, P) \tag{4b}$$

This model conservatively assumes that P is identical under both H_0 and H_1. A spoofing signal can introduce additional time variation in $\xi_k(\tau)$ due to its own dynamic multipath, which can inflate P in the positive definite sense. However, it is impossible to know the increase in the magnitude of P *a priori*, so a less-sensitive model of having a constant P is assumed.

Suppose one subtracts the static components of $\xi_k(\tau)$. This is analogous to performing nominal signal cancellation in the correlation domain by removing the component of $\xi_k(\tau)$ due to the authentic signal and removing the static multipath $\sum_{i=1}^{N_M} \xi_{M_s(k,i)}(\tau)$. Then the correlation deviation function $\xi_{zk}(\tau) = I_{zk}(\tau) + jQ_{zk}(\tau)$ can be obtained:

$$\xi_{zk}(\tau) = \xi_{Sk}(\tau) + \sum_{i=1}^{N_M} \xi_{M_d(k,i)}(\tau) + \xi_{Nk}(\tau) \tag{5}$$

where $\xi_{Sk}(\tau)$ denotes the contribution to $\xi_k(\tau)$ due to the spoofing signal. Let

$$\begin{aligned} \boldsymbol{z}_k &\triangleq \boldsymbol{q}_k - \bar{\boldsymbol{q}} \\ &= \left[I_{zk}(\delta_1), Q_{zk}(\delta_1), \ldots, I_{zk}(\delta_l), Q_{zk}(\delta_l)\right]^\mathsf{T} \in \mathbb{R}^{2l} \end{aligned}$$

be the vector composed of samples of $\xi_{zk}(\tau)$ at the tap locations in $\boldsymbol{\delta}$. The model in (4) can now be rewritten as

$$H_0 : \boldsymbol{z}_k \sim \mathcal{N}(\boldsymbol{0}, P) \tag{6a}$$

$$H_1 : \boldsymbol{z}_k \sim \mathcal{N}(\boldsymbol{\mu}_k, P) \tag{6b}$$

The model in (6) is a special case of the general Gaussian problem [22] for which the optimal detection test can be reduced to

$$L(\boldsymbol{z}_k) = \boldsymbol{z}_k^\mathsf{T} P^{-1}\boldsymbol{z}_k - (\boldsymbol{z}_k - \boldsymbol{\mu}_k)^\mathsf{T} P^{-1}(\boldsymbol{z}_k - \boldsymbol{\mu}_k) \underset{H_0}{\overset{H_1}{\gtrless}} \nu \tag{7}$$

where $L(\boldsymbol{z}_k)$ is the log likelihood ratio and $\nu > 0$ is the threshold that yields the chosen probability of false alarm P_F.

This paper tackles the detection problem using two different techniques, an *Anomaly Test* (AT), which simply measures the fit of the observation $\boldsymbol{z}_k$ to the H_0 distribution by considering only the first term of (7), and a *Generalized Likelihood Ratio Test* (GLRT), which estimates $\boldsymbol{\mu}_k$ from the observations $\boldsymbol{z}_k$ to form the full detection statistic $L(\boldsymbol{z}_k)$ for the hypothesis test. These two techniques are elaborated in the following subsections.

A. Anomaly Test (AT)

Consider the optimal test in (7), which can be simplified by evaluating just the likelihood of the $p_0(\boldsymbol{z}_k)$ distribution:

$$L^*_{\text{AT}}(\boldsymbol{z}_k) = \boldsymbol{z}_k^\mathsf{T} P^{-1}\boldsymbol{z}_k \underset{H_0}{\overset{H_1}{\gtrless}} \nu^*_{\text{AT}} \tag{8}$$

where $\nu^*_{\text{AT}} > 0$ is the threshold that yields the chosen P_F given the $p_0(\boldsymbol{z}_k)$ distribution.

This technique can be used to detect any changes from the nominal signal landscape due to the presence of RFI. Due to its low computational needs, it is favorable for round-the-clock surveillance of the signal landscape. However, it does not glean any insight into the characteristics of the spoofing signal, unlike the GLRT detector, which will be elaborated in the next subsection.

B. Generalized Likelihood Ratio Test (GLRT)

The set of correlation distortion parameters $\{\epsilon_{Dk}, \Delta\tau_{Dk}, \Delta\theta_{Dk}\}$ is first estimated using a modified maximum-likelihood (ML) technique proposed in [23]. The estimator derived from this ML technique can detect any anomalous signal over a wide range of spoofing-to-authentic code offsets. This subsection details the adaptation of this estimator for TRNS spoofing detection.

The complex-valued ith tap of the correlation distortion function at time index k, $\xi_{Dk}(\tau) \triangleq I_{Dk}(\tau) + jQ_{Dk}(\tau)$ is expressed in terms of its amplitude ϵ_{Dk}, code phase offset $\Delta\tau_{Dk}$ and carrier phase offset $\Delta\theta_{Dk}$ as

$$\xi_{Dk}(\delta_i) = \epsilon_{Dk} R(\delta_i - \Delta\tau_{Dk}) \exp(j\Delta\theta_{Dk}) + \xi_{Nk}(\delta_i) \tag{9}$$

The correlation distortion vector $\boldsymbol{\mu}_k$ is similarly obtained by stacking the correlation distortion function from multiple taps:

$$\boldsymbol{\mu}_k = \left[I_{Dk}(\delta_1), Q_{Dk}(\delta_1), \ldots, I_{Dk}(\delta_l), Q_{Dk}(\delta_l)\right]^\mathsf{T} \tag{10}$$

The estimation of the correlation distortion's code phase offset can be separated from the estimation of its amplitude and carrier phase offset by exploiting the linear relationship

$$\boldsymbol{\xi}_{Dk} = H(\Delta\tau_{Dk}, \boldsymbol{\delta})\epsilon_{Dk} \exp(j\Delta\theta_{Dk}) \tag{11}$$

where $\boldsymbol{\xi}_{Dk} = [\xi_{Dk}(\delta_1), \cdots, \xi_{Dk}(\delta_l)]^\mathsf{T}$ and the observation matrix $H(\Delta\tau_{Dk}, \boldsymbol{\delta})$ is

$$H(\Delta\tau_{Dk}, \boldsymbol{\delta}) = \begin{bmatrix} R(\delta_1 - \Delta\tau_{Dk}) \\ \vdots \\ R(\delta_l - \Delta\tau_{Dk}) \end{bmatrix} \tag{12}$$

A coarse search is first performed by setting the code phase estimate $\Delta\hat{\tau}_{Dk} = \delta_i$ for $i = 1, \cdots, l$ and solving for the ML estimate of $\epsilon_{Dk}\exp(j\Delta\theta_{Dk})$ for each candidate $\Delta\hat{\tau}_{Dk}$:

$$\hat{\epsilon}_{Dk}\exp(j\Delta\hat{\theta}_{Dk}) = \left[H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})Q^{-1}H(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})\right]^{-1} H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})Q^{-1}\boldsymbol{\xi}_{zk} \tag{13}$$

where Q is the $l \times l$ Toeplitz matrix that accounts for the correlation of the complex Gaussian thermal noise among the taps [24], and $\boldsymbol{\xi}_{zk} = \xi_{zk}(\boldsymbol{\delta})$ is the vector of correlation deviation function from all signal taps. The $(a, b)^{\text{th}}$ element of Q is $Q_{a,b} = R(|a - b|\Delta\delta)$, where $\Delta\delta$ is the tap spacing.

The cost J_k corresponding to each set of estimates $\left\{\hat{a}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\}$ is calculated as

$$J_k = \|\boldsymbol{\xi}_{zk} - H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})\hat{\epsilon}_{Dk}\exp(j\Delta\hat{\theta}_{Dk})\|_Q^2 \tag{14}$$

where the norm is defined such that $\|\boldsymbol{x}\|_Q^2 = \boldsymbol{x}^{\mathsf{T}}Q^{-1}\boldsymbol{x}$. The cost J_k is proportional to the negative log-likelihood function, so the set with the minimum cost is the ML estimate.

A bisecting search is then performed to obtain a refined code phase estimate using linear interpolation. At each bisection point, new amplitude and carrier phase estimates are determined by re-evaluating (13). The process is repeated until J_k converges, and the resulting estimates are accepted as the maximum-likelihood estimate $\left\{\hat{\epsilon}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\}$. This estimate, with an example shown in Fig. 1, can correspond to the signal characteristics of the dynamic multipath, or spoofing signal, depending on their relative signal amplitude and code offset.

The maximum-likelihood estimate of $\xi_{Dk}(\tau)$ can be computed as

$$\hat{\xi}_{Dk}(\tau) \triangleq \hat{I}_{Dk} + j\hat{Q}_{Dk} \tag{15}$$

$$= \hat{\epsilon}_{Dk}R(-\Delta\hat{\tau}_{Dk} + \tau)\exp(j\Delta\hat{\theta}_{Dk}) \tag{16}$$

from which the correlation distortion vector

$$\hat{\boldsymbol{\mu}}_k = \left[\hat{I}_{Dk}(\delta_1), \hat{Q}_{Dk}(\delta_1), \ldots, \hat{I}_{Dk}(\delta_l), \hat{Q}_{Dk}(\delta_l)\right]^{\mathsf{T}}$$

is obtained to evaluate the optimal test (7).

Since both $p_0(\boldsymbol{z}_k)$ and $p_1(\boldsymbol{z}_k)$ are assumed to have the same covariance, (7) can be reduced to

$$L'(\boldsymbol{z}_k) = \hat{\boldsymbol{\mu}}_k^{\mathsf{T}}P^{-1}\boldsymbol{z}_k \underset{H_0}{\overset{H_1}{\gtrless}} \nu' \tag{17}$$

where $\nu' > 0$ is the threshold that yields the chosen P_F based on the distribution of $L'(\boldsymbol{z}_k)$ under H_0.

Analysis can be further simplified by letting $\boldsymbol{z}_{a,k} = R_a^{-T}\boldsymbol{z}_k$ and $\boldsymbol{\mu}_{a,k} = R_a^{-T}\boldsymbol{\mu}_k$, where R_a is the Cholesky factorization of P. The optimal test then becomes

$$L^*_{\text{GLRT}}(\boldsymbol{z}_{a,k}) = \hat{\boldsymbol{\mu}}_{a,k}^{\mathsf{T}}\boldsymbol{z}_{a,k} \underset{H_0}{\overset{H_1}{\gtrless}} \nu^*_{\text{GLRT}} \tag{18}$$

which implies a correlation-and-accumulation structure, with ν^*_{GLRT} being the threshold derived from the H_0 distribution using a chosen P_F.

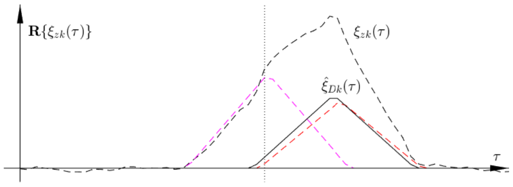

Fig. 1: The measured correlation distortion function $\xi_{Dk}(\tau)$ (dashed black) and its ML estimate $\hat{\xi}_{Dk}(\tau)$ (solid black) from an example scenario, shown in their in-phase components. The dotted black line corresponds to the delay of the authentic signal τ_A. Note that $\hat{\xi}_{Dk}(\tau)$ has a closer match to $\xi_{Sk}(\tau)$ (red) than to $\xi_{Mk}(\tau)$ (magenta), which implies that the estimated correlation distortion function is a good representation of the spoofing signal's correlation function.

This technique is sub-optimal, as the quality of the detector depends on the quality of the estimated parameters $\{\epsilon_{Dk}, \Delta\tau_{Dk}, \Delta\theta_{Dk}\}$ from ML estimation. Nonetheless, it is effective in discerning H_1 from H_0 for TRNS spoofing detection.

III. Simulations

The AT and GLRT spoofing detectors were tested in simulation under different scenarios. The following subsections outline the simulation setup, and the performance of the detectors under different operating conditions (different transmitter power level and receiver sensitivity range).

A. Simulation Setup

In order to have indoor positioning capability, the transmit power and spatial distribution of TRNS beacons have to compensate for high signal energy absorption by building materials, while minimizing infrastructure cost and near-far interference. Fig. 2 represents a small subset of a dense mesh deployment of TRNS beacons with a spacing of 10 km. The worst case scenario of spoofing is considered in all test cases, where a zero-latency spoofer was placed along the line-of-sight path between a pair of transmit and listening beacons. In each run, the spoofer power was set to reflect the spoofing power ratio (i.e. ratio of the spoofing power versus the authentic signal power) at the receiving beacon. A path loss exponent α of 3 was used to reflect a generic urban environment of the TRNS beacons [25]. The monitoring receiver's antenna experiences an ambient temperature T of 290 K, and has a front-end bandwidth B of 20 MHz. 10000 runs were conducted during the calibration phase using H_0 distribution, which is made up of 1 authentic signal, 8 static multipath and 1 dynamic multipath. Each post-correlation function $\xi_k(\tau)$ is computed across a correlation window of 20 chips from 1 ms of signal accumulation. The test statistics collated during calibration were used to compute the thresholds for each detector, based on a probability of false alarm P_{FA} of 1 in 1000. 2000 runs were then conducted during the trial phase, with an additional spoofing signal in the landscape, to determine the probability of detection

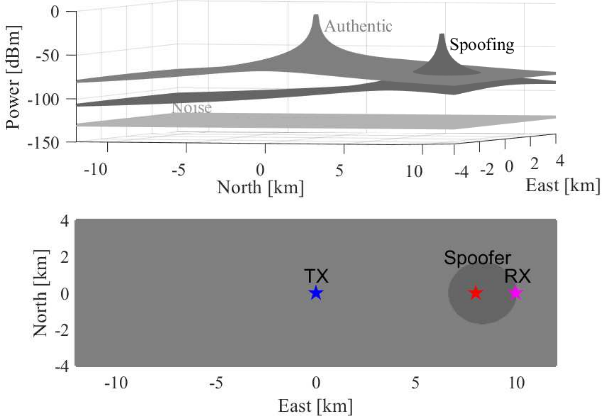

Fig. 2: Simulation setup used for all test cases. The transmitting beacon and the spoofer are located 10 km and 2 km away from the monitoring beacon respectively. The top plot shows the amplitude of the authentic and spoofing signals over a 10 km by 4 km grid, both of which are above the noise floor of the receiver.

P_D of the spoofing signal at each spoofing power ratio. The distributions of all the signal components were outlined in [16, Subsec. 5.2.2].

B. Detector Comparison

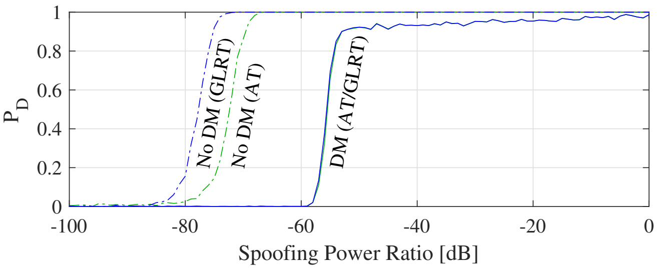

Fig. 3: Simulation results for AT and GLRT detectors, without dynamic multipath (No DM) and with dynamic multipath (DM). For discussion on the long-tail distribution on the right, see Subsection III-B. While the DM curve of GLRT appears similar to that of AT, it exhibits differences at the 5% level in the vicinity of the threshold.

Fig. 3 shows the performance of the AT and GLRT detectors, respectively, at a beacon transmit power of 30W. This power is sufficient to compensate for propagation and absorption losses over a 10 km spacing between beacons, as anticipated by a TRNS provider like NextNav. Each detector is simulated both with and without a dynamic multipath component. In each of these 4 cases, the condition under which the detector is trained and the condition under which it is evaluated is the same. It is no surprise that the confounding influence of dynamic multipath reduces the performance of each detector. Absent dynamic multipath, the GLRT exhibits a sensitivity advantage of roughly 5 dB. Under dynamic multipath, neither detector exhibits a significant advantage: the GLRT's 50% sensitivity threshold is 0.13 dB better (i.e. lower) than that of the AT.

In the dynamic multipath cases, each detector exhibits a sharp threshold and a long tail of false negatives. The region to the left of the threshold is dominated by noise. In this regime, P_D improves with increasing spoofing power ratio as the spoofing power approaches the noise floor at the receiver. To the right is the multipath-dominated region. Here, a false negative rate of 10% narrows towards zero with increasing spoofing power ratio. This occurs because, as discussed in [16, Subsec. 5.2.2], the spoofer's simulated code phase may coincide with the window of correlator output taps that are effectively desensitized by dynamic multipath. Due to the particular parameters used, this occurs 10% of the time. At high enough spoofing power ratio, this desensitization no longer prevents detection.

C. Different Levels of Transmitter Power

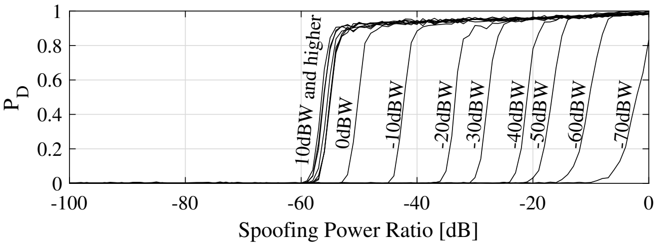

Fig. 4: Simulation results of the GLRT detector under different transmitter power level.

Fig. 4 shows the detection performance of the GLRT detector under different authentic transmitter power levels. Each simulated detection has access to only 1 ms of signal. Considering transmit power levels running upwards from −70 dBW, detection performances improve at all spoofing power ratios until the detector exhibits a saturation effect at a transmit power level of 10 dBW. Note that the spacing between adjacent curves is not uniform with transmit power level.

In order to interpret the saturation and non-uniform spacing effects, one may recast these observations in terms of received power (not spoofing power ratio) versus transmitted power. However, in order to do this, one must choose a single point on the P_D curve to summarize detector performance at a particular transmit power level. In Fig. 5, this point is arbitrarily chosen to be the 50% detection threshold. That is, at any given transmit power level, Fig. 5 shows the received power corresponding to a 50% rate of detection of the spoofer by the TRNS monitor.

Fig. 5 suggests that the saturation and non-uniform spacing phenomena in Fig. 4 indicate the presence of 3 quantitatively distinct regimes, in order from right to left:

- Region I: Quantization noise power P_Q dominates over thermal noise P_N at the receiver, where $P_N = S_{nn}B$ is the noise power over a channel bandwidth B and S_{nn} being the noise spectral density. Furthermore, the sensitivity threshold P_I is greater than P_N.

- Region II: Thermal noise dominates over quantization noise and the detection threshold is comparable to the thermal noise level, $P_I \approx P_N$.
- Region III: Thermal noise still dominates and the spoofing signal is only detectable post-correlation ($P_I \ll P_N$).

Naturally, if $P_I > P_A$, then we are "in clover": detection is not challenging!

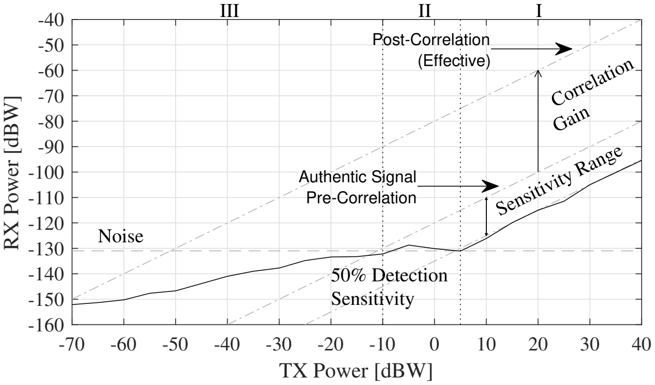

Fig. 5: Simulation results of the GLRT detector under different transmitter power, showing the 50% detection sensitivity curve with 3-bit quantization.

Receiver Front-End Details: The boundary between Regions I and II is sensitive to the behavior of the programmable gain amplifier (PGA) in the monitoring receiver. One common model for a quantizing receiver is to build a variable attenuator followed by a fixed-gain amplifier before the signal reaches the analogue-to-digital converter (ADC). In order to avoid saturating the ADC, that is, exceeding its input voltage range, the variable attenuator is commanded to reduce the power from the antenna according to the statistics of the ADC output in a feedback loop. In Fig. 4, the P_D curves begin "stacking up" when the transmit power becomes high enough to enter Region I: that is, when additional transmit power must be exactly offset by increased attenuation in the receiver. In this regime, thermal noise is negligible compared to quantization noise, which tracks with transmitter power. Thus, in Region I, the slope of the 50% detection curve in Fig. 5 is unity. Increasing the transmitter power in Region I does not improve P_D because the variable attenuator is forced to further suppress the incoming signal by the same amount, leading to no net increase in sensitivity.

In Region II, there is no suppression of the incoming signal by the variable attenuator, as all received signals are within the sensitivity range of the ADC at full PGA gain. Assuming as in Section II that cancellation of the authentic signal and the static multipath components at the monitoring receiver may be considered perfect in this regime, the detector need only distinguish the spoofing signal from thermal noise and dynamic multipath. So long as the dynamic multipath remains relevant (i.e. comparably strong to the spoofed signal), it will prevent the receiver from identifying spoofing signals that are below the noise floor. resulting in a relatively flat 50% detection curve.

In Region III, both the spoofing signal and dynamic multipath have processing gain advantage over thermal noise from despreading. The detector in this regime has to only differentiate the spoofing signal from dynamic multipath, with this sensitivity decreasing with lower transmit power level, resulting in the 50% detection curve having a slope less than unity.

D. Receiver Sensitivity Range

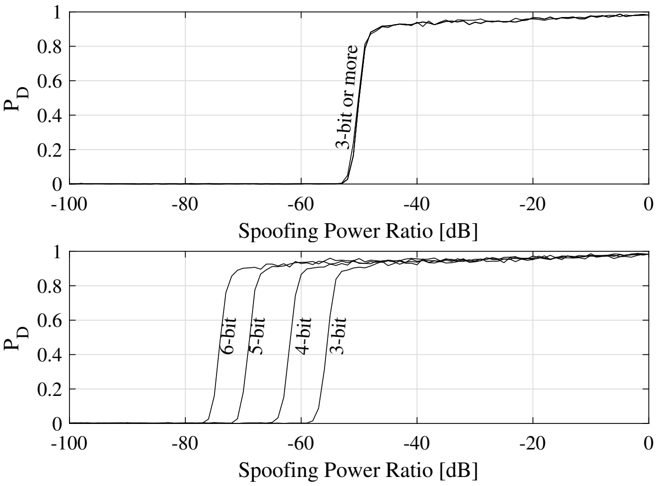

Fig. 6: Simulation results of the GLRT detector with different ADC bit depth, for a 0 dBW (top) and 40 dBW (bottom) transmitter located at 10 km away from a listening beacon.

Fig. 6 shows the detection performance of the GLRT detector with different ADC bit depths for two distinct transmit power levels, and Fig. 7 shows these data recast in terms of RX power at the 50% detection threshold versus authentic signal TX power. One may infer that the sensitivity threshold does not improve with bit depth at low transmit power levels. With regards to the regions discussed in Subsection III-C, these plots reveal two trends. First, a larger ADC bit depth results in a lower quantization noise level in Region I due to lower suppression by the variable attenuator. Second, the dividing line between Regions I and II moves rightward with increasing bit depth. That is, the thermal noise dominates up to a higher transmit power level. Quantization is not the performance-limiting factor in Region III.

IV. Conclusion

This paper proposes the addition of signal-situational-awareness (SSA) capability to the TRNS network, to augment cryptographic NME+NMA scheme in countering against SCER and meaconing attacks. Two signal authentication techniques are proposed for SSA that allow TRNS operator to detect weak signal spoofing in the presence of multipath without the use of costly full-duplex techniques. The first technique, the *Anomaly Test*, compares the current observations against an empirical model of typical (nominal) observations, and has an advantage in simplicity and performance. The second technique searches for the spoofing signal

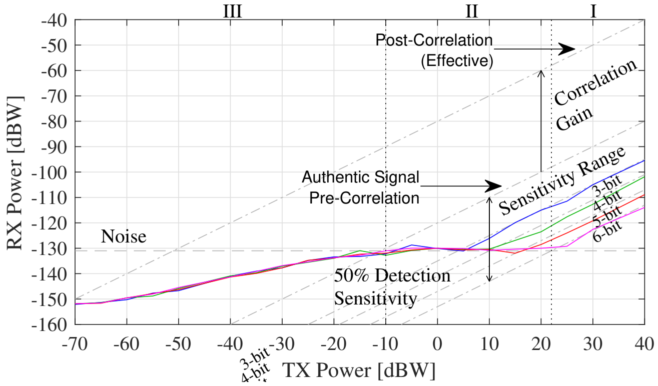

Fig. 7: Simulation results of the GLRT detector under different transmitter power, showing the 50% detection sensitivity curve with different levels of quantization. The boundary between Regions I and II varies with depth and is shown for 6-bit quantization.

and compares the observations against a reconstruction of the most likely spoofer: the *Generalized Likelihood Ratio Test* (GLRT) technique. The GLRT method performs as well or better than the Anomaly Test in all considered test conditions. The GLRT exhibits a sensitivity advantage of 5 dB over the Anomaly Test in the absence of dynamic multipath, which drops to 0.13 dB in the presence of dynamic multipath. In addition, the GLRT has a 50% spoofer detection threshold up to -74 dB with high transmit power level and 6-bit ADC quantization. Simulations of both detectors under various operating conditions encountered by a generic TRNS quantify their performance. Terrestrial radionavigation systems will benefit not only from techniques designed to secure traditional GNSS, but also from the exploitation of novel opportunities for signal situational awareness arising from the proximity and mutual audibility of the transmitting beacons, rendering TRNS more resilient against man-in-the-middle attacks.

Acknowledgments

This work was supported by the U.S. Department of Transportation (USDOT) under Grant 69A3552047138 for the CARMEN University Transportation Center (UTC). It was also supported by NextNav LLC as an affiliate of the The University of Texas Wireless Networking and Communications Group.

References

[1] C. Rizos, G. Roberts, J. Barnes, and N. Gambale, "Experimental results of Locata: A high accuracy indoor positioning system," in *2010 International Conference on Indoor Positioning and Indoor Navigation*. IEEE, 2010, pp. 1–7.

[2] S. Meiyappan, A. Raghupathy, and G. Pattabiraman, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*. Wiley-IEEE, 2020, vol. 2, ch. Position, Navigation and Timing with Dedicated Metropolitan Beacon Systems, pp. 1225–1241.

[3] T. E. Humphreys, *Interference*. Springer International Publishing, 2017, pp. 469–503.

[4] M. L. Psiaki and T. E. Humphreys, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*. Wiley-IEEE, 2020, vol. 1, ch. Civilian GNSS Spoofing, Detection, and Recovery, pp. 655–680.

[5] R. X. Kor, P. A. Iannucci, L. Narula, and T. E. Humphreys, "A proposal for securing terrestrial radio-navigation systems," in *Proceedings of the ION GNSS+ Meeting*, Online, 2020.

[6] C. Hegarty, "Analytical model for GNSS receiver implementation losses," *Navigation, Journal of the Institute of Navigation*, vol. 58, no. 1, p. 29, 2011.

[7] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, and A. Schofield, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proceedings of the ION GNSS+ Meeting*. Tampa, FL: Institute of Navigation, 2014.

[8] A. G. Dempster and E. Cetin, "Interference localization for satellite navigation systems," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1318–1326, June 2016.

[9] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[10] D. Egea-Roca, G. Seco-Granados, and J. A. López-Salcedo, "Comprehensive overview of quickest detection theory and its application to gnss threat detection," *Gyroscopy and Navigation*, vol. 8, no. 1, pp. 1–14, 2017.

[11] A. Broumandan, S. Kennedy, and J. Schleppe, "Demonstration of a multi-layer spoofing detection implemented in a high precision gnss receiver," in *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. IEEE, 2020, pp. 538–547.

[12] A. Cavaleri, M. Pini, L. L. Presti, M. Fantino, M. Boella, and S. Ugazio, "Signal quality monitoring applied to spoofing detection," *Proceedings of the ION GNSS Meeting*, 2011.

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

[14] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739–754, April 2018.

[15] C. Hegarty, A. Odeh, K. Shallberg, K. Wesson, T. Walter, and K. Alexander, "Spoofing detection for airborne GNSS equipment," in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 1350–1368.

[16] R. X. T. Kor, "A comprehensive proposal for securing radionavigation systems," Master's thesis, The University of Texas at Austin, 2021.

[17] L. Narula and T. E. Humphreys, "Requirements for secure clock synchronization," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 749–762, Aug. 2018.

[18] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[19] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-message robust authentication (Chimera) for GPS civilian signals," in *ION GNSS*, 2017, pp. 2388–2416.

[20] C. Rocken and C. Meertens, "Monitoring selective availability dither frequencies and their effect on GPS data," *Bulletin géodésique*, vol. 65, no. 3, pp. 162–169, 1991.

[21] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 1, pp. 469–475, 2018.

[22] H. L. Van Trees, *Detection, Estimation, and Modulation Theory*. Wiley, 2001.

[23] J. Gross and T. E. Humphreys, "GNSS spoofing, jamming, and multipath interference classification using a maximum-likelihood multi-tap multipath estimator," *Proceedings of the ION International Technical Meeting*, Jan. 2017.

[24] N. Blanco-Delgado and F. D. Nunes, "Multipath estimation in multicorrelator GNSS receivers using the maximum likelihood principle," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 4, pp. 3222–3233, 2012.

[25] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. prentice hall PTR New Jersey, 1996, vol. 2.