Protecting GNSS Open Service Navigation Message Authentication Against Distance-Decreasing Attacks

KEWEI ZHANG
KTH Royal Institute of Technology, Stockholm, Sweden

ERIK G. LARSSON, Fellow, IEEE
Linköping University, Linköping, Sweden

PANOS PAPADIMITRATOS, Fellow, IEEE
KTH Royal Institute of Technology, Stockholm, Sweden

As the security of global navigation satellite systems (GNSSs) for civilian usage is increasingly important, navigation message authentication (NMA) significantly improves resilience to spoofing attacks. However, not all attacks can be effectively countered: a strong variant of replay/relay attacks, distance-decreasing (DD) attacks, can shorten pseudorange measurements, without manipulating the cryptographically protected navigation message, thus manipulating the position, velocity, and time solution undetected. First, we discuss how DD attacks can tamper with GNSS signals, demonstrating the attack effectiveness on a recorded Galileo signal. DD attacks might introduce bit errors to the forged signals, but the adversary can keep this error rate very low with proper attack parameter settings. Then, based on our mathematical model of the prompt correlator output of the tracking phase at the victim receiver, we find that the correlator output distribution changes in the presence of DD attacks. This leads us to apply hypothesis testing to detect DD attacks, notably a goodness-of-fit (GoF) test and a generalized likelihood ratio test (GLRT), depending on the victim's knowledge on the DD attacks. Monte Carlo simulations are used to evaluate the detection probability and the receiver operating characteristic curves for two tests, for different adversary configuration and noise settings. Then, we evaluate the effectiveness of the GoF test and the GLRT with a synthesized DD signal. Both tests can detect DD attacks with similar performance in high-signal-to-noise-ratio (SNR) environments. The GLRT detection probability is approximately 20% higher than that of the GoF test in low-SNR environments.

Manuscript received July 7, 2020; revised December 13, 2020, June 2, 2021, and September 2, 2021; released for publication September 5, 2021. Date of publication October 26, 2021; date of current version April 12, 2022.

DOI. No. 10.1109/TAES.2021.3122512

Refereeing of this contribution was handled by J. T. Curran.

This work was supported in part by the SSF SURPRISE cybersecurity project and the Security Link strategic research center. The work of Erik G. Larsson was also supported by the Knut and Alice Wallenberg (KAW) Foundation. The work of Panos Papadimitratos was also supported by the Trustworthy IoT KAW Academy Fellowship.

Authors' addresses: Kewei Zhang and Panos Papadimitratos are with the Network Systems Security Group, KTH Royal Institute of Technology, 114 28 Stockholm, Sweden, E-mail: (kewei@kth.se, papadim@kth.se); Erik G. Larsson is with the Department of Electrical Engineering, Linköping University, 581 83 Linköping, Sweden, E-mail: (erik.g.larsson@liu.se). *(Corresponding author: Kewei Zhang.)*

I. INTRODUCTION

A multitude of applications and emerging systems, such as autonomous vehicles, unmanned aerial vehicles and intelligent transportation systems, rely on civilian global navigation satellite system (GNSS) signals for position, velocity, and timing (PVT) services. However, civilian GNSS signals are vulnerable to spoofing attacks, because of their public signal structures and predictable navigation messages. Researchers have demonstrated that one can build a GPS spoofer with dual frequency at a cost of $250–$400, based on a Raspberry Pi and a software-defined radio (SDR) [1], [2].

Significant work has been done on proposing countermeasures. One approach is to augment the GNSS receiver, in order to detect attacks. Some researchers propose to detect the presence of an attacker with abnormalities of the received signal strength, e.g., through monitoring the automatic gain control (AGC) level [3], [4] and received power monitoring [5]–[7]. Moreover, a properly designed receiver can determine signal arrival angles with especially designed antennas [8]–[10], because adversarial signals are usually transmitted from a same device/antenna. Comparing GNSS measurements with additional positioning information, e.g., from an inertial navigation system, to detect the replaying/spoofing attacks [11]–[14] was also proposed. Moreover, the detection based on GNSS-attack-induced clock drift can be used to limit the extent of adversarial manipulation [5], [6], [15]. Receiver autonomous integrity monitoring can also detect attacks, by checking the consistency of receiver positions calculated based on subsets of all available satellites, being effective when the adversary attacks a subset of available satellites [16]–[20]. The authors of [21]–[25] propose to monitor the signal quality by statistically testing the symmetric character of early correlator E and late correlator L or extra-correlator pairs.

Another approach is to enhance the GNSS system infrastructure, providing security features, notably signal authentication/encryption and navigation data authentication/encryption [26]–[31]. Military signals use signal encryption and/or navigation data encryption to restrict the access to the signals [32]–[34], e.g., the GPS M-code signals, the Galileo Public Regulated Service signals, and the BeiDou authorized signals. The European GNSS Agency developed and begun testing the civilian Galileo Open Service Navigation Message Authentication (NMA), to thwart spoofing attacks, with cryptographic message authentication code (MAC) [35], [36].

However, authenticated signals, in particular NMA, cannot alone effectively protect receivers from replay/relay attacks, including classic replay attacks, e.g., meaconing [37], security code estimation and replay (SCER) attacks [28], forward estimation attacks (FEAs) [38], [39], and distance-decreasing (DD) attacks [40], [41]. The SCER attack estimates authenticated data or secret code and generates a spoofed signal with a small or zero delay. While the FEA exploits the redundancy in the authentication message introduced by the forward error coding, to guess parts of the message, even prior to its transmission. DD attacks, first introduced in [42], are physical layer attacks against secure ranging and distance-bounding protocols. Their feasibility and effectiveness against ultrawide band [43]–[46] and chirp spread spectrum [47] systems was analyzed first. In the GNSS context, even with cryptographic protection in place, DD attacks can still decrease pseudorange measurements in real time.

DD attacks can be seen as a sophisticated replay/relay attack [15], adding, essentially, to a record-and-replay attack [37], the ability to perform real-time record and replay and to reduce the perceived satellite–receiver distance. The DD adversary needs a receiver and a transmitter that are interconnected. The adversarial transmitter (ATX) emits an adversary-chosen bit/symbol value before the adversarial receiver (ARX) has the corresponding value(s) transmitted by the satellite(s). Unlike legitimate receivers, the adversarial receiver seeks to estimate early each bit/symbol, i.e., using only a fraction of its duration. It can then relay this estimated (early detected) value to the ATX, which, in turn, can adjust its transmission to ensure that the legitimate receiver under attack obtains the value originally transmitted by the satellite. This is crucial to avoid data alteration and, thus, detection based on the cryptographic protection. The adversary's gain is the mistakenly early arrival of the signal at the victim receiver: due to the early detection (ED) and the in parallel initiated bit/symbol transmission, the legitimate receiver perceives the adversarial signal arrival to be earlier than the arrival of the actual signal. This allows the adversary, performing the attack for the entire navigation message, to reduce the computed pseudorange by an amount that corresponds to a fraction of a bit/symbol.

Zhang and Papadimitratos [41] investigated how DD attacks can be launched, with differing consequences on different GNSS signals. A preliminary result on countermeasure against the DD attacks is provided in [48]. The literature did not investigate in detail how effective DD attacks can be against modern civilian cryptographically protected signals and did not extensively evaluate the detection power at various adversary setups. Another question is how and how much we can improve the detection method. These are the gaps this work seeks to address.

More specifically, in this article, we contribute: 1) an investigation of the effectiveness of DD attacks against Galileo E1 OS signals in different noise environments; 2) the design of statistical tests, based on the prompt correlator outputs of the victim receiver, as countermeasures; and 3) the evaluation of the countermeasures with Monte Carlo simulation and with a synthesized Galileo signal. The statistical tests rely on the nature of the attack, notably the fact that the adversary-chosen value in the DD signals significantly affects the amplitude of the prompt correlator output: the correlator output follows a normal distribution in the absence of attacks, but not so in the presence of a DD attack. A Shapiro–Wilk test [49] tests normality of the correlator output, or the generalized likelihood ratio test (GLRT) [50] examines the ratio of likelihood of legitimate signals and likelihood of DD signals. We find that the two tests can effectively detect the DD attacks even in noisy environments when the adversary wants to shorten a large pseudorange measurement.

The rest of this article is organized as follows. Section II introduces the DD attacks on GNSS signals and details the adversary model. Section III demonstrates the performance, i.e., symbol error rate, of the receiving component of DD attacker on the Galileo E1 OS signals, and illustrates the correlator outputs of the victim receiver. Then, Section IV provides the mathematical model for attack detection and the design of two tests for the DD attack detection. It also presents the Monte Carlo simulation results of the tests, followed by detection results on a synthesized signal. Finally, Section V concludes this article.

II. ADVERSARY MODEL

The adversary is equipped, similarly to replay/relay/meaconing attackers [37], [51], with one or more radios that transmit GNSS signals the adversary wishes to manipulate. We term this the ATX. Unlike the replay of GNSS signals, which can be recorded over a period of time and then replayed by the ATX, the DD attack acts in real time, relaying GNSS signals received by an adversarial receiver (ARX) and passed to the ATX.

Section II-A explains how a DD attack is mounted in two stages, two adversarial components acting in unison: the "ED" running on the ARX, elaborated in Section II-B, and the "late commit (LC)," running on the ATX, as per Section II-C. Essentially, one or more satellite signals are received and early detected by the ARX, with the information passed over a fast link to the ATX, which has already initiated and adjusts accordingly an LC transmission. The sought result is to mislead the victim receiver that the pseudorange measurements are shorter than that they actually are. This, in turn, allows the manipulation of the computed position and time offset by acting solely at the physical layer, without any modification or guessing of the cryptographically protected parts of the navigation messages.

DD attacks are essentially an enhancement that allows such selective manipulations of authenticated signals/messages. They extend, or enhance from the adversarial viewpoint, replay/relay/meaconing attacks. For the simplified record-and-replay attack [37], let us consider two cases.

1) The adversary cannot manipulate each signal separately, using only one receiving antenna (and one

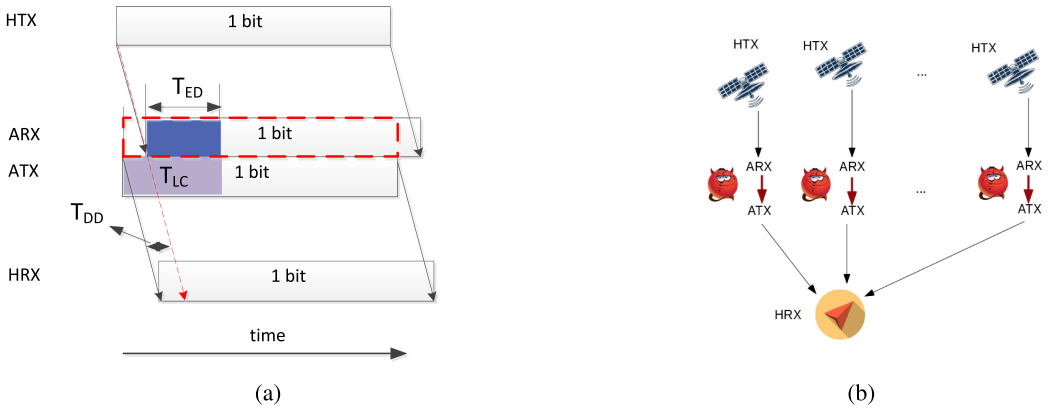


Fig. 1. DD attacks on GNSS signals. (a) Illustration of DD attack. (b) Adversary illustration for DD attack on the GNSS.

transmitting antenna). The victim receiver would compute its position to be the same as the position as the adversarial recorder and an erroneous clock offset, thus, false time. The DD attack is more potent than this type of the record-and-replay attack: it can manipulate each signal individually and reduce the perceived honest transmitter (HTX)—honest receiver (HRX) signal propagation delay.

2) The record-and-replay attacker is equipped with multiple antenna elements, which can isolate each signal individually. This attack type would be closer to the DD attack but still would lack the ability to reduce the perceived HTX—HRX signal propagation delay, which can offer finer-grained attack options (control of the victim PVT solution) and compensate the recorder and the replay latency; it eventually allows real-time record and replay.

Mounting a DD attack is orthogonal to the method chosen or needed for the ATX-sent LC signals to be received by the victim receiver, in lieu of the legitimate signals. The ATX can either transmit higher power DD signals that overshadow legitimate signals, so that the victim receiver locks on DD signals, or jam the victim and then transmit its DD LC signals [15], or implement a takeover attack [52]. The choice of action subjects to considerations pertinent to any spoofing attack and receiver possible reactions.

The exposition in Sections II-B and II-C will reveal the DD-specific considerations and how the adversary would need to act toward maximizing its chance to succeed with the DD attack, which is precisely meant to *stealthily* manipulate, as per the adversarial needs and in real time, pseudorange measurements. We emphasize that the DD-capable adversary is assumed to be cognizant of the DD-specific countermeasures in place, any potential countermeasure and notably those developed and evaluated in Section IV. The same is true in general, for countermeasures and receiver functionality that can mitigate (e.g., detect and/or reject) adversarial signals irrespective of the DD design. We do not dwell on the general-purpose countermeasures, but provide a discussion.

Overall, our adversarial model does not constrain the knowledge of the adversary in terms of countermeasures in place. Put differently, the countermeasures developed in Section IV do not rely on "security by obscurity." In fact, based on the evaluation in Section IV, an attack variant seeking to defeat the known DD countermeasure is identified. Our DD attack formulation is per signal and per pseudorange measurement, and it generalizes to multiple signals. It can further generalize to multiple ATX and ARX devices, as the sophistication and complexity of the attacker grows.

A. DD Attacks

DD attacks are physical layer attacks, illustrated in Fig. 1(a), aiming at shortening time-of-flight-based distance measurements, between an HTX and an HRX. To achieve intended manipulation, the adversary needs to act in two phases, with distinct components: 1) ED at the ARX and 2) LC at the ATX. The ATX starts transmitting signals based on an adversary-chosen bit/symbol value during T_{LC} period. When the ARX receives the data from the HTX, it estimates the data value only based on the early fraction of the bit period, T_{ED}. Hereafter, the ARX informs the estimated value to the ATX. Upon receipt, the ATX switches the transmission of the adversary-chosen value to the estimate. In consequence, the DD signal appears as if it arrives a time T_{DD} earlier than the legitimate HTX-originating signal at the HRX, thus shortening the measured distance between the HTX and the HRX by $T_{\mathrm{DD}} \cdot V_C$. Here, $T_{\mathrm{DD}} = T_{\mathrm{LC}} - T_{\mathrm{ED}} - T_d$ and V_C is the speed of light, with T_d being the delay introduced by the attacker, including processing and transmission time, at the ARX and the ATX and their communication.

The adversary deploys a pair of ARX–ATX for each targeted signal, as shown in Fig. 1(b). The ARX estimates the symbol value within the T_{ED} period and sends the estimated data value along with other signal parameters to the ATX. The ATX assembles new signals based on the ARX-provided values and sends the assembled signals to the HRX. More specifically, the ARX and the ATX can be located on the same hardware platform or can be

connected across a dedicated high-rate data link; then, the communication delay between them is negligible, compared to data bit length of the GNSS signals, e.g., Galileo E1 OS symbol length is 4 ms. However, each ARX does not have to be a dedicated hardware receiver. The ARX could be a processing thread/channel operating on each satellite signal with ARXs sharing one receiver antenna. The same is true for the ATX. Undoubtedly, a sophisticated DD attacker can have multiple distinct ARX and/or ATX devices. An advantage, for example, of having multiple antennas is that the adversary would be able to imitate the arriving angles of received signals at the HRX as if they originate from different satellites.

As discussed in the beginning of this section, DD attacks offer more flexibility from the adversarial viewpoint, compared to simple record-and-replay attack [53]. Without elaborating on this here, we discuss briefly how DD attacks can be used by the adversary. A GNSS receiver position can be obtained with

$$Y = HX + v \tag{1}$$

where Y is the pseudorange measurements, H is the observation matrix, X is the receiver state, including the 3-D coordinates and the clock offset, and v is the noise. Let the adversary-reduced shift of the victim receiver be ΔX, from its true state, more specifically $\Delta X = (\Delta x, \Delta y, \Delta z, \Delta t)$. If $\Delta x = \Delta y = \Delta z = 0$ and $\Delta t \neq 0$, the attack would be a synchronization attack, which only shifts the clock of the victim. Otherwise, for any or all of Δx, Δy, and Δz not being zero, the attack modifies the position of the victim receiver too. Then, the adversary can estimate how much each pseudorange measurement it can modify to achieve this goal

$$\hat{\Delta Y} = H\Delta X \tag{2}$$

where $\hat{\Delta Y} = [\Delta Y_1, \Delta Y_2, \ldots, \Delta Y_n]^T$ is a vector of pseudorange measurement changes corresponding to the n available signals. Based on this, the adversary can decide how to configure T_{LC} and T_{ED} to obtain the required change on each pseudorange measurement with $\Delta Y_i = V_C T_{\mathrm{DD}} = V_C(T_{\mathrm{LC}} - T_{\mathrm{ED}} - T_d)$, assuming that T_d is known to or under the control of the attacker. Moreover, the adversary could lengthen the pseudorange measurement if needed, by making $T_{\mathrm{DD}} < 0$ by choosing proper T_{LC} and T_{ED}.

B. ED on GNSS Signals

The signals transmitted by the satellites are written as

$$S_k(t) = \sqrt{2P_0}g_k(t)\cos(2\pi f t) \tag{3}$$

where P_0 is the power of the signals, k is the satellite index, f is the signal frequency, and $g(t)$ is a function of spreading sequence and data bits.

At the ARX, the received signals at baseband can be written as

$$\begin{aligned} R(t) &= \sum_k S_k(t - \tau_k) + N(t) \\ &= \sum_k \sqrt{2P_k}g_k(t - \tau_k)\cos\left(2\pi f_{d,k}t + \phi_k\right) + N(t) \end{aligned} \tag{4}$$

where P is the received signal power, τ is the time delay, f_d is the Doppler frequency, ϕ is the carrier phase, and $N(t)$ is the Gaussian noise.

The ARX, similarly to any legitimate receiver, has information on the signal modulation and navigation message format, including the preamble code. Each ARX first needs to lock on the satellite signal it wants to attack, so that the attacker has a precise estimate of the signal parameters.

With those precise estimates, the ARX can estimate the symbol value with coherent demodulation [54] by multiplying $R(t)$ with the local carrier wave and spreading code, without loss of generality, for satellite 1:

$$x_p(t) = R(t)\mathrm{PN}_1(t - \tau_1)\cos(2\pi f_{d,1}t + \phi_1) \tag{5}$$

where PN_1 is the pseudonoise sequence of satellite 1.

By integrating $x_p(t)$ over ED period T_{ED}, we obtain

$$x_p = \int_0^{T_{ED}} x_p(t)dt = S + \zeta \tag{6}$$

where S is the desired content of the decision statistic that is used to determine bit value, and ζ is a random variable, representing both environment noise and multiple access interference (MAI) from other spreading code sequences [55], [56].

We have

$$\begin{aligned} S &= \int_{t=0}^{T_{\mathrm{ED}}} \sqrt{2P_1}g_1(t - \tau_1)\cos\left(2\pi f_{d,1}t + \phi_1\right) \\ &\quad \times \mathrm{PN}_1(t - \tau_1)\cos(2\pi f_{d,1}t + \phi_1)dt \\ &= \sqrt{\frac{P_1}{2}}b\int_{t=0}^{T_{\mathrm{ED}}} \left(1 + \cos(4\pi f_{d,1}t + 2\phi_1)\right)dt \\ &\approx \sqrt{\frac{P_1}{2}}T_{\mathrm{ED}}b \end{aligned} \tag{7}$$

where b is the bit value.

Considering K available satellite signals in total, without loss of generality, the MAI for the first signal, $k = 1$, from the remaining ones can be written as follows:

$$\begin{aligned} \mathrm{MAI} = \sum_{k=2}^{K} \int_{t=0}^{T_{\mathrm{ED}}} &\sqrt{2P_k}g_k(t - \tau_k)\cos(2\pi f_{d,k}t + \phi_k) \\ &\times \mathrm{PN}_1(t - \tau_1)\cos(2\pi f_{d,1}t + \phi_1)dt \end{aligned} \tag{8}$$

where τ and ϕ are modeled as two independent uniformly distributed variables, over $[0, T_b]$ and $[0, 2\pi]$, respectively. Thus, MAI is a random variable with zero mean and variance [57]

$$\mathrm{Var}\{\mathrm{MAI}\} = \frac{NT_c^2}{6}\sum_{k=2}^{K} P_k = \frac{T_{\mathrm{ED}}T_c}{6}\sum_{k=2}^{K} P_k \tag{9}$$

where T_c is the chip length and N is the number of chips over ED period.

Therefore, the bit error rate, while considering noise and MAI, is written as [57]

$$P_e = Q\left(\frac{\sqrt{\frac{P_1}{2}T_{\mathrm{ED}}}}{\sqrt{\frac{T_{\mathrm{ED}}T_c}{6}\sum_{k=2}^{K}P_k + \frac{N_0 T_{\mathrm{ED}}}{4}}}\right) = Q\left(\frac{\sqrt{\frac{P_1}{2}T_{\mathrm{ED}}}}{\sqrt{\frac{T_c}{6}\sum_{k=2}^{K}P_k + \frac{N_0}{4}}}\right) \tag{10}$$

where $N_0/2$ is the two-sided power spectral density of the Gaussian noise in ζ.

C. LC on GNSS Signals

The ATX can be positioned in a way that is best for transmitting the adversarial signals to the HRX; for instance, the ATX having a good view of the HRX and/or being close enough to the HRX in order to relatively easily achieve, for example, similar reception power to that of authentic signals, allowing the ATX to adjust its transmission power and other parameters accordingly.

In the LC phase, the adversary adopts different approaches to craft the DD signals. In [41], four different approaches were discussed, on how to craft the transmitted signals for each bit/symbol/chip. Take an example of the Galileo E1 OS signals; the choices that can be applied are: 1) the adversary-chosen part for each symbol is a fixed value, $+1$ or -1, and 2) the adversary-chosen part is the same value as the last symbol that has already been decoded.

The signal assembled by the ATX for each symbol is written as

$$S_{\mathrm{ATX}}(t) = \begin{cases} A_1 f_1(t), & 0 \le t < T_{\mathrm{LC}} \\ A_2 f_2(t), & T_{\mathrm{LC}} \le t \le T_b \end{cases} \tag{11}$$

where $f_1(t)$ is a function of the adversary-chosen symbol value, spreading code, and carrier wave, and $f_2(t)$ is a function of the ARX-estimated symbol value, spreading code, and carrier wave. As the second part of each symbol, $f_2(t)$, is the one that needs to essentially convey the estimation of the actual HTX value as estimated by the ARX, so the accumulated energy by the HRX should be dominated by the second part in order to correctly decode the symbol. Therefore, we have

$$A_2 \cdot (T_b - T_{\mathrm{LC}}) > A_1 \cdot T_{\mathrm{LC}} \tag{12}$$

which is rewritten as

$$T_{\mathrm{LC}} < \frac{A_2}{A_1 + A_2} T_b. \tag{13}$$

Therefore, the adversary can configure A_1 and A_2 properly to allow higher T_{LC}, so that the ARX has more flexibility to set T_{ED} and higher effect on T_{DD}, due to $T_{\mathrm{DD}} = T_{\mathrm{LC}} - T_{\mathrm{ED}} - T_d$.

In order to force the HRX lock on DD signals, the adversary can either jam the reception of legitimate signals, then transmits the DD signals, or implements a smooth takeover attack, but the latter is difficult in practice. Therefore, with a jamming attack, the HRX loses its tracking on legitimate signals and then tries to do satellites re-acquisition. A within-symbol transition is not allowed for satellite acquisition, which must be considered while crafting the DD signals. The adversary can solve this challenge by starting assembling the DD signals from the preamble code [58], [59], since the preamble code is known publicly. Hence, the preamble code is transmitted correctly without a within-symbol transition. Then, the victim receiver will acquire and lock on the DD signals successfully.

Finally, the signals arriving at the HRX can be written as

$$R_{\mathrm{HRX}}(t) = \sum_k \sqrt{2P_k} S_k(t - \tau_k)\cos\left(2\pi(f + f_{d,k})t + \phi_k\right) + \sum_k S_{\mathrm{ATX},k}(t - \tau_{\mathrm{DD},k}) + N(t) \tag{14}$$

where the terms with DD subscript are for the assembled DD signals, otherwise for the authentic signals. $\tau_{\mathrm{DD}} = \tau - T_{\mathrm{DD}}$ indicates that the DD signals arrive T_{DD} earlier than the authentic signals.

III. DD ATTACK EFFECTIVENESS

As the European GNSS Agency is testing the Galileo E1 OS NMA service, we conduct experiments on the Galileo E1 OS signals in this article. Composite binary offset carrier $(6, 1, \frac{1}{11})$ modulation is used in the Galileo E1 OS signals, which consists of two components: 1) the data component on channel B and 2) the dataless component on channel C. The composite signal, i.e., $g(t)$ in (15), can be written as [58]

$$\begin{aligned} g(t) &= \frac{1}{\sqrt{2}}\left\{D(t)C_{E1B}(t)\left(\alpha sc_{E1-B,a}(t) + \beta sc_{E1-B,b}(t)\right)\right. \\ &\quad \left. -C_{E1C}(t)\left(\alpha sc_{E1-C,a}(t) - \beta sc_{E1-C,b}(t)\right)\right\} \\ &= \frac{1}{\sqrt{2}}\left\{S_{E1B}(t) + S_{E1C}(t)\right\} \end{aligned} \tag{15}$$

where $D(t)$ is the data message, $C_{E1B}(t)$ and $C_{E1C}(t)$ are ranging codes for channels B and C separately, $sc_{X,s}(t) = \mathrm{sgn}(\sin(2\pi R_{X,s}t))$ is the subcarrier, with rate, $R_{E1-B,a} = R_{E1-C,a} = 1.023$ MHz, $R_{E1-B,b} = R_{E1-C,b} = 6.138$ MHz, $\alpha = \sqrt{10/11}, \beta = \sqrt{1/11}$, and the composite signal is modulated on a carrier wave for transmission.

Based on the navigation message structure of the Galileo E1 OS signals, each nominal page of the data message is illustrated in Fig. 2 [58]. One proposal for NMA in Galileo E1 OS signals is to have 40 bits of the "Reserved 1" field assigned for the MAC and keys [36]. The convolutional encoding for all data pages is performed with coding rate 1/2, and the resultant symbols are written as $D(t)$ in (15). These symbol values are the "targets" that the ARX tries to estimate during the ED phase, as presented in (5).

The digitized RF signal we used for the evaluation is recorded by NT1065_USB3 [60] after the receiver front-end, with four Galileo E1 satellite signals: PRN[3, 5, 9, 22]. We developed a software receiver, based on [61], for the Galileo E1 OS signal and its message structure [58]. In the Galileo software receiver, we define two more correlators, Very Early (VE) and Very Late (VL), in addition to the three correlators in the GPS software receiver in [49], Early (E),

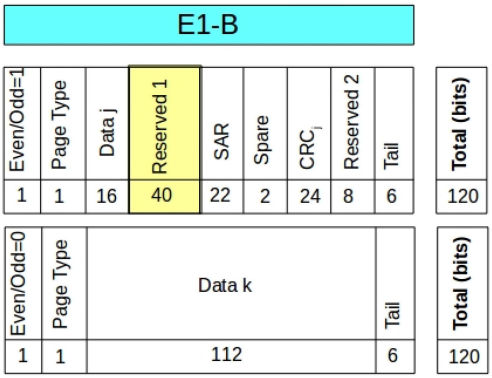


Fig. 2. One nominal page of the E1B I/NAV message.

Prompt (P), and Late (L), to avoid tracking a local maximum instead of a global maximum of the cross-ambiguity function [61], [62].

We synthesize the attack signals as follows: the ARX locks on to one signal; then, the adversary starts assembling the DD signal at the ATX with an adversary-chosen symbol value. After T_{DD}, the ARX starts ED on the received signal over period T_{ED}. Then, the ARX conveys the estimated parameters to the ATX. Hereafter, the ATX switches to transmitting the estimated value from the ARX. Finally, the mixture of the crafted signal and original signals is fed to the HRX.

The error probability of the ED phase is first evaluated for different signal-to-noise ratio (SNR) and T_{ED}. Since there is only one SNR value for each recorded signal, so we add simulated Gaussian noise with desired power to the signal during T_{ED} to manually change the signal SNR for the sake of evaluation. Consequently, the error probability of the ED phase can be evaluated based on a large range of SNR not present in the recorded signals.

In the dataset, the estimated carrier-to-noise ratio, notably $\mathrm{C/N_0}$, of the signal is 47 dB $\cdot$ Hz [dark blue line in Fig. 3(a)]. Together with the true $\mathrm{C/N_0}$, Fig. 3(a) shows the synthesized noise environment, $\mathrm{C/N_0} = 31 \sim 45$ dB $\cdot$ Hz, by adding the corresponding noise. The SNR at the tracking output is calculated based on the synthesized $\mathrm{C/N_0}$ [63]

$$\mathrm{C/N_0(dB \cdot Hz)} = \mathrm{SNR(dB)} - 10\log_{10}(T_{\mathrm{coh}}) \tag{16}$$

where T_{coh} is the coherent time, which is T_{ED} for the ED phase.

In Fig. 3, specifically in Fig. 3(b), we see the theoretical symbol error rate as per (10) as a function of $\mathrm{C/N_0}$, which can be converted to the SNR with the help of (16). As shown in Fig. 3(c), the ED performance, i.e., symbol error rate, at the ARX matches the theoretical results in the synthesized noise environment.

This provides the adversary a guidance about the choice of a proper T_{ED} based on its environment. A low T_{ED} is preferable, because it gives a wide range of choice for T_{LC} and T_{DD}, given $T_{\mathrm{DD}} = T_{\mathrm{LC}} - T_{\mathrm{ED}} - T_d$. However, the ED phase introduces unnegligible symbol errors with a low T_{ED} in a noisy environment, e.g., $T_{\mathrm{ED}} < 700$ chips at $\mathrm{C/N_0} = 38$ dB $\cdot$ Hz, as shown in Fig. 3(c). In Fig. 3(b) and (c), the lowest value in the y-axis represents zero symbol error rate. It requires higher T_{ED} to avoid introducing symbol errors in noisier environment, $\mathrm{C/N_0} < 38$ dB $\cdot$ Hz. Thus, the adversary needs to set a higher T_{LC} accordingly; in consequence, it requires the ATX to transmit the second part of the DD signal with a higher power, which can be a clear indication of an attack. Therefore, deployed at an open location to achieve high $\mathrm{C/N_0}$, e.g., $\mathrm{C/N_0} > 45$ dB $\cdot$ Hz in Fig. 3(b) and (c), the ARX can attain almost zero symbol errors even with a low T_{ED}.

In the simulation, the ATX assembles the first ten symbols with the preamble code, i.e., 0101100000, of the signal, allowing the HRX to acquire the DD signals correctly. The preamble code occurs every 2 s for the Galileo E1 OS signals; therefore, the attacker has exact information about when the next preamble code will come; thus, the ATX can start assembling the DD signals T_{DD} ahead of the actual preamble code reception time. Fig. 4 illustrates how the five correlator outputs perform at the HRX with different synthesized noise environment. The parameters for this illustration example are: $T_{\mathrm{LC}} = 1522$ chips and $A_2/A_1 = 6.5$ (12). In Fig. 4(a) and (b), the left corner plot is I–Q (in-phase and quadrature) prompt plot that represents symbol binary value constellation; the top right corner plot gives the in-phase prompt correlator output, i.e., I_P; the bottom plot is the correlation results of the five correlators, which shows that the power of the prompt correlator is much higher than that of other correlators when the receiver is locking on the signals. When the receiver has low SNR, as presented in Fig. 4(a), the DD signal gives similar correlator outputs as a legitimate signal. However, with a high SNR, as shown in Fig. 4(b), there is a clear separation of the in-phase prompt correlator output, due to that the adversary needs to transmit some predefined value before obtaining the estimation from the ARX. This is also the motivation of our proposed countermeasure presented in the next section.

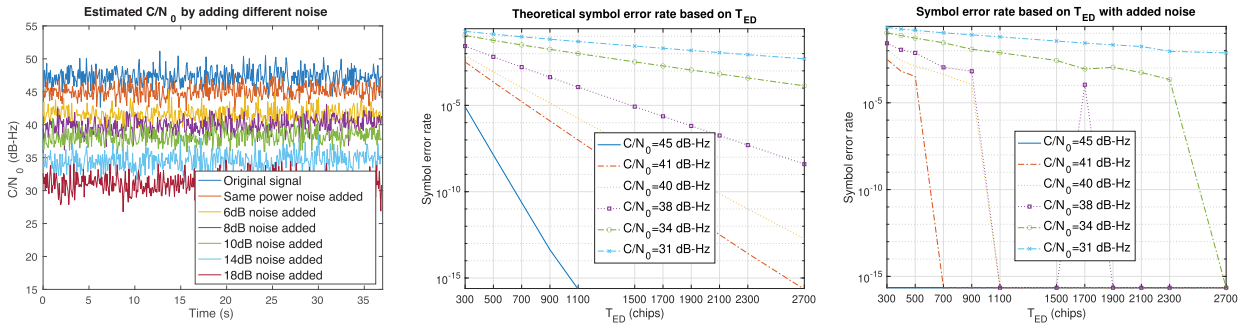
IV. THWARTING DD ATTACKS

The main observation of (11) is that the DD attack signal has a special feature that can be used to counter the attack: the transition within each symbol. The reason is that in the LC phase of a DD attack, each symbol has two independent parts, i.e., a within-symbol transition that is not present in a legitimate signal. Therefore, we can design a statistical test to examine the DD attack in a GNSS receiver with a software patch, providing a real-time countering solution.

A. Mathematical Model for Attack Detection

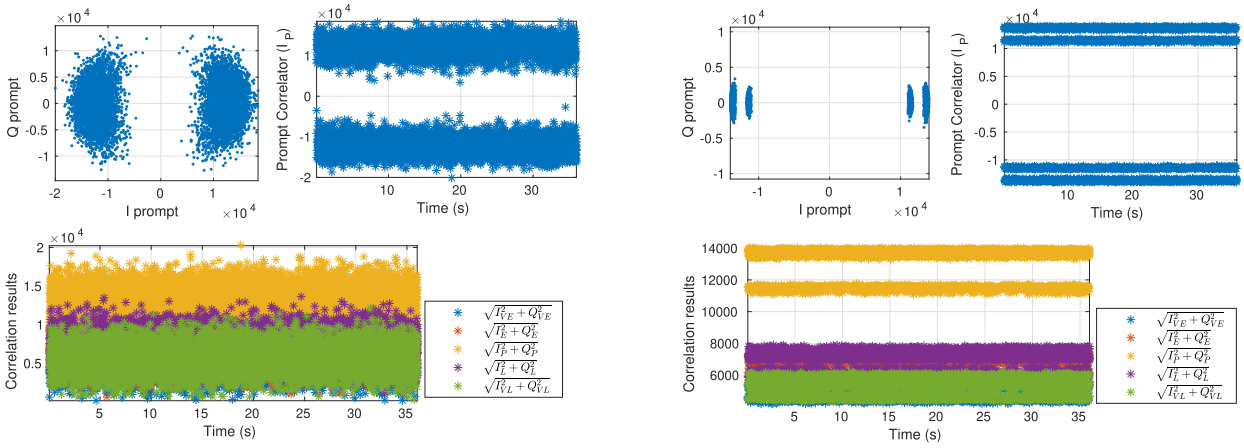
During the tracking phase in a GNSS receiver, the input signal is multiplied with a locally generated spreading code and carrier wave. Then, the result, $x(i)$, goes through a low-pass filter and is integrated over period T_{int}, which finally yields the outputs of different correlator, e.g., I_P and Q_P for prompt correlators.

For legitimate signals, the in-phase arm of the prompt correlator, i.e., I_P, of the HRX provides energy integration



(a) (b) (c)

Fig. 3. Performance evaluation of the ARX. (a) C/N_0 estimation in synthesized environment with added noise for one satellite signal. (b) Theoretical symbol error rate based on (10). (c) Symbol error rate of the dataset with different synthesized C/N_0.



(a) (b)

Fig. 4. Illustration of the tracking results with five correlators: Early (E), Very Early (VE), Prompt (P), Late (L), and Very Late (VL), at the HRX when $T_{\mathrm{LC}} = 1522$ chips for the Galileo E1 OS signal. (a) SNR = 15 dB at tracking output. (b) SNR = 22 dB at tracking output.

over period T_{int}, same length as the symbol period, i.e., T_b. With precise estimate of carrier phase and code delay, multiplying the received legitimate signal with local spreading code and carrier wave, we have the following sampled output:

$$x^0_{I_p,i} = R(iT_s - \tau)\mathrm{PN}(iT_s - \tau)\cos(2\pi f_d iT_s + \phi) \tag{17}$$

where PN(.) is the local spreading code, cos(.) is the local carrier wave, and $T_s = 1/f_s$ is the sampling interval.

Accumulating the sample energy, we have the accumulator output, for symbol n:

$$I^0_P[n] = \sum_{i=0}^{T_{\mathrm{int}} f_s} x^0_{I_p,i} = \sqrt{\frac{P}{2}} f_s T_{\mathrm{int}} b[n] + N_0[n] \tag{18}$$

where b is the data value: $\{+1, -1\}$, and N_0 is the Gaussian noise.

Therefore, I^0_P, representing legitimate signals, follows a normal distribution

$$\begin{aligned} I^0_{P_+}[n] &= E + N_0[n], \qquad b = +1 \\ I^0_{P_-}[n] &= -E + N_0[n], \qquad b = -1 \end{aligned} \tag{19}$$

where we define $E = \sqrt{\frac{P}{2}} \cdot f_s \cdot T_{\mathrm{int}}$, and $I^0_{P_+}$ and $I^0_{P_-}$ represent positive and negative elements of I^0_P, separately, which give $+1$ and -1 soft decision of the symbol value, respectively.

With the DD signals, i.e., S_{ATX} in (11), we have

$$\begin{aligned} x^{\mathrm{DD}}_{I_p,i} &= S_{\mathrm{ATX}}(iT_s - \tau)\mathrm{PN}(iT_s - \tau)\cos(2\pi f_d iT_s + \phi) \\ &= (u(iT_s - T_{\mathrm{LC}}) - u(iT_s))\, S_{\mathrm{ATX}}(iT_s - \tau) \\ &\quad \times \mathrm{PN}(iT_s - \tau)\cos(2\pi f_d iT_s + \phi) \\ &\quad + (u(iT_s - T_b) - u(iT_s - T_{\mathrm{LC}}))\, S_{\mathrm{ATX}}(iT_s - \tau) \\ &\quad \times \mathrm{PN}(iT_s - \tau)\cos(2\pi f_d iT_s + \phi) \end{aligned} \tag{20}$$

where $u(t)$ is the unit step function.

By accumulating the energy over T_{int}, for symbol n, we have

$$\begin{aligned} I^{\mathrm{DD}}_P[n] &= \sum_{i=0}^{T_{\mathrm{int}} f_s} x^{\mathrm{DD}}_{I_p,i} = b_{\mathrm{pre}}[n]\sqrt{\frac{P}{2}} f_s T_{\mathrm{LC}} \\ &\quad + b[n]A\sqrt{\frac{P}{2}} f_s (T_{\mathrm{int}} - T_{\mathrm{LC}}) + N_0[n] \\ &= b_{\mathrm{pre}}[n]E\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} + b[n]AE\frac{T_{\mathrm{int}} - T_{\mathrm{LC}}}{T_{\mathrm{int}}} + N_0[n] \end{aligned} \tag{21}$$

where b_{pre} is the adversary-chosen symbol value, and A is the amplitude ratio of the two parts within each symbol [as defined for (11)]

$$A = \frac{A_2}{A_1} \tag{22}$$

Therefore, I_p^{DD} follows

$$I_P^{\text{DD}}[n] = \begin{cases} bE\left(A + (1-A)\frac{T_{\text{LC}}}{T_{\text{int}}}\right) + N_1[n], & b_{\text{pre}} = b \\ bE\left(A - (1+A)\frac{T_{\text{LC}}}{T_{\text{int}}}\right) + N_2[n], & b_{\text{pre}} = -b \end{cases} \tag{23}$$

where $b = +1$ or -1 is the true symbol value. If b_{pre} is chosen based on approaches in Section II-C and b is assumed being generated by a binary signal source, then b_{pre} has 50% probability to be b or $-b$; therefore, I_p^{DD} has equal probability to follow either distribution in (23).

Specifically, for $b = +1$, we have

$$I_{P_+}^{\text{DD}}[n] = \begin{cases} E\left(A + (1-A)\frac{T_{\text{LC}}}{T_{\text{int}}}\right) + N_1[n], & b_{\text{pre}} = +1 \\ E\left(A - (1+A)\frac{T_{\text{LC}}}{T_{\text{int}}}\right) + N_2[n], & b_{\text{pre}} = -1 \end{cases} \tag{24}$$

which clearly presents the difference while comparing with $I_{P_+}^0$ in (19).

The difference between means of the two normal distributions in (23) is

$$\begin{aligned} \Delta\mu &= E\left(A + (1-A)\frac{T_{\text{LC}}}{T_{\text{int}}}\right) \\ &\quad - E\left(A - (1+A)\frac{T_{\text{LC}}}{T_{\text{int}}}\right) = 2E\frac{T_{\text{LC}}}{T_{\text{int}}} \end{aligned} \tag{25}$$

which shows that the distance between two normal distributions depends on T_{LC}. The bigger T_{LC} is, the easier the DD signals can be detected.

Assuming that the phase noise is negligible, the local generated carrier is perfectly aligned with the received signals, so that the noise power in the quadrature arm is same as the noise power in the in-phase arm. Therefore, the parameter of the noise, $N_i \sim N(0, \sigma_i^2)$ $i = \{1, 2\}$, can be estimated through the quadrature arm of the prompt correlator, Q_P. For the samples of the quadrature arm, when we multiply S_{ATX} with locally generated code and carrier wave, we obtain

$$\begin{aligned} x_{Q_p,i} &= S_{\text{ATX}}(iT_s - \tau)\text{PN}(iT_s - \tau)\sin(2\pi f_d iT_s + \phi) \\ &= \frac{\sqrt{2P}}{2} b(iT_s)\sin(4\pi f_d iT_s + 2\phi) \\ &= (u(iT_s - T_{\text{LC}}) - u(iT_s))\sqrt{\frac{P}{2}} b_{\text{pre}}(iT_s) \\ &\quad \times \sin(4\pi f_d iT_s + 2\phi) \\ &\quad + (u(iT_s - T_b) - u(iT_s - T_{\text{LC}}))A\sqrt{\frac{P}{2}} b(iT_s) \\ &\quad \times \sin(4\pi f_d iT_s + 2\phi). \end{aligned} \tag{26}$$

Same as the in-phase arm, $x_{Q_P}(i)$ is fed to a low-pass filter, and then, its energy, Q_P, is accumulated over T_{int}. And by assuming that $x_{Q_p}(i)$ are uncorrelated with $E\{x_{Q_p}(i)\} = 0$, Q_P can be used to estimate the noise power with the following:

$$E\{Q_P^2\} = \bar{Q}_P^2 = E\left\{\left(\sum_{i=1}^{f_s T_{\text{int}}} x_{Q_p,i}\right)^2\right\} = \sum_{i=1}^{f_s T_{\text{int}}} E\left\{\left(x_{Q_p,i}\right)^2\right\}. \tag{27}$$

Applying (26) to (27), we can get the variance of Q_P for cases when $b_{\text{pre}} = b$ and $b_{\text{pre}} = -b$ in (28), shown at the bottom of this page. We see that the variance of Q_P is higher if $b_{\text{pre}} = b$, compared to $b_{\text{pre}} = -b$. This explains the difference between two pair of eyes in the I–Q plot of Fig. 4(b): the variance of Q_P of the two outside eyes, drawn for case $b_{\text{pre}} = b$, is higher compared to that of the two inside eyes, drawn for case $b_{\text{pre}} = -b$.

B. Designing Hypothesis Tests

Depending on whether the HRX has knowledge about the special feature, i.e., within-symbol transition, of the DD attacks, one can design different tests to detect the attacks.

1) *Without Knowledge of DD Signals:* Without the knowledge of the DD attacks, the HRX can design a test with the following hypothesis:

$$\begin{cases} \text{Null hypothesis:} & I_P \sim N(\mu_0, \sigma^2) \\ \text{Alternative hypothesis:} & I_P \nsim N(\mu_0, \sigma^2) \end{cases} \tag{29}$$

where μ_0 is and σ^2 are unknown.

Without prior information about the attacks, the HRX can only test whether the correlator output follows a normal distribution or not, referring to (19) and (29). For such circumstances, we design a goodness-of-fit (GoF) test to detect the existence of attacks. The Kolmogorov–Smirnov test, the Anderson–Darling test, the Shapiro–Wilk test, and the Chi-squared test are typically used for GoF testing [64]. The Chi-squared test is used for categorical data that is not our case, and in [65], it was found that the Shapiro–Wilk test has the best power for a given significance level compared to

$$E\{Q_P^2\} = \begin{cases} \sum_{i=1}^{f_s T_{\text{int}}} E\left\{\left\{[(u(iT_s - T_{\text{LC}}) - u(iT_s)) + A\,(u(iT_s - T_b) - u(iT_s - T_{\text{LC}}))]\sqrt{\frac{P}{2}} b\sin(4\pi f_d iT_s + 2\phi)\right\}^2\right\}, & b_{\text{pre}} = b \\ \sum_{i=1}^{f_s T_{\text{int}}} E\left\{\left\{[-(u(iT_s - T_{\text{LC}}) - u(iT_s)) + A\,(u(iT_s - T_b) - u(iT_s - T_{\text{LC}}))]\sqrt{\frac{P}{2}} b\sin(4\pi f_d iT_s + 2\phi)\right\}^2\right\}, & b_{\text{pre}} = -b \end{cases} \tag{28}$$

Anderson–Darling, Kolmogorov–Smirnov, and Anderson–Darling tests. Therefore, we choose the Shapiro–Wilk test to examine whether the data are normally distributed.

The test statistics of the Shapiro–Wilk test are [49]

$$W = \frac{\left(\sum_{i=1}^{n} a_i x_{(i)}\right)^2}{\sum_{i=1}^{n}(x_i - \bar{x})^2} \tag{30}$$

where $x_{(i)}$ is the ith-smallest value in the sorted data samples (order statistics), $\bar{x} = (x_1 + \cdots + x_n)/n$ is the sample mean. The coefficients, a_i, are

$$(a_1, \ldots, a_n) = \frac{m^T V^{-1}}{||V^{-1}m||}$$

where $m = (m_1, \ldots, m_n)^T$ is the vector of expected values of the order statistics of independent and identically distributed (i.i.d.) random variables sampled from the standard normal distribution, and V is the covariance matrix of those order statistics.

2) *With Knowledge of DD Signals:* If the HRX has the knowledge, i.e., within-symbol transition, of the DD attacks and wants to detect the attacks based on that I_P^{DD} is a combination of two different Gaussian distribution, referring to (23), one can design a hypothesis test as

$$\begin{cases} \text{Null hypothesis:} & I_P \sim N(\mu_0, \sigma_0^2) \\ \text{Alternative hypothesis:} & I_P \sim \sum_{i=1}^{K} \phi_i N(\mu_i, \sigma_i^2) \end{cases} \tag{31}$$

where μ_i and σ_i^2, $i = 0, 1, 2$, are unknown, $K = 2$ indicates two components, and ϕ_i is mixture weight with $\sum_{i=1}^{K} \phi_i = 1$. More specifically, the alternative hypothesis is that I_P follows a Gaussian mixture model [66].

Given the null hypothesis in 31, I_P follows the distribution

$$f(I_P|\mu_0, \sigma_0^2) = \frac{1}{\sqrt{2\pi\sigma_0^2}} \exp\left(-\frac{(I_P - \mu_0)^2}{2\sigma_0^2}\right) \tag{32}$$

which can be written in the same format as the alternative hypothesis

$$\begin{aligned} &f(I_P|\mu_1 = \mu_2 = \mu_0, \sigma_1^2 = \sigma_2^2 = \sigma_0^2) \\ &\quad = \sum_{i=1}^{2} \phi_i \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(I_P - \mu_i)^2}{2\sigma^2}\right). \end{aligned} \tag{33}$$

For the alternative hypothesis, I_P follows the distribution

$$f(I_P|\mu_1, \mu_2, \sigma_1^2, \sigma_2^2) = \sum_{i=1}^{2} \phi_i \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp\left(-\frac{(I_P - \mu_i)^2}{2\sigma_i^2}\right) \tag{34}$$

where the two components have different mean and variance.

Therefore, given a model $f(I_P|\mu_1, \mu_2, \sigma_1^2, \sigma_2^2) = \sum_{i=1}^{2} \phi_i \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp(-\frac{(I_P-\mu_i)^2}{2\sigma_i^2})$, the testing hypotheses are

$$\begin{aligned} H_0 &: \mu_1 = \mu_2, \sigma_1^2 = \sigma_2^2 \\ H_1 &: \mu_1 \neq \mu_2, \sigma_1^2 \neq \sigma_2^2. \end{aligned} \tag{35}$$

Thus, a GLRT [67] can be used with the test statistic

$$\Lambda = \frac{\mathrm{lik}_{\max}(\mu_1 = \mu_2, \sigma_1^2 = \sigma_2^2)}{\mathrm{lik}_{\max}(\mu_1 \neq \mu_2, \sigma_1^2 \neq \sigma_2^2)} \underset{H_1}{\overset{H_0}{\gtrless}} \eta \tag{36}$$

where lik(.) is the likelihood function, i.e., with i.i.d. I_P samples, $\mathrm{like}(\mu_1, \mu_2, \sigma_1^2, \sigma_2^2) = \prod_{i=1}^{N} f(I_{P,i}|\mu_1, \mu_2, \sigma_1^2, \sigma_2^2)$, and η is the threshold that is calculated given significance level-α:

$$P[\Lambda \leq \eta | H_0] = \alpha. \tag{37}$$

The numerator of (36) is maximized when I_P follows a normal distribution, and the denominator is maximized when I_P follows a Gaussian mixture model with two components.

For the null hypothesis, we know that the maximum likelihood estimation of $\mu_{i=1,2}$ and $\sigma_{i=1,2}^2$ is

$$\begin{aligned} \hat{\mu}_1 = \hat{\mu}_2 &= \frac{1}{N}\sum_{i=1}^{N} I_{P,i} \\ \hat{\sigma}_1^2 = \hat{\sigma}_2^2 &= \frac{1}{N}\sum_{i=0}^{N} (I_{P,i} - \hat{\mu}_1)^2. \end{aligned} \tag{38}$$

For the alternative hypothesis, there are five parameters to be estimated. Given a series of observations, $x_1, \ldots, x_N$, of the normal mixture model, we have the joint probability distribution of $x_1, \ldots x_N$:

$$f(x_1, \ldots, x_N) = \prod_{i=1}^{N} f(x_i|\mu_1, \mu_2, \sigma_1^2, \sigma_2^2) \tag{39}$$

where $f(x_i|\mu_1, \mu_2, \sigma_1^2, \sigma_2^2)$ is derived from (34) by replacing I_P with x_i. Thus, the probability distribution can be rewritten as

$$\begin{aligned} &f(x_1, \ldots, x_N|\phi_1, \mu_1, \mu_2, \sigma_1^2, \sigma_2^2) \\ &\quad = \prod_{i=1}^{N} \left[\phi_1 \frac{1}{\sqrt{2\pi\sigma_1^2}} \exp\left(-\frac{(x_i - \mu_1)^2}{2\sigma_1^2}\right) \right. \\ &\qquad \left. + (1 - \phi_1) \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{(x_i - \mu_2)^2}{2\sigma_2^2}\right) \right] \end{aligned} \tag{40}$$

which is the likelihood function to estimate ϕ_1, $\mu_{i=1,2}$ and $\sigma_{i=1,2}^2$ given $x_{i=1,\ldots,N}$.

In order to find the maximum likelihood estimates, we set the first derivative of the natural logarithm of the likelihood function to zero

$$\frac{\partial \ln(f)}{\partial \mu_{i=1,2}} = 0, \quad \frac{\partial \ln(f)}{\partial \sigma_{i=1,2}^2} = 0, \quad \frac{\partial \ln(f)}{\partial \phi_1} = 0 \tag{41}$$

where the solution for ϕ_1, $\mu_{i=1,2}$, and $\sigma_{i=1,2}^2$ cannot be obtained analytically. The most popular method to find the maximum likelihood estimate is through the expectation–maximization algorithm [68]–[71], which iterates between an expectation (E) step, which builds an expectation function of the log-likelihood evaluated using the current estimate of the parameters, and a maximization (M) step, which computes parameters maximizing the expected likelihood function at the E step. The estimated parameters are used to

calculate the posterior probability of the latent observations in the next E step.

C. Parameters for Test Evaluation

In order to effectively evaluate the performance of the tests, we conduct simulations with parameters in (19) and (23) based on certain constraints. On the one hand, the attacker needs to transmit DD signals with power larger than the legitimate signals. On the other hand, the power of DD signals should not be too high since high power is also an indication of attack. Another parameter is T_{LC}, which has a constraint: $T_{\mathrm{DD}} = T_{\mathrm{LC}} - T_{\mathrm{ED}} - T_d > 0$ that gives $T_{\mathrm{LC}} > T_{\mathrm{ED}} + T_d$. Therefore, we consider the following settings for the DD signals for the evaluation:

1) $1 < P_{\mathrm{DD}}/P_{\mathrm{Legitimate}} < 10$;
2) $T_{\mathrm{LC}} \geq 1$ ms, i.e., 1023 chips for Galileo E1 OS signals.

Based on (23), we know that when $b_{\mathrm{pre}} = -b$

$$\frac{P_{\mathrm{DD}}}{P_{\mathrm{Legitimate}}} = \frac{E^2(A-(1+A)\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}})^2}{E^2} = \left(A-(1+A)\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}\right)^2 \tag{42}$$

and when $b_{\mathrm{pre}} = b$

$$\frac{P_{\mathrm{DD}}}{P_{\mathrm{Legitimate}}} = \frac{E^2(A+(1-A)\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}})^2}{E^2} = \left(A+(1-A)\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}\right)^2. \tag{43}$$

We know that the signal power with $b_{\mathrm{pre}} = -b$ is lower than that with $b_{\mathrm{pre}} = b$, so we let the lower power of I_P^{DD} satisfy

$$\frac{P_{\mathrm{DD}}^{\mathrm{low}}}{P_{\mathrm{Legitimate}}} = \frac{E^2(A-(1+A)\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}})^2}{E^2} > 1 \tag{44}$$

which yields

$$\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} < \frac{A-1}{A+1} \text{ and } \frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} > 1(\text{not applicable}). \tag{45}$$

Then, we let the higher power of I_P^{DD}, i.e., when $b_{\mathrm{pre}} = b$, satisfy

$$\frac{P_{\mathrm{DD}}^{\mathrm{high}}}{P_{\mathrm{Legitimate}}} = \frac{E^2\left(A+(1-A)\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}\right)^2}{E^2} < 10 \tag{46}$$

which, given $A > 1$, provides

$$\frac{A-\sqrt{10}}{A-1} < \frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} < \frac{\sqrt{10}+A}{A-1}. \tag{47}$$

Based on (45) and (47), we have

$$\frac{A-\sqrt{10}}{A-1} < \frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} < \min\left\{\frac{A-1}{A+1}, \frac{\sqrt{10}+A}{A-1}\right\} \tag{48}$$

which provides the bound of $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}$, constrained by signal power.

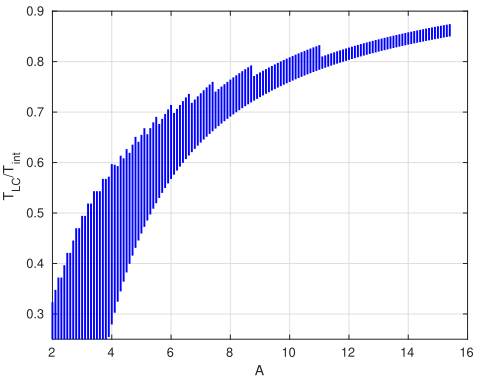


Fig. 5. Choices of $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}$ as a function of A.

TABLE I
Monte Carlo Simulation Setup for Two Tests

T_{LC}/T_{int}	[0.25, 0.372, 0.494, 0.616, 0.7136]
A	[3.8, 6.5]
SNR (dB)	0:2:30
Data size	2×10^7 samples
Sample size for each test	1000 samples

In particular, if the adversary attacks Galileo E1 OS signals, with $T_{\mathrm{LC}} \geq 1$ ms, i.e., $T_{\mathrm{LC}}/T_{\mathrm{int}} > 1/4$, as the lower bound of $T_{\mathrm{LC}}/T_{\mathrm{int}}$, we can bound $T_{\mathrm{LC}}/T_{\mathrm{int}}$ with

$$\max\left\{\frac{A-\sqrt{10}}{A-1}, \frac{1}{4}\right\} < \frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} < \min\left\{\frac{A-1}{A+1}, \frac{\sqrt{10}+A}{A-1}\right\} \tag{49}$$

where $T_{\mathrm{int}} = 4$ ms for Galileo E1 OS signals.

REMARK Note that the Galileo E1 OS signals are not the only signals that the DD signals can be applied to. Moreover, the T_{LC} value varies based on choice and objectives of the adversary and the length of T_{int} for different GNSS signals. Fig. 5 is plotted based on the relation between A and $T_{\mathrm{LC}}/T_{\mathrm{int}}$, i.e., (49), where there is a range of $T_{\mathrm{LC}}/T_{\mathrm{int}}$ corresponding to each A. With these constraints, we can see that the allowable $T_{\mathrm{LC}}/T_{\mathrm{int}}$ is small when A is set to be a small value, and the adversary can define a larger T_{LC}, in order to shorten higher pseudorange measurements, by setting a properly large A.

D. Monte Carlo Results

We first use the Monte Carlo method to evaluate the detection performance of the Shapiro–Wilk test and GLRT on the DD signals for the theoretical results. The simulation setup is illustrated in Table I, where 2×10^7 data samples are generated following the distribution of (19) and (23), separately, and the significance level is set to be $\alpha = 0.01$ for detection probability evaluation. With help of Fig. 5, $A = 3.8$ is for cases of $T_{\mathrm{LC}}/T_{\mathrm{int}} = [0.25, 0.373, 0.494]$, and $A = 6.5$ is for $T_{\mathrm{LC}}/T_{\mathrm{int}} = [0.616, 0.7136]$.

The simulation results show the power of the Shapiro–Wilk test, i.e., the detection probability, for different T_{LC}, as a function of SNR, shown in Fig. 6(a). We can see that

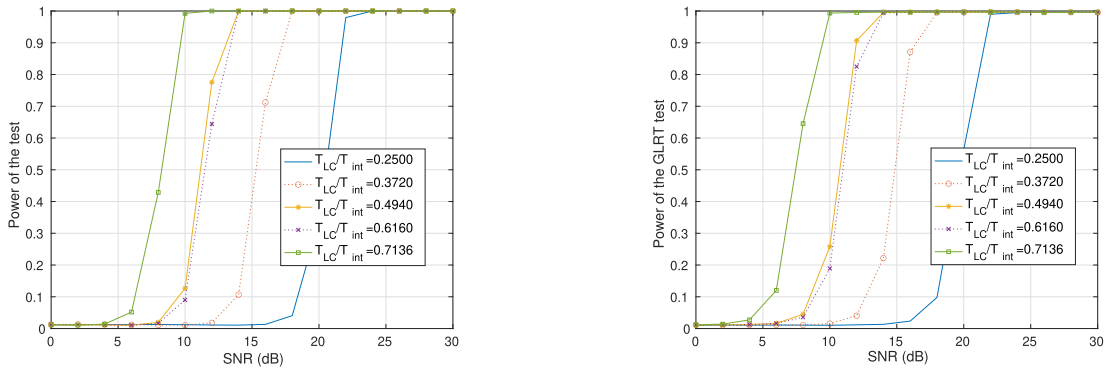


Fig. 6. Detection performance of two tests on DD attacks, with a significance level being 0.01. (a) Detection probability with the Shapiro–Wilk test. (b) Detection probability with the GLRT.

the detection probability starts approaching to 100%, when SNR $\geq$ 14 dB, for $T_{\text{LC}}/T_{\text{int}} = 0.494$, e.g., $T_{\text{LC}} = 1.976$ ms for Galileo E1 OS signals. With high SNR, e.g., SNR $>$ 22 dB, the detection probability can reach 100% with very low T_{LC}, $T_{\text{LC}}/T_{\text{int}} = 0.25$, e.g., $T_{\text{LC}} = 1$ ms for Galileo E1 OS signals. Thus, the Shapiro–Wilk test is a powerful test against the DD attacks. Moreover, we see that when the adversary attempts to shorten higher pseudorange measurements, i.e., attempt a longer T_{LC}, the Shapiro–Wilk test can detect the DD attacks even with very low SNR. For instance, the simulation shows that the detection probability approaches 100% with $T_{\text{LC}}/T_{\text{int}} = 0.7136$, i.e., $T_{\text{LC}} = 2.854$ ms for Galileo E1 OS signals, even when SNR $= 10$ dB. Essentially, one confirms that the more aggressive, the more impact the adversary attempts to be, i.e., the higher T_{DD} is, the higher T_{LC} is, the more likely to be detected.

Moreover, Fig. 6(b) shows the power of the GLRT against DD attacks when the significance level is 0.01. We can see that the GLRT is also very powerful on detecting the DD attacks when $T_{\text{LC}}/T_{\text{int}} > 0.494$, at low SNR, i.e., SNR $= 14$ dB, which is similar to the GoF test. And the detection performance is also good, almost 90%, when $T_{\text{LC}}/T_{\text{int}} > 0.372$ at SNR $= 16$ dB. Overall, the longer T_{LC} is, the larger the adversarial pseudorange measurements decrease, and thus the easier to detect the attacks. For a particular case when $T_{\text{LC}}/T_{\text{int}} = 0.372$, i.e., $T_{\text{LC}} = 1.488$ ms for Galileo E1 OS signals, the adversary has a very narrow space to shorten pseudorange measurements due to $T_{\text{LC}} > T_{\text{ED}} + T_d$; however, the GLRT can still provide 100% detection probability of the DD attacks when SNR $>$ 18 dB.

Looking at Fig. 6(a) and (b) together, we see that the GLRT outperforms the GoF test, with about 20% higher detection probability, for settings that the detection probability is close to 100%. For instance, when $T_{\text{LC}}/T_{\text{int}} = 0.372$ and SNR $= 16$ dB, the detection probability of GLRT is 88%, while it is 71% for the GoF test. We also see that the detection probability is similar for $T_{\text{LC}}/T_{\text{int}} = 0.494$ and $T_{\text{LC}}/T_{\text{int}} = 0.616$. The reason is that the performance depends on the separation of two normally distributed components. According to [72], the separation of two normal distributions in a mixed data samples can be qualitatively analyzed with

$$D = \frac{|\mu_1 - \mu_2|}{\sqrt{\sigma_1^2 + \sigma_2^2}} \tag{50}$$

where $\mu_{i=1,2}$ and $\sigma_{i=1,2}^2$ are means and variances of two distributions, respectively. The larger D is, the better separation they have. With the settings in Table I, D of $T_{\text{LC}}/T_{\text{int}} = 0.494$ and $T_{\text{LC}}/T_{\text{int}} = 0.616$ have similar values at different SNRs, which leads to similar performance, as shown in Fig. 6(a) and (b). Taking an example of SNR $= 12$ dB in the simulation, we have

$$D = [0.492, 0.867, 1.401, 1.349, 2.012] \tag{51}$$

for

$$T_{\text{LC}}/T_{\text{int}} = [0.25, 0.372, 0.494, 0.616, 0.7136] \tag{52}$$

separately, which shows that D is similar to each other for $T_{\text{LC}}/T_{\text{int}} = [0.494, 0.616]$, comparing to D for other $T_{\text{LC}}/T_{\text{int}}$ values. This confirms the similar detection performance for $T_{\text{LC}}/T_{\text{int}} = [0.494, 0.616]$ in Fig. 6(a) and (b). Moreover, the value of D for $T_{\text{LC}}/T_{\text{int}} = 0.494$ is slightly bigger than that for $T_{\text{LC}}/T_{\text{int}} = 0.616$, which also explains and confirms that the detection probability for $T_{\text{LC}}/T_{\text{int}} = 0.494$ is slightly higher than that for $T_{\text{LC}}/T_{\text{int}} = 0.616$, even the former has smaller T_{LC}.

As the detection heavily depends on the SNR, a noise generator could be used by the adversary, preferably close to the victim receiver. The adversary can transmit additive noise to reduce the C/N_0 at the receiver, with the SNR at the tracking output decreasing accordingly. Consequently, detection capability degrades due to the adversary-induced low SNR. The procedure, for such an augmented attack, a DD attack with the noise transmitter in parallel, can be as follows: the adversary can estimate approximately the victim receiver's C/N_0 due to its proximity to the receiver; together with a known T_{LC} chosen by the adversary, the adversary can estimate the level of noise to transmit to the victim receiver so that the detection degrades, while the HRX still decodes correctly the DD-crafted symbols.

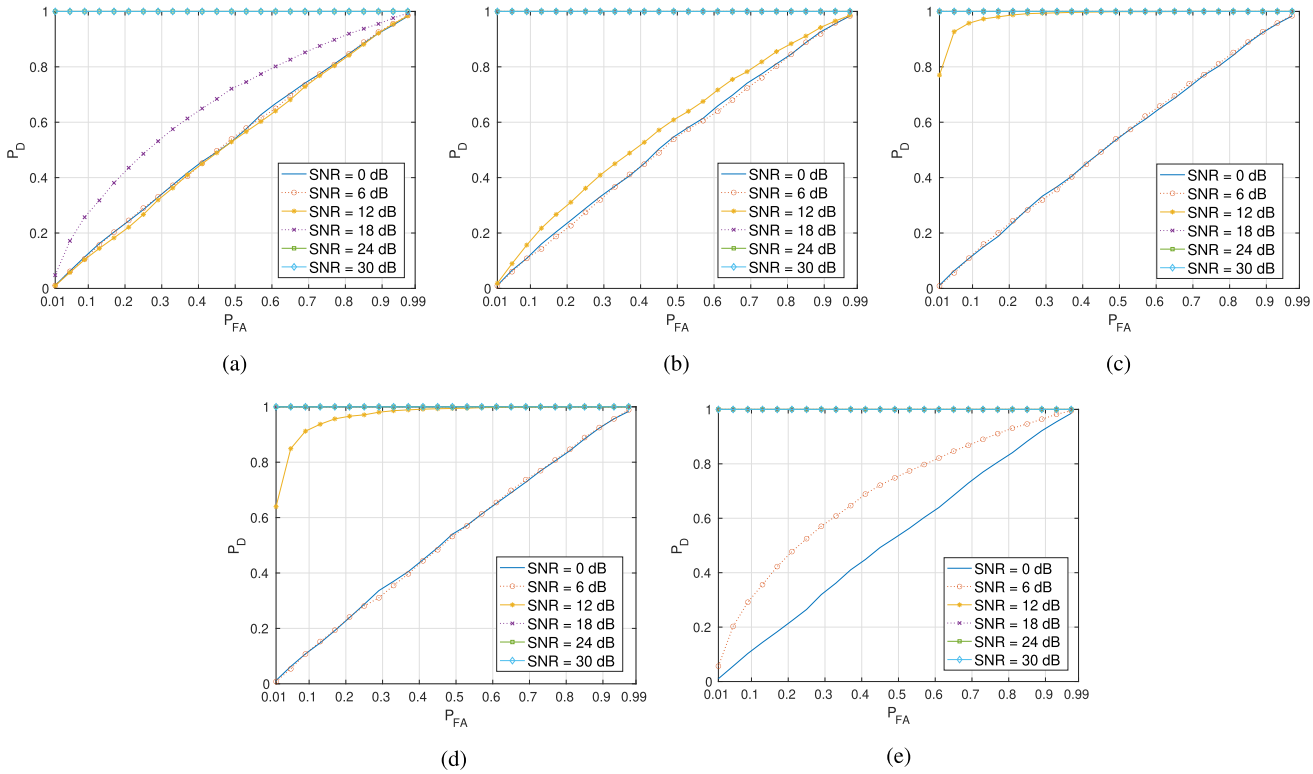


Fig. 7. ROCs for the GoF test with different settings of SNR and $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}$. (a) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.25$. (b) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.372$. (c) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.494$. (d) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.616$. (e) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.7136$.

We can term this a "DD with adversarial noise (DD-AN)" attack. However, the DD-AN can be countered by updating the HRXs, to reject or mark as suspicious signals in very low $\mathrm{C/N_0}$ conditions—setting a threshold and flagging the possibility of this variant of DD attack and, consequently, the computed PVT as not trustworthy. This would prevent the success of the DD-AN attack but, of course, would result in converting it, intended to be an attack that manipulates the victims PVT, into flagged suspicious setting and eventually a denial of service (exclusion of signals and no PVT computation).

Furthermore, we evaluate the optimality of the GOF test on detecting the DD attacks based on the receiver operating characteristic (ROC) curves [67], plotting the probability of detection, P_D, against the probability of false alarm, P_{FA}, in different settings, as shown in Fig. 7. These ROC curves can be beneficial for both parties: the adversary and the HRX. For instance, if the adversary estimates SNR at the HRX as 18 dB approximately, and the adversary does not want the HRX to detect the attack with high P_D and low P_{FA}, then the adversary can design the DD signals around $T_{\mathrm{LC}}/T_{\mathrm{int}} = 0.25$. On the HRX side, if the attack detection targets are $P_{\mathrm{FA}} < 5\%$ and $P_D > 93\%$ for situations of SNR > 12 dB, the HRX knows that this test can satisfy the targets when $T_{\mathrm{LC}}/T_{\mathrm{int}} \geq 0.494$. If the HRX wants to achieve the targets for lower T_{LC}, the HRX should try to increase the SNR accordingly with different techniques, e.g., adjusting tracking loop filter parameters or adopting a better low-noise amplifier with higher gain and lower noise figure.

Meanwhile, the ROC curves of the GLRT for different SNR and $T_{\mathrm{LC}}/T_{\mathrm{int}}$ values are shown in Fig. 8. The ROC curves can also serve both adversary and GNSS receiver for their purposes, as discussed for the GoF test. Looking at Figs. 7 and 8, we see that the GLRT outperforms the GoF test slightly at various settings. The reason behind this is that the receiver has prior knowledge about DD attacks, e.g., there are two Gaussian components in the alternative hypothesis. This prior information provides some help in accelerating the testing the hypotheses that the GLRT has better detection performance at low SNR with same T_{LC} settings. Taking $T_{\mathrm{LC}}/T_{\mathrm{int}} = 0.616$ as an example, the area under the ROC curve of SNR $= 12$ dB in GLRT is larger than that in the GoF test. For high SNR, both the GoF test and the GLRT provide very good performance, high or practically 100% probability of detection with very low false alarm probability.

Regarding the effectiveness at low SNR (this is the estimated SNR at the tracking output), in Fig. 6, we see that the countermeasures are not effective when the SNR is lower than 10 dB. With SNR $= 10$ dB, we can calculate the corresponding $\mathrm{C/N_0}$, according to (16)

$$\begin{aligned} \mathrm{C/N_0} &= \mathrm{SNR} - 10\log 10(T_{\mathrm{coh}}) \\ &= 10 - 10\log 10(4\mathrm{e}-3) = 34\ \mathrm{dB}\cdot\mathrm{Hz} \end{aligned} \tag{53}$$

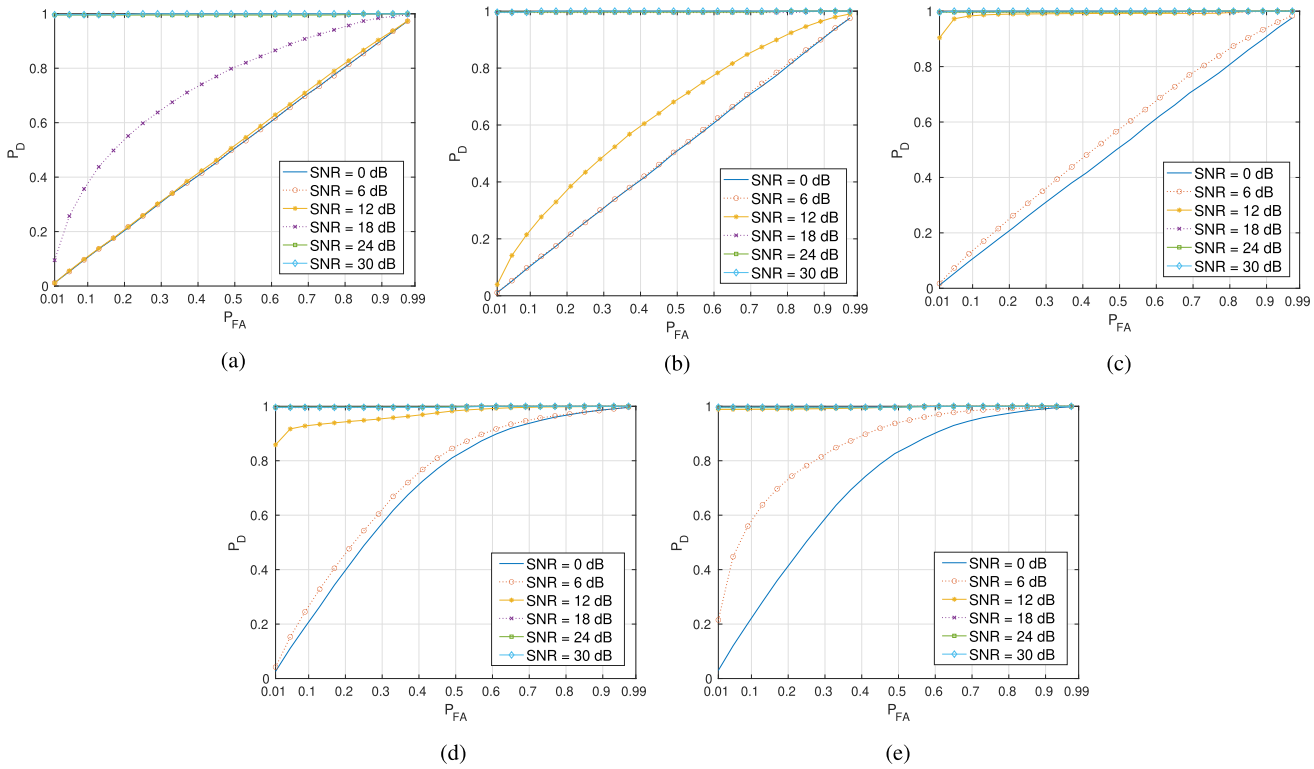


Fig. 8. ROCs for the GLRT with different settings of SNR and $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}}$. (a) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.25$. (b) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.372$. (c) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.494$. (d) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.616$. (e) $\frac{T_{\mathrm{LC}}}{T_{\mathrm{int}}} = 0.7136$.

when the coherence time is 4 ms. This C/N_0 is already very small, so the countermeasures work even with these weak signals when T_{LC} is large. But, of course, at higher SNR, the detection performance is better.

E. Test Results on Synthesized DD Attack

Furthermore, we check the detection performance of the two tests, analyzed in Section IV with the help of simulations, now using a synthesized DD signal at a software-defined receiver. The synthesized signal is a DD-replayed version of an original signal recorded with an NT1065_USB3 front-end. The tests proposed in this work are based on examining the distribution of prompt correlator outputs at the victim receiver, not checking any possible symbol errors occurred at the victim receiver/HRX, which actually would be detected due to cyclic redundancy check. Moreover, for an NMA-protected receiver, symbol errors in MAC can be detected by validation with its corresponding key. Therefore, to evaluate solely the effectiveness of the two tests on DD attack detection, we assume that the adversary configures parameters to minimize DD-induced errors, as presented in Section III, so that the ED phase and the ARX–ATX communication provide the ATX with a correct symbol value, the actual value transmitted by the HTX (satellite).

The synthesized attack signal is 110 s long, generated based on (11), with parameters A and $T_{\mathrm{LC}}/T_{\mathrm{int}}$ set in Table II. The intermediate frequency DD signal is crafted based on one satellite signal of the recorded signals. The different noise environments, i.e., SNR, are obtained by adjusting added Gaussian noise and modifying loop noise bandwidth of the tracking phase at the receiver. We implement a detection module at the receiver, which collects 1000 I_P samples, i.e., 1000×4 ms $= 4$ s for Galileo E1 OS signals, for each test. It means that the module provides a decision about existence of DD attack to the receiver every 4 s and triggers an alarm when the test is positive.

TABLE II
Evaluation Setup of Tests on a Synthesized Signal

A	[3.8, 6.5]
T_{LC}/T_{int}	[0.25, 0.372, 0.494, 0.616, 0.7136]
Signal length	110 s
SNR (dB)	[15, 22]
Test interval	4 s
Significance level	0.01

Fig. 9 shows the detection results with the two test methods, from which we can see that when the adversary configures T_{LC} as a small value, e.g., $T_{\mathrm{LC}}/T_{\mathrm{int}} = [0.25, 0.372]$, both the GoF test and the GLRT cannot detect the crafted DD signal both at low SNR, i.e., SNR $= 15$ dB. And at reasonably high SNR, i.e., SNR $= 22$ dB, both the GoF test and the GLRT can detect the crafted DD signal even with the lowest T_{LC}, i.e., $T_{\mathrm{LC}}/T_{\mathrm{int}} = 0.25$.

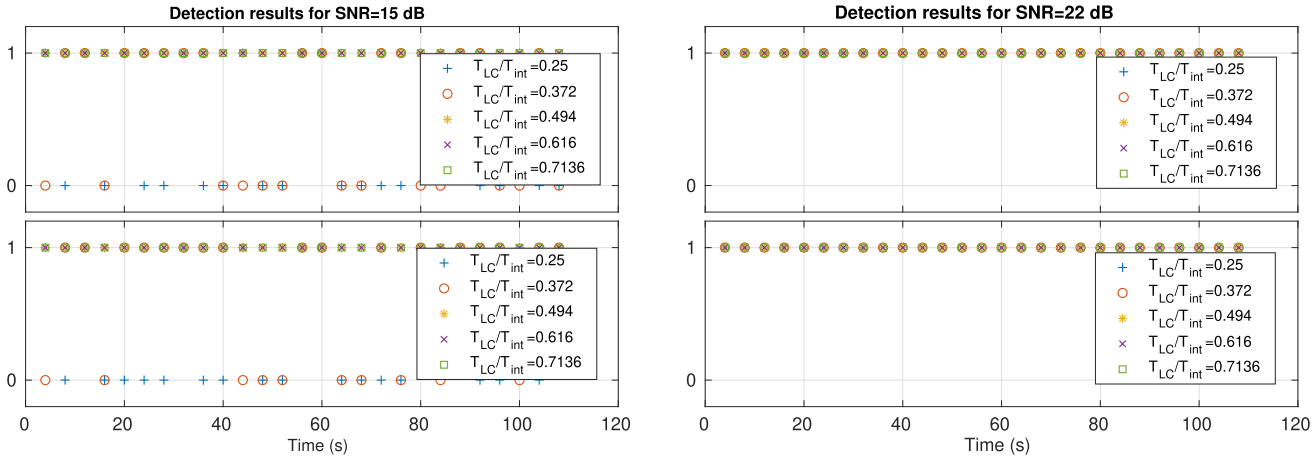


Fig. 9. Detection results of synthesized DD signal with GoF (top plot) and GLRT (bottom plot) for two SNR with significance level being 0.01: one detection result every four seconds; "1" indicates that the attack is detected and "0" indicates negative result.

F. Discussion on DD Attack Practicality

In practice, advanced GNSS receivers are equipped with protection methods to thwart spoofing or replay attacks. The adversary may need to consider this while mounting DD attacks. A basic detection method is signal power monitoring or AGC monitoring, which alone is not very strong but certainly a straightforward and effective method. The adversary can defeat this detection method by increasing its adversarial signal power gradually or starting transmitting the DD signals when the legitimate signals are blocked or disrupted, for instance when the receiver enters and exits a tunnel. A use case for NMA is when a user himself is the attacker, for example, to pay less for car insurance [73], transmitting DD signals while exiting a tunnel.

Correlation-based methods, both multicorrelator, e.g., [23], and our proposed method, can detect the DD attacks. The detection results of the correlation-based methods heavily depend on the C/N_0 of the received signals. Therefore, an attacker can transmit additive noise to the victim receiver to lower its C/N_0 of received signals to further degrade the detection results.

Another practical problem is that the ARX and the ATX should have stable and synchronized clocks, so that the attacker can coordinate the ATX transmitting the DD signals prior to the ARX receiving legitimate signals. If the ARX and the ATX are colocated (part of a platform), one clock can be used to synchronize their actions. If the ARX and the ATX are physically distinct, two devices possibly remote; then legitimate GNSS signals can be used to synchronize the clocks of the ARX and the ATX.

DD attacks have a scope limitation, in the sense that not all civilian GNSS signals are vulnerable to them. DD attacks are applicable to the signals that have same symbol length as the primary code, e.g., Galileo E1-B and GPS L2C CM signals. However, DD attacks will provoke a failed bit/symbol boundary detection when the primary code length is shorter than the symbol length, e.g., for GPS L1 C/A and Galileo E5a-I signals. For instance, in GPS L1 C/A signals, each bit is multiplied by 20 spreading codes. Therefore, the adversary-crafted LC signals may include a sign change within the bit period, depending on the early detected value. Consequently, the prompt correlator output would result in a failed bit boundary detection, e.g., based on the histogram approach [74]. In contrast, the Galileo E1-B and GPS L2C CM symbols are multiplied by one primary spreading code, with no need for bit/symbol synchronization, and, thus, not a failure due to the DD (LC) symbol construction.

V. CONCLUSION

In this article, we analyzed the ED and LC phases of DD attacks on GNSS signals. Furthermore, we quantified the ED performance, i.e., bit error rate, at the ARX and showed how the DD signal differs from the legitimate signal at the HRX. And we found that in reasonable, not difficult to implement, setups, the adversary can configure DD attacks to be effective, notably with low (or negligible) error probability and significant margins for reducing pseudorange measurements. Taking the Galileo E1 OS signals as an example, as shown in Fig. 3, the ARX only needs 0.5 ms to achieve almost 0 detection errors with $C/N_0 = 40$ dB $\cdot$ Hz; thus, with $T_{\mathrm{LC}} > 2$ ms and $T_d = 1$ ms, $T_{\mathrm{DD}} = T_{\mathrm{LC}} - T_{ED} - T_d > 0.5$ ms, equivalent to shortening 150-km pseudorange measurement.

Based on the tracking performance at the HRX, we presented the mathematical model of the prompt correlator output for the legitimate signals and DD signals, separately. This leads to the countermeasure based on statistic tests against the DD attacks, which are divided into two groups according to the knowledge of the HRX: a Shapiro–Wilk test when the HRX has no knowledge, i.e., within-symbol transition, about the DD attacks and a GLRT when the HRX has the knowledge.

We also provided the theoretical detection results based on our derived model with a Monte Carlo simulation. The

results show that detection probability of GLRT is higher than GOF, around 20%, when the detection probability is close to 100%. Then, we gave the detection results with a synthesized DD signal based on a recorded signal, which confirms the theoretical results: the GoF test and the GLRT can detect the DD attack at high SNR even when T_{LC} is as small as $T_{\mathrm{LC}}/T_{\mathrm{int}} = 0.25$; both tests cannot detect the DD attack with low SNR and small T_{LC} at the HRX, e.g., SNR =15 dB, with $T_{\mathrm{LC}}/T_{\mathrm{int}} < 0.372$.

In future, we plan to implement the DD attacks with SDR and test its effectiveness against a real GNSS receiver in a real environment, an open space with regulation permission or an isolated space.

REFERENCES

[1] K. C. Zeng *et al.*
All your GPS are belong to us: Towards stealthy manipulation of road navigation systems
In *Proc. 27th USENIX Secur. Symp.*, Baltimore, MD, USA, 2018, pp. 1527–1544.

[2] J. T. Curran, A. Morrison, and C. O'Driscoll
(In)Feasibility of multi-frequency spoofing
2019. Accessed: Nov. 25, 2019. [Online]. Available: https://insidegnss.com/infeasibility-of-multi-frequency-spoofing/

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

[4] F. Bastide, D. Akos, C. Macabiau, and B. Roturier
Automatic gain control (AGC) as an interference assessment tool
In *Proc. 16th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2003, pp. 2042–2053.

[5] D. Marnach, S. Mauw, M. Martins, and C. Harpes
Detecting meaconing attacks by analysing the clock bias of GNSS receivers
Artif. Satell., vol. 48, no. 2, pp. 63–83, 2013.

[6] P. Papadimitratos and A. Jovanovic
Method to secure GNSS based locations in a device having GNSS receiver
U.S. Patent 8 159 391, Apr. 2012.

[7] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans
GNSS signal authentication via power and distortion monitoring
IEEE Trans. Aerosp. Electron. Syst., vol. 54, no. 2, pp. 739–754, Apr. 2018.

[8] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina
Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer
In *Proc. 22nd Int. Tech. Meeting Satell. Division Inst. Navigat.*, Savannah, GA, USA, 2009, pp. 124–130.

[9] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys
GNSS spoofing detection using two-antenna differential carrier phase
in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Tampa, FL, USA, 2014, pp. 2776–2800.

[10] D. Borio and C. Gioia
A sum-of-squares approach to GNSS spoofing detection
IEEE Trans. Aerosp. Electron. Syst., vol. 52, no. 4, pp. 1756–1768, Aug. 2016.

[11] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan
GPS spoofing detection using RAIM with INS coupling
In *Proc. IEEE/ION Position, Location Navigat. Symp.*, Monterey, CA, USA, 2014, pp. 1232–1239.

[12] J. T. Curran and A. Broumendan
On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications
In *Proc. Int. Tech. Symp. Navigat. Timing*, Toulouse, France, 2017, pp. 1–8.

[13] C. Tanil, S. Khanafseh, and B. Pervan
An INS monitor against GNSS spoofing attacks during GBAS and SBAS-assisted aircraft landing approaches
In *Proc. 29th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2016, pp. 2981–2990.

[14] Ç. Tanıl, S. Khanafseh, M. Joerger, and B. Pervan
An INS monitor to detect GNSS spoofers capable of tracking vehicle position
IEEE Trans. Aerosp. Electron. Syst., vol. 54, no. 1, pp. 131–143, Feb. 2018.

[15] P. Papadimitratos and A. Jovanovic
GNSS-based positioning: Attacks and countermeasures
In *Proc. IEEE Mil. Commun. Conf.*, San Diego, CA, USA, 2008, pp. 1–7.

[16] R. G. Brown
A baseline GPS RAIM scheme and a note on the equivalence of three RAIM methods
Navigation, vol. 39, no. 3, pp. 301–316, 1992.

[17] J. Blanch, T. Walter, and P. Enge
RAIM with optimal integrity and continuity allocations under multiple failures
IEEE Trans. Aerosp. Electron. Syst., vol. 46, no. 3, pp. 1235–1247, Jul. 2010.

[18] K. Zhang, R. A. Tuhin, and P. Papadimitratos
Detection and exclusion RAIM algorithm against spoofing/replaying attacks
in *Proc. Int. Symp. GNSS*, Kyoto, Japan, Nov. 2015, pp. 1–10.

[19] S. Han, D. Luo, W. Meng, and C. Li
Antispoofing RAIM for dual-recursion particle filter of GNSS calculation
IEEE Trans. Aerosp. Electron. Syst., vol. 52, no. 2, pp. 836–851, Apr. 2016.

[20] K. Zhang and P. Papadimitratos
Secure multi-constellation GNSS receivers with clustering-based solution separation algorithm
In *Proc. 40th IEEE Aerosp. Conf.*, Big Sky, MT, USA, 2019, pp. 1–9.

[21] R. E. Phelts, D. M. Akos, and P. Enge
Robust signal quality monitoring and detection of evil waveforms
In *Proc. 13th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Salt Lake City, UT, USA, 2000, pp. 1180–1190.

[22] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti
Signal quality monitoring applied to spoofing detection
In *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2011, pp. 1888–1896.

[23] M. Pini, B. Motella, and M. T. Gamba
Detection of correlation distortions through application of statistical methods
In *Proc. 26th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Nashville, TN, USA, 2013, pp. 3279–3289.

[24] M. T. Gamba, M. D. Truong, B. Motella, E. Falletti, and T. H. Ta
Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets
GPS Solutions, vol. 21, no. 2, pp. 577–589, 2017.

[25] E. Schmidt, N. Gatsis, and D. Akopian
A GPS spoofing detection and classification correlator-based technique using the LASSO
IEEE Trans. Aerosp. Electron. Syst., vol. 56, no. 6, pp. 4224–4237, Dec. 2020.

[26] B. C. Barker *et al.*
Overview of the GPS M code signal
MITRE Corp., Bedford MA, USA, Tech. Rep., pp. 1–9, 2006.

[27] K. Wesson, M. Rothlisberger, and T. Humphreys
Practical cryptographic civil GPS signal authentication
Navigation, vol. 59, no. 3, pp. 177–193, 2012.

[28] T. E. Humphreys
Detection strategy for cryptographic GNSS anti-spoofing
IEEE Trans. Aerosp. Electron. Syst., vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[29] G. Caparra, S. Sturaro, N. Laurenti, C. Wullems, and R. T. Ioannides
A novel navigation message authentication scheme for GNSS open service
In *Proc. 29th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2016, pp. 2938–2947.

[30] J. M. Anderson *et al.*
Chips-message robust authentication (Chimera) for GPS civilian signals
In *Proc. 30th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2017, pp. 2388–2416.

[31] Z. Wu, R. Liu, and H. Cao
ECDSA-based message authentication scheme for BeiDou-II navigation satellite system
IEEE Trans. Aerosp. Electron. Syst., vol. 55, no. 4, pp. 1666–1682, Aug. 2019.

[32] C. T. Mills
M-code benefits and availability
2015. Accessed: Feb. 19, 2020. [Online]. Available: https://www.gps.gov/multimedia/presentations/2015/04/partnership/mills.pdf

[33] *GSA* Galileo commercial service implementing decision enters into force
2019. Accessed: Nov. 25, 2019. [Online]. Available: https://www.gsa.europa.eu/newsroom/news/galileo-commercial-service-implementing-decision-enters-force

[34] Y. Yang, W. Gao, S. Guo, Y. Mao, and Y. Yang
Introduction to BeiDou-3 navigation satellite system
Navigation, vol. 66, no. 1, pp. 7–18, 2019.

[35] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle
A navigation message authentication proposal for the Galileo open service
Navigation, vol. 63, no. 1, pp. 85–102, 2016.

[36] B. Motella, D. Margaría, and M. Paonni
SNAP: An authentication concept for the Galileo open service
In *Proc. IEEE/ION Position, Location Navigat. Symp.*, Monterey, CA, USA, 2018, pp. 967–977.

[37] J. A. Volpe
Vulnerability assessment of the transportation infrastructure relying on the global positioning system
Nat. Transp. Syst. Center, Cambridge, MA, USA, Tech. Rep. 816459, 2001.

[38] J. T. Curran and C. O'Driscoll
Message authentication, channel coding & anti-spoofing
In *Proc. 29th Int. Tech. Meeting Satell. Division Inst. Navigat.*, Portland, OR, USA, 2016, pp. 2948–2959.

[39] J. T. Curran and C. O'Driscoll
Message authentication as an anti-spoofing mechanism
Working Paper, 2017. [Online]. Available: https://www.researchgate.net/publication/317950338_Message_Authentication_as_an_Anti-Spoofing_Mechanism

[40] K. Zhang and P. Papadimitratos
GNSS receiver tracking performance analysis under distance-decreasing attacks
In *Proc. Int. Conf. Location GNSS*, Gothenburg, Sweden, 2015, pp. 1–6.

[41] K. Zhang and P. Papadimitratos
On the effects of distance-decreasing attacks on cryptographically protected GNSS signals
In *Proc. Int. Tech. Meeting Inst. Navigat.*, Reston, VA, USA, 2019, pp. 363–372.

[42] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore
So near and yet so far: Distance-bounding attacks in wireless networks
In *Proc. Eur. Workshop Secur. Ad-Hoc Sens. Netw.*, Hamburg, Germany, 2006, pp. 83–97.

[43] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec
Effectiveness of distance-decreasing attacks against impulse radio ranging
In *Proc. 3rd ACM Conf. Wireless Netw. Secur.*, Hoboken, NJ, USA, 2010, pp. 117–128.

[44] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec
On secure and precise IR-UWB ranging
IEEE Trans. Wireless Commun., vol. 11, no. 3, pp. 1087–1099, Mar. 2012.

[45] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec
The cicada attack: Degradation and denial of service in IR ranging
In *Proc. IEEE Int. Conf. Ultra-Wideband*, Nanjing, China, 2010, pp. 1–4.

[46] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec
Distance bounding with IEEE 802.15.4a: Attacks and countermeasures
IEEE Trans. Wireless Commun., vol. 10, no. 4, pp. 1334–1344, Apr. 2011.

[47] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun
Physical-layer attacks on chirp-based ranging systems
In *Proc. 5th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Tucson, AR, USA, 2012, pp. 15–26.

[48] K. Zhang and P. Papadimitratos
Safeguarding NMA enhanced Galileo OS signals from distance-decreasing attacks
In *Proc. 32nd Int. Tech. Meeting Satell. Division Inst. Navigat.*, Miami, FL, USA, 2019, pp. 4041–4052.

[49] S. Shaphiro and M. Wilk
An analysis of variance test for normality
Biometrika, vol. 52, no. 3, pp. 591–611, 1965.

[50] J. Fan, C. Zhang, and J. Zhang
Generalized likelihood ratio statistics and Wilks phenomenon
Ann. Statist., pp. 153–193, 2001.

[51] P. Teunissen and O. Montenbruck
Springer Handbook of Global Navigation Satellite Systems. New York, NY, USA: Springer, 2017.

[52] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner
Assessing the spoofing threat: Development of a portable GPS civilian spoofer
In *Proc. 21st Int. Tech. Meeting Satell. Division The Inst. Navigation*, Savannah, GA, USA, 2008, pp. 2314–2325.

[53] R. Blum, D. Dötterböck, and T. Pany
Investigation of the vulnerability of mobile networks against spoofing attacks on their GNSS timing-receiver and developing a meaconing protection
In *Proc. Int. Tech. Meeting Inst. Navigat.*, Reston, VA, USA, 2019, pp. 345–362.

[54] G. P. John and S. Masoud
Digital Communications, 5th ed. New York, NY, USA: McGraw-Hill, 2007.

[55] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt
Spread Spectrum Communications Handbook. New York, NY, USA: McGraw-Hill, 1994.

[56] A. A. Hassani, M. Zouak, M. Mrabti, and F. Abdi
MAI statistics estimation and analysis in a DS-CDMA system
In *Proc. IOP Conf. Ser.: Mater. Sci. Eng.*, 2018, vol. 353, pp. 12–26.

[57] T. S. Rappaport
Wireless Communications: Principles and Practice, vol. 2, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[58] *Galileo Open Service Signal-in-Space Interface Control Document (OS SIS ICD), Issue 1.2*, European Union, Brussels, Belgium, 2015.

[59] *NAVSTAR GPS Space Segment/Navigation User Segment Interfaces, IS-GPS-200 K*, Space & Missile Systems Center, Los Angeles, CA, USA, 2019.

[60] NT1065_USB3 Module.
Accessed: Jun. 19, 2019. [Online]. Available: http://ntlab.com/section/sec:v:44979.htm

[61] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen
A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach. New York, NY, USA: Springer, 2007.

[62] C. Fernández-Prades, J. Arribas, L. Esteve, D. Pubill, and P. Closas
An open source Galileo E1 software receiver
In *Proc. 6th ESA Workshop Satell. Navigat. Technol.*, Noordwijk, The Netherlands, 2012, pp. 1–8.

[63] K. Muthuraman and D. Borio
C/N0 estimation for modernized GNSS signals: Theoretical bounds and a novel iterative estimator
Navigation, vol. 57, no. 4, pp. 309–323, 2010.

[64] C. Huber-Carol, N. Balakrishnan, M. Nikulin, and M. Mesbah
Goodness-of-Fit Tests and Model Validity. New York, NY, USA: Springer, 2012.

[65] N. M. Razali *et al.*
Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling tests
J. Statist. Model. Anal., vol. 2, no. 1, pp. 21–33, 2011.

[66] J. Behboodian
On the modes of a mixture of two normal distributions
Technometrics, vol. 12, no. 1, pp. 131–139, 1970.

[67] H. L.
Van Trees, Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, and Linear Modulation Theory. Hoboken, NJ, USA: Wiley, 2004.

[68] A. P. Dempster, N. M. Laird, and D. B. Rubin
Maximum likelihood from incomplete data via the EM algorithm
J. Roy. Statist. Soc.: Ser. B. (Methodol.), vol. 39, no. 1, pp. 1–22, 1977.

[69] K. Basford and G. McLachlan
Likelihood estimation with normal mixture models
J. Roy. Statist. Soc.: Ser. C. (Appl. Statist.), vol. 34, no. 3, pp. 282–289, 1985.

[70] P. Rossi
Bayesian Non- and Semi-Parametric Methods and Applications. Princeton, NJ, USA: Princeton Univ. Press, 2014.

[71] G. McLachlan and D. Peel
Finite Mixture Models. Hoboken, NJ, USA: Wiley, 2004.

[72] K. M. Ashman, C. M. Bird, and S. E. Zepf
Detecting bimodality in astronomical datasets
Astronom. J., vol. 108, no. 6, pp. 2348–2361, 1994.

[73] G. Caparra
Authentication and integrity protection at data and physical layer for critical infrastructures
Ph.D. dissertation, Dept. Inf. Eng., Univ. Padua, Padua, Italy, 2017.

[74] J. J. Spilker, Jr., P. Axelrad, B. W. Parkinson, and P. Enge
Global Positioning System: Theory and Applications, vol. I. Reston, VA, USA: Amer. Inst. Aeronaut. Astronaut., 1996.

Kewei Zhang received the B.Sc. degree in telecommunication engineering from Jilin University, Changchun, China, in 2009, and the M.Sc. degree in electrical engineering from the KTH Royal Institute of Technology, Stockholm, Sweden, in 2013, where he is currently working toward the Ph.D. degree with the Networked Systems Security Group under the supervision of Prof. Panos Papadimitratos.

His research interests include localization and timing, global navigation satellite system receiver technologies, and signal detection and estimation.

Erik G. Larsson (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Uppsala University, Uppsala, Sweden, in 2002.

He is currently a Professor of Communication Systems with Linköping University, Linköping, Sweden. He was with the KTH Royal Institute of Technology, Stockholm, Sweden; The George Washington University, Washington, DC, USA; The University of Florida, Gainesville, FL, USA; and Ericsson Research, Stockholm. He coauthored the books entitled *Space-Time Block Coding for Wireless Communications* (Cambridge, U.K.: Cambridge Univ. Press, 2003) and *Fundamentals of Massive MIMO* (Cambridge, U.K.: Cambridge Univ. Press, 2016). He is co-inventor of 19 issued U.S. patents. His main research interests include wireless communications and signal processing.

Dr. Larsson received the IEEE Signal Processing Magazine Best Column Award twice in 2012 and 2014, the IEEE ComSoc Stephen O. Rice Prize in Communications Theory in 2015, IEEE ComSoc Leonard G. Abraham Prize in 2017, IEEE ComSoc Best Tutorial Paper Award in 2018, and IEEE ComSoc Fred W. Ellersick Prize in 2019. He is an Editorial Board Member of *IEEE Signal Processing Magazine* and a member of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS Steering Committee. He was the Chair of the Signal Processing for Communications and Networking Technical Committee of the IEEE Signal Processing Society from 2015 to 2016, the Chair of the IEEE WIRELESS COMMUNICATIONS LETTERS Steering Committee from 2014 to 2015, the General, respectively, Technical Chair of the Asilomar SSC Conference in 2012 and 2015, the Technical Co-Chair of the IEEE Communication Theory Workshop in 2019, and a member of the IEEE Signal Processing Society Awards Board from 2017 to 2019. He was an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS from 2010 to 2014 and IEEE TRANSACTIONS ON SIGNAL PROCESSING from 2006 to 2010.

Panos Papadimitratos (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from Cornell University, Ithaca, NY, in 2005.

He is currently with the KTH Royal Institute of Technology, Stockholm, Sweden, where he leads the Networked Systems Security Group and is a member of the Steering Committee of the Security Link Center. He has delivered numerous invited talks, keynotes, panel addresses, and tutorials in flagship conferences.

Dr. Papadimitratos serves or served as an Associate Editor for IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE/ACM TRANSACTIONS ON NETWORKING, and *IET Information Security*, as a member of the Privacy Enhancing Technologies Symposium (PETS) Editorial and Advisory Boards and steering committees of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) and International Conference on Cryptology and Network Security (CANS), as a Program Chair for 2016 ACM WiSec, 2016 International Conference on Trust and Trustworthy Computing, and 2018 CANS, and as a General Chair for 2018 ACM WiSec, 2019 PETS, and 2019 IEEE European Symposium on Security and Privacy. He is a Fellow of the Young Academy of Europe and the Knut and Alice Wallenberg Academy. He is an ACM Distinguished Member. His group webpage is available at https://www.eecs.kth.se/nss.