A Proposal for Securing Terrestrial Radio-Navigation Systems

Ronnie X.T. Kor, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys
Radionavigation Laboratory
The University of Texas at Austin

Biography

Ronnie X.T. Kor is an M.S. student in the Department of Aerospace Engineering and Engineering Mechanics (ASE) at The University of Texas at Austin (UT). He is a member of the UT Radionavigation Laboratory (RNL). His research interests are in estimation and terrestrial position, navigation, and timing (PNT) security.

Peter A. Iannucci is a postdoctoral research fellow at the UT RNL and a member of the UT Wireless Networking and Communications Group (WNCG). He completed his B.S. in Physics, Electrical Engineering, and Computer Science, and his doctorate in Computer Science from MIT. His research includes satellite navigation from LEO.

Lakshay Narula is a Ph.D. candidate in the UT Department of Electrical and Computer Engineering. He is a member of the RNL and the WNCG. His research includes PNT security and robust lane-level accurate localization of ground vehicles in urban areas.

Todd E. Humphreys is an associate professor in the UT Department of ASE, Director of the UT RNL, and Fellow of the Institute of Navigation (ION). He received a B.S. and M.S. in Electrical and Computer Engineering from Utah State University, and a Ph.D. in Aerospace Engineering from Cornell University.

Abstract

The security of terrestrial radio-navigation systems (TRNS) has not yet been addressed in the literature. This proposal builds on what is known about securing global navigation satellite systems (GNSS) to address this gap, re-evaluating proposals for GNSS security in light of the distinctive properties of TRNS. TRNS of the type envisioned in this paper are currently in their infancy, unburdened by considerations of backwards compatibility: security for TRNS is a clean slate. This paper argues that waveform- or signal-level security measures are irrelevant for TRNS, preventing neither spoofing nor unauthorized use of the service. Thus, only security measures which modify navigation message bits merit consideration. This paper proposes orthogonal mechanisms for navigation message encryption (NME) and authentication (NMA), constructed from standard cryptography primitives and specialized to TRNS: message encryption allows providers to offer tiered access to navigation parameters on a bit-by-bit basis, and message authentication disperses the bits of a message authentication code across all data packets, posing an additional challenge to spoofers. The implementation of this proposal will render TRNS more secure and resilient than traditional civil GNSS.

I. Introduction

Global Navigation Satellite Systems (GNSS) have provided excellent positioning solutions in open, outdoor environments, enabling a wide range of navigation and timing applications. However, the indoor environment remains largely out of reach to these weak signals. The requirement for accurate and assured indoor positioning limits the effectiveness of GNSS in high-stakes, safety-of-life applications like enhanced E911, as well as in a new generation of commercial applications like warehouse automation and asset tracking.

Terrestrial radionavigation systems (TRNS), such as the commercial systems Locata [1] and NextNav [2], are emerging to address these needs. These systems are marketed to provide position, navigation, and timing (PNT) solutions in environments where GNSS signals are degraded or denied. TRNS consist of networks of synchronized terrestrial transmitters, or *pseudolites*, which operate analogously to GNSS satellites. These pseudolites broadcast signals powerful enough to reach the interiors of typical buildings, permitting the acquisition of terrestrial PNT service by urban or indoor users. A TRNS may serve to augment GNSS signals, improving solution geometry and availability in dense urban areas [3], [4], or it may serve as a primary navigation aid in the indoor environment [5].

The TRNS architecture [1], [2] and its sensitivity to wide-band radio-frequency interference (RFI) [6], [7] have been investigated in the literature. There have not, however, been any public proposals for how to secure TRNS–or even any substantive discussion of security considerations.

Broadly, the security of TRNS parallels that of other historical radio-navigation systems, and thus security considerations for TRNS can draw from lessons learned in

the vibrant body of research on GNSS signal security. The important distinctions are threefold: first, the vastly different dynamic range of terrestrial versus space-based transmissions; second, the largely indistinguishable angular distribution of spoofed and authentic signals; and third, the possibility of multi-lateral (i.e. network) sensing of transmissions within the space bounded by the pseudolites. Of particular note is the way in which the adversary's receive power advantage renders exotic signal-level security techniques like spreading code authentication [8], [9] or deterministic code-phase dithering irrelevant: the adversary can always produce a pristine signal replica.

Contributions. This paper makes two contributions. First, it analyzes the security considerations of TRNS with these three differences in mind. Second, it offers a concrete proposal for how to secure TRNS, with a focus on data-level security in recognition of the futility of waveform- or signal-level security. This concrete proposal has two non-obvious aspects: MAC leavening, whereby a modest number of message authentication bits spread throughout the transmitted packets provide a significant improvement in security, and multi-level encryption, which has not been used before in PNT security and makes the adoption of this proposal more enticing for commercial service providers.

Organization of this paper. Section II analyzes the security considerations of TRNS. Section III gathers results from past proposals for GNSS security, and discusses the relevance of each technique for TRNS. Section IV details this paper's proposal for securing TRNS with navigation message encryption and/or navigation message authentication. Section V concludes the paper.

II. Security Considerations for TRNS

From the perspective of a radio-navigation system, there are essentially two types of adversaries: parties wishing to obtain service without authorization (stow-aways), and parties wishing to deny, degrade, or deceive authorized users of the service (jammers or spoofers). This divides radio-navigation security into two domains, termed Encryption (denying stow-aways) and Authentication (detecting spoofing). (N.B. that cryptographic encryption techniques are a useful tool in both domains). The focus of this work on terrestrial commercial systems prompts the adoption of the term "subscriber" to refer to an authorized user.

A. Dynamic Range

The greater dynamic range of terrestrial signals is a fundamental difference in the following sense: with GNSS, a spoofer cannot easily gain an advantage in received signal strength by moving closer to the transmitter, because this would require climbing thousands of kilometers above the ground. Instead, the adversary who wishes to obtain a pristine signal must build a large antenna. In TRNS, however, the adversary can "walk right up to" the pseudolite, obtaining a signal as clear as they could wish. Furthermore, because a subscriber cannot anticipate how much path loss may be present, it cannot anticipate how strong a signal ought to be after de-spreading. These asymmetries enable an adversary to obtain pristine signal replicas at low cost and high reliability, by locating a receive antenna close to the pseudo-lite. This renders spreading code encryption (SCE) (after the fashion of the GPS P(Y) code) largely irrelevant for TRNS: an adversary can always build a network of receivers to obtain both the pseudolites' spreading codes and position.

B. Radio-Frequency Interference

Radio-navigation systems, both GNSS and TRNS alike, are susceptible to RFI caused by jammers and spoofers. Fig. 1 gives an overview of RFI. Spoofing is of particular interest among all the RFI threats, as it stealthily fools a victim receiver without leaving obvious telltale signs. As a matched spectrum interference, spoofing signal is statistically correlated with the authentic signal, and a spoofer can achieve maximum spoofing efficacy by arbitrarily adjust this signal's power, code phase, carrier phase, and signal structure. Spoofing can be broadly classified into the following types of attack:

1) Self-consistent spoofing: This attack synthesizes false code phases and beat carrier phases, such that a desired position/timing fix is induced at the victim receiver without triggering an alarm from an unusual code/carrier divergence [10].
2) Data/Time spoofing: This attack generates a signal that has counterfeit data bits but is otherwise in near-perfect code-phase alignment with the authentic signal within the tracking channel of the victim receiver [11].
3) Security Code Estimation and Replay (SCER): This attack generates a counterfeit signal with a delay, by tracking individual signals and attempting to estimate each signal's unpredictable security code chips or navigation data bits on the fly [10].
4) Meaconing: This attack records the ensemble of authentic signals and replays them to create a desired position/timing offset. This can be done by either rebroadcasting the authentic signals recorded from a remote antenna at the intended position, or inducing independent delay variations in each authentic signal using phased-array signal processing [12].

C. Spoofing

The threat from GNSS spoofing has been a concern within the GNSS community, ever since a portable spoofer was developed and successfully tested against a COTS

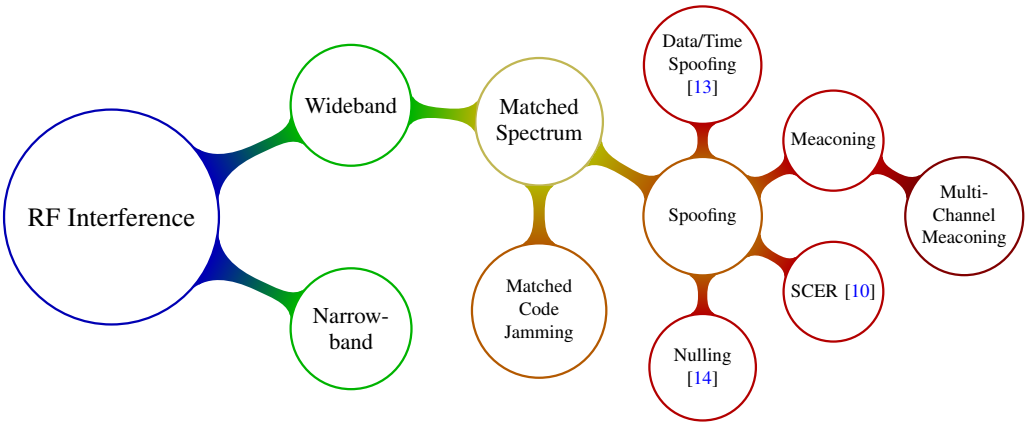

Fig. 1: A taxonomy of RF interference (i.e. an attaxonomy).

receiver [15]. A number of live-signal spoofing tests in a controlled environment which followed thereafter also affirmed the effect [16]–[18]. This threat continues to be relevant today, with recent rumors of spoofing "in the wild" seen in specific spots such as Black Sea [19], Syria [20] and China [21], or affecting multiple victim receivers which coincidentally move along the same track [22]. With recent advancements in RF microelectronics, together with open-source GNSS signal generation software, building a functional GNSS spoofer will become more accessible to the masses in the near future [23]. The spoofing threat is also relevant to TRNS because a functional TRNS spoofer can be modified from a GNSS spoofer, given sufficient resources and knowledge of the TRNS signal architecture.

TRNS has differentiated itself by having a high SNR and a limited-access standard, which is perceived to be able to counter against conventional spoofers that rely on high signal power and accurate prediction of spreading code and/or navigation data bit to mount a successful attack. However, these characteristics do not make TRNS foolproof against all spoofing threats. In fact, TRNS system has to tackle additional challenges due to high signal strength, wider signal dynamic range, proximity of threats to transmitters, as well as a potential reliance on GNSS for network synchronization. TRNS therefore faces a longer list of vulnerabilities from its signal and physical characteristics than GNSS.

Unlike GNSS signals that have signal strength below noise floor, the spreading code sequence of TRNS can be exposed without the use of high-gain antenna due to its high SNR. Reference [24] shows that the time slot usage, transmitters' PRN and navigation data bit of the Metropolitan Beacon System (MBS) from NextNav can be derived by analyzing the power spectrum of the MBS signal. This makes the cost of SCER attack on TRNS lower than that on GNSS, since the embedded security codes of TRNS can be more easily observed and hence estimated. In addition, even if TRNS adopts a restricted access standard and requires the use of secure tamper-resistant receiver to store the secret key like military GNSS signals, it is still susceptible to record-and-replay attacks.

TRNS provides a wide-area positioning service using a network of synchronized terrestrial transmitters. To ensure high accuracy in the PNT solution, stringent synchronization and frequency stability requirements are placed on all pseudolites, which may be satisfied either by: (1) the use of dedicated low-latency fiber-optic connection across the entire network, which will incur significant setup cost and will limit the deployment sites, or (2) the use of GNSS-disciplined atomic clocks, which reduces infrastructure cost and offers greater flexibility in the placement of the pseudolites. While option 2 may be preferable to providers, it exposes TRNS to an additional attack surface through its reliance upon GNSS. In addition, the relative accessibility of the pseudolites compared to the Earth-orbiting GNSS satellites indicates that TRNS is more susceptible to direct attacks, either by physical or cyber tampering, or by co-locating a high-power interference transmitter to overwhelm its signal.

III. Lessons Learned from GNSS Security

TRNS inherits from traditional radio-navigation a bevy of well-known attacks. For the same reason, TRNS can benefit from the products of a vibrant research effort over the past 20 years to secure GNSS. Not all the techniques that have been proposed for securing GNSS are applicable to TRNS— but it is equally true that the obligation of GNSS operators to backwards compatibility has prevented them from fully exploiting these developments. The time is right to incorporate what has been learned about GNSS security into TRNS. The purpose of this section is to review some of the most powerful security techniques that have been proposed for GNSS and to identify those ideas that are compatible with TRNS.

GNSS spoofing defenses proposed in recent literature can be broadly classified into two categories: (1) cryptographic techniques that utilize unpredictable but verifiable signal modulation in the GNSS spreading code or navigation data, and (2) non-cryptographic techniques such as signal processing techniques, geometric techniques, or drift monitoring techniques. A comprehensive review of GNSS spoofing defenses is presented in [14]. While these techniques have been proven to be effective for GNSS, there are challenges to their implementation for TRNS.

A. Non-cryptographic Defenses

The preliminary ideas of GNSS spoofing defenses fall within the realm of non-cryptographic defenses, as they do not require any changes to GNSS signal-in-space (SIS). These techniques are categorized based on their method of differentiating spoofing signals from authentic signals, by looking for consistency in the signal characteristics, signal geometry, or PNT solution.

Geometric techniques exploit the RF signals' geometric diversity to verify the authenticity of the signal source. This includes angle-of-arrival (AOA) discrimination techniques [25]–[28] or Doppler frequency difference of arrival (FDOA) [29] discrimination using multiple antennas. Other geometric techniques advocate the use of single antenna, and discriminate spoofed and authentic signals either with a known perturbation profile [30] or random motion profile [31], or using multiple feeds from a single antenna [32]. The assumptions made by these techniques are: (1) the spoofing signals generally arrive from below or near the horizon [32], (2) the observations from spoofing signals is not aligned with the actual geometry between the satellites and the victim receiver [25], [27], and (3) there are strong correlation of signal characteristics of different satellites from the spoofing signals [26], [28], [30], [31]. However, it is not costly for a sophisticated spoofer to co-locate dedicated spoofing sources at each of the TRNS pseudolites, thereby defeating all the assumptions made by these techniques. In addition, the need for hardware modification or additional hardware might not be suitable for applications that either use an existing hardware for mass-market adoption, or have SWaP-C constraints.

Drift monitoring techniques, on the other hand, look for unusual changes in the output of the receiver, such as position or clock fix, by coupling with external sensors. These include the use of an oscillator to check for inconsistency in the clock bias or clock drift [33], or the use of visual/inertial/radar odometry to place constraints on the reasonable error growth of a position fix [34], [35]. The applicability of these techniques is limited by the SWaP-C constraints of the applications, and the authentication performance is limited by the accuracy of these sensors.

Signal processing techniques look for sudden deviations in the received signal characteristics to indicate an onset of a spoofing attack. These techniques detect changes in the received carrier amplitude or the RF front-end's AGC set-point, or a distortion in the complex correlation function [36]. Signal processing techniques can be implemented in software, unlike the previous categories of techniques discussed which require additional hardware. These techniques are effective for GNSS which has signal strength below the noise floor and narrow signal dynamic range. However, this is not applicable to TRNS, which generally has high SNR and a wide signal dynamic range for quick acquisition in both dense-urban and indoor environments. A potential spoofer will have a wide margin to change the total received power and create a distortion-free correlation function using the spoofing signal, and these indicators will not be picked up by the PD detector proposed by [36].

B. Cryptographic Defenses

The main objective of cryptographic spoofing defenses is to ensure information security. Cryptographic techniques include encryption, which enforces the secrecy of data from unauthorized access, and authentication which verifies the origin of the data. They provide three features: (1) authentication, by verifying the origin of information, (2) confidentiality, by protecting the information from disclosure to non-authorized parties, and (3) integrity, by detecting any unauthorized information modification. These features increase the resilience of the signal against spoofing.

Several GNSS cryptographic spoofing defenses have been proposed and/or implemented in both civil and limited-access GNSS signals. These spoofing defenses add cryptographic features in small segments or in entire portion to either the fast-rate spreading code or the low-rate navigation data. These cryptographic techniques can be classified into the following groups: (1) navigation message encryption (NME), which encrypts the whole navigation data message before being modulated onto the spreading code, (2) spreading code encryption (SCE), which encrypts the whole spreading code sequence, (3) navigation message authentication (NMA), which adds unpredictable digital signature into the navigation data using asymmetric cryptography, and (4) spreading code authentication (SCA), which inserts unpredictable watermark sequences within the open spreading code.

The straightforward, blanket encryption of a navigation signal may be attractive as a means both to deny service to stow-aways and to authenticate the signal to subscribers. However, there are sigificant caveats in both applications. The first regards the use of symmetric cryptography.

One may apply symmetric encryption to the entire navigation message (NME) and/or the spreading code (SCE,

a la the GPS P(Y) code). The premise is that a spoofer who does not know the symmetric key cannot produce a valid spoofing signal, or equivalently that a receiver can be confident in a signal that appears in the output of a correlator tuned to the secret spreading sequence (with similar reasoning for NME). However, a symmetric approach to authentication is extremely fragile, because a leaked symmetric key can be used for spoofing. For this reason, military deployment of SCE involves tamper-resistant hardware and costly, elaborate procedures for secure distribution and management of the secret symmetric keys. This approach is untenable for civil or commercial radio-navigation.

NMA and SCA, in contrast, avoid the fragility of symmetric key management by adopting asymmetric cryptography, using either delayed release approach or public-private key pair. In SCA, short segments of unpredictable spreading code sequences (termed as "watermarks") are interleaved with long segments of predictable spreading codes in fixed or random positions [8]. The receiver uses the predictable sequences to track the broadcast signal, and stores the unpredictable segments in the buffer while waiting for the information about the watermarks. Once this information arrives, the receiver can synthesize the unknown spreading sequence with the correct watermarks embedded in the right position, and correlates this code segment with the relevant segment from its recorded signal to verify signal authenticity. This technique requires modifications to the GNSS signal generation. Hence, it will be difficult or impossible to be implemented on existing GNSS which requires backward compatibility. However, TRNS, which comes with a green-field waveform, can consider the implementation of SCA into its waveform design.

A growing literature advocates the use of NMA for civil GNSS signal authentication, with proposed implementations for GPS [8], [37], [38], Galileo [39], [40], QZSS [41] and SBAS [42]–[44]. NMA is already implemented in the Galileo Open Service, which will start its Open Service Navigation Message Authentication (OSNMA) signal-in-space transmission in the first quarter of 2020 and have full service available in 2021 [45]. This technique uses either an asymmetric private-key/public-key approach such as the *elliptic curve digital signature algorithm* (ECDSA) [38], or a delayed symmetric key release approach such as *timed efficient stream loss-tolerant authentication* (TESLA) [37]. Unlike SCA, this technique can be implemented into existing GNSS signal, provided that there are available unused bits in the navigation message to store the digital signature. However, the leftover bits in the navigation message are usually limited. A trade-off has to be made between the cryptographic strength of the NMA scheme, which is determined by the size of the key and the digital signature, and the authentication latency, which is determined by the frequency of digital signature validation. TRNS has more flexibility in incorporating NMA into their waveform design, and can offer low *time-to-first-authenticated-fix* (TTFAF) while maintaining strong cryptographic security.

In contrast to GNSS, TRNS comes with a clean-slate waveform design, and is not constrained by the need of backward compatibility. This offers TRNS providers flexibility in their application of the latest cryptographic defense techniques—many of which were originally proposed for GNSS. The next section proposes one implementation of NME and NMA for a TRNS.

IV. TRNS Security Design

As discussed in Sec. I, this paper addresses TRNS vulnerabilities to two types of adversaries: spoofers and unauthorized users.

With regard to a spoofing adversary, a subscriber is said to have assured PNT from its TRNS network if either (1) the subscriber's pseudorange measurements are not substantially affected by the spoofing signal, or, (2) the spoofing attack is flagged as such. The security proposal outlined in this section aspires not only to aid a protected TRNS subscriber in meeting one of these conditions, but also to enable provision of tiered subscriber segments *a la* selective availability.

Broadly, there are two types of spoofing attacks: one in which the adversary forges a valid signal (navigation message and spreading code) that has not been previously generated by an authentic transmitter, and the other in which the adversary simply re-broadcast a signal previously broadcasted by an authentic transmitter. Authentication mechanisms are designed to thwart the first kind of attack via SCA and/or NMA. Crucially, neither SCA nor NMA can defend against the second type of spoofing attack [46]. This section focuses on design of an NMA scheme for TRNS that also provides some benefits of SCA.

At this point, the reader might point out that the GPS P(Y) code in fact uses SCE to prevent the first kind of spoofing attack. This is true. In the special case where the subscriber (e.g., a SAASM receiver) has *a priori* access to the spreading code (i.e., the plaintext) and the symmetric key, but the spoofer does not, SCE can provide authentication. However, this is untenable in the case of TRNS because a general TRNS subscriber cannot be trusted as benign. As such, this section does not propose SCE/NME for anti-spoofing.

With regard to unauthorized usage, it is important to concede that it is not possible to prevent the usage of TRNS signals as a signal-of-opportunity, whereby unauthorized users estimate the position and clock states of the authentic transmitters by means other than the navigation message. With that said, unauthorized use as a signal-of-opportunity

is much more involved than the case where the navigation message is plainly available. Accordingly, this section proposed the use of NME to limit terrestrial PNT service to authorized users.

A. Selective Navigation Message Encryption

This sub-section considers an adversary that is not a valid subscriber of the TRNS service, but nevertheless wishes to exploit the service. Data confidentiality provided by symmetry key encryption is sufficient to defeat this type of adversary. Beyond the traditional GNSS NME scheme, which envisions a single segment of authorized users, this paper proposes a scheme that can be customized for multiple tiers of subscribers. For example, the highest tier subscribers may decrypt the full navigation message and access the most accurate transmitter position and clock states, whereas lower tier subscribers may only decrypt a few most significant bits of such information.

Fig. 2 provides an overview of the proposed encryption scheme. This scheme is based on the counter mode (CTR) of the block cipher operation, which is a standard method to generate a pseudo-random keystream from a short shared secret. The use of this method requires two components: a shared secret key and a unique initial value (IV). The rest of this sub-section describes a method that involves tiered distribution of secret keys and the provision of a unique IV.

Each tier of subscription grants access to some subset of the pre-shared secrets (PSS) and corresponding encryption bit masks (EBM) used by the system. Subscribers download these secrets in batches via a secure secondary channel and store them in their receivers' non-volatile memory. At each encryption period (e.g. day of the month), a unique value of $\mathrm{PSS} = (\mathrm{PSS1}, \mathrm{PSS2})$, is retrieved from storage. PSS1 takes the role of a symmetric key. PSS2 is concatenated with the pseudolite ID (TxID) and time of day (ToD), e.g. GPS or UTC time, to form a unique IV, from which the block cipher E generates the key stream (KS).

$$\mathrm{KS} = \mathrm{E}(\mathrm{PSS1}, (\mathrm{TxID} \parallel \mathrm{ToD} \parallel \mathrm{PSS2}))$$

Note that while PSS2 is a not publicly-known in this scenario, this is not necessary a requirement. The most important consideration here is that the same key-IV pair must never be re-used. For example, if ToD were chosen to be "seconds since midnight", then the same key-IV pair would repeat every 24 hours until a new PSS pair is retrieved. Accordingly, it must be ensured that ToD does not repeat faster than the key-swapping period.

A suitable block cipher to be used is AES-128 (Advanced Encryption Scheme, using block size of 128 bits), which offers an equivalent symmetric-key strength of 128 bits. This symmetric-key strength of 128 bits is recommended by U.S. National Institute of Standards and Technology (NIST) guidelines for cryptographic security beyond 2030. The IV to the block cipher has to match its block size. The key stream KS is combined with the EBM to form the masked key stream MKS. The EBM enables tiered usage of NME.

$$\mathrm{MKS} = \mathrm{KS} \wedge \mathrm{EBM}$$

The masked key stream is then XOR with the ciphertext C to reveal the plaintext P.

$$P = \mathrm{MKS} \oplus C$$

Each masked key stream applies to a different set of message bits. A high-accuracy subscriber, for instance, will be provided with the full suite of pre-shared secrets, enabling it to reconstruct each of the masked key streams and thus to decrypt the entire message. A mid-accuracy subscriber will only be able to reconstruct the masked key streams protecting the most significant bits of each of the navigation parameters encoded in the message. Access is further limited to the period of a subscription by limiting which days' pre-shared secrets are provided to which receivers. (Naturally, such a scheme cannot prevent subscribers from sharing secrets with non-subscribers, beyond what protection is possible through e.g. software obfuscation. Such insider attacks may call for remedies of a legal, rather than technical, nature.)

It must be noted that the stream cipher structure (i.e. XOR-based encryption) is not suitable to ensure the authenticity of data. That is, it does not prove that an incoming navigation message to a TRNS receiver originates from an authentic TRNS pseudolite, because it is *malleable*: an attacker can take a valid encrypted packet $(\mathrm{E}(M) \parallel \mathrm{CRC}(\mathrm{E}(M)))$ and XOR it with $(X \parallel \mathrm{CRC}(X))$ for any bit string X, producing a new valid encrypted packet which decrypts to $M \oplus X$.

More generically, the symmetric structure of this cipher is not suitable to prevent real-time forgery of encrypted signals by a spoofer who might also, secretly, be a subscriber with access to the symmetric keys. This type of spoofing attack will be mitigated with NMA in the next subsection.

B. Combined Data and Signal Authentication

This sub-section presents an NMA method based on the TESLA protocol [47] that additionally provides limited signal authentication against a *half duplex* re-broadcast-type spoofing attack.

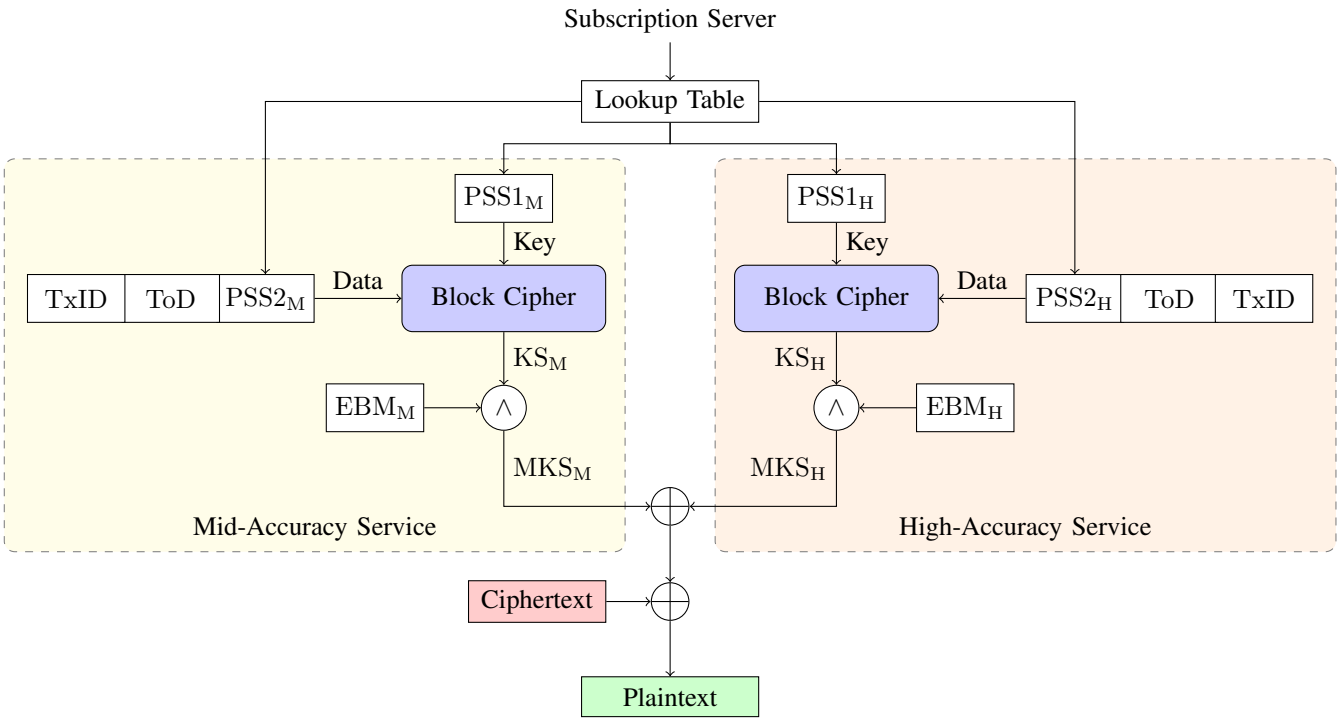

Fig. 2: Proposed TRNS NME scheme from the perspective of a high-accuracy service receiver. Note that in the high-accuracy receiver, both mid- and high-accuracy key streams are computed in order to decrypt the entire message.

Notionally, NMA requires asymmetric cryptography to generate and verify digital signatures, and thereby to perform data origin authentication. Naïve alternatives using symmetric cryptography suffer from the validator-can-spoof problem: anyone who can validate such a "signature" can also forge one. However, asymmetric cryptography is substantially more costly in both computation and communication overhead than symmetric cryptography when compared at an equivalent level of security (i.e. $\log_2$ of the number of operations in the best-known attack). For instance, ECDSA produces signatures whose length in bits is roughly four times the equivalent security level.

The TESLA protocol introduced a key innovation that bypassed this dilemma and enabled the use of lightweight symmetric cryptography for NMA. TESLA involves a form of asymmetry based on the delayed release of symmetric keys. This protocol has emerged as a strong contender among broadcast authentication proposals for GNSS [45]. The communication overhead of TESLA in bits per authentication epoch is roughly twice the equivalent security level.

1) Data Authentication: This sub-section considers an adversary attempting to spoof the subscribers of a TRNS. Importantly, such an adversary may be a highest-tier subscriber, and hence have access to all symmetric encryption keys. As such, all navigation message and spreading code bits, encrypted or otherwise, are known to the adversary.

The authentication design proposed in this paper relies on the vanilla TESLA protocol for data-level authentication. Fig. 3 describes the key chain and message authentication code generation per the TESLA protocol. The TESLA protocol progresses in a reverse direction along a one-way key chain generation, starting with the root key K_n obtained from the control segment (i.e. subscription server) and ending with the public key K_0 to be dispersed to all subscribers via secondary channels for bootstrapping. Each downstream key K_{i-1} is derived from the upstream key K_i using a one-way hash function H_{A1}, and subsequently disclosed in the ith broadcast message.

$$K_{i-1} = \mathrm{H}_{\mathrm{A1}}(K_i)$$

The specific key corresponding to each epoch K_i is then passed into a different hash function H_{A2} to generate the input key K_i' for a hash-based message authentication code (HMAC) function. The authentication code MAC_i is computed from the concatenation M_i of all messages in the ith epoch. The reason for having a second hash function before HMAC is subtle; interested readers should refer to [47, Sec. 3.4].

Note that authentication is orthogonal to encryption: the scheme works equally well in deployments with no encryption at all; in this case, the input M_i to the HMAC is the plaintext. In either case, the input to the HMAC is

whichever bit string is known to all receivers once forward error correction has been removed.

$$\begin{aligned}\mathrm{MAC}_i &= \mathrm{trunc}(\mathbf{HMAC}(K_i', M_i)) \\ &= \mathrm{trunc}(\mathbf{HMAC}(\mathrm{H}_{\mathrm{A2}}(K_i), M_i))\end{aligned}$$

Fig. 4 shows the process of authentication in an NMA-enabled receiver, which operates in two phases. During the warm-start phase, the receiver obtains the first packet $P_i = [M_i, \mathrm{MAC}_i, K_{i-1}]$ from the broadcast. As MAC_i cannot be verified instantaneously without the corresponding K_i, the packet is stored in the receiver's memory until the arrival of K_i. However, the first received key K_{i-1} can still be validated. This is done by applying K_{i-1} through the prescribed chain of one-way hash functions, and by matching the terminal key from the chain with the public key K_0 obtained from the server. At the next epoch, K_i arrives and the receiver can transit into the steady-state phase, where it can perform both key and MAC validation. The MAC generated from passing M_i and K_i into the HMAC function is compared with the broadcasted MAC_i. The broadcasted MAC is deemed to be authentic if it matches the locally generated MAC. In addition, the broadcasted K_i goes through a shorter one-way key hash chain to obtain an output key. K_i is considered authentic if the output key matches with the previously-validated key K_{i-1}. An authentication event (AE) occurs when both components of the MAC-key pair are deemed to be valid by the NMA scheme.

TESLA's security draws from the cryptographic strength of the keyed-hash MAC (HMAC) construction and the one-way key hash chain, both of which depend on the strength of the underlying hash function, the length of the key, and the size of the MAC tag. To meet the equivalent key symmetric-key strength of 128 bits for cryptographic security beyond 2030 [48], SHA-256 is recommended as the hash function to be used, and the key size is required to be at least 128 bits. NIST also recommends the size of the MAC tag to be at least 32 bits, to minimize the occurrence of MAC tag forgery [49]. Hence, the authentication overhead is at least 160 bits per AE. In addition, [50] mentions that the collision resistance of the hash chain decreases linearly with its length. The length of the key generation chain should therefore either be appropriately limited, or be circumvented by increasing the key length at the cost of a higher authentication overhead.

2) Signal Authentication: The proposed NMA scheme—that is, the TESLA-based MAC-and-key mechanism described thus far—only serves to verify the origin of the data. Hence, the data fields relevant to the PNT calculation, such as the pseudolites' positions and timing offsets, are authenticated. However, NMA does not prevent attacks wherein the spoofer re-broadcasts an authentic TRNS signal.

One type of re-broadcast attack, known as *security code estimation and replay* (SCER), requires the spoofer to measure and estimate the current broadcast symbol, and then generate and transmit a forged signal with the desired delay. There is known to be no absolute defense against SCER spoofing in a uni-directional radionavigation system. However, a mitigating factor is that SCER attacks are somewhat challenging to execute because of the need for the spoofer to *full duplex*.

In a lower-cost *half-duplex* attack, the spoofer transmits either intermittently or in an open-loop fashion, generating the spoofing waveform using only information collected while not transmitting. Removing the requirement for nanosecond-latency real-time bit estimation removes substantial engineering challenges in mounting this attack. However, such a spoofer faces a dilemma when dealing with the unpredictable segments of the broadcast message: it can continue with its open-loop transmission and make random guesses about the unpredictable bits, thereby running a high risk of triggering an alarm from NMA; or it can modulate its transmission amplitude to leave an open window for the true signal to pass through. This is significant, because this modulation is potentially detectable by a clever receiver, which will raise an alarm. To avoid detection, the spoofer must limit the rate of change of amplitude and phase variables that it is introducing in between these open windows. Thus, while the half-duplex spoofer would like to introduce controlled delays (and hence position offsets) into the victim's delay-locked loop, each open window forces it to smoothly transition these delay variables back to zero. This limits the size of possible undetectable offsets. The rest of this section extends the TESLA-based NMA scheme to maximize the number of open windows that the half-duplex adversary must deal with, thus providing limited signal authentication.

Since the adversary considered here is potentially a highest-tiered subscriber, everything but MAC_i and K_i are already known to the adversary. If the unknown bits are packaged together at the end of an epoch, as is conventional in data networks, the half-duplex adversary is very effective: the only open windows the receiver can expect are those covering the (infrequent) MAC and key packets; otherwise, the attacker is free to transmit faulty timings provided that they send valid data.

The key idea introduced in this paper is to leaven the unpredictable MAC_i bits into the navigation message packets such that the time duration between any two open windows is as short as possible. This process is shown in Figs. 5 and 6. The watermark bits are placed at predictable positions in the navigation message stream so that the receiver can still access the relevant fields for

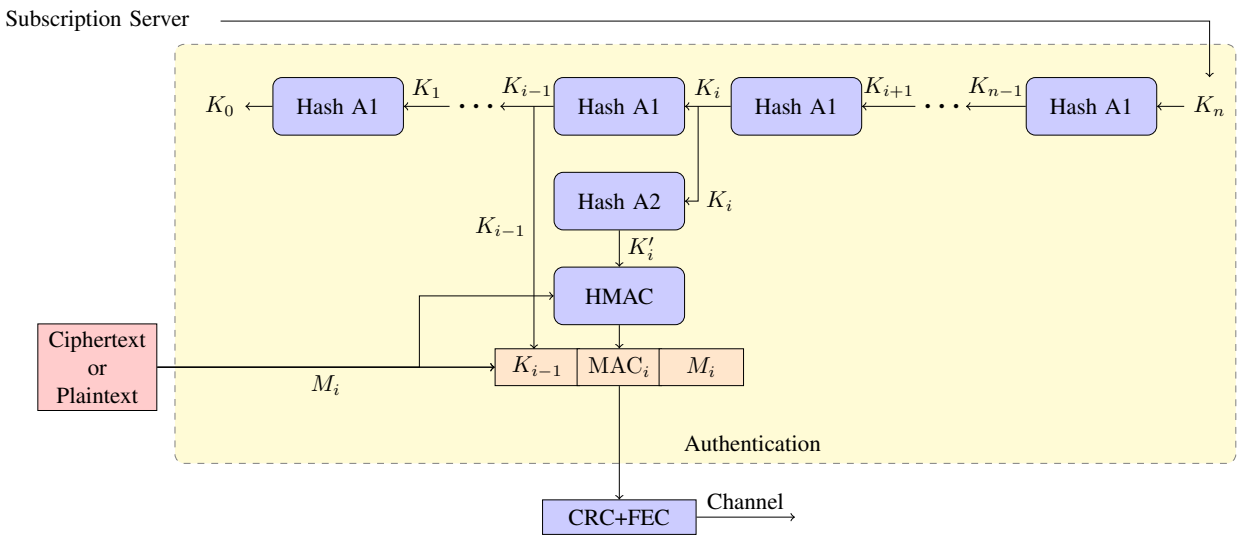

Fig. 3: Authentication processes at the TRNS pseudolite, which include one-way key chain generation, MAC generation, and broadcast packet formation.

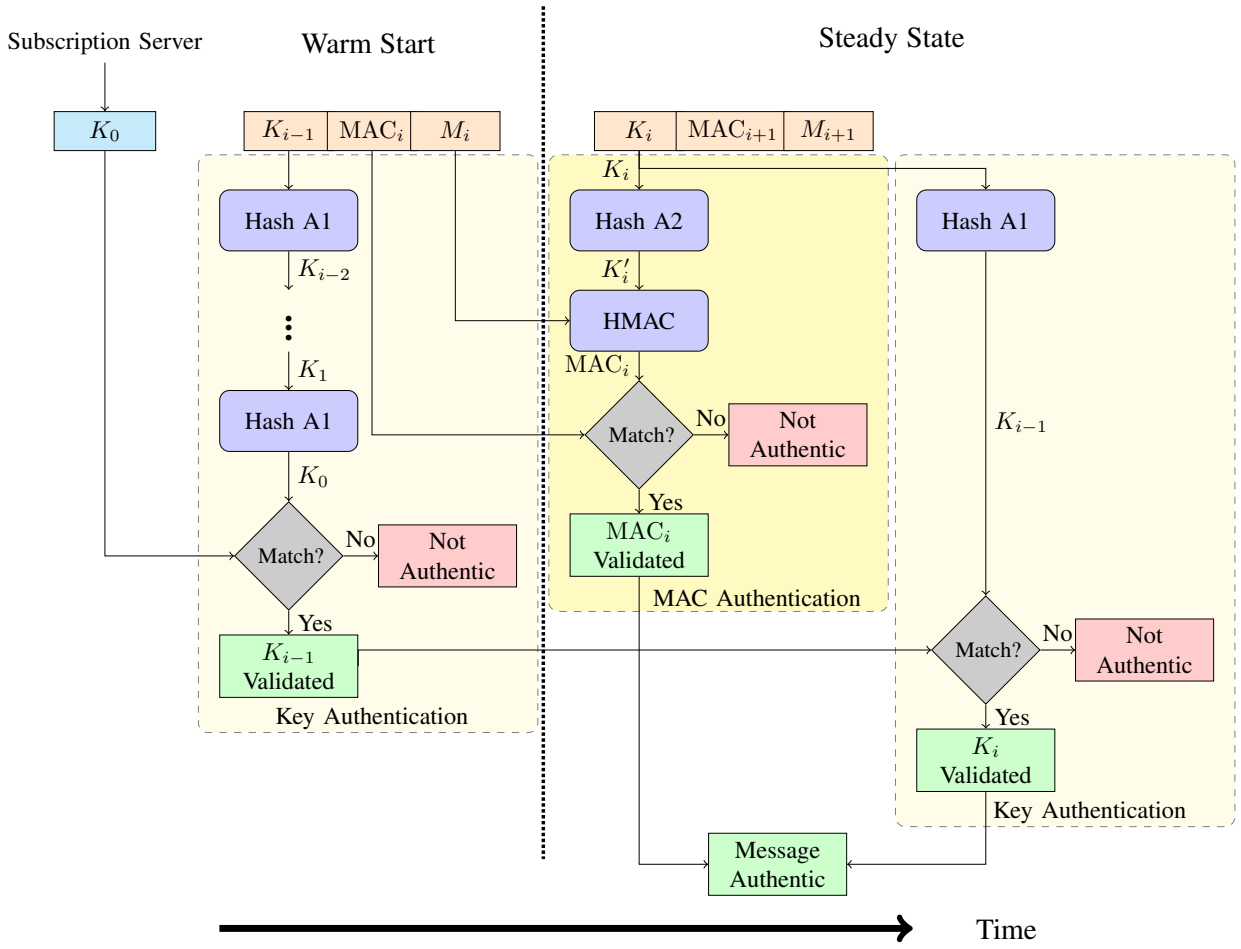

Fig. 4: Authentication processes within the TRNS receiver, which includes key validation during bootstrapping, and both key and MAC validation during steady-state phase.

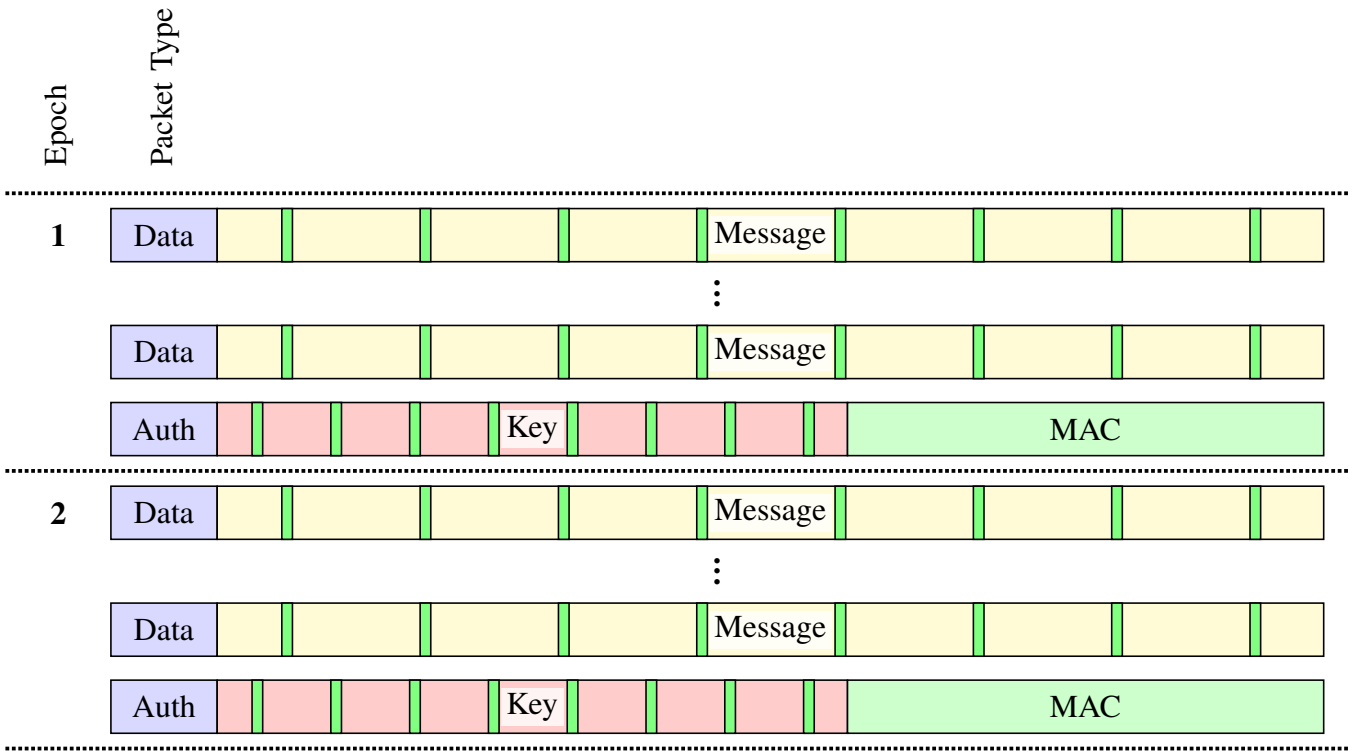

Fig. 5: NMA for a TRNS navigation stream. Error detection, forward error correction, and encryption are not shown. Authentication packets terminate each authentication epoch, and contain the TESLA key for the previous epoch (red), together with a message authentication code (green) computed from the preceding packets in the current epoch. "Watermark" MAC bits (green stripes) are inserted at fixed positions to frustrate half-duplex spoofing attacks. Note that while authentication can proceed without all MAC bits, it cannot proceed without all key bits. For this reason, HMAC output bits (green) may be truncated to trade reduced security for reduced authentication overhead, but key bits (red) cannot be truncated.

PNT calculation. The exact locations of these watermark bits are non-critical, as they will be spread throughout the transmitted waveform by the interleaver. However, the watermarks should be spaced out by at least the constraint length of the convolutional code in order to maximize the number of affected code bits.

The requirement to introduce controlled delays and transition them to zero before the next open window, together with maximal frequency of open windows, limits the adversary's ability to spoof large position incursions.

The duration between open windows is minimized if all of the MAC_i and K_i bits are uniformly distributed across the navigation message. However, note that while authentication can proceed without all MAC bits, it cannot proceed without all key bits. Leavening key bits in the navigation message would increase the likelihood of failed authentication due to a packet error containing a key bit. Accordingly, the proposed protocol leavens only the HMAC output bits to trade reduced security for reduced authentication overhead. Another consequence of a packet error would be incomplete recovery of the navigation message bits, which would also preclude authentication. Fortunately, a receiver may re-construct lost navigation message bits before computing the MAC if these bits are known to be repeated verbatim on a set schedule, and at least one was successfully decoded.

Although this elaboration of the proposed NMA scheme provides a degree of signal authentication, it is not foolproof against all types of spoofing attacks. It aims for the lesser goal of defeating half-duplex attacks and forcing attackers to turn to more costly alternatives like SCER. Unfortunately, SCA fares no better against SCER attacks than the proposed MAC-leavened NMA scheme. As such, use of exotic signal-level authentication schemes provide no additional advantage.

V. Conclusion

This paper outlines the unique vulnerabilities of a generic T-PNT system due to its terrestrial infrastructure, high signal strength with wide dynamic range for deep-urban and indoor coverage, and a potential reliance on GNSS for network synchronization. Despite these challenges, this

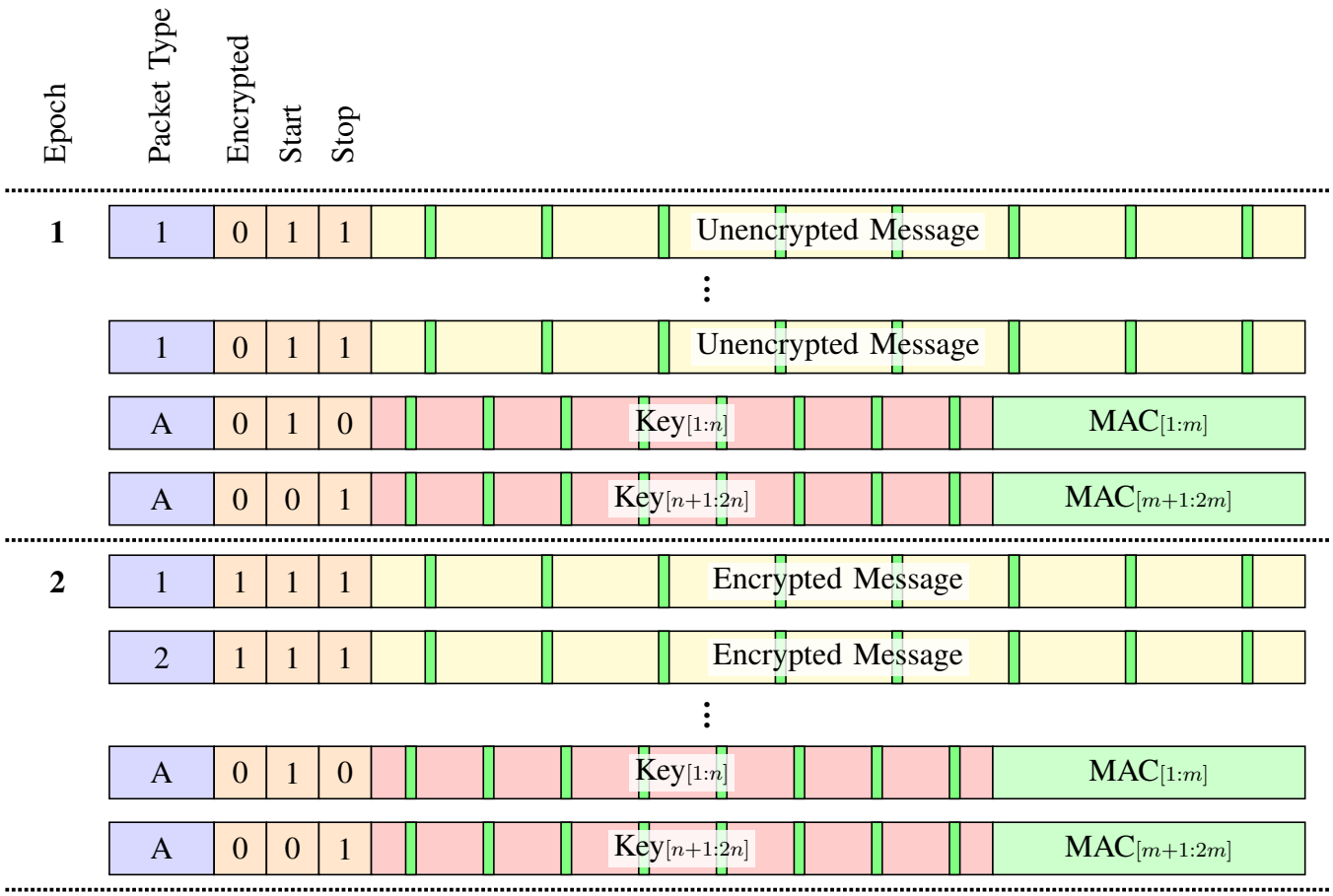

Fig. 6: NMA for a short-packet TRNS navigation stream. Packets may be fragmented (e.g. Start, Stop) as required. The schedule of packet types, analogous to almanac pages in GPS, determines the time-to-first-fix. To improve authentication robustness, a receiver may re-construct lost packets before computing the MAC if these packets are known to be repeated verbatim on a set schedule, and at least one was successfully decoded. Note that a spoofer attempting a downgrade attack (spoofing a zero bit in the "Encrypted" field) will trigger authentication alarms.

paper draws upon the flexibility offered by a clean-slate TRNS waveform to propose cryptographic schemes that offers more than protection against both low-cost spoofers and unauthorized users. An NME scheme is introduced, which not only limits T-PNT service to authorized users, but also can be customized for multiple subscriber tiers by implementing selective decryption. In addition, a novel TESLA-based NMA scheme that leavens unpredictable MAC bits into the navigation message packets is presented, which provides both data authentication and a certain degree of signal authentication against half-duplex spoofing attacks. While the proposed schemes are not foolproof against all types of spoofing attacks and unauthorized use (e.g. as signals of opportunity), they offer robust and accurate PNT service only to TRNS subscribers with selective availability and enhanced data security.

ACKNOWLEDGEMENTS

This work has been supported by NextNav LLC as an affiliate of the The University of Texas Situation-Aware Vehicular Engineering Systems (SAVES) Center (http://utsaves.org/), an initiative of the 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, "Positioning in GPS challenged locations-the NextNav terrestrial positioning constellation," *Proc. ION GNSS+ 2013*, 2013.

[3] C. Rizos, D. A. Grejner-Brzezinska, C. K. Toth, A. G. Dempster, Y. Li, N. Politi, J. Barnes, and H. Sun, "A hybrid system for navigation in GPS-challenged environments: Case study," *Proceedings, ION GNSS, Savannah, Georgia, Sept*, pp. 16–19, 2008.

[4] C. Rizos and L. Yang, "Background and recent advances in the locata terrestrial positioning and timing technology," *Sensors*, vol. 19, no. 8, p. 1821, 2019.

[5] J. Barnes, C. Rizos, M. Kanli, D. Small, G. Voigt, N. Gambale, J. Lamance, T. Nunan, and C. Reid, "Indoor industrial machine guidance using Locata: A pilot study at BlueScope Steel," in *60th Annual Meeting of the US Inst. Of Navigation*, 2004, pp. 533–540.

[6] F. A. Khan, C. Rizos, and A. G. Dempster, "Novel time-sharing scheme for virtual elimination of locata-WiFi interference effects," in *Int. Symp. on GPS/GNSS*, 2008, pp. 526–530.

[7] ——, "Locata performance evaluation in the presence of wide-and narrow-band interference," *Journal of Navigation*, vol. 63, no. 3, p. 527, 2010.

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

[9] 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.

[10] 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.

[11] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," in *Proceedings of the ION International Technical Meeting*, San Diego, CA, Jan. 2010.

[12] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE signal processing magazine*, vol. 34, no. 5, pp. 27–37, 2017.

[13] T. E. Humphreys, *Springer Handbook of Global Navigation Satellite Systems*. Springer, 2017, ch. Interference, pp. 469–504.

[14] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[15] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS Meeting*. Savannah, GA: Institute of Navigation, 2008.

[16] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[17] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[18] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, T. E. Humphreys, and A. Schofield, "GNSS lies, GNSS truth: Spoofing detection with two-antenna differential carrier phase," *GPS World*, vol. 25, no. 11, pp. 36–44, Feb. 2014.

[19] C4ADS, "Above us only stars: Exposing GPS spoofing in Russia and Syria," April 2019, https://c4ads.org/reports.

[20] M. J. Murrian, L. Narula, and T. E. Humphreys, "Characterizing terrestrial GNSS interference from low earth orbit," in *Proceedings of the ION GNSS+ Meeting*, Miami, FL, 2019.

[21] M. Harris, "Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai," *MIT Technology Review*, 11 2019. [Online]. Available: https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

[22] B. Bergman, "AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco," 05 2020. [Online]. Available: https://skytruth.org/2020/05/ais-ship-tracking-data-shows-false-vessel-tracks-circling-above-point-reyes-near-san-francisco/

[23] T. E. Humphreys, "Lost in Space: How Secure Is the Future of Mobile Positioning?" 02 2016. [Online]. Available: https://www.comsoc.org/publications/ctn/lost-space-how-secure-future-mobile-positioning

[24] C. Yang, A. Soloviev, M. Veth, and D. Qiu, "Opportunistic Use of Metropolitan RF Beacon Signals for Urban and Indoor Positioning," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, Oregon*, 2016, pp. 394–403.

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

[26] 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.

[27] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," in *Proceedings of the 25th Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2012)*. ION, 2012.

[28] D. Borio, "PANOVA tests and their application to GNSS spoofing detection," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 1, pp. 381–394, Jan. 2013.

[29] L. He, H. Li, and M. Lu, "Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival," *GPS Solutions*, vol. 23, no. 3, p. 78, 2019.

[30] M. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proceedings of the ION GNSS+ Meeting*, 2013, pp. 2949–2991.

[31] A. Broumandan, A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proceedings of the IEEE/ION PLANS Meeting*. Myrtle Beach, SC: Institute of Navigation, April 2012.

[32] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications," in *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2014), Tampa, FL*. Citeseer, 2014, pp. 2233–2242.

[33] J.-P. Poncelet and D. M. Akos, "A low-cost monitoring station for detection & localization of interference in GPS L1 band," in *2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing*. IEEE, 2012, pp. 1–6.

[34] Y. C. Lee and D. G. O'Laughlin, "Performance Analysis of a Tightly Coupled GPS/Inertial System for Two Integrity Monitoring Methods 1," *Navigation*, vol. 47, no. 3, pp. 175–189, 2000.

[35] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*. IEEE, 2014, pp. 1232–1239.

[36] 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.

[37] C. Wullems, O. Pozzobon, and K. Kubik, "Signal authentication and integrity schemes for next generation global navigation satellite systems," in *Proc. European Navigation Conference GNSS*, Munich, July 2005.

[38] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

[39] J. T. Curran and M. Paonni, "Securing GNSS: An end-to-end feasibility study for the Galileo open service," in *International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GNSS*, 2014, pp. 1–15.

[40] 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.

[41] K. Chino, D. Manandhar, and R. Shibasaki, "Authentication technology using QZSS," in *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*. IEEE, 2014, pp. 367–372.

[42] S. C. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts," in *IEEE/ION Position, Location and Navigation Symposium*. IEEE, 2010, pp. 708–717.

[43] A. Neish, T. Walter, and P. Enge, "Quantum-resistant authentication

algorithms for satellite-based augmentation systems," *Navigation*, vol. 66, no. 1, pp. 199–209, 2019.
[44] A. Neish, T. Walter, and J. D. Powell, "Design and analysis of a public key infrastructure for sbas data authentication," *Navigation*, vol. 66, no. 4, pp. 831–844, 2019.
[45] P. Gutierrez, "Galileo to Transmit Open Service Authentication," *Inside GNSS*, 2020.
[46] F. Dovis, M. Luciano, B. Motella, and E. Falletti, *GNSS interference threats and countermeasures*. Artech House, 2015, ch. Classification of Interfering Sources and Analysis of the Effects on GNSS Receivers, pp. 31–66.
[47] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.
[48] NIST, "Recommendation for key management—Part I: General (revised)," National Institute of Standards and Technology, SP 800-57, July 2012.
[49] Q. Dang, "Recommendation for applications using approved hash algorithms (revised)," National Institute of Standards and Technology, SP 800-107, Aug. 2007.
[50] G. Caparra, S. Sturaro, N. Laurenti, and C. Wullems, "Evaluating the security of one-way key chains in TESLA-based GNSS Navigation Message Authentication schemes," in *2016 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2016, pp. 1–6.