The Thesis Committee for Ronnie Xian Thong Kor
Certifies that this is the approved version of the following Thesis:

A Comprehensive Proposal for Securing Terrestrial Radionavigation Systems

APPROVED BY

SUPERVISING COMMITTEE:

Todd E. Humphreys, Supervisor

Peter A. Iannucci, Co-Supervisor

A Comprehensive Proposal for Securing Terrestrial Radionavigation Systems

by

Ronnie Xian Thong Kor

THESIS

Presented to the Faculty of the Graduate School of
The University of Texas at Austin
in Partial Fulfillment
of the Requirements
for the Degree of

MASTER OF SCIENCE IN ENGINEERING

THE UNIVERSITY OF TEXAS AT AUSTIN
May 2021

“If I have seen further, it is by standing on the shoulders of Giants.”

– Isaac Newton, 1675.

Dedicated to my wife Qiu Yan, and all my benefactors.

Acknowledgments

My research accomplishments would have been difficult, if not impossible, without the generous help of the many wonderful people I have been blessed to know. I would like to express my utmost gratitude to the following people.

To my advisor, Prof. Todd E. Humphreys, for welcoming me into UT Radionavigation Laboratory, and for his guidance and support over the past two years. Our research discussions, as well as his classes on Statistical Estimation and GNSS Signal Processing, helped me gain a deeper understanding on navigation systems. In addition, I have learned much from Prof. Humphreys on technical writing and personnel management.

To my co-supervisor, Dr. Peter A. Iannucci, who has guided me in research since day one. He has been very generous with both his time and advice. He has also been very accommodative over the period when we have to work with a time zone difference. I would not have accomplished so much within this short span of time without his selfless guidance.

To all outstanding members of the Radionavigation Laboratory for their inspiration and friendship. Special shout-out to Dr. Lakshay Narula, who is always generous with his advice and time in streamlining my research.

To the sponsor of this research, NextNav LLC, and the U.S. Department of Transportation, for their generous funding. Special shout-out to Dr. Arun Raghu-

pathy and Dr. Cristina Seibert from NextNav LLC for providing valuable insights during our bi-weekly discussions.

To my sponsor and employer, DSO National Laboratories for the Post-Graduate Scholarship Award. Special thanks to CEO Mr. Cheong Chee Hoo, Senior Director Dr. Tan Kok Tin, Director Mr. Aldrin Wong, Program Directors Mr. Yee Kwong Min and Dr. Poh Eng Kee for believing in me, and my mentor Dr. Gabriel Wong for his advice on managing the challenges of postgraduate education.

To my friend Stefanie, whom I have ‘struggled’ through the rigorous ASE coursework with, and without whom I would not have sailed through my postgraduate study with ease. Also to my friend and fellow Singaporean Timothy Yap, for his friendship and support throughout my M.S. journey.

To my parents, sisters, and in-law family, whom I have always missed from 10,000 miles away, for their selfless love and encouragement, and their help in settling all household matters during my absence from Singapore.

To my cute daughter Ryoko, who always surprises me with her tenacity and intelligence, for being the ideal distraction to take my mind off from the stress of coursework and research.

Last but not least, to my wonderful and capable wife Qiu Yan, for holding back her career progression to take on the tough role of a household director, and for being my strong pillar of support throughout this journey.

Hook ’em Horns.

A Comprehensive Proposal for Securing Terrestrial Radionavigation Systems

Ronnie Xian Thong Kor, M.S.E.
The University of Texas at Austin, 2021

Supervisors: Todd E. Humphreys
Peter A. Iannucci

The security of terrestrial radionavigation 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 thesis 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 thesis proposes orthogonal mechanisms combining navigation message encryption (NME) and navigation message 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. This cryptographic proposal, however, is still vulnerable to certain types of replay threats. This thesis addresses this gap by augmenting TRNS with autonomous signal-situational-awareness (SSA) capability, allowing TRNS operators to detect spoofing and meaconing attacks. Two signal authentication techniques for SSA are developed to detect a weak spoofing signal in the presence of static and dynamic multipath. This thesis also proposes enhancements to these signal authentication techniques. These enhancements exploit the synergy from combining information across multiple epochs, or over multiple monitoring beacons, to further lower the spoofer detection threshold. Both techniques with their enhancements are shown to be effective in simulations of the varied operating environments that a generic TRNS will encounter. With both proposed cryptographic NME+NMA scheme and autonomous SSA in place, TRNS gains a defensive capability that GNSS cannot easily match: a comprehensive defense against most man-in-the-middle attacks on position, navigation and timing services.

Table of Contents

List of Tables

List of Figures

Chapter 1

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, GNSS struggle to provide coverage in deep-urban and indoor environments. The requirement for accurate and assured indoor positioning limits the effectiveness of GNSS in high-stakes, safety-of-life applications like enhanced 911 (E911), as well as in a new generation of commercial applications like warehouse automation and asset tracking.

Current and upcoming terrestrial radionavigation systems (TRNS) like Locata [75] and NextNav [53, 54] seek 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 ranging beacons, 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 [74, 76], or it may serve as a primary navigation aid in the indoor environment [3].

TRNS sensitivity to wide-band radio-frequency interference (RFI) [37, 38] has 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 radionavigation systems, as the shared vulnerabilities between the two domains arise from fundamental properties of radio systems. Thus, security considerations for TRNS can draw from lessons learned in the vibrant body of research on GNSS signal security [67].

However, TRNS have unique vulnerabilities that have been recently outlined in reference [42], which include: (1) the vastly different dynamic range of signal power for terrestrial versus space-based transmission; (2) the overlapping angular distribution of spoofed, authentic, and multipath signals; and (3) the relative physical accessibility of TRNS transmitters. This means that TRNS operate in a quantitatively distinct region of parameter space compared to GNSS: security code estimation and replay (SCER) spoofing attacks [28] are facilitated by attackers' access to high signal-to-noise ratio (SNR) signals; receiver quantization and dynamic range effects limit mitigations based on simultaneous demodulation of spoofed and authentic waveforms [26]; and the potential for poor angular separation between authentic and spoofed signals renders angle-of-arrival techniques based on multi-element antennas [7, 15, 70] less effective.

Nevertheless, novel commercial TRNS's design is a *tabula rasa*, offering an opportunity to exploit unique advantages for enhanced security. These new security measures can, of course, also leverage the best spoofing defenses produced by two decades of research effort in securing GNSS [68,80]. These includes cryptographic and non-cryptographic techniques [16], which represents an overlapping and layered defense against radionavigation spoofing: receivers should seek to identify reliable signals both by their content and by their context. The clean-slate design of TRNS waveform offers flexibility in the application of the latest cryptographic defense techniques without being constrained by the need of backward compatibility. Mutual observability using signal multiplexing and bi-directional communication between adjacent beacons can be built into the design of TRNS system architecture, which will augment the TRNS system with secure time synchronization, integrity monitoring, and autonomous signal-situational-awareness (SSA) capabilities.

TRNS networks have great potential to advance the security of PNT beyond what is possible with traditional GNSS alone. With green-field signals and autonomous SSA, TRNS may finally offer a solid, comprehensive defense against MITM (man-in-the-middle) attacks on PNT.

1.1 Thesis Statement and Expected Contributions

This thesis makes four primary contributions:

(i) It analyzes the security considerations of TRNS due to their wide signal dynamic range, proximity of threats to pseudolites, and potential dependence on GNSS to meet the stringent synchronization and frequency stability requirements.

(ii) It offers a cryptographic security proposal for TRNS mobile users, with a focus on data-level security in recognition of the futility of waveform- or signal-level security. This proposal has two non-obvious aspects: MAC leavening, whereby a modest number of navigation message authentication (NMA) bits spread throughout the transmitted packets provide a significant improvement in security, and multi-tiered navigation message encryption (NME), which has not been used before in PNT security and makes the adoption of this proposal more enticing for commercial service providers.

(iii) To address the cryptographic security proposal's gap in the defense against SCER and meaconing attacks, this thesis proposes an autonomous signal-situational-awareness (SSA) overlay capability within a TRNS network. The SSA capability augments basic TRNS operations with cooperative monitoring among nearby beacons. While not all spoofers can be detected in this way, SSA gives TRNS operators the best possible chance of detecting threats and warning users without resorting to costly full-duplex techniques. Although this contribution is similar to prior works by [91] and [21], it addresses a TRNS-relevant problem of detecting a spoofing signal in the presence of dynamic multipaths. This thesis also looks into the enhancement of TRNS performance by performing joint detection across multiple epochs, and with multiple monitoring beacons.

(iv) It conducts an urban multipath propagation measurement campaign at The University of Texas at Austin. The statistical analysis on the data logs validated the empirical multipath model used in SSA simulations, and gleaned insights on the characteristics of dynamic multipath.

1.2 List of Publications

1.2.1 Journal Publications

[J1] **Ronnie X.T. Kor**, Peter A. Iannucci, and Todd E. Humphreys. Comprehensive PNT Security for a Terrestrial Radionavigation System. *Navigation, Journal of the Institute of Navigation*, 2021. In preparation.

1.2.2 Conference Publications

[C1] **Ronnie X.T. Kor**, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys. A Proposal for Securing Terrestrial Radio-navigation Systems. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020.

[C2] **Ronnie X.T. Kor**, Peter A. Iannucci, and Todd E. Humphreys. Autonomous Signal-Situational Awareness in a Terrestrial Radionavigation System. In *Proceedings of the 24th IEEE International Conference on Intelligent Transportation*, 2021. Submitted for review.

[C3] Todd E. Humphreys, **Ronnie X.T. Kor**, Peter A. Iannucci, and James E. Yoder. Open-World Virtual Reality Headset Tracking. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020.

1.3 Thesis Organization

Chapter 2 analyzes the primary security considerations of TRNS. Chapter 3 gathers results from past proposals for GNSS security,and discusses the relevance of each technique for TRNS. Chapter 4 presents a cryptographic security proposal for securing TRNS mobile users with multi-tiered NME + message authentication code (MAC)-leavened NMA. Chapter 5 details the signal authentication techniques considered for SSA and their enhancements, and presents an analysis that quantifies the effectiveness of autonomous SSA under some of the myriad operating conditions encountered by a generic TRNS. Chapter 6 presents an empirical analysis of multipath in an urban environment. Chapter 7 concludes this thesis with a summary of the main contributions.

Chapter 2

TRNS Security Considerations

From the perspective of a radionavigation 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 radionavigation security into two domains, termed Encryption (denying stow-aways) and Authentication (detecting spoofing). (N.B. that cryptography is a useful tool in both domains). The focus of this work on commercial TRNS prompts the adoption of the term "subscriber" to refer to an authorized user.

2.1 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,

This chapter is based on: Ronnie X.T. Kor, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys. A proposal for securing terrestrial radio-navigation systems. In *Proceedings of the ION GNSS+ Meeting*, Online, 2020.

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 placing 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 their coordinates.

2.2 Radio-Frequency Interference

Radionavigation systems, GNSS and TRNS alike, are susceptible to RFI caused by jammers and spoofers. Fig. 2.1 gives an overview of RFI. Among all the RFI threats, spoofing is of particular interest, 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. A spoofer can arbitrarily adjust its signal’s power, code phase, carrier phase, and signal structure to smoothly overtake a victim receiver’s tracking loops, achieving maximum spoofing efficacy in the process. Spoofing can be broadly classified into the following types of attacks:

[S1] 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 [28].

[S2] 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 [43].

[S3] Security Code Estimation and Replay (SCER): This attack synthesizes a counterfeit replica 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 [28].

[S4] 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 [51].

2.3 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 receiver [31]. A number of live-signal spoofing tests in a controlled environment which followed thereafter also confirmed the effect [5, 35, 69]. This threat continues to be relevant today, with reports of spoofers being used at 9 different

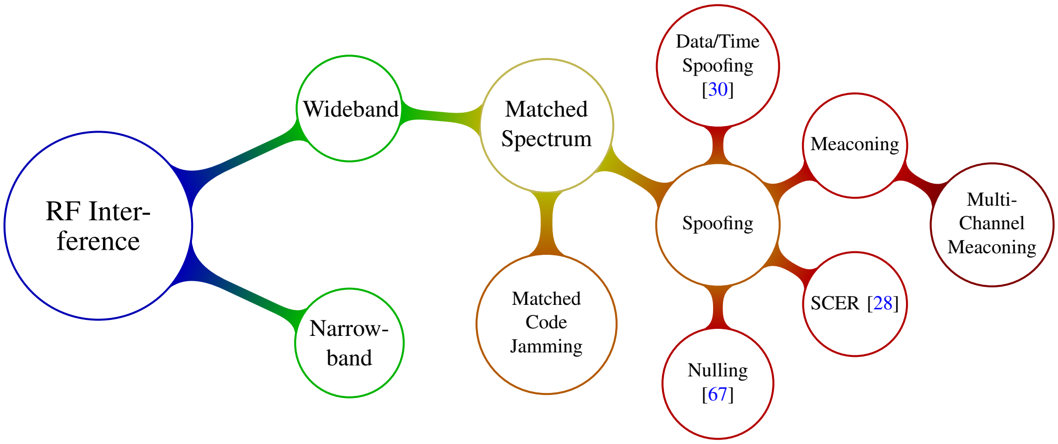


Figure 2.1: A taxonomy of RF interference (i.e. an attaxonomy).

locations, each of which has the capability of "fooling" multiple victim receivers to coincidentally move along the same track [4]. There are also recent rumors of spoofing "in the wild" seen in specific spots such as Black Sea [9], Syria [58] and China [23]. 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 [29]. The spoofing threat is also relevant to TRNS because a functional TRNS spoofer is essentially a modified 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 codes and/or navigation data bits 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, with signal strength below noise floor at the receiver, the spreading code sequence of TRNS can be exposed without the use of high-gain antenna due to its high SNR. Reference [95] 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 a 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.

2.4 Conclusion

This chapter provides an discussion of TRNS security considerations with respect to its vulnerabilities to spoofing threats, resulting from: (1) its high SNR and wide signal dynamic range, (2) the indistinguishable angular distribution of spoofed signal from that of the authentic and multipath signals, and (3) the accessibility of its transmitters to physical or cyber tampering. Chapter 3 reviews existing GNSS spoofing detection techniques and the challenges to their implementation for TRNS, and identifies compatible methods for TRNS security.

Chapter 3

Lessons Learned from GNSS Security

TRNS inherits from traditional radionavigation 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 [16, 82]: (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

This chapter is based on: Ronnie X.T. Kor, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys. A proposal for securing terrestrial radio-navigation systems. In *Proceedings of the ION GNSS+ Meeting*, Online, 2020.

GNSS spoofing defenses is presented in [67].

3.1 Non-cryptographic Defenses

Non-cryptographic defenses are attractive because 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.

3.1.1 Geometric Techniques

Geometric techniques exploit the RF signals' geometric diversity to verify the authenticity of the signal source. This includes angle-of-arrival (AOA) discrimination techniques [7, 56, 57, 70], Doppler frequency difference of arrival (FDOA) discrimination [24], or beamforming feature extraction [55] using multiple antennas. Other geometric techniques advocate the use of single antenna, and discriminate spoofed and authentic signals either with a known perturbation profile [66], a random motion profile [8], or using multiple feeds from a single antenna [52]. The assumptions made by these techniques are (1) the spoofing signals generally arrive from below or near the horizon [52], (2) the observations from spoofing signals are not aligned with the actual geometry between the satellites and the victim receiver [56, 57], and (3) there is a strong correlation between signal characteristics of different satellites from the spoofing signals [7, 8, 66, 70].

Geometric techniques are less applicable to TRNS because, unlike with GNSS, it is not costly for a sophisticated spoofer to co-locate dedicated spoofing sources at each of the TRNS pseudolites in a local network, thereby defeating all the assumptions made by geometric techniques. In addition, the need for hardware modification or additional hardware might not be suitable for applications that either use existing hardware for mass-market adoption, or have SWaP-C constraints.

3.1.2 Drift-Monitoring Techniques

Drift monitoring techniques 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 external oscillator to check for inconsistency in the clock bias or clock drift [65], or the use of visual/inertial/radar odometry [39, 45] or a height sensor [44] to place constraints on the reasonable error growth of a position fix. 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.

3.1.3 Signal Processing Techniques

Several techniques proposed in the GNSS literature apply advanced signal processing algorithms for spoofing detection. Unlike other non-cryptographic spoofing defenses, these techniques can be readily implemented on existing GNSS receivers via a firmware upgrade, and do not need additional hardware for their operations. They can be categorized into two classes, one that detects the inception of a spoofing attack, and another that does a brute-force search for all signals in the landscape for post-inception detection.

Included in the first class are techniques that look for a sudden deviation in the received signal characteristics (carrier amplitude, beat carrier phase, code phase, carrier-to-noise density ratio, or received power) to detect the onset of a spoofing attack [1, 58]. Also included are techniques based on Signal Quality Monitoring (SQM) that identify asymmetry or other distortion in the complex correlation function [11, 92]. Multiple signal metrics can be derived by combining observations of both the received power and the correlation function distortion [91].

The second class of techniques performs a brute-force acquisition search for the presence of known signals using Complex Ambiguity Function (CAF) monitoring [25]. This approach avoids the problem of missed detection due to the transient nature of initial spoofing drag-off.

These techniques generally work for GNSS, as it has signal strength below the noise floor and a narrow dynamic range of signal power. In contrast, TRNS generally have high SNR—for quick acquisition in both dense-urban and indoor environments—and a wide signal power dynamic range. Analogous to variations in the received signal strength from low-elevation GNSS satellites in an urban environment, without complete knowledge of its deep-fading channel model, a mobile receiver cannot straightforwardly predict the received signal strength of the authentic signal emanating from a particular TRNS beacon. A potential spoofer will thus have a wide margin to adjust its power in its attempt to overtake a victim receiver's tracking loops. Therefore, it is challenging for mobile receivers to perform spoofing detection using these techniques, given the wide dynamic range of their received power.

In contrast, TRNS infrastructural monitors can fully exploit these signal processing techniques for spoofing detection. Assuming that each of them has multiple correlators, and a secure clock synchronization [59] embedded in its network, these monitors can narrowly characterize all signals in their nominal operating environments, such that any signal anomalies in their surveilled landscape will stand out. This thesis capitalizes on these merits by proposing two signal authentication techniques in Chapter 5 customized for these TRNS monitors, such that a spoofing signal, with an SNR below that of the authentic signal, can be detected even in the presence of static and dynamic multipath.

3.2 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 radionavigation.

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 [79]. 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 [36,79,93], Galileo [13,19], QZSS [12] and SBAS [50, 60, 61]. 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 [22]. This technique uses either a delayed symmetric key release approach such as *timed efficient stream loss-tolerant authentication* (TESLA) [93], or an asymmetric private-key/public-key approach such as the *elliptic curve digital signature algorithm* (ECDSA) [36]. 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. Chapter 4 proposes one implementation of NME and NMA for a TRNS.

3.3 Cooperative Sensing

Cooperative sensing for signal authentication has been considered in recent GNSS literature. These can be broadly classified into: (1) temporal variations in GNSS observables, and (2) code-less cross-correlation of unpredictable code sequences. The first method presents a spoofing detection mechanism which compares the raw GNSS observables between two connected GNSS devices, which includes carrier phase differential GNSS (CDGNSS) measurements [34] or signal monitoring metrics [78]. The limitations of its applicability to TRNS has been outlined in Subsection 3.1.1 and 3.1.2.

The second method by [49] is based on code-less cross-correlation of the unpredictable encrypted military P(Y) code between two civil GPS receivers. Fig. 3.1 illustrates the relationship between the publicly-known C/A and encrypted P(Y)

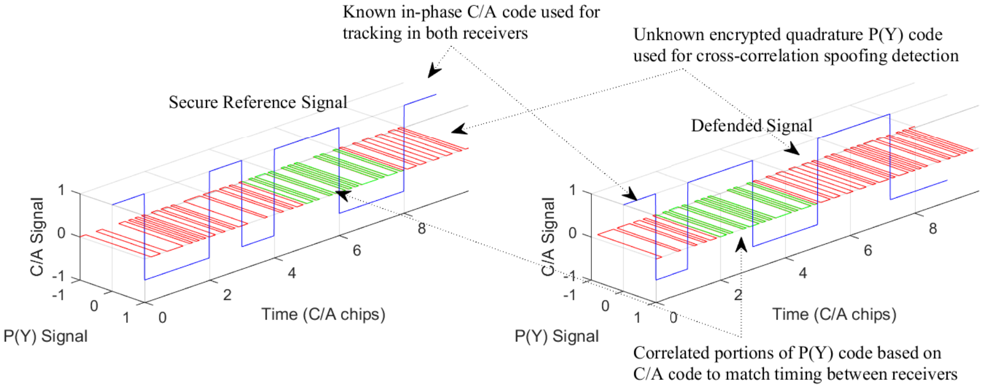

Known in-phase C/A code used for tracking in both receivers
Unknown encrypted quadrature P(Y) code used for cross-correlation spoofing detection
Secure Reference Signal
Defended Signal
C/A Signal
P(Y) Signal
Time (C/A chips)
1
0
-1
-1
0
1
0
2
4
6
8
C/A Signal
P(Y) Signal
Time (C/A chips)
1
0
-1
-1
0
1
0
2
4
6
8
Correlated portions of P(Y) code based on C/A code to match timing between receivers

Figure 3.1: Relationship between publicly-known C/A signal and encrypted P(Y) signals on reference receiver (left) and user receiver (right) (adapted from [71]). The C/A codes (in blue vertical pulses) are in phase quadrature with the P(Y) codes (in red horizontal pulses). The green portion of the P(Y) codes are extracted for cross-correlation at each epoch.

signals on the GPS L1 frequency, and outlines the strategy of this cross-correlation method outlined in [49]. First, each receiver estimates the delay and phase offset of the blue C/A signals in their code and carrier tracking loops. A snippet of L1 signal (in green) is then extracted from both receivers for authentication. These snippets are then cross-correlated with each other based on known phase and timing relationships between the C/A and P(Y) codes in each receiver. Although the green snippets are encrypted, distorted by a narrow-band radio-frequency (RF) front-end [71], and corrupted by thermal and quantization noise, the correlation of these green snippets will result in a high correlation peak only if neither receivers are spoofed.

Two techniques have been developed from this cooperative approach. The first technique by [63, 71] adopts a client-server architecture, in which a number of dedicated reference receivers provide GNSS authentication service for many client receivers over a wide area via a secure communication link. Although this technique offers advantages similar to signal processing techniques outlined in Subsection 3.1.3, the security of the fixed reference stations (similar to those outlined for TRNS in Section 2.3) affects the reliability of signal authentication. Recognizing these limitations, [27] proposes a peer-to-peer architecture, which performs pair-wise check between multiple voluntary peers followed by decision aggregation from the detection statistics resulting from code-less cross-correlation. However, its spoofing detection performance is dependent on the quantity and quality of crowd-sourced data, and its implementation will be impeded by surveillance and privacy concerns of end-users [32].

The code-less cross-correlation method rides on the existence of dual spreading codes on the GPS L1 signal. However, this requirement might not be favored by TRNS providers due to interoperability issues and bandwidth limitation. In addition, a tenet of the code-less cross-correlation method is the asymmetry created by the encryption mechanism, which is only possessed by the service provider. However, this tenet can be shattered by SCER or meaconing attacks [71]. TRNS, on the other hand, has bi-directional communication between infrastructural monitors, allowing it to escape from the security ”no-go” theorem of [59] that prevents traditional GNSS from defeating full-duplex spoofing attacks. Chapter 5 outlines the merits of autonomous SSA by having mutual observability within TRNS network.

3.4 Conclusion

Both cryptographic and non-cryptographic techniques represent an overlapping and layered defense against spoofing: receivers should like to identify reliable signals both by their content and by their context. While these above-mentioned techniques have been proven to be effective for GNSS, there are challenges to their implementation for TRNS. However, 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 and non-cryptographic defense techniques—many of which were originally proposed for GNSS. In this framework, one may envision two types of receivers with differing needs: mobile users, and infrastructural monitors. Chapter 4 details a multi-tiered NME + MAC-leavened NMA scheme to counter against unauthorized access and half-duplex spoofer. Chapter 5 presents an autonomous SSA capability that complements with the cryptographic proposal, and provides a deterrence against SCER spoofing and meaconing attacks.

Chapter 4

TRNS Cryptographic Security Design

This chapter presents a cryptographic security design proposal that addresses the vulnerabilities of TRNS mobile users to two types of adversaries: spoofers and unauthorized users.

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 in the event that significant disruption results from the spoofing signal. The security proposal outlined in this chapter 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) similar to that generated by an authentic transmitter but of different delay and/or content, and the other in which the adversary simply re-broadcast a signal previously broadcasted

This chapter is based on: Ronnie X.T. Kor, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys. A proposal for securing terrestrial radio-navigation systems. In *Proceedings of the ION GNSS+ Meeting*, Online, 2020.

by an authentic transmitter. Authentication mechanisms such as SCA and NMA are designed to thwart the first kind of attack. However, neither SCA nor NMA can defend against the second type of spoofing attack [17]. This chapter focuses on the design of an NMA scheme with some SCA elements that can provide alerts to the first type of attack.

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

With regard to unauthorized usage, it is not possible to prevent the use of TRNS signal as a signal-of-opportunity, whereby unauthorized users estimate the position and clock states of the authentic transmitters so that these signals can be used for localization. Nonetheless, unauthorized use as a signal-of-opportunity is much more involved when the navigation message is not plainly available. Accordingly, this chapter proposed the use of NME to limit terrestrial PNT service to authorized users.

4.1 Selective Navigation Message Encryption

This 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 thesis 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. 4.1 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. $\mathrm{PSS1}$ takes the role of a symmetric key. $\mathrm{PSS2}$ 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).

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

Note that while $\mathrm{PSS2}$ 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

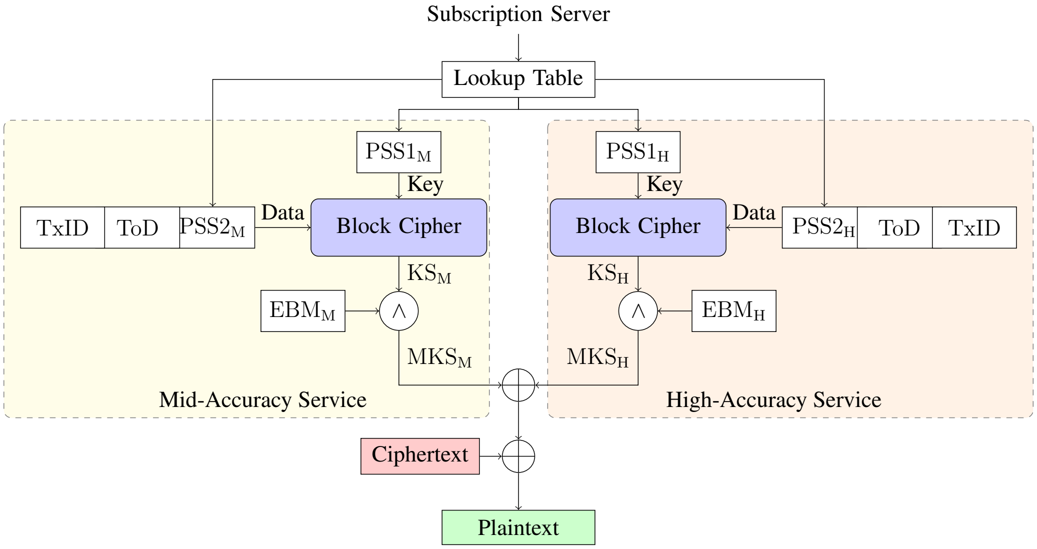


Figure 4.1: Proposed TRNS NME scheme from the perspective of a high-accuracy service receiver. Note that in the high-accuracy receiver, both mid- and high-accuracy key streams are computed in order to decrypt the entire message.

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 $(\mathrm{E}(M) \,\|\, \mathrm{CRC}(\mathrm{E}(M)))$ and XOR it with $(X \,\|\, \mathrm{CRC}(X))$ 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 section.

4.2 Combined Data and Signal Authentication

This section presents an NMA method based on the TESLA protocol [64] that additionally provides limited signal authentication against a *half duplex* rebroadcast-type spoofing attack.

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 [22]. The communication overhead of TESLA in bits per authentication epoch is roughly twice the equivalent security level.

4.2.1 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 thesis relies on the vanilla TESLA protocol for data-level authentication. Fig. 4.2 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 [64, 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.

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

Fig. 4.3 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

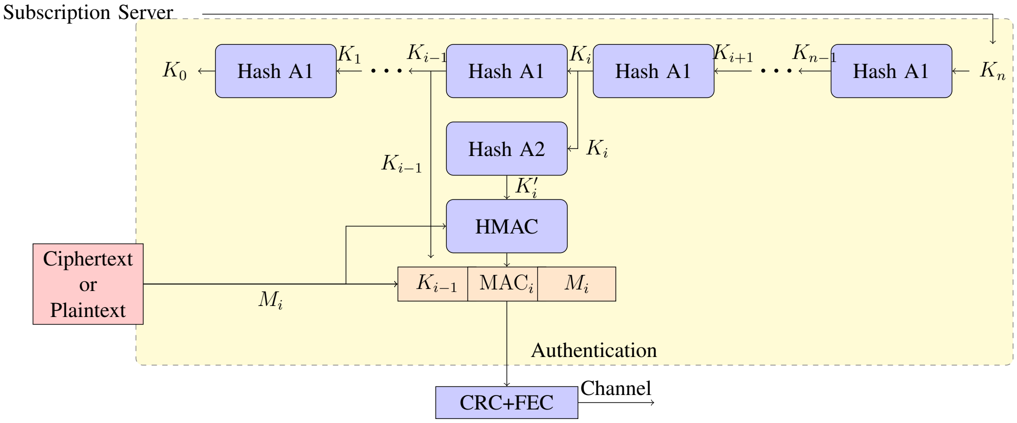


Figure 4.2: Authentication processes at the TRNS pseudolite, which include one-way key chain generation, MAC generation, and broadcast packet formation.

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 [62], 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

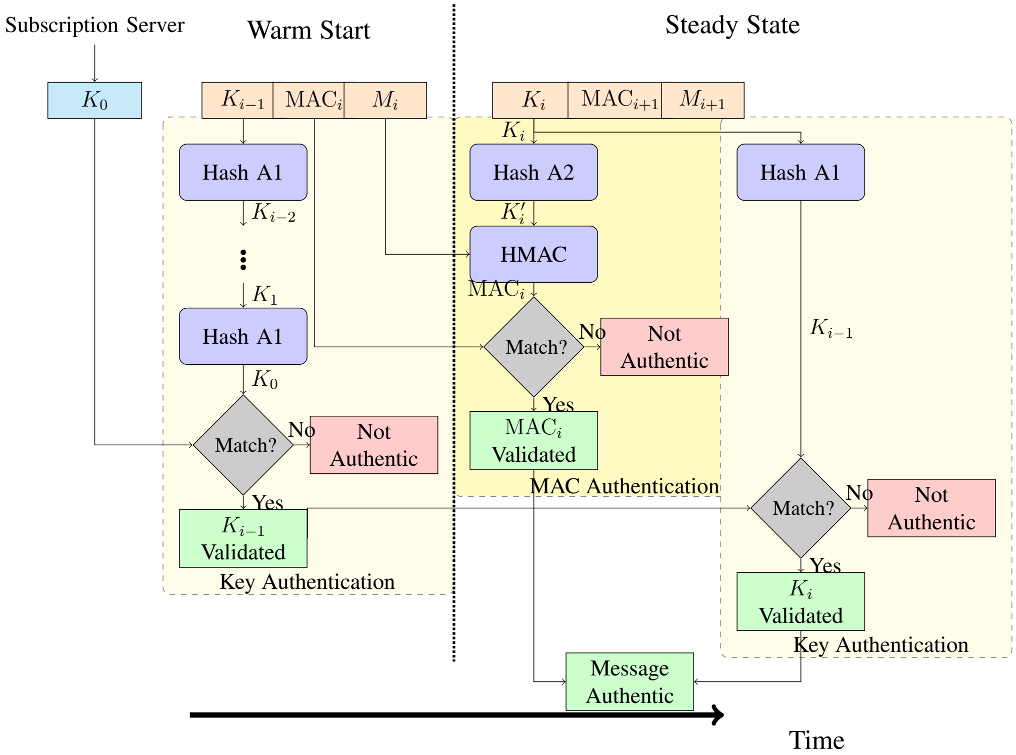


Figure 4.3: Authentication processes within the TRNS receiver, which includes key validation during bootstrapping, and both key and MAC validation during steady-state phase.

occurrence of MAC tag forgery [14]. Hence, the authentication overhead is at least 160 bits per AE. In addition, [10] 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.

4.2.2 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 thesis 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. 4.4 and

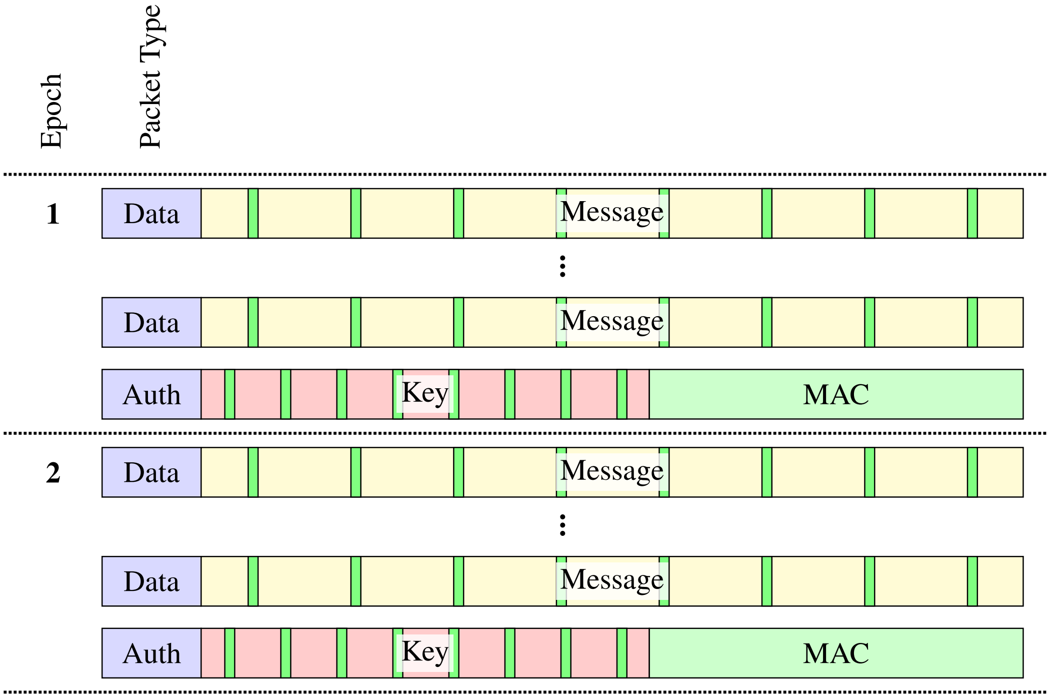


Figure 4.4: NMA for a TRNS navigation stream. Error detection, forward error correction, and encryption are not shown. Authentication packets terminate each authentication epoch, and contain the TESLA key for the previous epoch (red), together with a message authentication code (green) computed from 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.

4.5. The watermark bits are placed at predictable positions in the navigation message stream so that the receiver can still access the relevant fields for 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

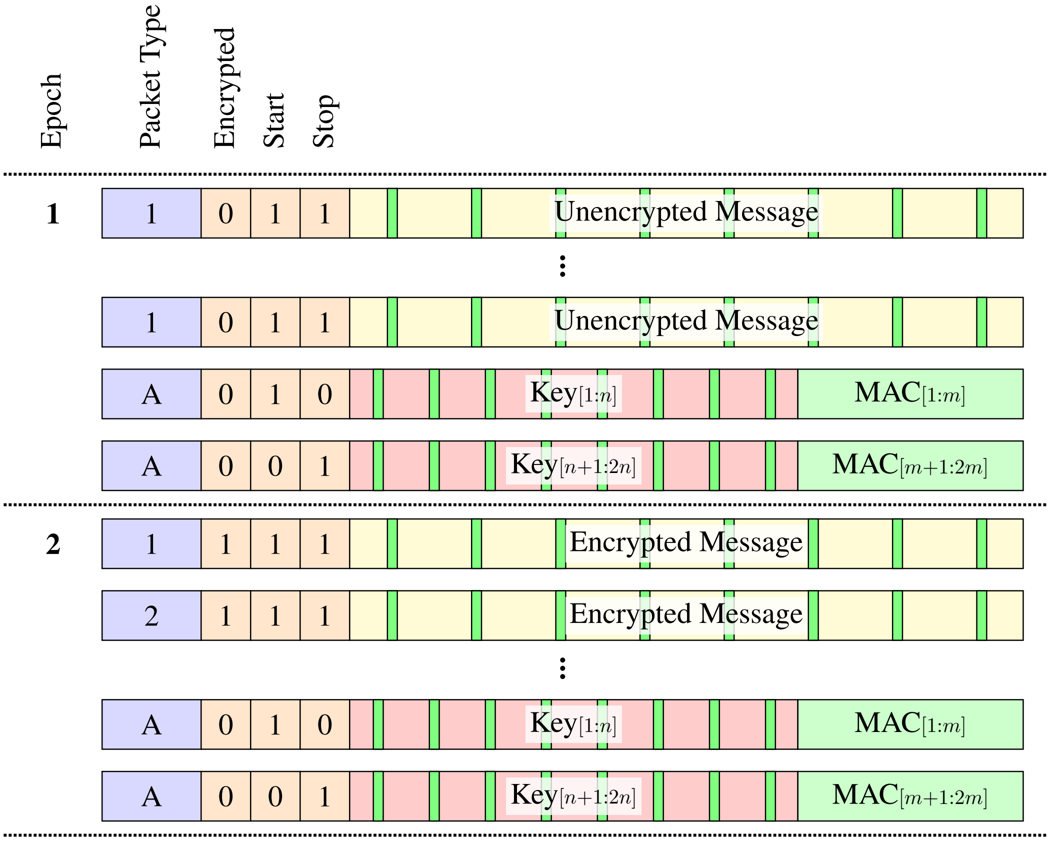

Epoch
Packet Type
Encrypted
Start
Stop
1
1 0 1 1 Unencrypted Message
⋮
1 0 1 1 Unencrypted Message
A 0 1 0 Key$_{[1:n]}$ MAC$_{[1:m]}$
A 0 0 1 Key$_{[n+1:2n]}$ MAC$_{[m+1:2m]}$
2
1 1 1 1 Encrypted Message
2 1 1 1 Encrypted Message
⋮
A 0 1 0 Key$_{[1:n]}$ MAC$_{[1:m]}$
A 0 0 1 Key$_{[n+1:2n]}$ MAC$_{[m+1:2m]}$

Figure 4.5: 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.

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.

4.3 Conclusion

In this chapter, this thesis proposed a multi-tiered NME + MAC-leavened NMA scheme, which provides: (1) selective availability and enhanced data security, (2) data authentication, and (3) protection against half-duplex spoofing attacks.

However, the exposed spreading codes of a high-SNR TRNS signal makes it trivial to replicate the embedded spreading codes in a SCER or meaconing attack: that is, NME+NMA cannot fully protect against ultra-low-latency record-and-replay attacks. In addition, the adversary's receive power advantage renders exotic signal-level security techniques like SCA or SCE irrelevant. Chapter 5 addresses this gap in the spoofing defense by augmenting TRNS network with autonomous signal-situational-awareness.

Chapter 5

Signal Situational Awareness (SSA)

5.1 Introduction

This thesis aims to augment a terrestrial radionavigation system (TRNS) with autonomous signal-situational-awareness capability, allowing the TRNS operator to detect spoofing and meaconing attacks. This addresses the remaining vulnerabilities of the technique proposed in Chapter 4 to full-duplex spoofing threats such as SCER spoofing and meaconing attacks.

5.1.1 Related Work in Signal-Processing-Based Spoofing Detection.

Several techniques proposed in the GNSS literature apply advanced signal processing algorithms for spoofing detection. Unlike other non-cryptographic spoofing defenses, the signal processing-based techniques outlined in Subsection

This chapter is based on:

Ronnie X.T. Kor, Peter A. Iannucci, and Todd E. Humphreys. Autonomous Signal-Situational Awareness in a Terrestrial Radionavigation System. 2021. Submitted for review.

Ronnie X.T. Kor, Peter A. Iannucci, and Todd E. Humphreys. Comprehensive PNT Security for a Terrestrial Radionavigation System. *Navigation, Journal of the Institute of Navigation*, 2021. In preparation..

3.1.3 can be readily implemented on existing GNSS receivers via a firmware upgrade, and do not need additional hardware for their operations. They can be categorized into two classes, one that detects the inception of a spoofing attack, and another that does a brute-force search for all signals in the landscape for post-inception detection.

As highlighted in Subsection 3.1.3, these signal processing techniques will be effective for TRNS infrastructural monitors, which can narrowly characterize the signals in their nominal operating environment. This thesis proposes two signal authentication techniques customized for these monitors, such that a spoofing signal, with SNR below that of the authentic signal, can be detected even in the presence of static and dynamic multipath.

5.1.2 Related Work in TRNS Security.

The work presented in this chapter is complementary with the cryptographic proposal presented in Chapter 4, which focuses on cryptographic techniques for improved navigation security in TRNS. Briefly, Chapter 4 proposes a multi-tiered navigation message encryption (NME) + message authentication code (MAC)-leavened navigation message authentication (NMA) scheme. One can think of Chapter 4's proposal as offering a basic level of security via cryptographic methods. No TRNS should be fielded without such basic measures.

However, the techniques proposed in Chapter 4 are not sufficient to secure TRNS because the exposed spreading codes of a high-SNR TRNS signals makes them vulnerable to replication in a SCER or meaconing attack. Consequently, NME+NMA cannot fully protect TRNS against ultra-low-latency record-and-replay attacks. Even exotic signal-level security techniques like spreading code authentication (SCA) [2] or deterministic code-phase dithering [77] can be rendered ineffective by a spoofer's ability to access high-power authentic signals in a TRNS network.

5.1.3 Contributions.

To address the vulnerability to SCER and meaconing attacks, this thesis proposes an autonomous signal-situational-awareness (SSA) overlay capability within a TRNS network. The SSA capability augments basic TRNS operations with cooperative monitoring among nearby beacons. While not all spoofers can be detected in this way, SSA gives TRNS operators an improved chance of detecting threats and warning users without resorting to costly full-duplex techniques (those that require bi-directional communication with users). This type of autonomous SSA would not be possible for GNSS space vehicles in medium Earth orbit, which can neither hear each other's signals nor detect low-power ground-based spoofers. This work seeks to place TRNS SSA on a solid theoretical and practical footing. First, signal authentication techniques for SSA are defined and developed. Second, enhancements to these techniques are proposed, that exploit the synergy from combining measurements across multiple epochs or over multiple monitoring beacons. Third, simulations with a theoretical model of multipath and spoofing signals are presented to quantify the effectiveness of autonomous SSA under operating conditions representative of those encountered by a generic TRNS.

5.1.4 Organization of this chapter.

TRNS signal model is introduced in Section 5.2. Section 5.3 details the signal authentication techniques considered for SSA. Section 5.4 proposes enhancements to autonomous SSA by combining measurements from multiple beacons or across multiple epochs. Simulation set-up and results are presented in Section 5.5, and Section 5.6 provides concluding remarks.

5.2 Signal Model

To provide the context for SSA framework proposed in this chapter, the GNSS signal models outlined in [91] are adapted to describe TRNS pre-correlation and post-correlation single-interferer scenarios in a multipath environment.

5.2.1 Pre-Correlation Model

An authentic signal exiting a TRNS receiver's radio frequency (RF) front-end downconversion chain can be expressed by the following complex baseband representation:

$$r_A(t) = \sqrt{P_A} D(t - \tau_A) C(t - \tau_A) \exp(j\theta_A) \tag{5.1}$$

where t is time in seconds, P_A is the received power of the authentic signal in watts, $D(t)$ is the navigation data modulation, $C(t)$ is the spreading code modulation, τ_A is the code phase in seconds, and $\exp(j\theta_A)$ is the carrier with phase θ_A in radians. Without loss of generality, the navigation data modulation is assumed to be unity, i.e. $D(t) = 1$.

Let $r_S(t)$ represent a single complex-valued spoofing signal that is structurally identical to $r_A(t)$, which can be modeled as

$$r_S(t) = \sqrt{\eta_S P_A} C(t - \tau_S) \exp(j\theta_S) \tag{5.2}$$

where $\eta_S = P_S/P_A$ is the spoofing power ratio (i.e. the ratio of the spoofing signal power over the authentic signal power), and τ_S and θ_S are the spoofing signal's code and carrier phase respectively. Similarly, the ith multipath signal can be modeled as

$$r_{M,i}(t) = \sqrt{\eta_{M,i} P_A} C(t - \tau_{M,i}) \exp(j\theta_{M,i}) \tag{5.3}$$

where $\eta_{M,i} = P_M/P_A < 1$ is the multipath power ratio of the ith multipath signal relative to the authentic signal, and $\tau_{M,i}$ and $\theta_{M,i}$ are its code and carrier phase respectively.

The full received signal model post-attenuation is given by

$$r(t) = \beta \left[r_A(t) + r_S(t) + \sum_{i=1}^{N_M} r_{M,i}(t) \right] + r_N(t) \tag{5.4}$$

where β is the fixed attenuation determined by the receiver's variable attenuator, N_M is the number of multipath signals captured by the receiver, and $r_N(t)$ represents the sum of thermal noise and quantization noise, which is modeled as a white zero-mean complex-valued Gaussian process with constant spectral density N_0.

In the tracking loop of the receiver, the incoming signal $r(t)$ is correlated with a local replica, which is modeled as

$$l(t, \tau) = C_l(t - \hat{\tau} - \tau) \exp(j\hat{\theta}) \tag{5.5}$$

where $C_l(t)$ is the local code replica, τ is an arbitrary code phase lag in seconds, and $\hat{\tau}$ and $\hat{\theta}$ are the best estimates of the code and carrier phase of the composite signal $r(t)$.

5.2.2 Post-Correlation Model

The complex-valued accumulation product S_k, which is produced from the correlation of the incoming composite signal $r(t)$ with the local replica $l(t,\tau)$ and accumulation over an interval T ending at time $t_k = kT, k \in \{1, 2, \cdots\}$, is modeled as [89]:

$$\xi_k(\tau) = \xi_{Ak}(\tau) + \xi_{Sk}(\tau) + \sum_{i=1}^{N_M} \xi_{Mk,i}(\tau) + \xi_{Nk}(\tau) \tag{5.6}$$

where $\xi_{Ak}(\tau)$, $\xi_{Sk}(\tau)$, $\xi_{Mk,i}(\tau)$ and $\xi_{Nk}(\tau)$ are the complex correlation function components corresponding to the authentic signal, spoofing signal, multipath signals and thermal noise respectively as shown in Fig. 5.1.

The correlation components $\xi_{Ak}(\tau)$, $\xi_{Sk}(\tau)$ and $\xi_{Mk,i}(\tau)$ can be modeled as

$$\begin{aligned}
\xi_{Ak}(\tau) &= \sqrt{P_{Ak}} R(\tau) \exp(j\Delta\tilde{\theta}_{Ak}) \\
\xi_{Sk}(\tau) &= \sqrt{\eta_{Sk} P_{Ak}} R(-\Delta\tilde{\tau}_{Sk} + \tau) \exp(j\Delta\tilde{\theta}_{Sk}) \\
\xi_{Mk,i}(\tau) &= \sqrt{\eta_{Mk,i} P_{Ak}} R(-\Delta\tilde{\tau}_{Mk,i} + \tau) \exp(j\Delta\tilde{\theta}_{Mk,i})
\end{aligned}$$

where P_{Ak}, η_{Sk} and $\eta_{Mk,i}$ are the average values of P_A, η_S and $\eta_{M,i}$ respectively over the kth accumulation interval, $\Delta\tilde{\tau}_{Sk}$ is the average value of $\tau_S - \hat{\tau}$ over the accumulation interval, with similar definitions for $\Delta\tilde{\tau}_{Mk,i}$, $\Delta\tilde{\theta}_{Ak}$, $\Delta\tilde{\theta}_{Sk}$ and $\Delta\tilde{\theta}_{Mk,i}$. Note that $\Delta\tilde{\tau}_{Ak} = 0$, based on the assumption that the path delay between the

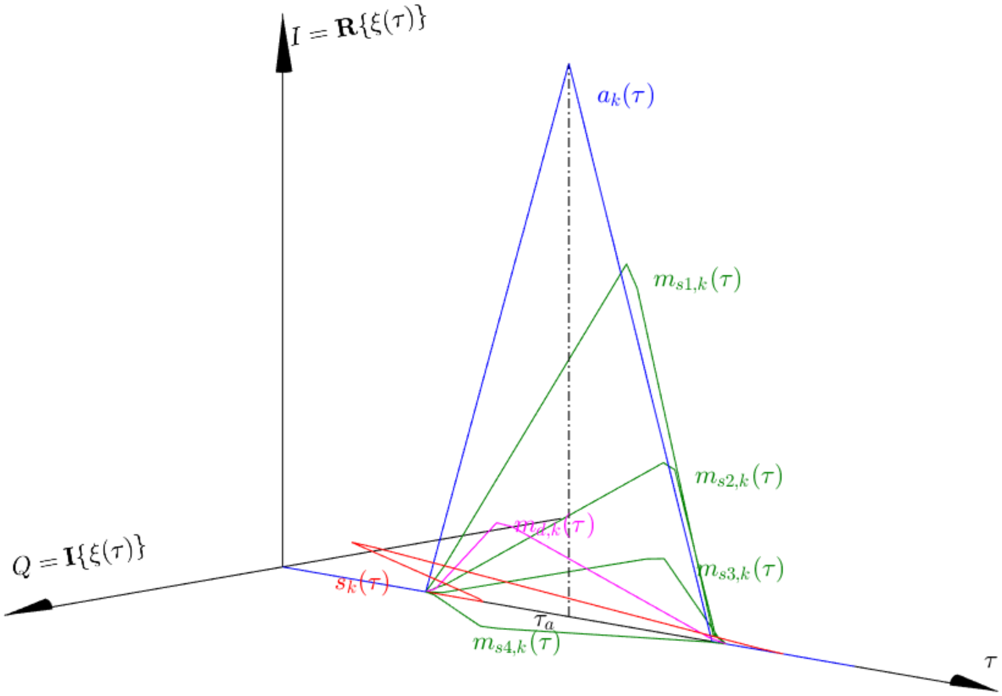


Figure 5.1: Components of the triangular-shaped post-correlation function made up of an authentic signal (blue), its static (green) and dynamic (magenta) multipath, and a weak spoofing signal (red). The amplitude and phase angle of each individual components are relative to that of the local replica $l(t,\tau)$.

transmitter and monitoring receiver is accurately known *a priori* for secure synchronization [59]. The correlation function $R(\tau) = \mathbb{E}[C(t)C_l(t-\tau)]$ approximates the interaction between $C(t)$ and $C_l(t)$ over the correlation and accumulation operations:

$$R(\tau) \approx \frac{1}{T} \int_{t_{k-1}}^{t_k} C(t) C_l(t-\tau) dt$$

5.2.3 Hypothesis Testing Framework

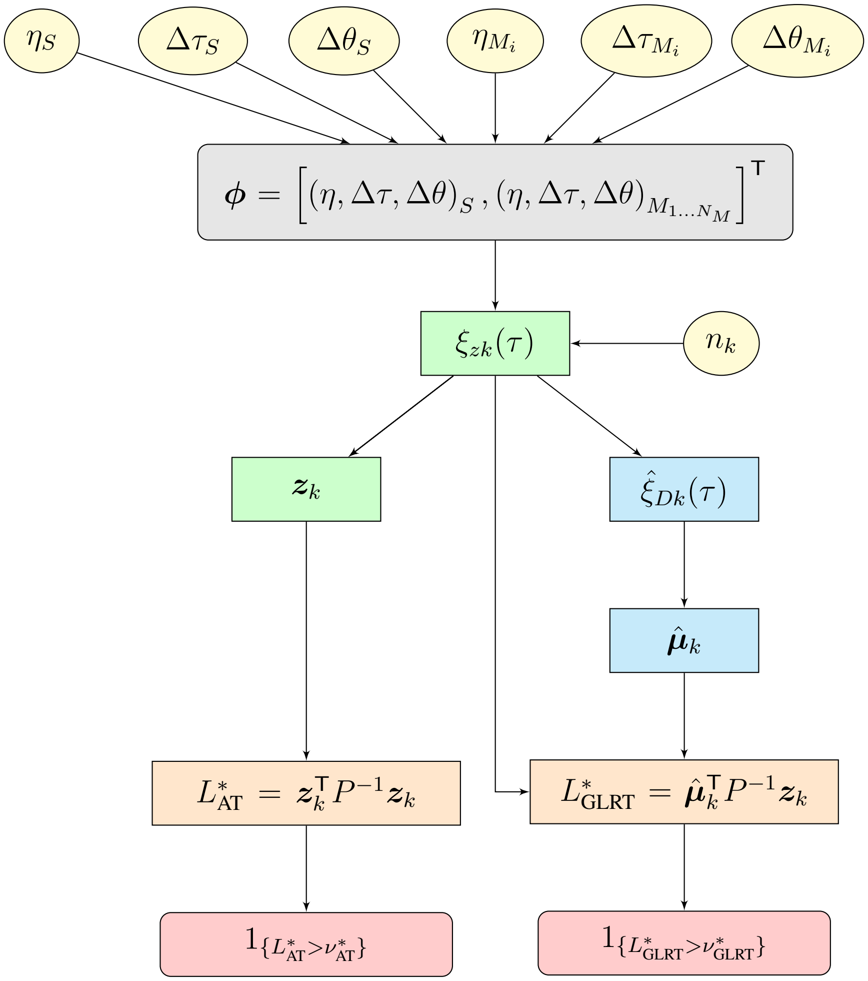
This thesis adopts a Bayesian binary hypothesis framework for distinguishing between the null hypothesis H_0 for the spoof-free case, and the alternate hypothesis H_1 for the spoofing case. In a Bayesian formulation of this binary hypothesis testing problem, the parameter vector $\boldsymbol{\phi}$ is viewed as a random quantity $\boldsymbol{\Phi}$, having density $w(\boldsymbol{\phi})$, with $\pi_l \triangleq P(\boldsymbol{\Phi} \in \Lambda_l)$ being the prior probability that $\boldsymbol{\Phi}$ falls in Λ_l. Subsection 5.2.2 reveals three parameters relevant to describe the parameter vector $\boldsymbol{\phi}$: signal power ratio η, code and carrier offsets $\Delta\tau \triangleq \tau - \tau_A$ and $\Delta\theta \triangleq \theta - \theta_A$ of all signal components:

$$\boldsymbol{\phi} = \left[(\eta, \Delta\tau, \Delta\theta)_S \,, (\eta, \Delta\tau, \Delta\theta)_{M_1} \ldots (\eta, \Delta\tau, \Delta\theta)_{M_{N_M}} \right]^{\mathsf{T}}$$

where $\Delta\tau_S \triangleq \tau_S - \tau_A$ with similar definition for $\Delta\tau_{M_i}$, and $\Delta\theta_S \triangleq \theta_S - \theta_A$ with similar definition for $\Delta\theta_{M_i}$, $i = \{1, 2, \cdots, N_m\}$. The vector $\boldsymbol{\phi}$ is assumed to lie in the parameter space Λ that can be divided into disjoint parameter sets Λ_0 and Λ_1 corresponding to H_0 and H_1 hypotheses respectively.

In what follows, we will define all of the quantities rigorously. Fig. 5.2 shows the dependence relationship between all these quantities as a directed graphical model.

The conditional density of $\boldsymbol{\Phi}$ given that $\boldsymbol{\Phi} \in \Lambda_l$ is denoted as $w_l(\boldsymbol{\phi})$, which



η_S
$\Delta\tau_S$
$\Delta\theta_S$
η_{M_i}
$\Delta\tau_{M_i}$
$\Delta\theta_{M_i}$
$\boldsymbol{\phi} = \left[(\eta, \Delta\tau, \Delta\theta)_S, (\eta, \Delta\tau, \Delta\theta)_{M_{1\ldots N_M}}\right]^\mathsf{T}$
$\xi_{zk}(\tau)$
n_k
$\boldsymbol{z}_k$
$\hat{\xi}_{Dk}(\tau)$
$\hat{\boldsymbol{\mu}}_k$
$L^*_{\text{AT}} = \boldsymbol{z}_k^\mathsf{T} P^{-1} \boldsymbol{z}_k$
$L^*_{\text{GLRT}} = \hat{\boldsymbol{\mu}}_k^\mathsf{T} P^{-1} \boldsymbol{z}_k$
$1_{\{L^*_{\text{AT}} > \nu^*_{\text{AT}}\}}$
$1_{\{L^*_{\text{GLRT}} > \nu^*_{\text{GLRT}}\}}$

Figure 5.2: Directed graphical model showing the conditional dependence between parameters. The grey box denotes the parameter set, yellow ellipses are the random variables, green boxes are the observations, cyan boxes are the estimates, orange boxes are the test statistics, and red boxes represent indications of detection.

is defined as

$$w_l(\boldsymbol{\phi}) = \begin{cases} 0 & \boldsymbol{\phi} \notin \Lambda_l \\ w(\boldsymbol{\phi})/\pi_l & \boldsymbol{\phi} \in \Lambda_l \end{cases}$$

This thesis proposes to decide between the two hypotheses based on the observed correlation deviation function $\boldsymbol{z}_k$ at each t_k, which will be detailed in Section 5.3. The observation $\boldsymbol{z}_k$, which resides in the observation set Γ, can be modeled as a random variable $\boldsymbol{Z}_k$ with conditional density $p(\boldsymbol{z}_k|\boldsymbol{\phi})$. H_l is defined as the hypothesis that $\boldsymbol{Z}_k$ is distributed as $p(\boldsymbol{z}_k|\boldsymbol{\Phi} \in \Lambda_l)$, $l \in \{0, 1\}$.

A decision rule $\delta(\boldsymbol{z}_k)$ is a partition of Γ into disjoint decision regions Γ_l, $l \in \{0, 1\}$, such that H_l is chosen when $\boldsymbol{z}_k \in \Gamma_l$:

$$\delta(\boldsymbol{z}_k) = \begin{cases} 0 & \text{if } \boldsymbol{z}_k \in \Gamma_0 \\ 1 & \text{if } \boldsymbol{z}_k \in \Gamma_1 \end{cases} \tag{5.7}$$

To find the optimal rule δ, Λ_l and $w_l(\boldsymbol{\phi})$ have to be defined by the physical characteristics and limitations of each signal. In particular, the conditional distribution of $w_l(\boldsymbol{\phi})$ are formed from the marginal conditional density of the multipath signals' parameters ($w_{\eta_{M_i}}(x)$, $w_{\Delta\tau_{M_i}}(x)$ and $w_{\Delta\theta_{M_i}}(x)$) and the spoofing signal's parameters ($w_{\eta_S}(x)$, $w_{\Delta\tau_S}(x)$ and $w_{\Delta\theta_S}(x)$). The remainder of this subsection describes the marginal distributions of these parameters.

This thesis adopts the empirical model of the multipath signal presented in [91, Sec. III], which is derived from the analysis on simulations using the Land Mobile Satellite Channel Model (LMSCM) [48]). In this empirical model, the relative phase $\Delta\theta_{M_i}$ is uniformly distributed on $[0, 2\pi)$ and independent of η_{M_1} and $\Delta\tau_{M_i}$, and there is a significant correlation between the parameters η_{M_i} and $\Delta\tau_{M_i}$, with a linear correlation coefficient of approximately $\rho = -0.26$. $w_{\eta_{M_i}}(x)$ is log-normally distributed with a mean of -21 dB and a standard deviation of -5 dB and has a supremum $\eta_M = 1$, consistent with the statistical model derived by [87]. As for the marginal distribution $w_{\Delta\tau_{M_i}}(x)$, it is modeled as an exponential distribution:

$$w_{\Delta\tau_{M_i}}(x) = \frac{1}{\mu}\text{exp}\left(-\frac{x}{\mu}\right), \quad x \geq 0$$

with μ being a quadratic function of the received signal's elevation angle α_e,

$$\mu = 0.012\alpha_e^2 - 2.4\alpha_e + 134$$

where $\Delta\tau$ and α_e are expressed in nanoseconds and degrees respectively. This distribution is consistent with that in [84], with an upper-bound $\Delta\tau_M = 2\tau_c$, where τ_c is the chip interval of the spreading code $C(t)$. In our study, the worst-case effect of the multipath signal without severe shadowing is considered, such that the elevation angle α_e is assumed to be 0°.

As for the spoofing signal, we consider the case where the power of the spoofing signal is below that of the authentic signal, with the ratio of the spoofing signal power over authentic signal power termed as spoofing power ratio. $w_{\eta_S}(x)$ is modeled as a log-normal distribution with a mean of $\eta_S \leq 1$ and a standard deviation of 1 dB. $w_{\Delta\theta_S}(x)$ is uniformly distributed over the interval $[0, 2\pi)$ (similar to the multipath signals). Unlike [91] where $w_{\Delta\tau_S}(x)$ is modeled as a carry-off-type spoofing, the detector in this thesis is designed to expose any potential spoofer in the signal landscape using a wide correlation window τ_w, therefore $w_{\Delta\tau_S}(x)$ is modeled as uniform over the interval $[-\tau_w/2, +\tau_w/2]$.

Under the spoofer-free H_0 case, the parameter set Λ_0 is defined as

$$\Lambda_0 = \{\boldsymbol{\phi} \in \Lambda | \eta_S = 0\}$$

whereas for the spoofing hypothesis H_1, the parameter set Λ_1 is

$$\Lambda_1 = \{\boldsymbol{\phi} \in \Lambda | 0 < \eta_S \leq 1\}$$

The thermal noise component $\xi_{Nk}(\tau)$ has independent in-phase and quadrature components, each being modeled as a zero-mean Gaussian white discrete-time process:

$$\mathbb{E}\left[\mathbb{R}\left\{\xi_{Nk}(\tau_1)\right\}\mathbb{I}\left\{\xi_{Nj}(\tau_2)\right\}\right] = 0 \quad \forall \ k \neq j$$

As discussed in [88], with $C(t)$ being pseudorandom, only samples of $\xi_{Nk}(\tau)$ within $2\tau_c$ of each other are correlated:

$$\mathbb{E}\left[\xi_{Nk}(\tau_1)\xi^*_{Nk}(\tau_2)\right] = \begin{cases} 2\sigma_n^2(1 - \frac{|\tau_1 - \tau_2|}{\tau_c}), & |\tau_1 - \tau_2| \leq 2\tau_c \\ 0 & |\tau_1 - \tau_2| > 2\tau_c \end{cases}$$

where * indicates the complex conjugate, and $\sigma_n^2 = \frac{N_0}{2T}$ is the variance of the in-phase and quadrature components of $\xi_{Nk}(\tau)$ with constant spectral density N_0.

5.3 Signal Authentication

Consider a TRNS monitoring beacon listening to a transmitting TRNS beacon at a distance d away, with its post-correlation output described by Eq. 5.6. There will typically be a significant number N_M of multipath components evident in the post-correlation function $\xi_k(\tau)$, but due to the quasi-static nature of the urban environment, the variation in $\xi_k(\tau)$ will be small within an accumulation interval. These variations are caused by: (1) thermal noise, (2) time-varying receiver non-idealities, and (3) urban environment movement. The first two factors are modeled by the additive white Gaussian noise $r_N(t)$, while the third factor can be modeled as a dynamic multipath component. Revisiting Eq. 5.6, each multipath components can be further segregated into a static $\xi_{M_s(k,i)}$ and a dynamic $\xi_{M_d(k,i)}$ components:

$$\sum_{i=1}^{N_M} \xi_{M(k,i)}(\tau) = \sum_{i=1}^{N_M} \xi_{M_s(k,i)}(\tau) + \xi_{M_d(k,i)}(\tau) \tag{5.8}$$

Let l be the number of signal taps across the correlation window of interest τ_w, with the center-most tap being aligned with the receiver's estimated correlation function peak of the authentic signal and the remaining taps being evenly spaced across the correlation window τ_w. The uniform tap interval is

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

and the $l \times 1$ vector of tap locations is given by

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

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

The post-correlation function $\xi_k(\tau) = I_k(\tau) + jQ_k(\tau)$ can be viewed as having an in-phase component $I_k(\tau)$ and a quadrature component $Q_k(\tau)$. The post-correlation function evaluated at all tap locations can be stacked into a single correlation measurement vector:

$$\boldsymbol{q}_k = \left[I_k\left(-\tfrac{\tau_w}{2}\right), \quad \cdots, \quad I_k\left(\tfrac{\tau_w}{2}\right), \quad Q_k\left(-\tfrac{\tau_w}{2}\right), \quad \cdots, \quad Q_k\left(\tfrac{\tau_w}{2}\right)\right]^{\mathsf{T}} \tag{5.9}$$

A hypothesis test for signal anomaly detection can be formulated in terms of the change in the distributions of $\boldsymbol{q}_k$ due to an additional signal component or components. Let $p_0(\boldsymbol{q}_k)$ and $p_1(\boldsymbol{q}_k)$ be the distribution of $\boldsymbol{q}_k$ under the null (H_0) and alternate (H_1) hypotheses respectively, with H_0 and H_1 previously defined in Subsection 5.2.3.

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

$$H_0 : \boldsymbol{q}_k = \bar{\boldsymbol{q}} + \boldsymbol{w}_k \tag{5.10a}$$

$$H_1 : \boldsymbol{q}_k = \bar{\boldsymbol{q}} + \boldsymbol{\mu}_k + \boldsymbol{w}_k \tag{5.10b}$$

where $\bar{\boldsymbol{q}} = \mathbb{E}(\boldsymbol{q}_k)$ is the mean of the correlation measurement vector $\boldsymbol{q}_k$ measured under H_0, and $\boldsymbol{w}_k \sim \mathcal{N}(\mathbf{0}, P)$ is the measurement noise. $P = \mathbb{E}[(\boldsymbol{q}_k - \bar{\boldsymbol{q}})(\boldsymbol{q}_k - \bar{\boldsymbol{q}})^\mathsf{T}]$ is the covariance of $\boldsymbol{q}_k$ under H_0, which describes properties of the dynamic multipath, thermal noise, and receiver non-idealities. Under H_1, there exists a correlation distortion vector $\boldsymbol{\mu}_k$ that is a function of the signal anomaly's code and carrier offset $\Delta\tau_{Dk}$ and $\Delta\theta_{Dk}$ respectively, scaled by the amplitude of this signal $\epsilon_{Dk} > 0$. $\boldsymbol{\mu}_k$ will be detailed in Subsection 5.3.2. In the case of a successful detection, the parameters of the signal anomaly (amplitude and code and carrier offset) match those of the spoofing signal, whereas in the case of a false alarm, they match those of dynamic multipath.

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

$$H_0 : \boldsymbol{q}_k \sim \mathcal{N}(\bar{\boldsymbol{q}}, P) \tag{5.11a}$$

$$H_1 : \boldsymbol{q}_k \sim \mathcal{N}(\bar{\boldsymbol{q}} + \boldsymbol{\mu}_k, P) \tag{5.11b}$$

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

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

$$\xi_{zk}(\tau) = \xi_{Sk}(\tau) + \sum_{i=1}^{N_M} \xi_{M_d(k,i)}(\tau) + \xi_{Nk}(\tau) \tag{5.12}$$

Let

$$\boldsymbol{z}_k \triangleq \boldsymbol{q}_k - \bar{\boldsymbol{q}} = \left[I_{zk}\left(-\tfrac{\tau_w}{2}\right), \quad \cdots \quad, I_{zk}\left(\tfrac{\tau_w}{2}\right), \quad Q_{zk}\left(-\tfrac{\tau_w}{2}\right), \quad \cdots \quad, Q_{zk}\left(\tfrac{\tau_w}{2}\right)\right]^{\mathsf{T}}$$

be the vector of this correlation deviation function sampled at the tap locations. The model in Eq. 5.11 can now be redefined as

$$H_0 : \boldsymbol{z}_k \sim \mathcal{N}(\boldsymbol{0}, P) \tag{5.13a}$$

$$H_1 : \boldsymbol{z}_k \sim \mathcal{N}(\boldsymbol{\mu}_k, P) \tag{5.13b}$$

The model in Eq. 5.13 is a special case of the general Gaussian problem [90] for which the optimal test $L(\boldsymbol{z}_k)$ can be reduced to

$$L(\boldsymbol{z}_k) = \boldsymbol{z}_k^\mathsf{T} P^{-1} \boldsymbol{z}_k - (\boldsymbol{z}_k - \boldsymbol{\mu}_k)^\mathsf{T} P^{-1} (\boldsymbol{z}_k - \boldsymbol{\mu}_k) \underset{H_0}{\overset{H_1}{\gtrless}} \nu \tag{5.14}$$

where $\nu > 0$ is the threshold that yields the chosen probability of false alarm P_F given the distribution of $L(\boldsymbol{z}_k)$ under H_0.

This thesis tackles this problem using two different techniques. The first technique, *Anomaly Test* (AT), simply looks at the fit of the observation $\boldsymbol{z}_k$ to the H_0 distribution by considering only the first term of Eq. 5.14. The second technique, *Generalized Likelihood Ratio Test* (GLRT), estimates $\boldsymbol{\mu}_k$ from the observations $\boldsymbol{z}_k$ to form the detection statistic $L(\boldsymbol{z}_k)$ for the hypothesis test. These two techniques will be elaborated in their respective subsections.

5.3.1 Anomaly Test (AT)

Consider the optimal test in Eq. 5.14, which can be simplified by evaluating just the likelihood of the $p_0(\boldsymbol{z}_k)$ distribution:

$$L_{\text{AT}}^*(\boldsymbol{z}_k) = \boldsymbol{z}_k^\mathsf{T} P^{-1} \boldsymbol{z}_k \underset{H_0}{\overset{H_1}{\gtrless}} \nu_{\text{AT}}^* \tag{5.15}$$

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

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

5.3.2 Generalized Likelihood Ratio Test (GLRT)

The set of correlation distortion parameters $\{\epsilon_{Dk}, \Delta\tau_{Dk}, \Delta\theta_{Dk}\}$ is first estimated using a modified maximum-likelihood (ML) technique proposed in [20]. The estimator derived from this ML technique can detect any anomalous signal over a wide range of spoofing-to-authentic code offsets. This subsection details the adaptation of this estimator for TRNS spoofing detection.

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

$$\xi_{Dk}(\delta_i) = \epsilon_{Dk} R(\delta_i - \Delta\tau_{Dk}) \exp(j\Delta\theta_{Dk}) + \xi_{Nk}(\delta_i) \tag{5.16}$$

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

$$\boldsymbol{\mu}_k = \left[I_{Dk}\left(-\tfrac{\tau_w}{2}\right), \quad \cdots \quad, I_{Dk}\left(\tfrac{\tau_w}{2}\right), \quad Q_{Dk}\left(-\tfrac{\tau_w}{2}\right), \quad \cdots \quad, Q_{Dk}\left(\tfrac{\tau_w}{2}\right)\right]^{\mathsf{T}} \tag{5.17}$$

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

$$\boldsymbol{\xi}_{Dk} = H(\Delta\tau_{Dk}, \boldsymbol{\delta})\epsilon_{Dk} \exp(j\Delta\theta_{Dk}) \tag{5.18}$$

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

$$H(\Delta\tau_{Dk}, \boldsymbol{\delta}) = \begin{bmatrix} R(\delta_1 - \Delta\tau_{Dk}) \\ \vdots \\ R(\delta_l - \Delta\tau_{Dk}) \end{bmatrix} \tag{5.19}$$

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

$$\begin{aligned} &\hat{\epsilon}_{Dk} \exp(j\Delta\hat{\theta}_{Dk}) = \\ &\left[H^\mathsf{T}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta}) Q^{-1} H(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})\right]^{-1} H^\mathsf{T}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta}) Q^{-1} \boldsymbol{\xi}_{zk} \end{aligned} \tag{5.20}$$

where Q is the $l \times l$ Toeplitz matrix that accounts for the correlation of the complex Gaussian thermal noise among the taps [6], and $\boldsymbol{\xi}_{zk} = \xi_{zk}(\boldsymbol{\delta})$ is the vector of correlation deviation function from all signal taps. The $(a, b)^{\text{th}}$ element of Q is $Q_{a,b} = R(|a - b|\Delta\delta)$, where $\Delta\delta$ is the tap spacing.

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

$$J_k = \|\boldsymbol{\xi}_{zk} - H^\mathsf{T}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta}) \hat{\epsilon}_{Dk} \exp(j\Delta\hat{\theta}_{Dk})\|_Q^2 \tag{5.21}$$

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

A bisecting search is then performed to obtain a refined code phase estimate using linear interpolation. At each bisection point, new amplitude and carrier phase estimates are determined by re-evaluating Eq. 5.20. The process is repeated until

J_k converges, and the resulting estimates are accepted as the maximum-likelihood estimate $\left\{\hat{\epsilon}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\}$. This estimate can correspond to the signal characteristics of the dynamic multipath, spoofing signal, or thermal noise, depending on their relative signal amplitude and code offset. Fig. 5.3 shows an example scenario in which the signal characteristics of the ML estimate $\hat{\xi}_{Dk}(\tau)$ matches that of the spoofing signal $\xi_{Sk}(\tau)$ rather than the dynamic multipath $\xi_{M_d(k,i)}(\tau)$. The larger code offset of the spoofing signal skews the ML estimate more than the higher signal power of the dynamic multipath.

The maximum-likelihood estimate of the correlation distortion function can be computed as

$$\hat{\xi}_{Dk}(\tau) \triangleq \hat{I}_{Dk} + j\hat{Q}_{Dk} \tag{5.22}$$

$$= \hat{\epsilon}_{Dk} R(-\Delta\hat{\tau}_{Dk} + \tau) \exp(j\Delta\hat{\theta}_{Dk}) \tag{5.23}$$

where the correlation distortion vector

$$\hat{\boldsymbol{\mu}}_k = \begin{bmatrix} \hat{I}_{Dk}\left(-\frac{\tau_w}{2}\right) & \cdots & \hat{I}_{Dk}\left(\frac{\tau_w}{2}\right) & \hat{Q}_{Dk}\left(-\frac{\tau_w}{2}\right) & \cdots & \hat{Q}_{Dk}\left(\frac{\tau_w}{2}\right)\end{bmatrix}^{\mathsf{T}}$$

is obtained to evaluate the optimal test of Eq. 5.14.

Since both $p_0(\boldsymbol{z}_k)$ and $p_1(\boldsymbol{z}_k)$ are assumed to have the same covariance P, the optimal test in Eq. 5.14 can be reduced to

$$L'(\boldsymbol{z}_k) = \hat{\boldsymbol{\mu}}_k^{\mathsf{T}} P^{-1} \boldsymbol{z}_k \underset{H_0}{\overset{H_1}{\gtrless}} \nu' \tag{5.24}$$

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

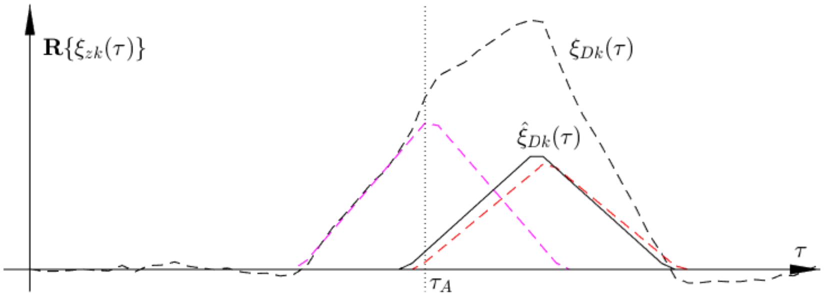


Figure 5.3: The measured correlation distortion function $\xi_{Dk}(\tau)$ (black dashed line) and its ML estimate $\hat{\xi}_{Dk}(\tau)$ (solid black) from an example scenario, shown in their in-phase components. The dotted black line corresponds to the delay of the authentic signal τ_A. Note that $\hat{\xi}_{Dk}(\tau)$ has a closer match to $\xi_{Sk}(\tau)$ (red) than to $\xi_{Mk}(\tau)$ (magenta), which implies that the estimated correlation distortion function is a good representation of the spoofing signal's complex correlation function.

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

$$L^*_{\text{GLRT}}(\boldsymbol{z}_{a,k}) = \hat{\boldsymbol{\mu}}^{\mathsf{T}}_{a,k}\boldsymbol{z}_{a,k} \underset{H_0}{\overset{H_1}{\gtrless}} \nu^*_{\text{GLRT}} \tag{5.25}$$

which implies a correlation-and-accumulation structure, with ν^*_{GLRT} being the threshold derived from the H_0 distribution using a chosen P_F. The full procedure is summarized in Algorithm 1.

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

Algorithm 1: Multi-Tap Maximum-Likelihood Correlation Function Estimator (reproduced with permission from [20]), which takes in the correlation deviation function $\boldsymbol{\xi}_{zk}$ and outputs the ML estimate of its amplitude, code phase and carrier offset $\left\{\hat{\epsilon}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\}$.

```
Input  : $\boldsymbol{\xi}_{zk}$
Output: $\left\{\hat{a}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\}$

for $i$ = $1{:}l$ do
    $\Delta\hat{\tau}_{Dk} = \delta_i$
    $\hat{\epsilon}_{Dk}\exp(j\Delta\hat{\theta}_{Dk}) = \left[H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})Q^{-1}H(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})\right]^{-1} H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})Q^{-1}\boldsymbol{\xi}_{zk}$
    $J_{k,i} = \|\boldsymbol{\xi}_{zk} - H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk}, \boldsymbol{\delta})\hat{\epsilon}_{Dk}\exp(j\Delta\hat{\theta}_{Dk})\|_Q^2$
end
$\Delta\hat{\tau}_{Dk,min} = \text{argmin}(\boldsymbol{J}_k)$
$\Delta\hat{\tau}_{Dk,min2} = \text{argmin}(\boldsymbol{J}_k \neq J_{k,min})$

while $J_{k,min2} > J_{k,min}$ do
    $\Delta\hat{\tau}_{Dk,b} = \frac{\Delta\hat{\tau}_{Dk,min}J_{k,min2} + \Delta\hat{\tau}_{Dk,min2}J_{k,min}}{J_{k,min} + J_{k,min2}}$
    $\hat{\epsilon}_{Dk}\exp(j\Delta\hat{\theta}_{Dk}) =$
     $\left[H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,b}, \boldsymbol{\delta})Q^{-1}H(\Delta\hat{\tau}_{Dk,b}, \boldsymbol{\delta})\right]^{-1} H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,b}, \boldsymbol{\delta})Q^{-1}\boldsymbol{\xi}_{zk}$
    $J_{k,b} = \|\boldsymbol{\xi}_{zk} - H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,b}, \boldsymbol{\delta})\hat{\epsilon}_{Dk}\exp(j\Delta\hat{\theta}_{Dk})\|_Q^2$
    if $J_{k,b} < J_{k,min2}$ then
        $J_{k,min2} = J_{k,b}$
        $\Delta\hat{\tau}_{Dk,min2} = \Delta\hat{\tau}_{Dk,b}$
    end
end
$\left\{\hat{\epsilon}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\} = \text{argmin}(J_k)$
```

5.4 SSA Enhancements

Section 5.3 talks about a ‘single-shot’ detector that uses either signal authentication techniques, where the detection statistics are derived from a short accumulation interval (e.g. 1 ms) in each monitoring beacon. There exists a threshold for a single monitor, beyond which a spoofer might be too weak to be detected in a single experiment. However, this spoofer will be visible to TRNS operator if information about the spoofer are gathered from multiple perspectives of the signal landscape, or over a longer observation period. This section presents two enhancements to the detection performance of autonomous SSA: (1) coherently or non-coherently combine measurements over a longer accumulation interval, and (2) combining detection statistics from multiple monitoring beacons at the same epoch. These enhancements are orthogonal to each other, and can work in tandem to improve SSA detection performance at low spoofing power ratio.

5.4.1 Joint Detection across Multiple Epochs

One can lower the detection threshold by combining measurements across multiple epochs. These measurements can be summed coherently or non-coherently, depending on the signal dynamics.

Coherent Integration. Assuming that each components of $\xi_{zk}(\tau)$ do not vary over multiple accumulation intervals, the measured distortion vector $\boldsymbol{z}_k$ can be summed coherently to form a new measurement vector $\boldsymbol{Z} = \left(\sum_{k=1}^{N_{\text{coh}}} \boldsymbol{z}_k\right)$. In the AT, the new test statistic $L^*_{\text{AT,coh}}$ becomes

$$L^*_{\text{AT,coh}}(\boldsymbol{Z}) = \boldsymbol{Z}^{\mathsf{T}} P^{-1} \boldsymbol{Z} \underset{H_0}{\overset{H_1}{\gtrless}} \nu^*_{\text{AT,coh}} \tag{5.26}$$

where $\nu^*_{\text{AT,coh}}$ is the threshold that yields a user-chosen P_F, based on the distribution of $L^*_{\text{AT,coh}}(\boldsymbol{Z})$ under H_0.

For the GLRT, a single combined correlation distortion $\hat{\boldsymbol{M}}$ is similarly estimated from $\boldsymbol{Z}$ using the ML estimation outlined in Subsection 5.3.2, and then combined with $\boldsymbol{Z}$ to form the test statistic $L^*_{\text{GLRT,coh}}$:

$$L^*_{\text{GLRT,coh}}(\boldsymbol{Z}) = \hat{\boldsymbol{M}}^{T} P^{-1} \boldsymbol{Z} \underset{H_0}{\overset{H_1}{\gtrless}} \nu^*_{\text{GLRT,coh}} \tag{5.27}$$

with $\nu^*_{\text{GLRT,coh}}$ being the threshold based on the distribution of $L^*_{\text{GLRT,coh}}(\boldsymbol{Z})$ under H_0 that meets the user-chosen P_F.

Non-coherent Integration. In the case where the individual components of $\xi_{zk}(\tau)$ are distinct in each accumulation interval, the test statistic computed in each epoch can instead be non-coherently combined to form a new test statistic. In the case of AT, the new test statistic $L^*_{\text{AT,ncoh}}$ is

$$L^*_{\text{AT,ncoh}} = \sum_{k=1}^{N_{\text{ncoh}}} L^*_{\text{AT}}(\boldsymbol{z}_k) \underset{H_0}{\overset{H_1}{\gtrless}} \nu^*_{\text{AT,ncoh}} \tag{5.28}$$

where $\nu^*_{\text{AT,ncoh}}$ is the threshold that meets a chosen P_F, based on the distribution of $L^*_{\text{AT,ncoh}}$ under H_0.

Revisiting Eq. 5.14 and re-arranging terms, the test statistic at each epoch can be defined as

$$L^*_{\text{GLRT}}(\boldsymbol{z}_{a,k}) = \boldsymbol{\mu}_{a,k}^{\mathsf{T}} \boldsymbol{z}_{a,k} + \boldsymbol{\mu}_{a,k}^{\mathsf{T}} \boldsymbol{\mu}_{a,k} \tag{5.29}$$

The new test statistic $L^{*}_{\text{GLRT,ncoh}}$ from non-coherent combination of statistics from multiple epochs is

$$L^{*}_{\text{GLRT,ncoh}} = \sum_{k=1}^{N_{\text{ncoh}}} L^{*}_{\text{GLRT}}(\boldsymbol{z}_k) \underset{H_0}{\overset{H_1}{\gtrless}} \nu^{*}_{\text{GLRT,ncoh}} \tag{5.30}$$

with $\nu^{*}_{\text{GLRT,ncoh}}$ being the threshold based on the distribution of $L^{*}_{\text{GLRT,ncoh}}$ under H_0 that meets the user-chosen P_F.

5.4.2 Joint Detection using Multiple Monitoring Beacons

The existence of bi-directional communication between monitoring beacons in a TRNS network allows these beacons to mutually share information about the signal landscape, using either peer-to-peer or client-server architecture. This method enhances TRNS network's detection performance, allowing the network to expose a spoofer at a much lower spoofing power threshold than what is achievable using a signal monitoring beacon. This subsection outlines the modification of AT and GLRT for this purpose.

Anomaly Test Network Detector. For the anomaly test detector, the test statistics from multiple beacons are summed to form a network test statistic $L^{\text{AT}}_{k,net}$:

$$L^{\text{AT}}_{k,net} = \sum_{j=1}^{N_{\text{beacon}}} L_{k,j} \underset{H_0}{\overset{H_1}{\gtrless}} \nu^{*}_{net}$$

where $\nu^{*}_{net} > 0$ is the threshold that yields the chosen P_F based on the distribution of $L^{\text{AT}}_{k,net}$ under H_0.

GLRT Network Detector. The GLRT network detector takes a joint estimation-detection approach, where the detection of the spoofer is conditional on the maximum-likelihood estimation of the spoofer's position and clock bias. First, the cost of the spoofer at each tap corresponding to each jth monitoring beacons is calculated based on their correlation distortion observation $\boldsymbol{\xi}_{zk,j}$:

$$\boldsymbol{J}_{k,j} = \|\boldsymbol{\xi}_{zk,j} - H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})\hat{a}_{Dk,j}\exp(j\Delta\hat{\theta}_{Dk,j})\|_Q^2 \tag{5.31}$$

The TRNS network pre-defines a grid of possible spoofer's position (x, y) and an array of possible spoofer's clock bias dt. At each point (x, y, dt) in this grid, there is one particular correlator output i that corresponds to the geometric and secular delay of the spoofer $\tau_{k,j}$ observed by the beacon, which correspond to the cost $\boldsymbol{J}_{k,j}(\Delta\hat{\tau}_{Dk} = \tau_{k,j})$. Combining the likelihood costs from all beacons gives a score for that point,

$$\boldsymbol{J}_{net,k}(x, y, dt) = \sum_{j=1}^{N_{\text{beacon}}} \boldsymbol{J}_{k,j}(\Delta\hat{\tau}_{Dk} = \tau_{k,j}) \tag{5.32}$$

and the lowest score gives the GLRT hypothesis for the spoofer's location and clock bias $(\hat{x}, \hat{y}, \hat{dt})$.

Using this ML estimate, the correlation distortion vector $\hat{\boldsymbol{\mu}}_{k,j}$ for each beacon j can be calculated using Eq. 5.23, and the network-wide test statistic $L_{k,net}^{\text{GLRT}}$ is

$$L_{k,net}^{\text{GLRT}} = \sum_{j=1}^{N_{\text{beacon}}} L_{k,j} = \sum_{j=1}^{N_{\text{beacon}}} \left(\hat{\boldsymbol{\mu}}_{k,j}^T P_j^{-1} \boldsymbol{z}_{k,j} + \hat{\boldsymbol{\mu}}_{k,j}^T P_j^{-1} \hat{\boldsymbol{\mu}}_{k,j}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \nu_{net}^* \tag{5.33}$$

where ν_{net}^* is the threshold that meets a chosen P_F, based on the distribution of $L_{k,net}^{\text{GLRT}}$ under H_0. Algorithm 2 outlines the pseudo-code for the joint estimation-detection approach of the GLRT network detector.

Algorithm 2: Multi-Beacon Multi-Tap Maximum-Likelihood Correlation Function Estimator

```
Input  : $\boldsymbol{\xi}_{zk,1}, \boldsymbol{\xi}_{zk,2}, \cdots, \boldsymbol{\xi}_{zk,N}$
Output: $\left\{\hat{a}_{Dk}, \Delta\hat{\tau}_{Dk}, \Delta\hat{\theta}_{Dk}\right\}, L_{k,net}^{\mathrm{GLRT}}$

for j = 1:$N_{beacon}$ do
    for i = 1:l do
        $\Delta\hat{\tau}_{Dk,j} = \delta_i$
        $\hat{a}_{Dk,j}\exp(j\Delta\hat{\theta}_{Dk,j}) = \left[H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})Q^{-1}H(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})\right]^{-1} H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})Q^{-1}\boldsymbol{\xi}_{zk,j}$
        $J_{k,ij} = \|\boldsymbol{\xi}_{zk,j} - H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})\hat{a}_{Dk,j}\exp(j\Delta\hat{\theta}_{Dk,j})\|_Q^2$
    end
end

for x = $x_{min}$:$x_{max}$ do
    for y = $y_{min}$:$y_{max}$ do
        for dt = $dt_{min}$:$dt_{max}$ do
            for j = 1:$N_{beacon}$ do
                $\tau_{k,j} = \frac{\texttt{diffRange}(x,y,dt)}{c}\tau_c$
                $\boldsymbol{J}_{net,k}(x,y,dt) = \boldsymbol{J}_{net,k}(x,y,dt) + \boldsymbol{J}_{k,j}(\Delta\hat{\tau}_{Dk} = \tau_{k,j})$
            end
        end
    end
end
$\left\{\hat{x}, \hat{y}, \hat{dt}\right\} = \mathrm{argmin}(\boldsymbol{J}_{net,k})$

for j = 1:$N_{beacon}$ do
    $\Delta\hat{\tau}_{Dk,j} = \frac{\texttt{diffRange}(\hat{x},\hat{y},\hat{dt})}{c}\tau_c$
    $\hat{a}_{Dk,j}\exp(j\Delta\hat{\theta}_{Dk,j}) = \left[H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})Q^{-1}H(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})\right]^{-1} H^{\mathsf{T}}(\Delta\hat{\tau}_{Dk,j}, \boldsymbol{\delta})Q^{-1}\boldsymbol{\xi}_{zk,j}$
    $\hat{\xi}_{Dk,j}(\tau) \triangleq I_{Dk,j} + jQ_{Dk,j} = \hat{a}_{Dk,j}R(-\Delta\hat{\tau}_{Dk,j} + \tau)\exp(j\Delta\hat{\theta}_{Dk,j})$
    $L_{k,j} = \hat{\boldsymbol{\mu}}_{k,j}^T P_j^{-1}\boldsymbol{z}_{k,j} + \hat{\boldsymbol{\mu}}_{k,j}^T P_j^{-1}\hat{\boldsymbol{\mu}}_{k,j}$
end
$L_{k,net}^{\mathrm{GLRT}} = \sum_{j=1}^{N_{\mathrm{beacon}}} L_{k,j} \gtrless_{H_0}^{H_1} \nu_{net}^*$
```

5.5 Simulations

The AT and GLRT spoofing detectors were tested in simulation under different scenarios. The following subsections outline the simulation setup, and the performance of the detectors under different operating conditions (different transmitter power level and receiver sensitivity range) and with the use of joint detection techniques outlined in Section 5.4.

5.5.1 Simulation Setup

Fig. 5.4 shows the simulation setup that was used for all test cases involving a single monitoring beacon. In each run, the spoofer power was set to reflect the spoofing power ratio (i.e. ratio of the spoofing power versus the authentic signal power) at the receiving beacon. A path loss exponent α of 3 was used to reflect a generic urban environment of the TRNS beacons [72]. The monitoring receiver's antenna experiences an ambient temperature T of 290 K, and has a front-end bandwidth B of 20 MHz. 10000 runs were conducted during the calibration phase using H_0 distribution, which is made up of 1 authentic signal, 8 static multipath and 1 dynamic multipath. Each post-correlation function $\xi_k(\tau)$ is computed across a correlation window of 20 chips from 1 ms of signal accumulation. The test statistics collated during calibration were used to compute the thresholds for each detector, based on a probability of false alarm P_{FA} of 1 in 1000. 2000 runs were then conducted during the trial phase, with an additional spoofing signal in the landscape, to determine the probability of detection P_D of the spoofing signal at each spoofing power ratio. The distributions of all the signal components were outlined in

Subsection 5.2.2.

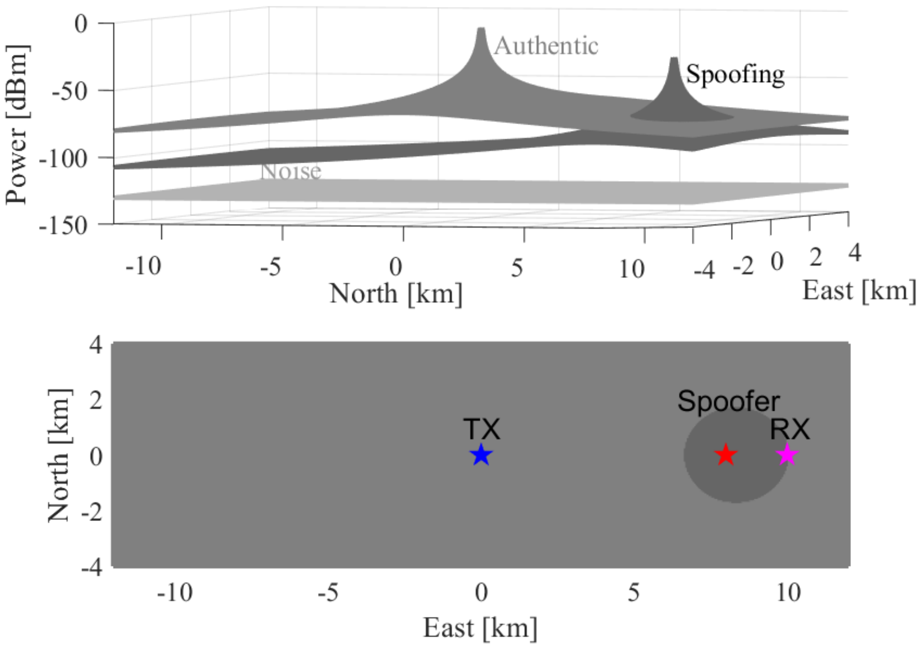


Figure 5.4: Simulation setup used for all test cases. The transmitting beacon and the spoofer are located 10 km and 2 km away from the monitoring beacon respectively. The top plot shows the amplitude of the authentic and spoofing signals over a 10 km by 4 km grid, both of which are above the noise floor of the receiver.

5.5.2 Detector Comparison

Figs. 5.5 show the performance of the AT and GLRT detectors, respectively, at a beacon transmit power of 30W. Each detector is simulated both with and without a dynamic multipath component. In each of these 4 cases, the condition under which the detector is trained and the condition under which it is evaluated is the same. It is no surprise that the confounding influence of dynamic multipath reduces

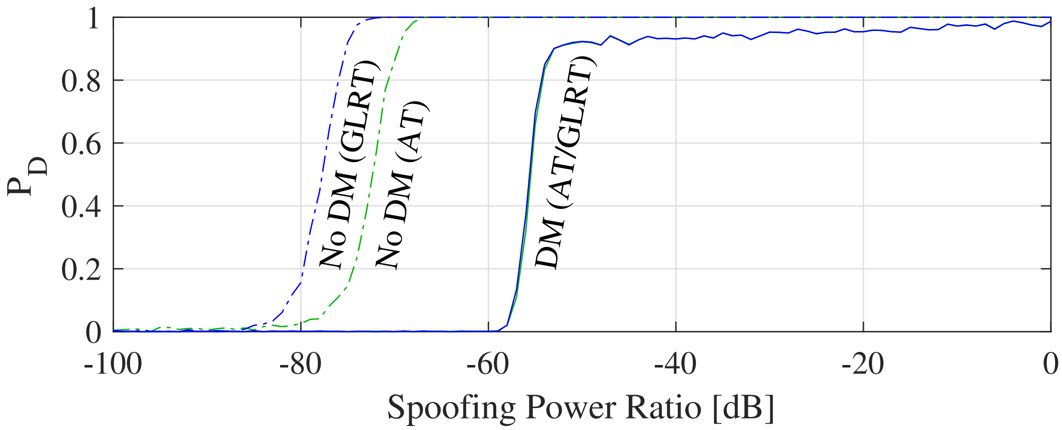


Figure 5.5: Simulation results for AT detector, without dynamic multipath (No DM) and with dynamic multipath (DM). For discussion on the long-tail distribution on the right, see Subsection 5.5.2. While the DM curve of GLRT appears similar to that of AT, it exhibits differences at the 5% level in the vicinity of the threshold.

the performance of each detector. Absent dynamic multipath, the GLRT exhibits a sensitivity advantage of roughly 5 dB. Under dynamic multipath, neither detector exhibits a significant advantage: the GLRT's 50% sensitivity threshold is 0.13 dB better (i.e. lower) than that of the AT.

In the dynamic multipath cases, each detector exhibits a sharp threshold and a long tail of false negatives. The region to the left of the threshold is dominated by noise. In this regime, P_D improves with increasing spoofing power ratio as the spoofing power approaches a noise floor at the receiver. To the right is the multipath-dominated region. Here, a false negative rate of 10% narrows towards zero with increasing spoofing power ratio. This occurs because, as discussed in Subsection 5.2.2, the spoofer's simulated code phase may coincide with the window of correlator output taps that are effectively desensitized by dynamic multipath.

Due to the particular parameters used, this occurs 10% of the time. At high enough spoofing power ratio, this desensitization no longer prevents detection.

5.5.3 Different Levels of Transmitter Power

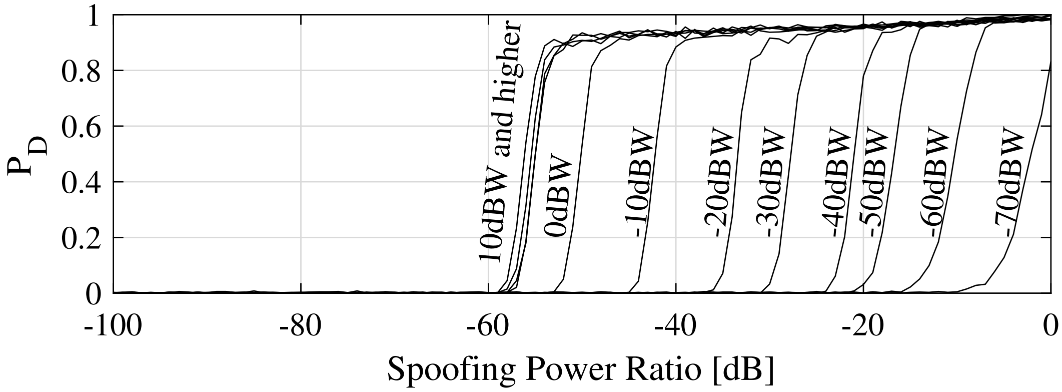


Figure 5.6: Simulation results of the GLRT detector under different transmitter power level.

Fig. 5.6 shows the detection performance of the GLRT detector under different authentic transmitter power levels. Each simulated detection has access to only 1 ms of signal. Considering transmit power levels running upwards from -70 dBW, detection performances improves at all spoofing power ratios until the detector exhibits a saturation effect at a transmit power level of 10 dBW. Note that the spacing between adjacent curves is not uniform with transmit power level.

In order to interpret the saturation and non-uniform spacing effects, one may recast these observations in terms of received power (not spoofing power ratio) versus transmitted power. However, in order to do this, one must choose a single point on the P_D curve to summarize detector performance at a particular transmit

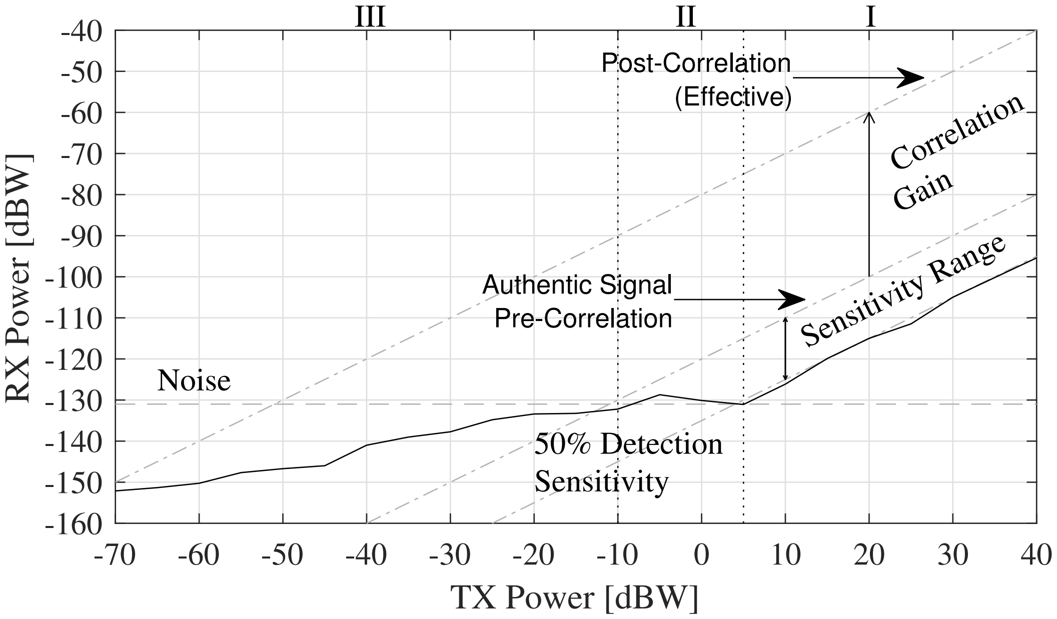


Figure 5.7: Simulation results of the GLRT detector under different transmitter power, showing the 50% detection sensitivity curve with 3-bit quantization in the presence of dynamic multipath. Notice that the GLRT detector has a 23 dB detection advantage in the absence of dynamic multipath, which is also shown in Fig. 5.5. This advantage diminishes with lower spoofing power ratio as thermal noise dominates.

power level. In Fig. 5.7, this point is arbitrarily chosen to be the 50% detection threshold. That is, at any given transmit power level, Fig. 5.7 shows the received power corresponding to a 50% rate of detection of the spoofer by the monitoring receiver.

Fig. 5.7 suggests that the saturation and non-uniform spacing phenomena in Fig. 5.6 indicate the presence of 3 quantitatively distinct regimes, in order from right to left:

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

II: Thermal noise dominates over quantization noise and the detection threshold is comparable to the thermal noise level, $P_I \approx P_N$.

III: Thermal noise still dominates and the spoofing signal is only detectable post-correlation ($P_I \ll P_N$).

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

Receiver Front-End Details The boundary between Regions I and II is sensitive to the behavior of the programmable gain amplifier (PGA) in the monitoring receiver. One common model for a quantizing receiver is to build a variable attenuator followed by a fixed-gain amplifier before the signal reaches the analogue-to-digital converter (ADC). In order to avoid saturating the ADC, that is, exceeding its input voltage range, the variable attenuator is commanded to reduce the power from the antenna according to the statistics of the ADC output in a feedback loop. In Fig 5.6, the P_D curves begin “stacking up” when the transmit power becomes high enough to enter Region I: that is, when additional transmit power must be exactly offset by increased attenuation in the receiver. In this regime, thermal noise is negligible compared to quantization noise, which tracks with transmitter power. Thus, in Region I, the slope of the 50% detection curve in Fig. 5.7 is unity. Increasing the transmitter power in Region I does not improve P_D because the variable attenuator is forced to further suppress the incoming signal by the same amount, leading to no net increase in sensitivity.

In Region II, there is no suppression of the incoming signal by the variable attenuator, as all received signals are within the sensitivity range of the ADC at full PGA gain. Assuming as in Section 5.3 that cancellation of the authentic signal and the static multipath components at the monitoring receiver may be considered perfect in this regime, the detector need only distinguish the spoofing signal from thermal noise and dynamic multipath. So long as the dynamic multipath remains relevant (i.e. comparably strong to the spoofed signal), it will prevent the receiver from identifying spoofing signals that are below the noise floor, resulting in a relatively flat 50% detection curve.

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

5.5.4 Receiver Sensitivity Range

Fig. 5.8 shows the detection performance of the GLRT detector with different ADC bit depths for two distinct transmit power levels, and Fig. 5.9 shows these data recast in terms of RX power at the 50% detection threshold versus authentic signal TX power. One may infer that the sensitivity threshold does not improve with bit depth at low transmit power levels. With regards to the regions discussed

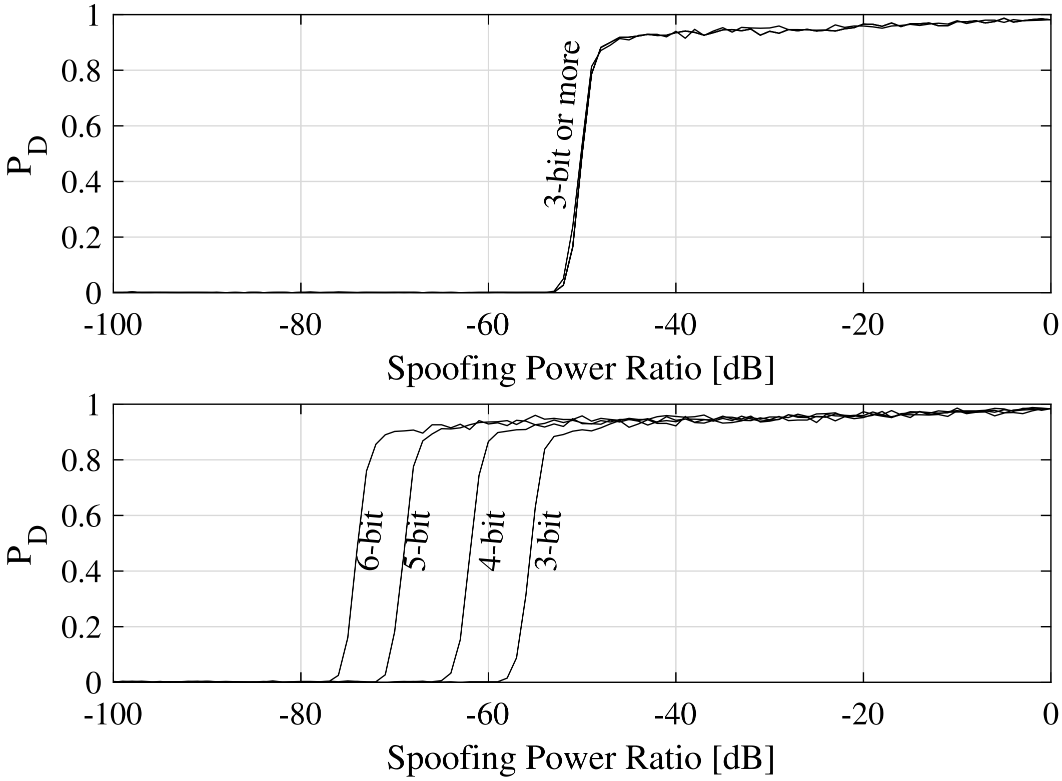


Figure 5.8: Simulation results of the GLRT detector with different ADC bit depth, for a 0 dBW (top) and 40 dBW (bottom) transmitter located at 10 km away from a listening beacon.

in Subsection 5.5.3, these plots reveal two trends. First, a larger ADC bit depth results in a lower quantization noise level in Region I due to lower suppression by the variable attenuator. Second, the dividing line between Regions I and II moves rightward with increasing bit depth. That is, the thermal noise dominates up to a higher transmit power level. Quantization is not the performance-limiting factor in Region III.

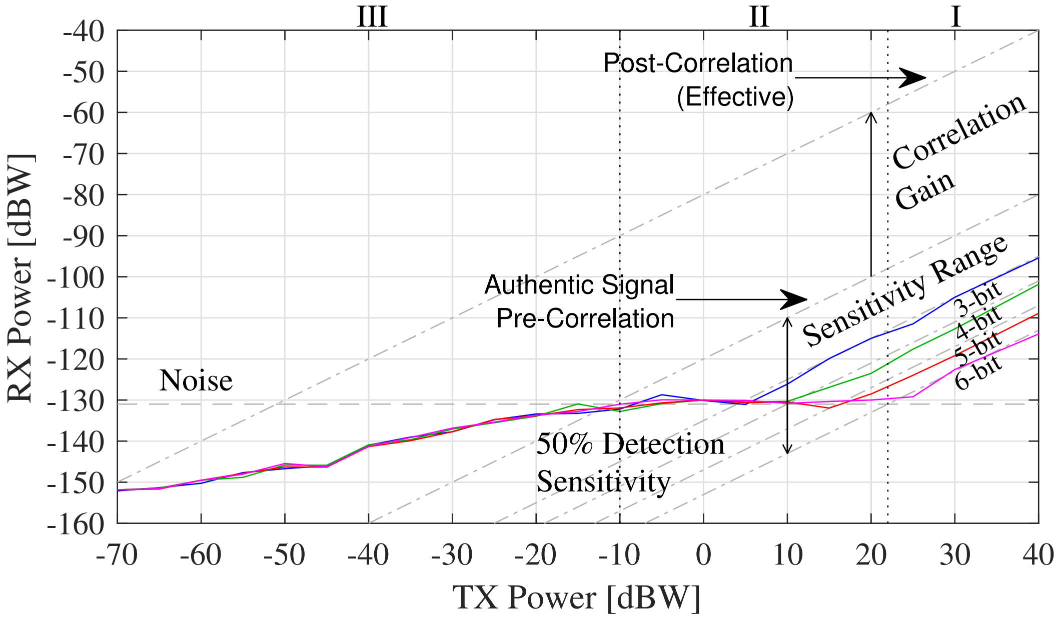


Figure 5.9: Simulation results of the GLRT detector under different transmitter power, showing the 50% detection sensitivity curve with different levels of quantization. The boundary between Regions I and II varies with depth and is shown for 6-bit quantization.

5.5.5 Joint Detection over Multiple Epochs

From Fig. 5.9, one can observe that given a transmit power level and ADC bit quantization, a monitoring beacon taking a ‘single-shot’ measurement of 1 ms has a limit in its detection sensitivity. One way to increase this performance ceiling is to accumulate measurements over a longer interval, as outlined in Subsection 5.4.1. This sub-section presents the simulation results from the implementation of coherent and non-coherent combining of measurements.

Fig. 5.10 shows the detection performance of the GLRT detector with different coherent accumulation intervals. For both test cases with or without dynamic multipath, increasing the coherent accumulation interval to 50 ms improves the detection performance of the GLRT detector by approximately 17 dB.

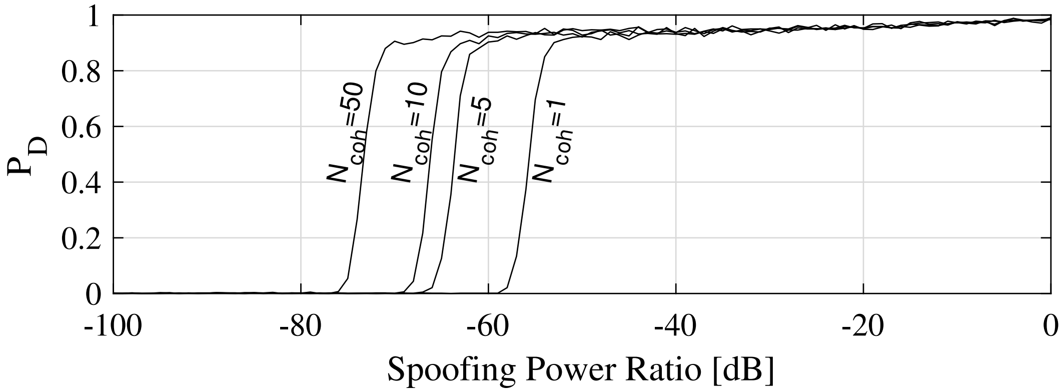


Figure 5.10: Simulation results for the detection performance of a GLRT detector using different coherent accumulation interval, for a 30 W transmitter located 10 km away from the listening beacon.

In contrast, Fig. 5.11 shows a slight improvement of 0.04 dB in the GLRT detector's sensitivity threshold with increasing non-coherent integration intervals. This indicates that the presence of dynamic multipath prevents a naïve additive combining of test statistics from effectively concentrating information over multiple epochs. This is because the presence of dynamic multipath has the same desensitizing effect to the joint detection threshold as to each single epoch threshold, such that combining test statistics across epochs does not increase detection sensitivity.

In summary, a sufficiently long coherent accumulation interval should be implemented to maximize the detection performance of the GLRT detector. However, the length of the accumulation interval should be constrained such that the assumption of each signal component's parameters being constant remains true.

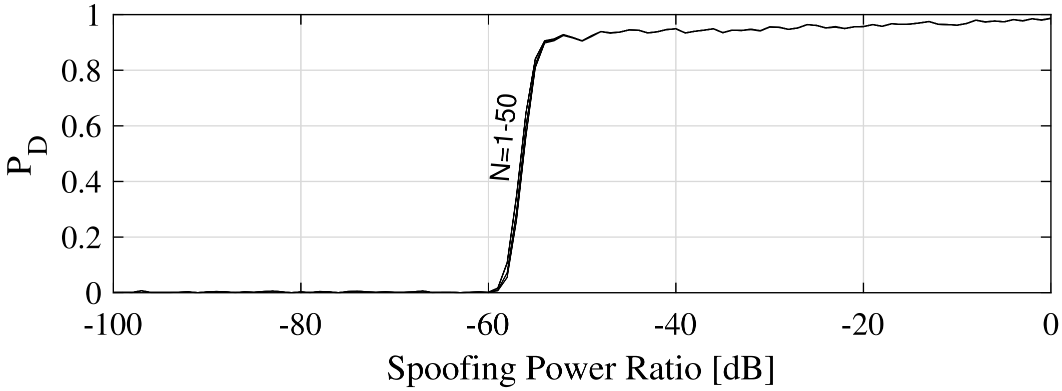


Figure 5.11: Simulation results for the GLRT detector with different non-coherent integration, for a 30 W transmitter located 10 km away from the listening beacon.

5.5.6 Joint Detection with Multiple Monitoring Beacons

As outlined in Sub-section 5.4.2, combining measurements from a network of monitoring beacons enhances detection performance beyond what is achievable with the standalone operation of each individual beacon. This subsection quantifies this improvement in detection performance, as well as the spoofer localization accuracy of the GLRT network detector.

5.5.6.1 Simulation Setup

In the setup shown in Fig. 5.12, all four monitoring beacons are equidistant from the 1 W transmitting beacon. At zero clock bias, the reference monitoring beacon B1 observes the spoofer's delay to be aligned with the authentic signal, while other beacons observe this delay at an offset with the authentic peak. In this simulation, the spoofer's clock bias is modeled to be uniformly distributed over two chip interval $[-\tau_c, \tau_c]$. In addition, each monitoring beacon has a unique set of H_0 distribution. While the same multipath parameter set outlined in Sub-section 5.2.2 is implemented in this simulation, every monitoring beacon observes a distinct set of multipath delay at each epoch. The pre-defined array of possible spoofer's location covers an area spanning 2 km by 2 km and is discretized at 20 m, which is less than the tap spacing of 0.1 chip. In addition, the pre-defined spoofer's clock bias array covers an interval of 2 chips, and is discretized at $\frac{1}{3}$ of the tap spacing. Other simulation parameters, such as the number of runs for calibration and trial, path-loss exponent, and characteristics of the monitoring receiver's antenna and front-end, have been outlined in Sub-section 5.5.1.

5.5.6.2 Network SSA Performance

From both Fig. 5.13 and Fig. 5.14, one observes that the detection performance of both AT and GLRT network detectors outperform their individual monitoring beacons, as they exploit the synergy from combining information across multiple observers. However, a closer comparison between both figures reveal the 3 dB sensitivity advantage of the AT network detector over the GLRT network detector. This can be explained by four observations made from the comparison between the performances of individual beacons' AT network detectors with their GLRT counterparts. First, the AT/GLRT detection performances of B3 and B4 are similar, as the spoofer appears at the correlation windows of both beacons with the same spoofing power ratio, and geometric delay. Second, the GLRT detectors of B2–B4 underperform their AT equivalents by 3 dB, due to inaccuracies in the ML estimates of the spoofer's position and clock bias. The ML estimation accuracy of

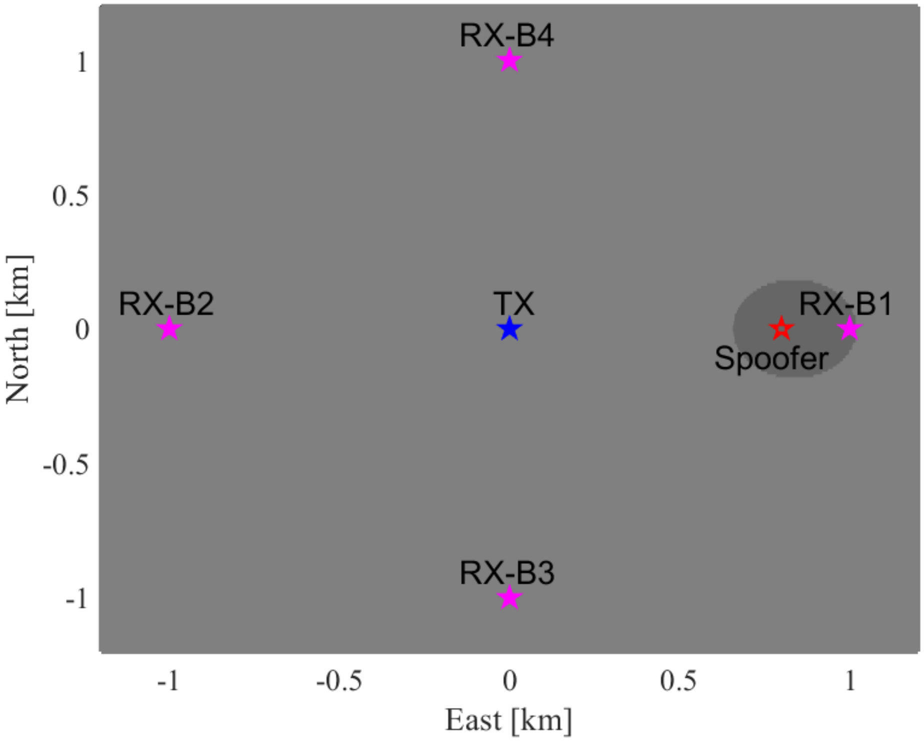


Figure 5.12: Simulation setup with 4 monitoring beacons. In this scenario, the 4 monitoring beacons are located 1 km away from the transmitting beacon. In addition, the spoofer is 200 m away from the reference monitoring beacon B1. The dark area is the region where the spoofing signal power level is above that of the authentic signal, and the spoofing power ratio at the reference beacon is unity.

the spoofer's physical parameters, shown in Fig. 5.15, reaches a steady-state value of 40 m at a spoofing power ratio of -22 dB and above, as a result of two factors: the position geometry between the monitoring beacons and the spoofer; and the mesh fineness of the pre-defined grid of spoofer's possible position and clock bias. The residual error of 40 m indicates a misalignment of the estimated spoofer's code offset $\Delta\hat{\tau}_{Dk,j}$ by at least one-tenth of a chip, which leads to approximately 3 dB

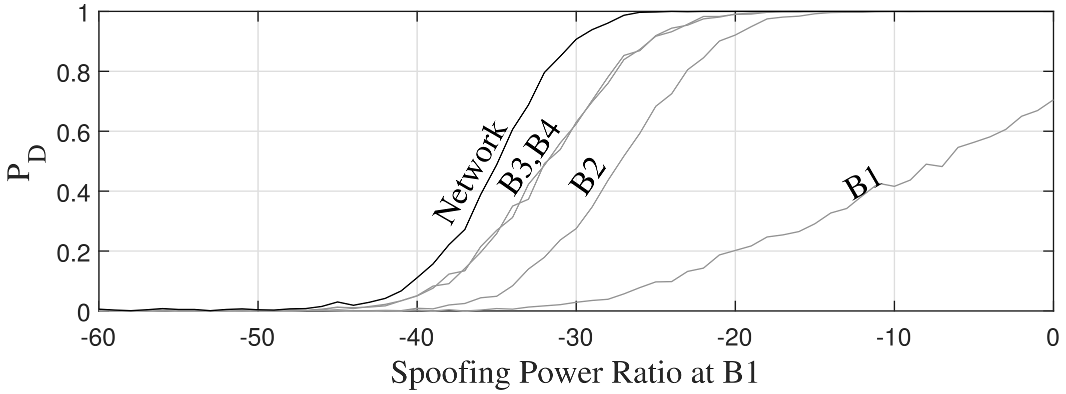


Figure 5.13: AT detection performance of each individual monitoring beacons, and of the TRNS network (in black).

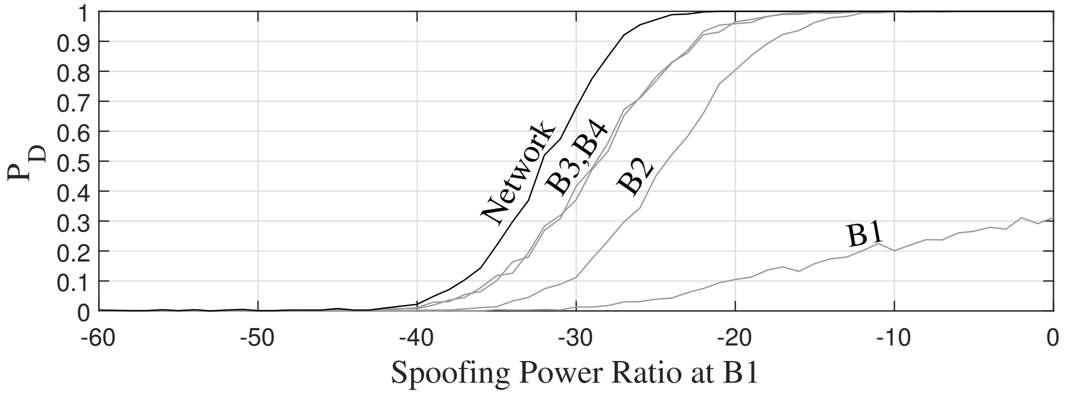


Figure 5.14: GLRT detection performance of each individual monitoring beacons, and of the TRNS network (in black).

degradation in detection performance. Third, B1's AT and GLRT detectors perform sub-optimally, having P_D less than unity even at high spoofing power ratio. This is because the spoofer's secular delay from its simulated clock bias coincides with B1's window of correlator output taps that are desensitized by dynamic multipath. Fourth, there is an increasing gap in the detection performance between GLRT and AT detectors of B1 with the rise in spoofing power ratio. This is due to the coupling between a misaligned spoofer delay estimate and B1's desensitized window of correlator output taps, which further degrades B1's GLRT detection performance. However, this does not drastically affect either AT or GLRT network detection performance, as the contribution of B1 to the GLRT network-wide test statistic is small compared to the other beacons.

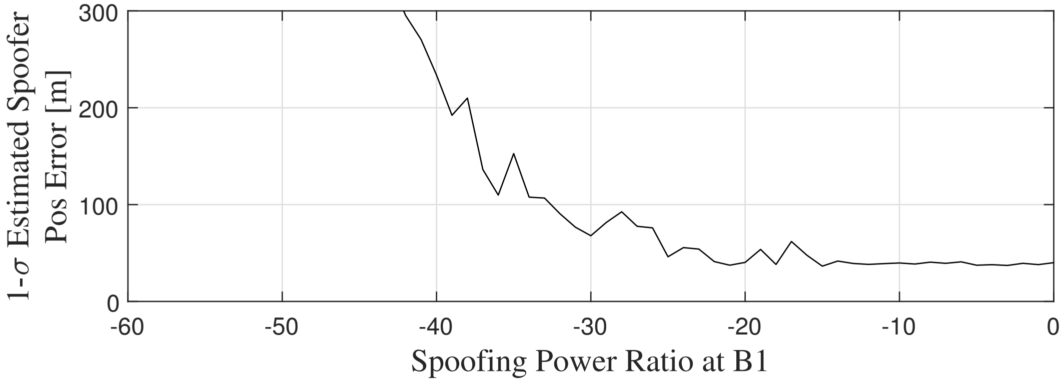


Figure 5.15: 1-σ estimated spoofer position error at different spoofing power ratio referenced at B1.

Even though GLRT network detection performance pales in comparison to AT, it augments TRNS network with a spoofer localization capability. However, the spoofer localization accuracy is only assured at high spoofing power ratio, as shown in Fig. 5.15. This is further illustrated in two example scenarios. In the scenario with low spoofing power ratio of -60 dB shown in Fig. 5.16, dynamic multipath dominates over the spoofing signal at both B3 and B4. A lower cost is assigned to the cells that match these multipath delays, which form the dark ellipses in the plot. The intersection of these ellipses has the lowest likelihood cost and denotes the ML estimate of the spoofer's position, which is far from the true spoofer position in this example. In contrast, for the scenario with higher spoofing power ratio of -30 dB shown in Fig. 5.17, all monitoring beacons assign lower cost to the observed spoofing signal instead of the unique dynamic multipath that each observes. This forms four dark concentric ellipses, each of which represents the spoofer's delay observed by each beacon. The cell with the lowest likelihood cost occurs at the intersection of these ellipses, and this represents the ML estimate of the spoofer's position, which matches the true spoofer position perfectly in this case.

5.5.6.3 Enhanced Network SSA with Multiple Observers

A natural question to ask is, does having more monitoring beacons improve network SSA performance, and by how much? This section seeks to answer this by comparing detection and localization performances between a 4-beacons TRNS network (in Fig. 5.12) and a 8-beacons TRNS network (in Fig. 5.18).

Figs. 5.19 and 5.20 show the AT and GLRT network detection performances respectively, along with the detection performance from each individual monitoring beacons. Similar to Fig. 5.13 and 5.14, the network detectors using 8 monitoring beacons outperform all its constituents, again highlighting the benefit of joint detection across multiple beacons. One also observes similar detection performance between beacon pairs B3–B4, B5–B6, and B7–B8, as the spoofing signal arrives at their antenna with the same geometric delay and spoofing power ratio. The marked improvements in detection performance and localization accuracy using 8 monitoring beacons are shown in Fig. 5.21 and Fig. 5.22 respectively, where the detection

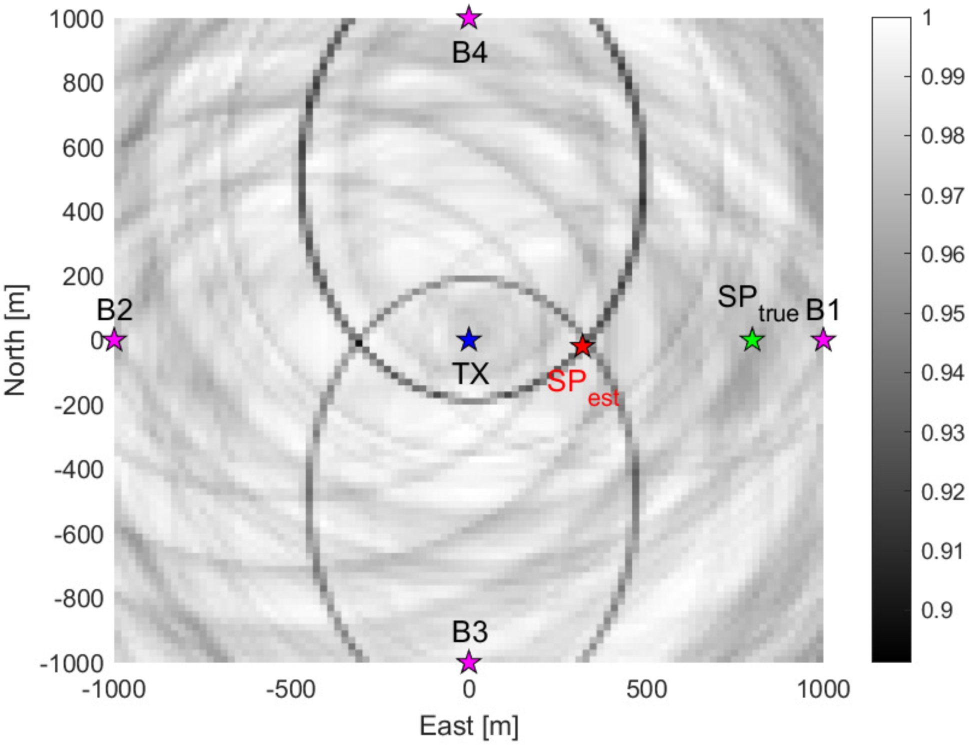


Figure 5.16: Normalized likelihood cost across a pre-defined grid of potential spoofer's position, at a spoofing power ratio of -60 dB using a 1 W transmitter. The dark ellipses denote the dynamic multipath's delay observed by beacons B3 and B4.

sensitivity increases by 7 dB, while the residual estimated position error drops by 48% to 21 m. One notable reason is the placement of beacons B5 and B6 relative to the spoofer. Their positions aid them to observe the spoofing signal outside the desensitized correlation window unlike that of B1, and at a higher spoofing power ratio than other beacons (namely B2, and beacon pairs B3–B4 and B7–B8). These factors help beacon pair B5–B6 achieve the best detection performance among all monitoring beacons, which in turn improves the overall network detection perfor-

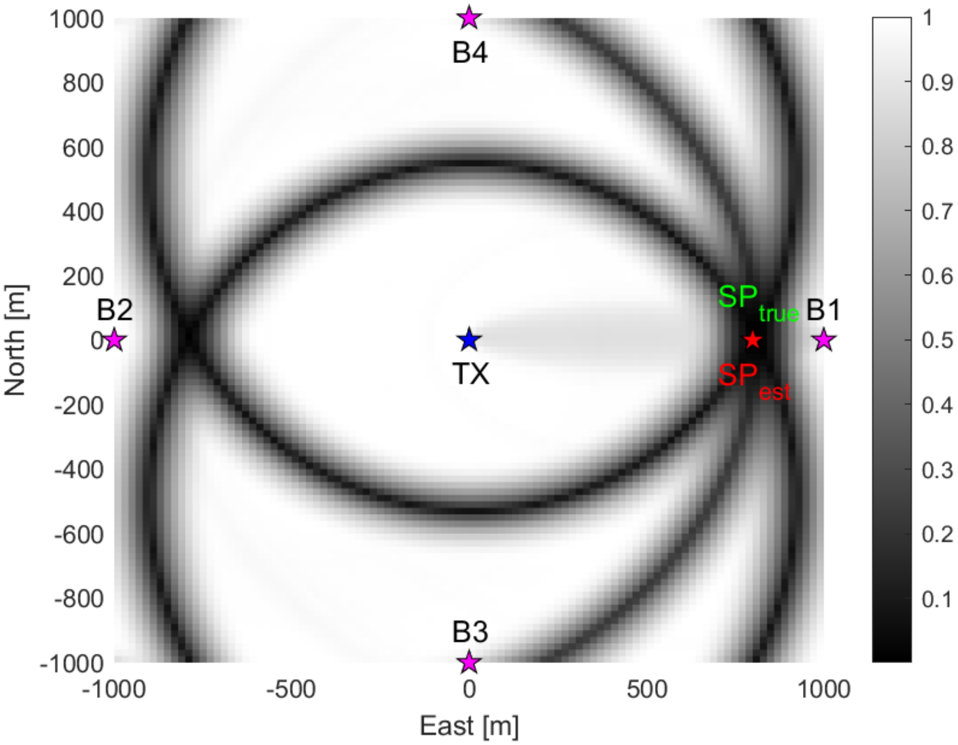


Figure 5.17: Normalized likelihood cost across a pre-defined grid of potential spoofer's position, at a spoofing power ratio of -30 dB using a 1 W transmitter. The dark concentric ellipses denote the spoofer's delay

mance.

5.5.6.4 Summary

This section illustrates the merits of performing joint detection across multiple beacons from simulation results. While GLRT network detection offers SSA with spoofer localization augmentation, it has a 3 dB lower detection sensitivity compared to AT network detection, and also comes with a higher computational

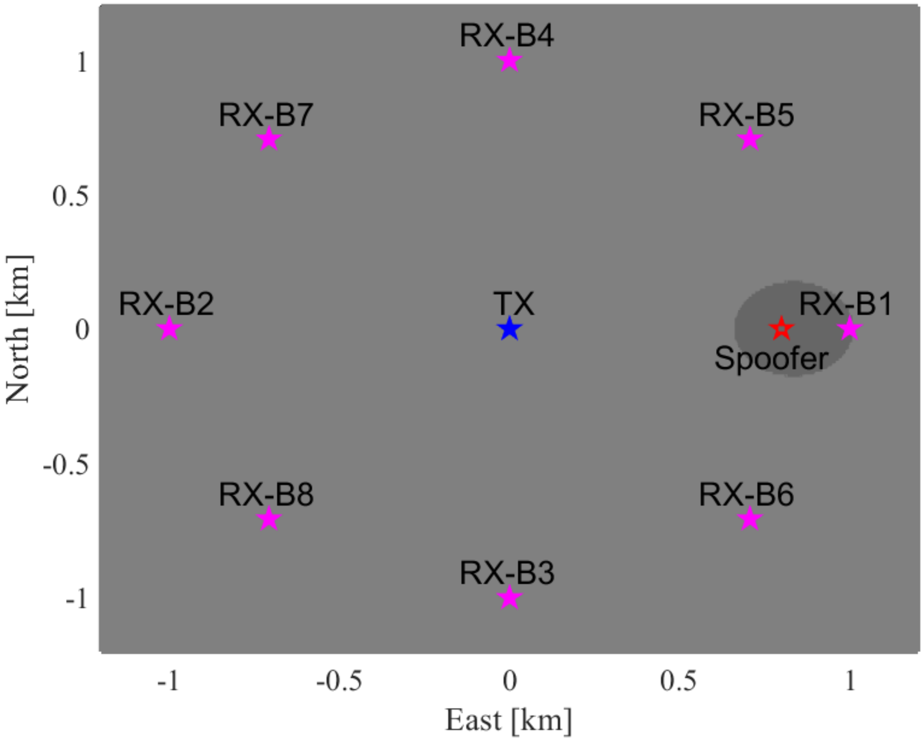


Figure 5.18: Simulation setup used for spoofer detection and localization using 8 monitoring beacons which are located 1 km away from the transmitting beacon. The spoofer's setup is similar to Fig. 5.12

cost from its ML estimation and detection algorithm. However, GLRT offers a better assurance of a spoofer's existence in the signal landscape, as compared to AT which only looks for any signal anomalies. One potential implementation that allows TRNS operator to circumvent the higher computational load is to operate the AT network detector for round-the-clock surveillance, and activates GLRT network detector only upon detection of a signal anomaly.

This section also highlights the improvements in detection performance and

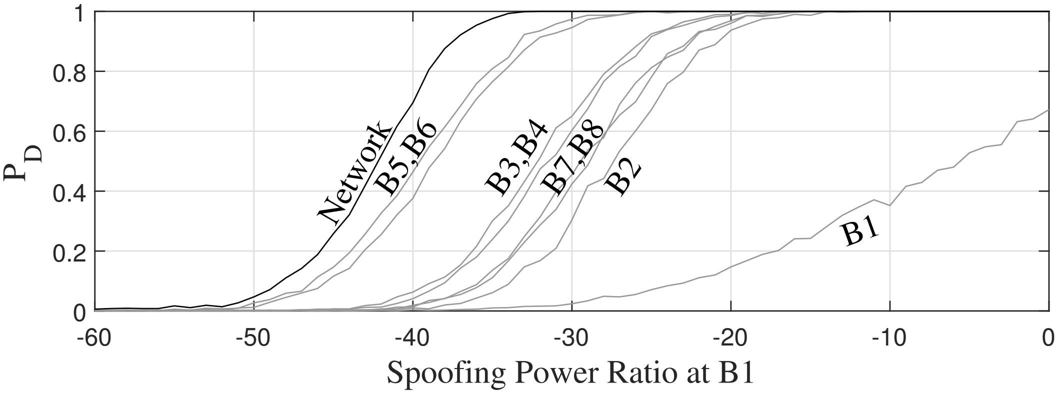


Figure 5.19: AT detection performance of 8 individual monitoring beacons, and of TRNS network (in black).

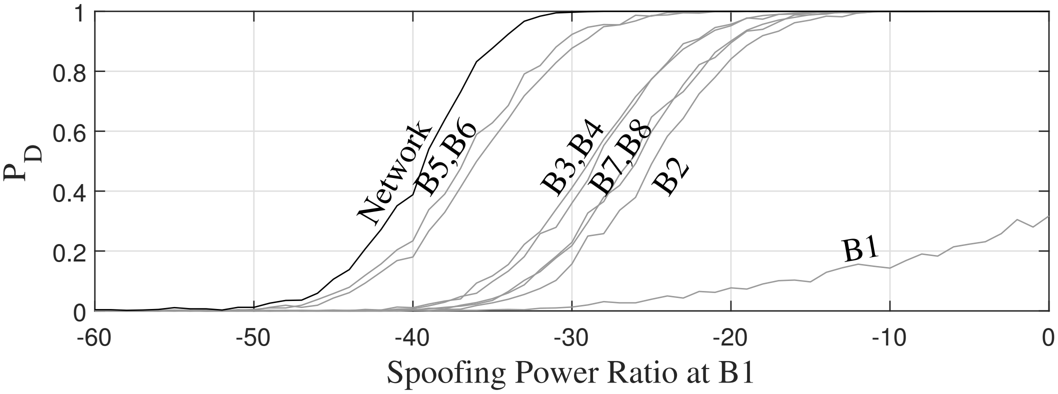


Figure 5.20: GLRT detection performance of individual monitoring beacons, and of the TRNS network (in black). The degraded detection performance of B1 across all spoofing power ratio has been discussed in Fig. 5.14.

localization accuracy with an increase in the number of monitoring beacons. However, TRNS operator should also consider the additional costs involved in siting more beacons, such as higher infrastructure cost, and greater instances of mutual near-far interference resulting in degraded PNT performance.

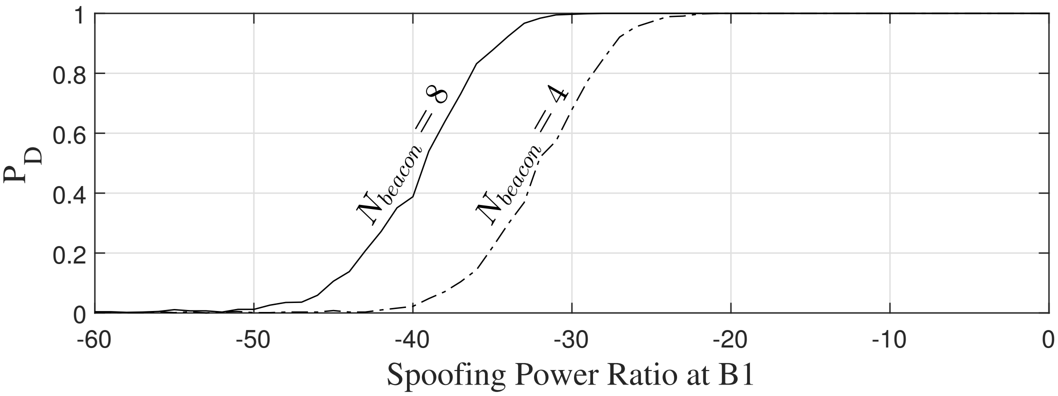


Figure 5.21: Comparison between the network detector's performance using different number of monitoring beacons.

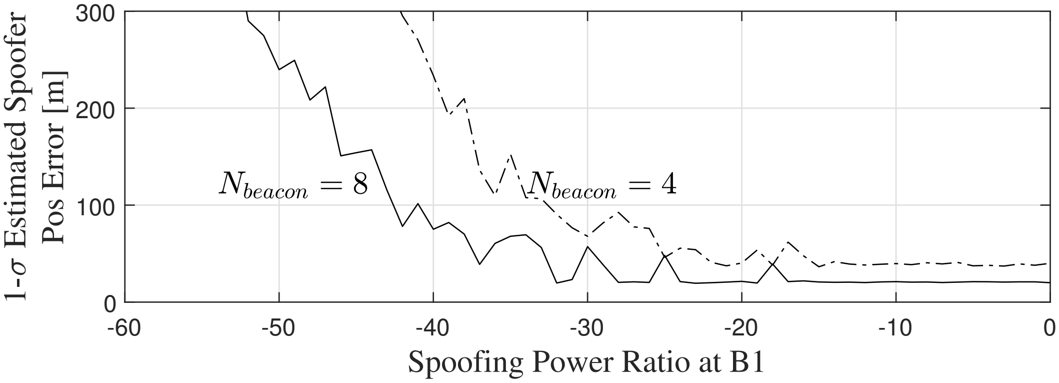


Figure 5.22: Comparison between the network detector's spoofer localization accuracy using different number of monitoring beacons.

5.6 Conclusion

This thesis proposes the addition of signal-situational-awareness (SSA) capability to the TRNS network, to augment cryptographic NME+NMA scheme in countering against SCER and meaconing attacks. Two signal authentication techniques are proposed for SSA that allow TRNS operator to detect weak signal spoofing in the presence of multipath without the use of costly full-duplex techniques.

The first technique, the anomaly test, compares the current observations against an empirical model of typical (nominal) observations, and has an advantage in simplicity and performance. The second technique searches for the spoofing signal and compares the observations against a reconstruction of the most likely spoofer: the GLRT technique. The GLRT method performs as well or better than the anomaly test in all considered test conditions. The GLRT exhibits a sensitivity advantage of 5 dB over the anomaly test in the absence of dynamic multipath, which drops to 0.13 dB in the presence of dynamic multipath. In addition, the GLRT has a 50% spoofer detection threshold up to -74 dB with high transmit power level of 30 W and 6-bit ADC quantization. Simulations of both detectors under operating conditions encountered by a generic TRNS quantify their performance. In addition, techniques to enhance SSA performance are also proposed, which includes joint detection across multiple epochs, or using multiple monitoring beacons. The detection performance of the GLRT detector improves by approximately 17 dB when the coherent accumulation interval increases from 1 ms to 50 ms. In addition, the GLRT network detector made up of 8 monitoring beacons has a lower detection threshold of -39 dB with a transmit power level of 1 W, and is augmented with a spoofer localization capability that has an accuracy of 21 m above spoofing power ratio of -28 dB. Terrestrial radionavigation systems will benefit not only from techniques designed to secure traditional GNSS, but also from the exploitation of novel opportunities for signal situational awareness arising from the proximity and mutual audibility of the transmitting beacons, rendering TRNS more resilient against man-in-the-middle attacks.

Chapter 6

Urban Environment Multipath Profiling

6.1 Introduction

This chapter presents the statistical results of an urban multipath propagation measurement campaign. This campaign was carried out in an attempt to validate the multipath empirical model by [91] presented in Subsection 5.2.2, which was derived from the statistical analysis on the Land Mobile Satellite Channel Model (LMSCM) [84].

Urban multipath propagation experiments had been conducted in the past with the following goals: to accurately quantify the performance of radionavigation systems in an urban setting [87]; and to minimize the performance degradation of high sensitivity receivers due to multipath [46]. Extensive multipath measurement and characterization studies in urban canyon environments had been carried out in near GNSS L1-band in the last two decades by [84] and [94]. In [84], a blimp took on the role of a simulated satellite to transmit a 10 W measurement signal over a

This chapter is based on: Ronnie X.T. Kor, Peter A. Iannucci, and Todd E. Humphreys. Comprehensive PNT Security for a Terrestrial Radionavigation System. *Navigation, Journal of the Institute of Navigation*, 2021. In preparation..

bandwidth of 100 MHz, with the center frequency at 1.51 GHz. A receiver mounted on a measurement bus traveled through different environments (e.g. rural, suburban, and urban) around Munich, and at varying speeds to characterize the multipath observed by a car [83] or a pedestrian [47]. Post-processing of data logs using the ESPRIT (Estimation of Signal Parameters via Rotational Invariance Techniques)-based super-resolution algorithm yielded sparse impulse response reconstructions for the channel with a time resolution of 1 ns. Reference [85] used these results to analyze the magnitude of the Doppler shifts and path delays of reflected signals in both urban and suburban settings. Reference [94] extended this work by conducting data collection in downtown Calgary, AB, Canada, and using the post-processed data to characterize the Doppler offsets and path delays of all line-of-sight and multipath signals.

Current commercial TRNS operate at either digital cellular band [54] or ISM band [75]. A number of multipath propagation characterization studies for various cellular bands had been carried out three decades ago in major cities of United States [73], Japan [86], and Toronto [81]. However, these studies were largely based on sky–ground channels and roof–ground channels. Past studies placed less emphasis on profiling roof–roof channels, which have their unique multipath characteristics. This thesis seeks to address this gap by characterizing the roof–roof channels, which will be instrumental in understanding the multipath environments of TRNS infrastructural monitors. A measurement campaign was carried out at various baselines at The University of Texas at Austin, in order to profile the multipath environment arising from different traffic and environmental conditions at these sites. Statistical analysis of the data logs validates the multipath empirical model used for autonomous TRNS SSA that was outlined in Subsection 5.2.2.

6.2 Experimental Setup

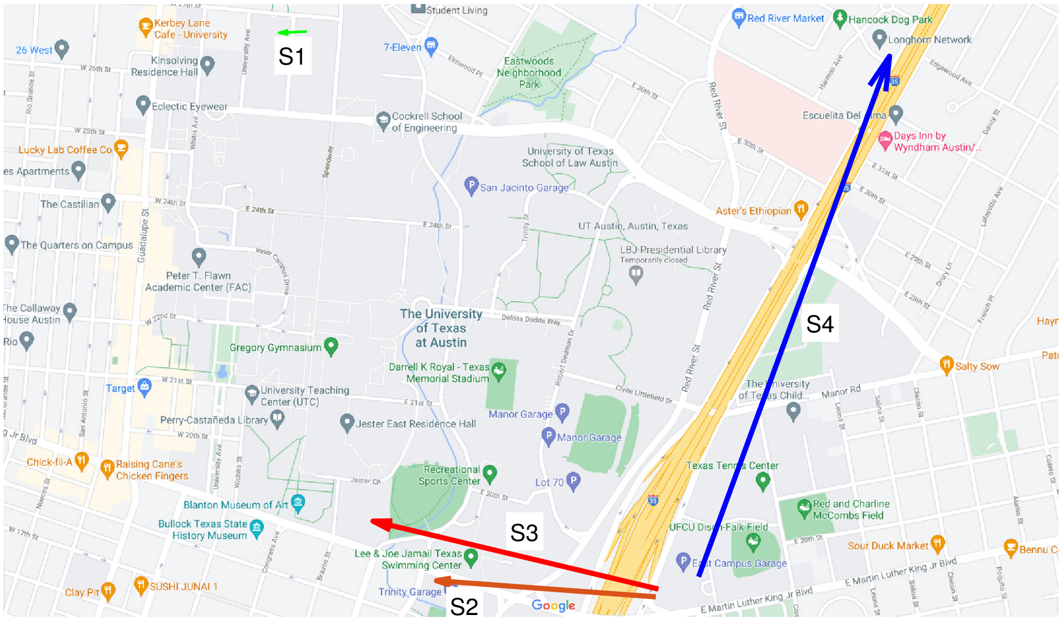

S1
S2
S3
S4
The University of Texas at Austin
Darrell K Royal - Texas Memorial Stadium
Cockrell School of Engineering
University of Texas School of Law Austin
LBJ Presidential Library
Gregory Gymnasium
Perry-Castañeda Library
Blanton Museum of Art
Bullock Texas State History Museum
Lee & Joe Jamail Texas Swimming Center
Recreational Sports Center
Texas Tennis Center
UFCU Disch-Falk Field
Red and Charline McCombs Field
Manor Garage
San Jacinto Garage
Trinity Garage
East Campus Garage
Red River St
E Martin Luther King Jr Blvd
Guadalupe St
Google

Figure 6.1: Overview of the 4 baselines on the campus ground of The University of Texas at Austin, and the direction of signal transmission for each baseline.

Four different baselines within the University of Texas at Austin were selected, with the objective of profiling roof–roof urban channels over different transmission ranges. Table. 6.1 summarizes the locations of 8 sites corresponding to 4 different baselines with their duration of recording, and Fig. 6.1 shows their individual directions of signal transmission. Table. 6.2 lists the ranges and height differences of signal transmission for each baseline. Figs 6.2 to 6.5 outlines the locations of the transmitter (TX) and receiver (RX) in each baseline, the placement of the test equipment, as well as the view from the receive antenna. Each of these baselines has its unique characteristics:

S1: This setup profiles the multipath environment between two parking garages along a quiet intersection of *27th Street* and *Wichita Street* (see Fig. 6.2).

S2: This setup characterizes the environment along a busy road (*East MLK Jr Boulevard*) within the campus (see Fig. 6.3).

S3: This setup depicts the multipath that emanates from the *I-35* highway (see Fig. 6.4)

S4: This setup profiles the multipath from a longer cross-section of the *I-35* highway, at a longer signal transmission range (see Fig. 6.5).

Table 6.1: List of test sites at each baseline and the duration of data collection.

Baseline	TX Sites	RX Sites	Duration [hr]
S1	27 St Garage	Speedway Garage	8
S2	East Campus Garage	Trinity Garage	1
S3	East Campus Garage	Brazos Garage	12
S4	East Campus Garage	Uni. Park Garage	2

Fig. 6.6 shows the measurement setup for both transmitter and receiver. In each setup, the Intel NUC runs an application using *GNU Radio*, which controls the signal generation/reception on the Ettus Research USRP N200 software-defined radio (SDR). Each SDR draws its frequency reference from the Hewlett Packard Z3801A oven-controlled crystal oscillator (OCXO), which is GPS-disciplined in

Table 6.2: List of test sites' estimated heights relative to the ground, the distances and height differences of signal transmission.

Baseline	TX Hgt [m]	RX Hgt [m]	Range [m]	Hgt Diff [m]
S1	12	18	88	-6
S2	21	12	550	9
S3	21	33	733	-12
S4	24	36	1330	-12

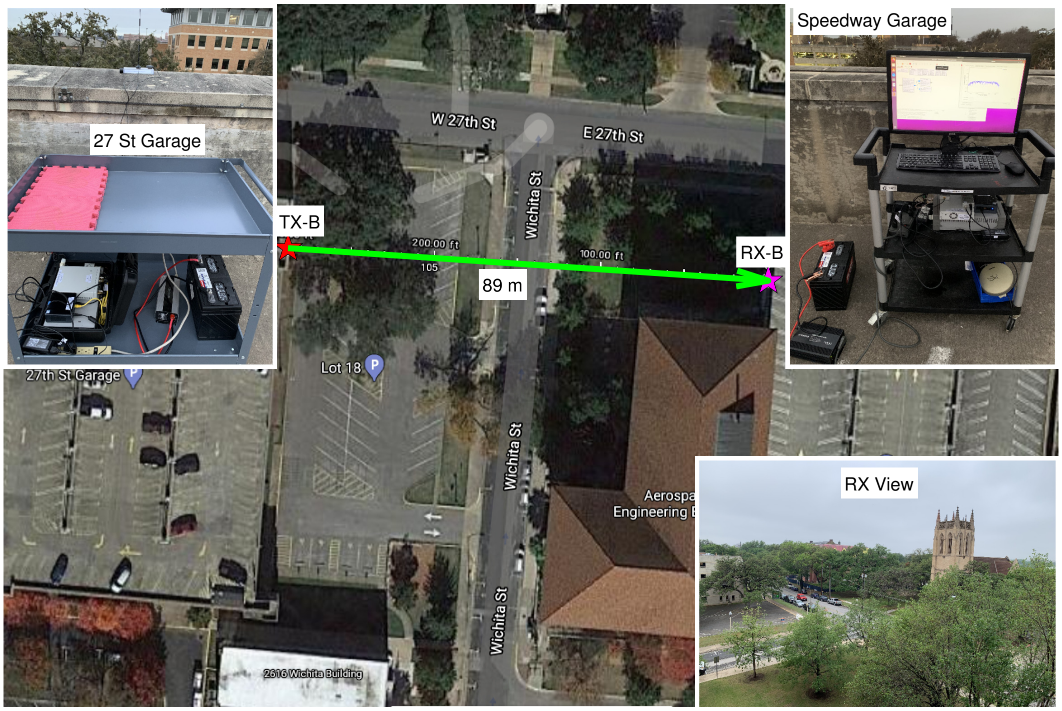


Figure 6.2: Position of the transmitter setup at 27th Street Garage (in red star) and receiver setup at Speedway Garage (in magenta star), across a distance of 88 m.

both transmitter and receiver setup, and has an Allan variance of 10^{-11} s over an integration time of 1 s. Ideally, this ensures that both ends of the link share a common time origin. The SDR of the transmitter was programmed to generate

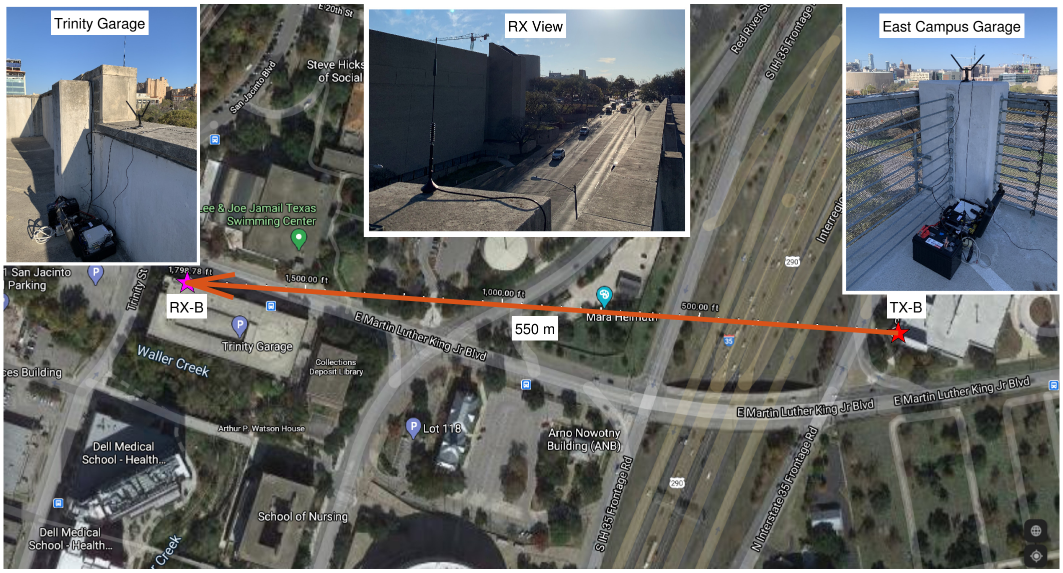


Figure 6.3: Position of the transmitter setup at East Campus Garage (in red star) and receiver setup at Trinity Garage (in magenta star), across a distance of 550 m.

a 10-stage maximal-length sequence of 1023 chips that forms a sinc-shaped line spectrum of several hundred single carriers over a bandwidth of 10 MHz at a center frequency of 915 MHz.

The center frequency of 915 MHz was selected for three reasons. First, this thesis is interested in validating the empirical model used in characterizing the SSA performance of a generic TRNS network operating within the industrial, science, and medical (ISM) band. This frequency band is attractive for TRNS because low-frequency signals are more penetrating in urban environments. Second, testing in the ISM band (902–928 MHz) offers two advantages: it is one of the few wide-band channels (i.e. 10 MHz or greater) that are available for experimentation, allowing fine multipath delay resolution of 15 m and above to be achieved; and

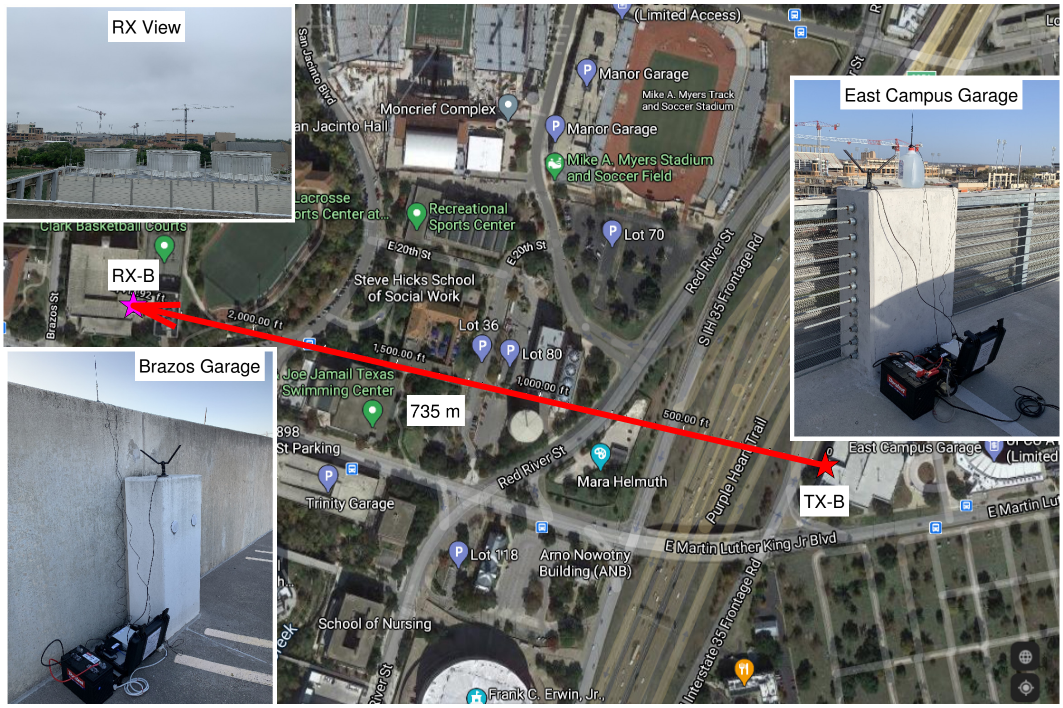


Figure 6.4: Position of the transmitter setup at East Campus Garage (in red star) and receiver setup at Brazos Garage (in magenta star), across a distance of 733 m.

higher signal power can be used under Part 97 Amateur Radio Service Rules [18] to achieve longer-range experimentation. Third, quarter-wave "whip" antennas, which are conveniently sized and nearly omni-directional, can be used to collect multipath arriving from all directions. This is more faithful to the TRNS SSA scenario, where infrastructural monitors are listening to authentic signals from adjacent beacons, and spoofing signals coming in all directions.

Amateur radio convention dictates that experimental operation should be polite: vacating the channel if it is busy, using the minimum power necessary for the duration of the experiment, and announcing at the end of the experiment that the

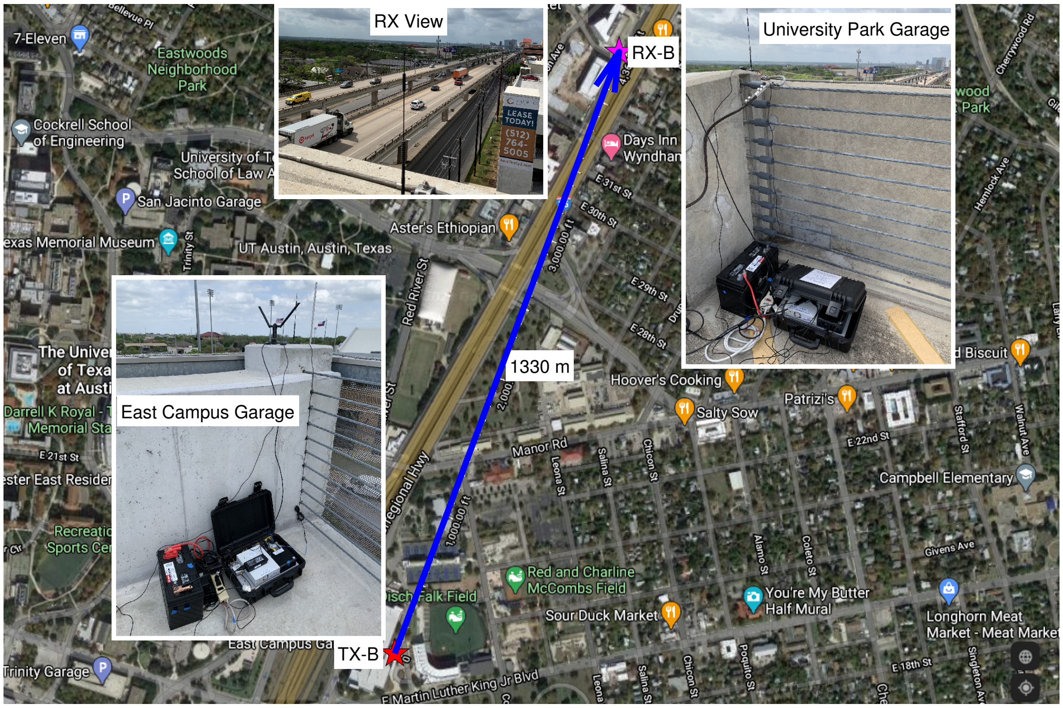


Figure 6.5: Position of the transmitter setup at East Campus Garage (in red star) and receiver setup at University Park Garage (in magenta star), across a distance of 1330 m.

channel is clear for other users. An amateur operator also has to send out an identification every 10 min in a format that any listener can understand. Because of these constraints, the transmission power is set at 300 mW at the antenna output, and the longest transmission duration was 1 hr. In addition, the spreading code transmission is interrupted by periodic identification sequences consisting of pre-recorded Morse code waveforms bearing the Amateur callsign of the licensed operator overseeing the experiment, along with a message indicating the experimental nature of the signal. These interruptions necessitate careful data post-processing when estimating long-term correlations (see Section 6.3).

The received signal is sampled at 12.5 MHz at the receiver's SDR, with 30 dB gain added along the processing chain. Applying a FFT on the received signal shows a time resolution of 80 ns for the channel impulse response (CIR), which is further refined to a time resolution of 20 ns by up-sampling the complex correlation function. Further processing of the correlation function described in Section 6.3 reveals the characteristics of multipath in each baseline, which will be elaborated in Section 6.4.

6.3 Data Processing

Let τ_j represent the time that sample j is acquired, $A(\tau_j)$ is the signal amplitude, $f_s = 12.5$ MHz is the sampling frequency, $\Delta t(\tau_j)$ is the code phase (potentially time-varying), $N_c = 1023$ is the number of chips in the spreading code, $T_c = 0.1\ \mu$s is the chip interval, $C(\tau \bmod N_c T_c)$ is the spreading code, $\Delta\theta(\tau_j)$ is the beat carrier phase in radians, and n_j is i.i.d. zero-mean Gaussian noise. We model the discrete-time TRNS signal as it exits the ADC of the RX USRP as

$$x_j = A(\tau_j)\, C((\tau_j - \Delta t(\tau_j)) \bmod N_c T_c)\, \cos\left[2\pi f_s \tau_j + \Delta\theta(\tau_j)\right] + n_j \tag{6.1}$$

where x_j is the jth sample.

The sequence x_j is cross-correlated with $C(\tau)$. The resulting complex function may be modeled as

$$\begin{aligned}\xi_k &\triangleq I_k + jQ_k \\ &= \frac{N_k \bar{A}_k}{2} \bar{R}(\Delta t_k) \left[\frac{1}{N_k} \sum_{j=j_k}^{j_k+N_k-1} \exp[i\Delta\theta(\tau_j)]\right] + n'_k\end{aligned} \tag{6.2}$$

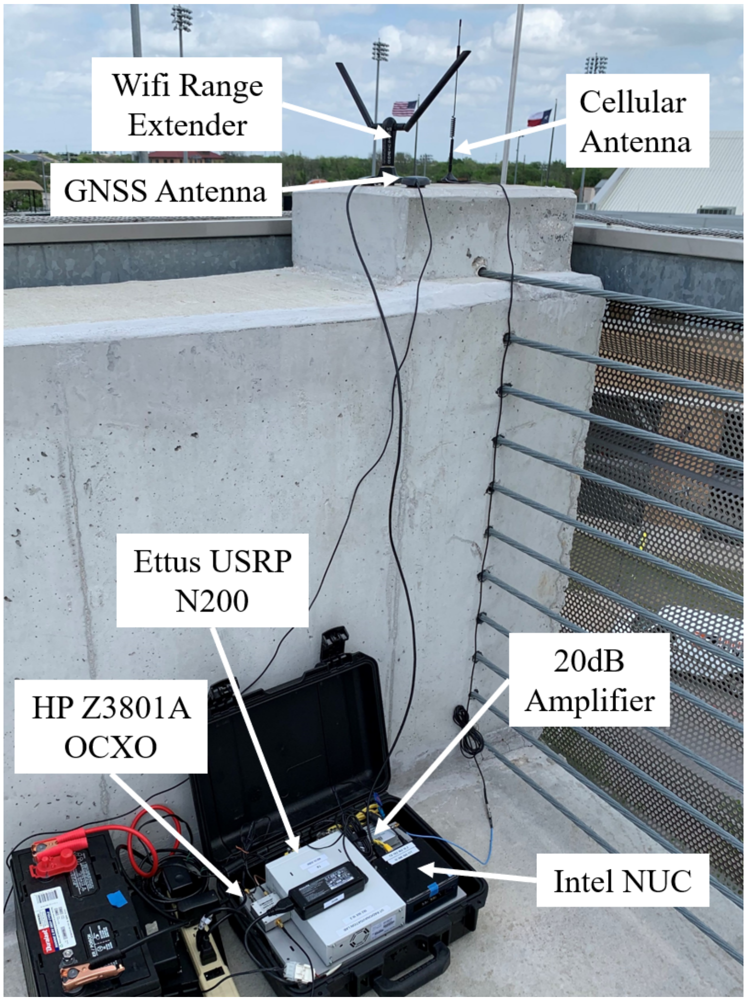
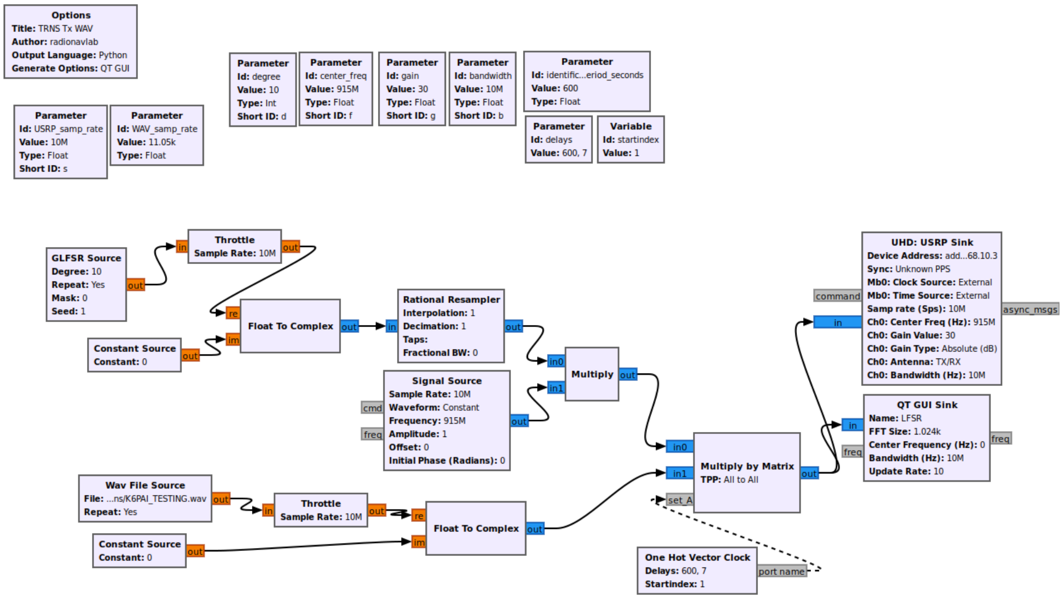


Figure 6.6: Measurement setup for both transmitter and receiver, which is made up of the following: i. Intel NUC computer running an application that uses *GNU Radio* for signal generation/reception, ii. Ettus Research N200 software-defined radio that generates or processes TRNS-like signal, iii. Hewlett Packard Z3801A GPS-disciplined OCXO that provides frequency references to the USRP, iv. Mini-Circuit ZRL-3500+ low-noise amplifier to boost the transmit signal, v. an omni-directional cellular antenna for signal transmission and reception, and vi. a WiFi range extender for remote control of the setup.



Options
Title: TRNS Tx WAV
Author: radionavlab
Output Language: Python
Generate Options: QT GUI

Parameter
Id: USRP_samp_rate
Value: 10M
Type: Float
Short ID: s

Parameter
Id: WAV_samp_rate
Value: 11.05k
Type: Float

Parameter
Id: degree
Value: 10
Type: Int
Short ID: d

Parameter
Id: center_freq
Value: 915M
Type: Float
Short ID: f

Parameter
Id: gain
Value: 30
Type: Float
Short ID: g

Parameter
Id: bandwidth
Value: 10M
Type: Float
Short ID: b

Parameter
Id: identific...eriod_seconds
Value: 600
Type: Float

Parameter
Id: delays
Value: 600, 7

Variable
Id: startindex
Value: 1

GLFSR Source
Degree: 10
Repeat: Yes
Mask: 0
Seed: 1

Throttle
Sample Rate: 10M

Constant Source
Constant: 0

Float To Complex

Rational Resampler
Interpolation: 1
Decimation: 1
Taps:
Fractional BW: 0

Signal Source
Sample Rate: 10M
Waveform: Constant
Frequency: 915M
Amplitude: 1
Offset: 0
Initial Phase (Radians): 0

Multiply

Multiply by Matrix
TPP: All to All

UHD: USRP Sink
Device Address: add...68.10.3
Sync: Unknown PPS
Mb0: Clock Source: External
Mb0: Time Source: External
Samp rate (Sps): 10M
Ch0: Center Freq (Hz): 915M
Ch0: Gain Value: 30
Ch0: Gain Type: Absolute (dB)
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 10M

QT GUI Sink
Name: LFSR
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 10M
Update Rate: 10

Wav File Source
File: ...ns/K6PAI_TESTING.wav
Repeat: Yes

Throttle
Sample Rate: 10M

Constant Source
Constant: 0

Float To Complex

One Hot Vector Clock
Delays: 600, 7
Startindex: 1

Figure 6.7: Flowgraph of an application that controls signal generation, developed using *GNU Radio Companion*.

where N_k is number of samples in kth accumulation, $\bar{A}_k$ is the average signal amplitude over an accumulation interval, Δt_k is the code phase error at midpoint of code interval, $\bar{R}(\Delta t_k)$ is the spreading code auto-correlation function model, $\Delta\theta(\tau_j)$ is the carrier phase error at τ_j, and $n'_k \triangleq n_{I_k} + jn_{Q_k}$ is a no-longer-i.i.d. complex noise sequence.

An ideal data-logging scenario to characterize the multipath in an urban landscape would be to record the signal transmission over a long duration with both TX and RX being phase-aligned, such that $\Delta\theta(\tau_j) = 0$ and $\xi_k \triangleq I_k = \frac{N_k \bar{A}_k}{2}\bar{R}(\Delta t_k)$. A delay-locked-loop (DLL) can be used to estimate the average code phase error Δt_k at the initial stage, and this value is subsequently used to align the local replica with the authentic signal's code phase for cross-correlation across the entire recording interval.

However, the measurement campaign faced three challenges. First, the spreading code transmission was interrupted every 10 minutes in order to transmit a periodic identification sequences bearing the operator's callsign and the experimental nature of the signal. Second, data overruns occurred due to random fluctuations in USRP data logging to an external hard disk. The dropouts due to overruns and periodic identification are shown in Fig. 6.8. Third, even though both OCXO clocks are frequency-locked to GPS, there is a slow drift in their phases over time, as shown in Fig. 6.9.

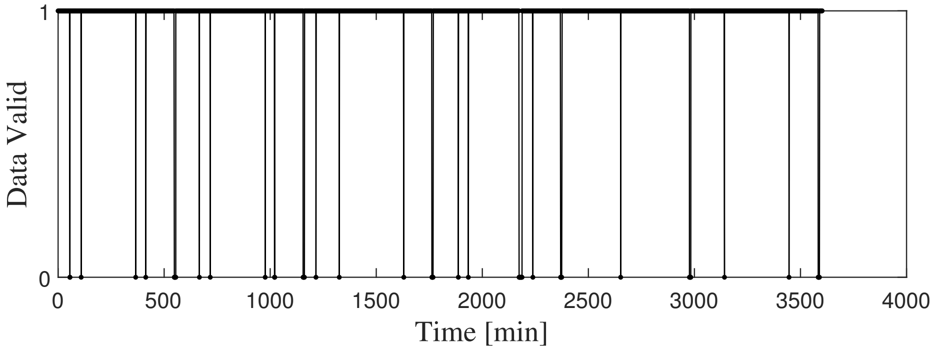


Figure 6.8: Time profile of the good intervals without operator identification and data overrun, for a 1300 hr – 1350 hr log from S3.

A number of heuristics are implemented in the post-processing of these data logs to overcome the above-mentioned challenges, and also to condense the enormous data logs for analysis. First, data samples are cross-correlated with a local replica, and are non-coherently combined over an interval of 100 ms to form the complex correlation function at each epoch. Data segments corresponding to the periods of data overrun are identified by looking for discontinuities in correlation

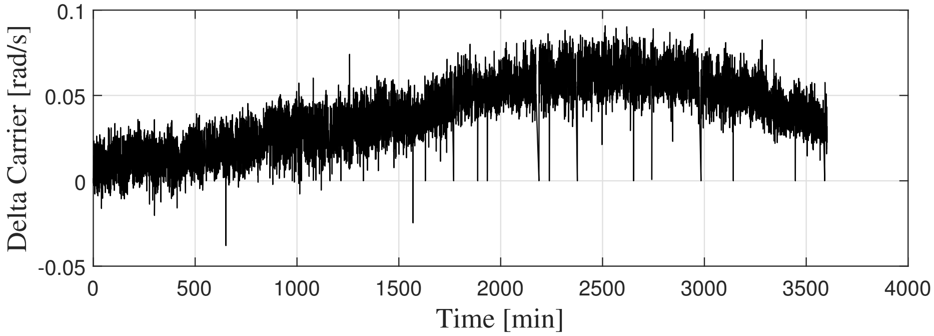


Figure 6.9: Time profile of the carrier phase misalignment between the TX and RX OCXO clocks, for a 1300 hr – 1350 hr log from S3.

magnitude, and the segments of operator identification are picked out by sharp drops in correlation amplitude. With these data segments removed, a vector of good intervals is formed, within which the correlation function is up-sampled to a 20 ns resolution and then aligned in the lag domain. A filtered phase model $\theta(\tau_j)$ is then estimated from the profile of carrier phase delta changes $\Delta\theta(\tau_j)$, which is then used to transform the complex correlation function into its baseband equivalent I_k. Lastly, spectral analysis is performed on this baseband correlation function, and the results are presented in the next section.

6.4 Statistical Analysis

A total of 33 hours of recordings were collected in this measurement campaign, as described in Table. 6.1. This section presents the statistical analysis performed for each baseline to highlight the unique multipath characteristic of each urban channel, as well as the impact of weather on the multipath distribution.

6.4.1 Multipath Characteristics

6.4.1.1 Baseline 1

Fig. 6.10 (top) shows the time profile of the channel impulse responses over a 50 min recording interval, which is marked by periods of data overrun and operator identification in blue stripes. Multipath are generally concentrated close to the authentic signal peak within a 1 μs interval, affirming the exponential power-delay distribution discussed in Ref. [33]. However, there are accumulations of echoes at larger delays, evident by bright bands in the plot. The consistency in correlation peak amplitudes of these bright bands indicate that these contributions are from static multipath.

Fig. 6.10 (bottom) shows the time profile of the channel impulse responses from the dynamic components of the received signal, after the static components have been removed from the complex correlation function. The bright bands on this plot indicate the existence of dynamic multipath, evident by fluctuations in peak amplitudes with time. The contribution of dynamic multipath to the overall channel impulse responses is shown in Fig. 6.11, which compares the mean amplitude value of the channel impulse responses (consisting of both static and dynamic component), with that from the dynamic component only. There are 12 distinct echoes in the mean channel impulse responses, of which 9 of them have dynamic components. The likely source of these dynamic multipath are the strong reflections from the trees that are along the line-of-sight transmission between TX and RX, as shown in map view of Fig. 6.2.

Fig. 6.12 shows the power spectrum of the prompt correlator tap at S1 over the recording interval. One interesting note from this plot is the consistency in the amplitude of dynamic multipath, which can be up to 10 s. The amplitude distribution of S1 in Fig. 6.13 confirms the log-normal distribution of multipath.

6.4.1.2 Baseline 2

Fig. 6.14 (top) shows the time profile of the channel impulse responses over a 50 min recording interval, which is marked by periods of data overrun and operator identification in blue stripes. The larger number of bright bands outside the 1 μs interval from the authentic signal peak are due to reflections off the walls and deck of *Trinity Garage* rooftop, as well as the walls of adjacent *Texas Swimming Center* (shown in the RX view of Fig. 6.3).

Fig. 6.14 (bottom) shows the time profile of the channel impulse responses from the dynamic components of the received signal. Unlike Fig. 6.10 (bottom), which has a number of bright bands appearing across the whole recording interval, Fig. 6.14 (bottom) has only two such distinct echoes at 1.6 μs and 2.5 μs, which is likely due to strong reflections from the trees that are along the line-of-sight transmission between TX and RX, as shown in the map view of Fig. 6.3. However, there are other bright bands with shorter intervals, which likely originates from reflections off motor vehicles traveling along *I-35* highway and *E Martin Luther King Jr Blvd* road.

Fig. 6.16 and Fig. 6.17 respectively show the power spectrum and the amplitude distribution of the prompt correlator tap at S2 over the recording interval, highlighting the log-normal distribution of multipath, and the consistency in the amplitude of its dynamic component (up to 10 s).

6.4.1.3 Baseline 3

Fig. 6.18 (top) shows the time profile of the channel impulse responses over a 60 min recording interval. A number of distinct echoes (indicated by the bright bands on the plot) are from the reflections of the authentic signal off the structure of the *Central Chilling Station* (seen in the RX view of Fig. 6.4).

The dynamic channel impulse response plot (in Fig. 6.18 (bottom)) is marked by a distinct constant-amplitude echo at 3.8 μs, and a number of bright bands with much shorter interval. Similar to Fig. 6.18 (bottom), the short bright bands are due to reflections off motor vehicles traveling along *I-35* highway. The constant-amplitude echo at 3.8 μs (with a distinct mean value shown in Fig. 6.19) comes from strong reflections off the trees that line the *Red River St* road.

The power spectrum plot of the prompt correlator output in Fig. 6.20, and its amplitude distribution shown in Fig. 6.21, also reveal the log-normal amplitude distribution of multipath, and the consistency in the amplitude of its dynamic component.

6.4.1.4 Baseline 4

Lesser trees and building structures are observed along the line-of-sight path between TX and RX in S4, which results in less distinct echoes observed from the channel impulse response plot of Fig. 6.22 (top). From the RX view photo in Fig. 6.5, the distinct echo at 0.6 μs is due to signal reflection from *Development*

Office Building. The source of the echo at 7.4 μs, which has a dynamic component evident from the plots shown in Figs. 6.22 (bottom) and 6.23, is the strong reflections off trees that are along the line-of-sight path of signal transmission. The dynamic multipath from the reflections off motor vehicles on the *I-35* highway are not evident in Fig. 6.22 (bottom) and 6.23, as the delays of these reflections are within 0.2 μs. The 20 ns time resolution from data processing is too coarse to discern multipath within this short time interval. Similarly, the log-normal amplitude distribution of multipath, and the consistency in their signal amplitude, are presented in Fig. 6.25 and 6.24 respectively.

6.4.2 Weather Condition

Measurement exercises on two different days were carried out for Baseline S1: a calm and sunny day on March 3, and a windy day on March 6. Figs. 6.26 and 6.27 show the mean values of the channel impulse responses at S1, collected over the same time duration, for March 3 and March 6 respectively. The TX and RX antenna were placed on the same spot on the two test dates, therefore a number of distinct peaks are similar across these two plots. However, a closer comparison of these plots reveal that a larger number of distinct dynamic echoes were visible on March 6 as compared to March 3. This is because the wind creates significant movement among the tree leaves, inducing greater signal reflections that were not seen on a calm day. Based on this observation, it is recommended that the TRNS operators calibrate the multipath parameter set discussed in Subsection 5.2.2 under varied environmental conditions in order to obtain an accurate H_0 distribution for spoofing detection.

6.5 Conclusion

A measurement campaign was carried out at 4 different sites in The University of Texas at Austin, to characterize multipath signals in an urban setting with application to TRNS Signal-Situational-Awareness outlined in Chapter 5. A statistical analysis is performed on the post-processed data-logs, which includes identifying the peaks in the correlator outputs across each recording interval, and assessing the path delays of both authentic and multipath signals. Four insights were gained from this measurement campaign: First, observations of the dynamic correlator output waterfall plots reveal the delays of the dynamic multipath, from which one can infer their sources from these delays; Second, the empirical data affirms the log-normal amplitude distribution used in multipath signal model; Third, the range of duration of dynamic multipath can be derived from the power spectrum plot of the prompt correlator output; And lastly, a comparison between two measurement exercises conducted at the same baseline highlights the correlation between weather and multipath observation. These insights will be useful to TRNS operator not only in the design of SSA calibration trials for their network of monitoring beacons, but also in the implementation of multipath mitigation techniques for their mobile receivers.

Had time permitted, it would have been possible to access lower-level interfaces to the USRP that would give explicit notifications of overruns, obviating the need for code-phase alignment heuristics across overrun gaps. Additionally, upgrading the OCXO to phase-locked variants (rather than merely frequency-locked devices) would significantly reduce the complexity of post-processing. Fortunately, all observed outages were brief, and the phase drift was very slow. These properties allow us to have confidence that the long-time (i.e. low-frequency) portions of the auto-correlation (power-spectrum) are nevertheless good approximation.

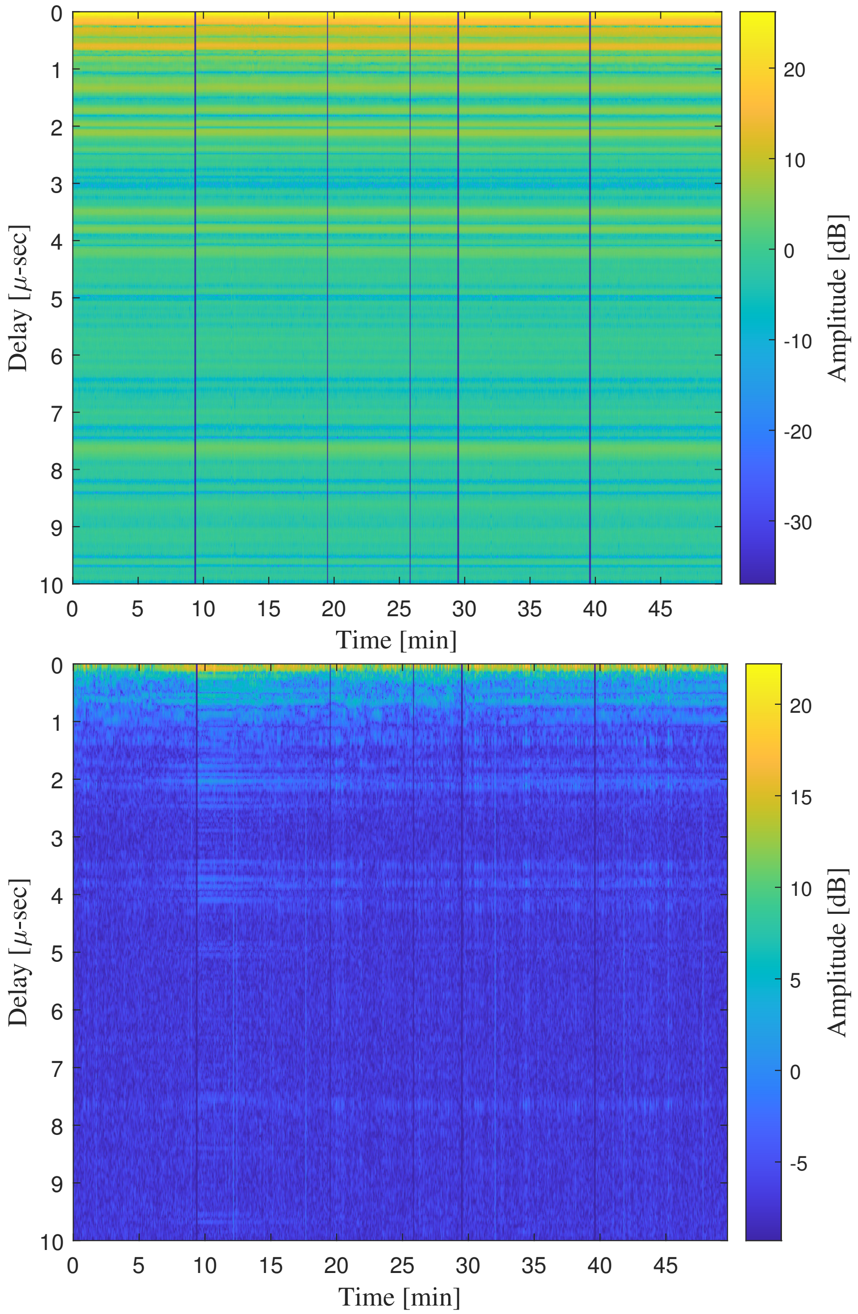


Figure 6.10: Waterfall plot of the channel impulse responses at S1 (top), and its dynamic component only (bottom), over a duration of 50 min. The dark line at 26th min marks a short period of data overrun, while the other dark lines at every 10-min interval are the periods of operator identification.

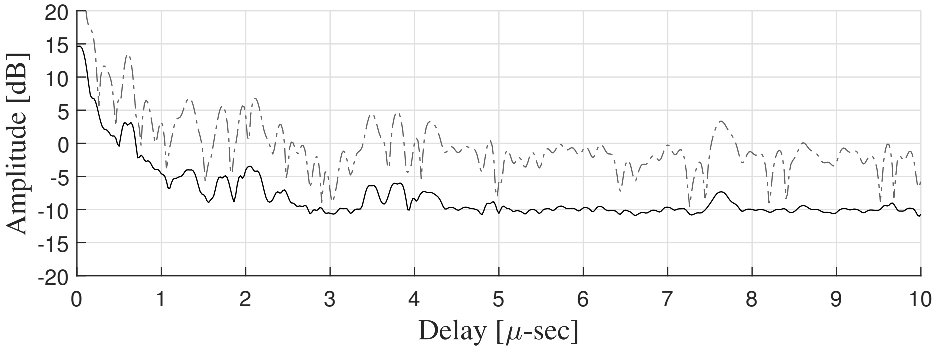


Figure 6.11: Comparison between the mean values of the channel impulse responses (in dotted line), and its dynamic component (in solid line) at S1, computed using 8 hours of recordings.

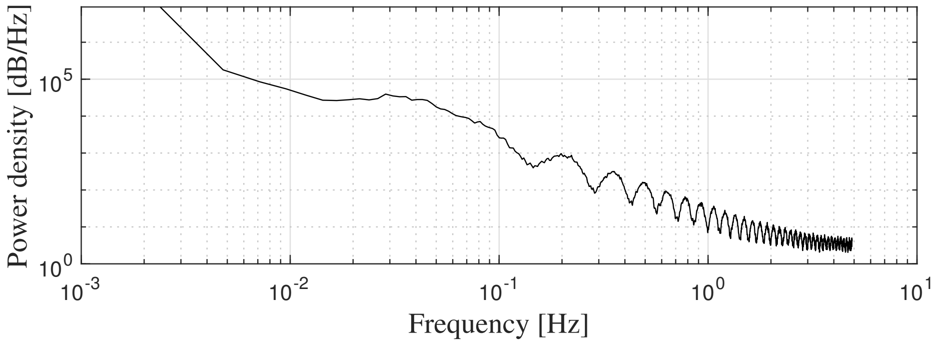


Figure 6.12: Power spectrum plot of the variations in the prompt correlator tap for S1, computed using 8 hours of recordings.

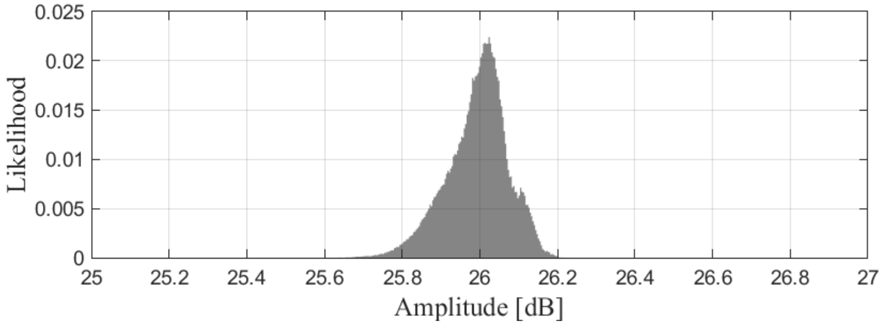


Figure 6.13: Amplitude distribution of the prompt correlator tap for S1, computed using 8 hours of recordings.

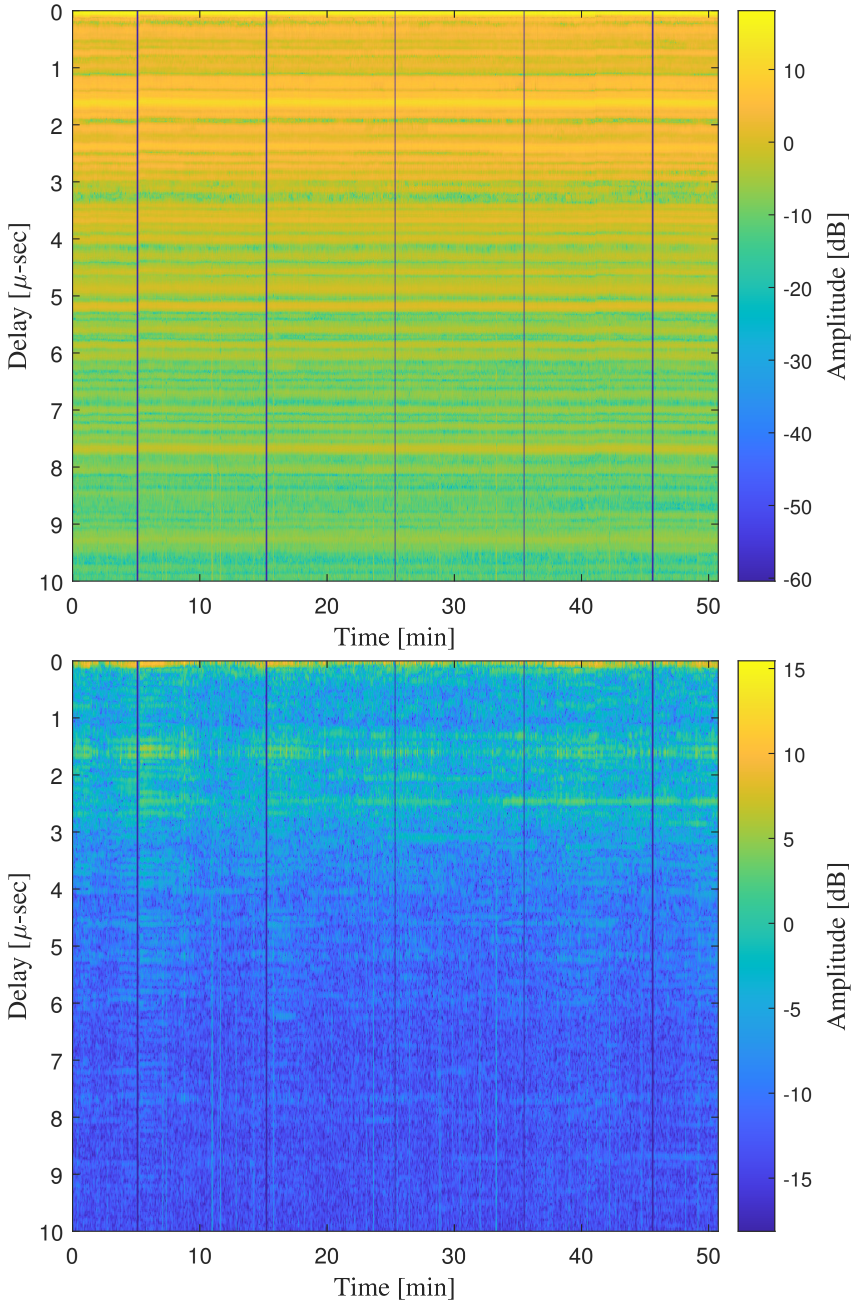


Figure 6.14: Waterfall plot of the channel impulse responses at S2 (top), and its dynamic component only (bottom), over a duration of 50 min. The dark lines at every 10-min interval mark the periods of operator identification, and its thickness is due to data overruns during the transition of spreading code change.

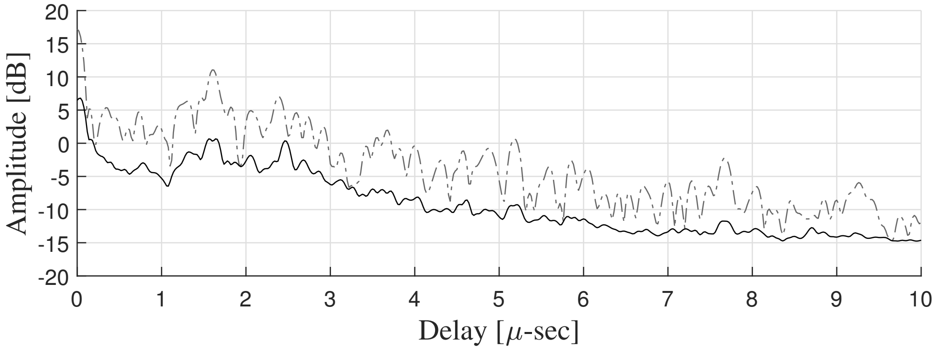


Figure 6.15: Comparison between the mean values of the channel impulse responses (in dotted line), and its dynamic component (in solid line) at S2, computed from a 50 min recording.

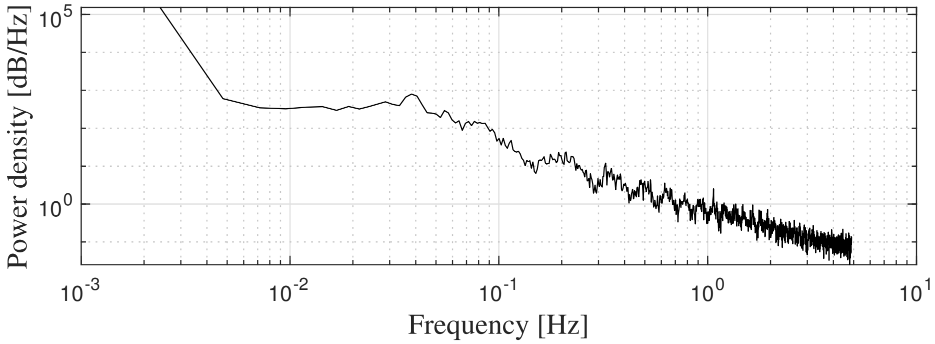


Figure 6.16: Power spectrum plot of the variations in the prompt correlator tap for S2, computed from a 50 min recording.

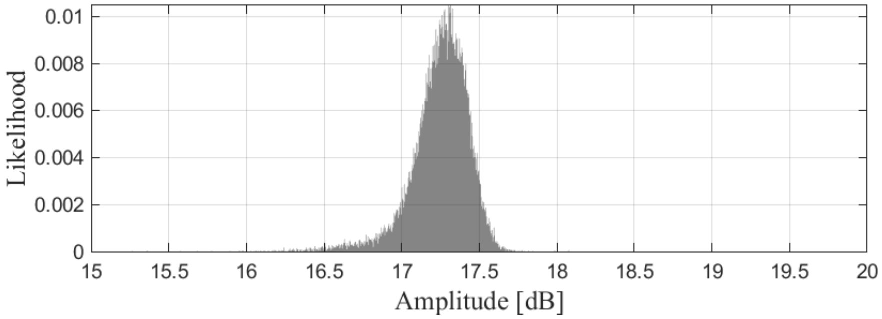


Figure 6.17: Amplitude distribution of the prompt correlator tap for S2, computed from a 50 min recording.

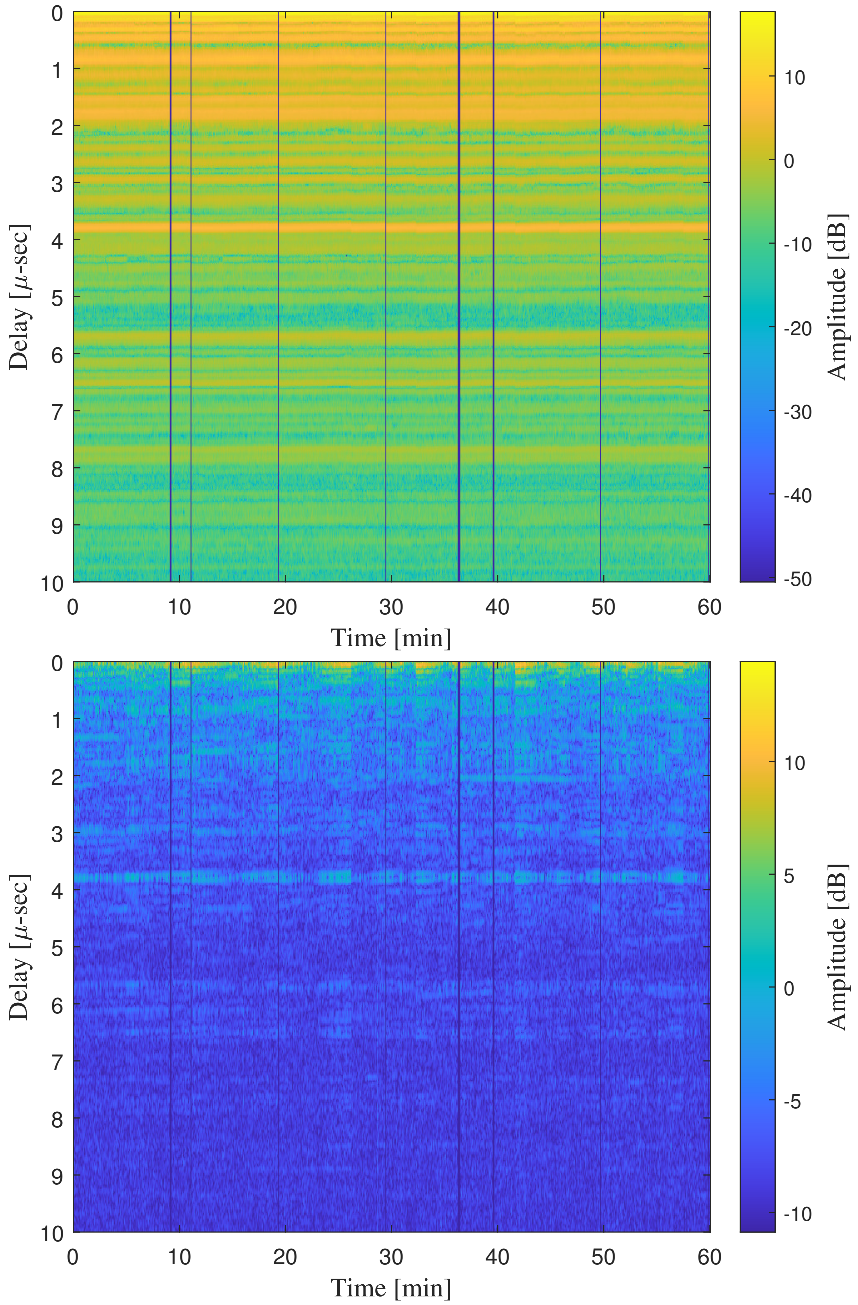


Figure 6.18: Waterfall plot of the channel impulse responses from S3 (top), and its dynamic component only (bottom), over a duration of 60 min. The dark lines at 11th and 37th are the periods of data overrun, while the other dark lines at every 10-min interval are the periods of operator identification.

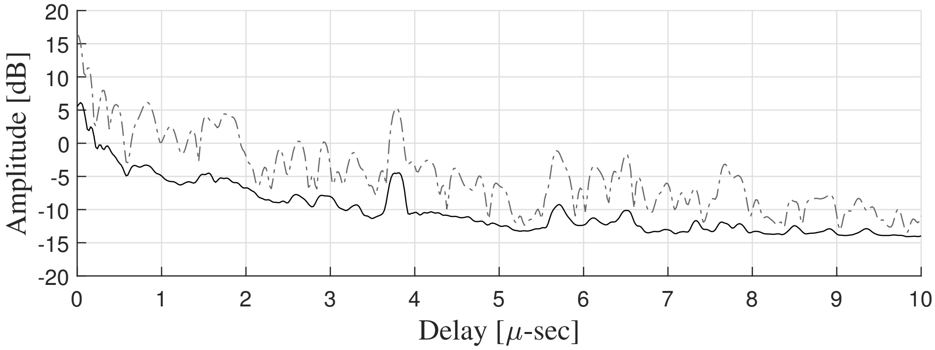


Figure 6.19: Comparison between the mean values of the channel impulse responses (in dotted line), and its dynamic component (in solid line) at S3, computed using 12 hours of recordings.

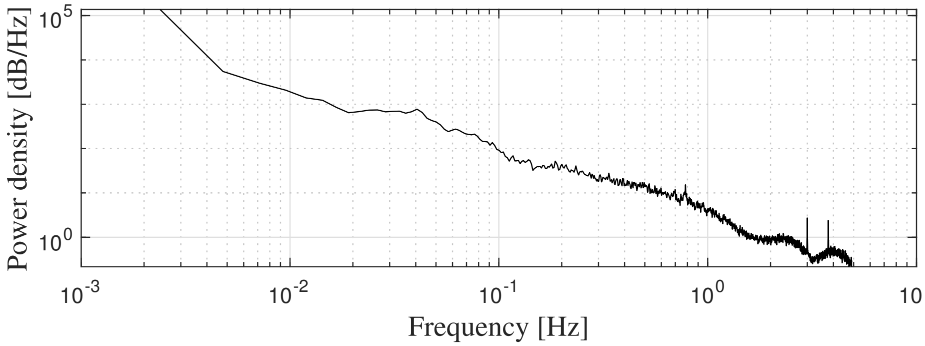


Figure 6.20: Power spectrum plot of the variations in the prompt correlator tap for S3, computed using 12 hours of recordings.

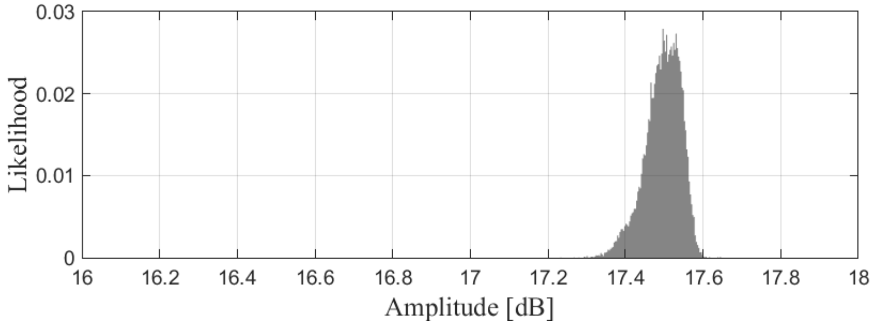


Figure 6.21: Amplitude distribution of the prompt correlator tap for S3, computed using 12 hours of recordings.

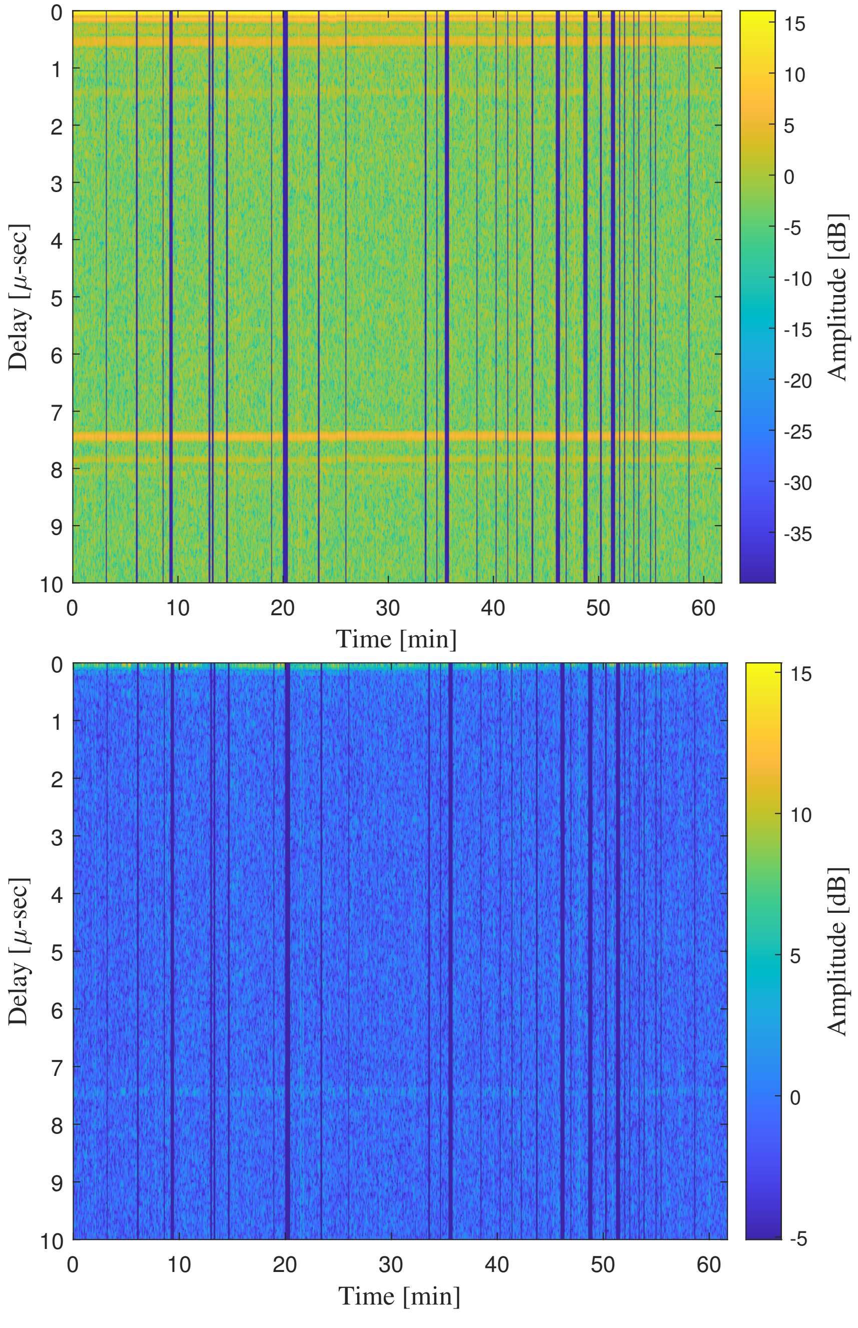


Figure 6.22: Waterfall plot of the channel impulse responses from S4 (top), and its dynamic component only (bottom), over a duration of 60 min. This recording is marked by frequent data overruns which overlap with the periods of operator identification.

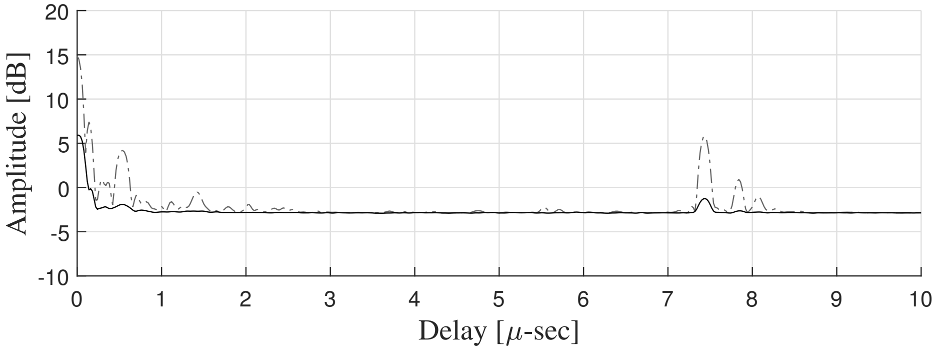


Figure 6.23: Comparison between the mean values of the channel impulse responses (in dotted line), and its dynamic component (in solid line) at S4, computed from a 60 min recordings.

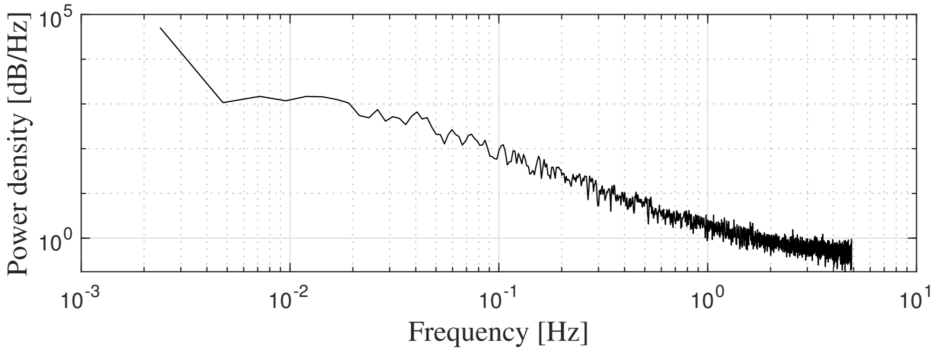


Figure 6.24: Power spectrum plot of the variations in the prompt correlator tap for S4, computed from a 60 min recording.

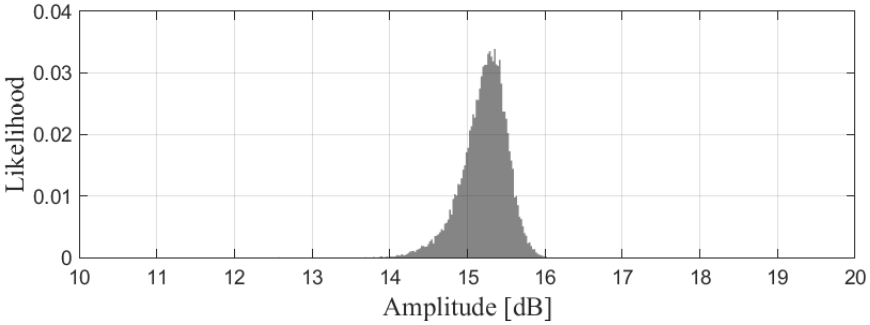


Figure 6.25: Amplitude distribution of the prompt correlator tap for S4, computed from a 60 min recording.

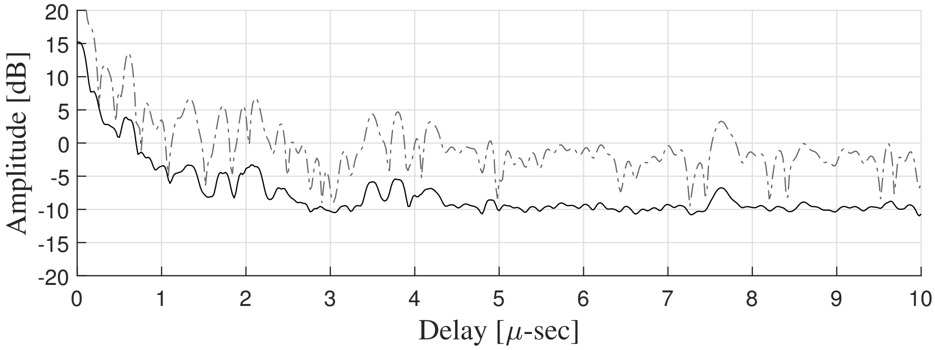


Figure 6.26: Comparison between the mean values of the channel impulse responses (in dotted line), and its dynamic component (in black solid line) at S1, using logged data between 1300 hr – 1400 hr on March 3, 2021.

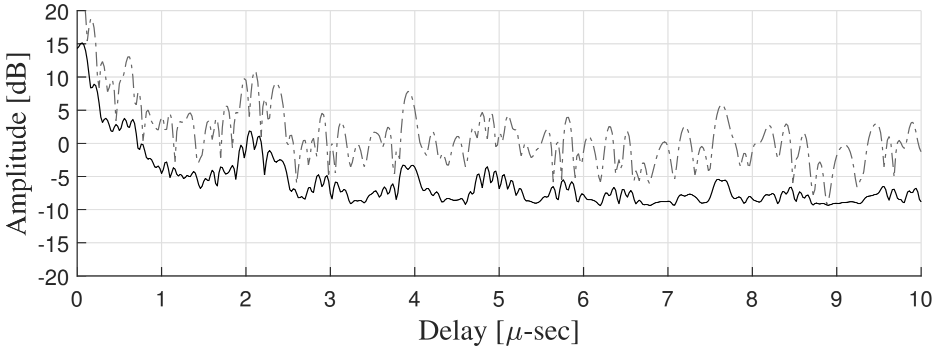


Figure 6.27: Comparison between the mean values of the channel impulse responses (in dotted line), and its dynamic component (in black solid line) at S1, using logged data between 1300 hr – 1400 hr on March 6, 2021.

Chapter 7

Conclusion

This thesis first outlines the unique vulnerabilities of a generic TRNS 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 thesis draws upon the flexibility offered by a clean-slate TRNS waveform and architecture to propose cryptographic and non-cryptographic schemes that cater to two types of receivers with differing needs: mobile users, and infrastructural monitors. The cryptographic security proposal focuses on the needs of a mobile TRNS user. It is made up of two orthogonal schemes: a multi-tiered NME scheme, which not only limits TRNS service to authorized users, but also can be customized for multiple subscriber tiers using selective decryption; and a novel MAC-leavened TESLA-based NMA scheme which provides both data authentication, and a certain degree of signal authentication against half-duplex spoofing attacks. However, this proposal is not fool-proof against SCER spoofing and meaconing threats. To address this gap in spoofing defense, this thesis proposes the addition of signal-situational-awareness (SSA) to the TRNS network of infrastructural monitors. Two signal authentication techniques, the Anomaly Test, and the Generalized Likelihood Ratio Test (GLRT), are proposed for SSA. These detectors allow TRNS operator to detect weak signal spoofing in the presence of multipath, without the use of costly full-duplex techniques. Simulations of both detectors under operating conditions encountered by a generic TRNS quantify their performance. In particular, the GLRT has a 50% spoofer detection threshold up to -74 dB with high transmit power level of 30 W and 6-bit ADC quantization. Two enhancements to the autonomous SSA's detection performance are also proposed which are complementary to each other: combining measurements across multiple epochs, and over multiple beacons. In particular, coherent integration of measurements over an accumulation interval of 50 ms improves the threshold of the GLRT detector by 17 dB. In addition, increasing the number of monitoring beacons from 4 to 8 reduces the GLRT network detector's threshold by 8.5 dB while reducing the spoofer localization accuracy by 48%. This thesis also embarked on a multipath measurement campaign in The University of Texas at Austin. Statistical analysis of the post-processed data logs affirms the TRNS multipath power-delay empirical model used in SSA simulations, and also provides insights into the characteristics of dynamic multipath in an urban setting. The comprehensive security proposal for TRNS outlined in this thesis not only provides robust and accurate PNT service only to TRNS mobile subscribers with selective availability and enhanced data security, but also exploits novel opportunities for signal situational awareness arising from the proximity and mutual audibility of the transmitting beacons. The implementation of this proposal renders TRNS more resilient against man-in-the-middle attacks than what is achievable with traditional GNSS.

7.1 Future Work

The MAC-leavened TESLA-based NMA scheme presented in Subsection 4.2.2 provides a degree of protection against half-duplex spoofing attacks, in that a potential spoofer can perturb a victim receiver's delay lock loop (DLL) output during the closed window. This level of protection is dependent on the victim receiver's local oscillator drift, and its un-modeled dynamics. A detailed analysis that quantifies the level of spoofing protection provided by the proposed NMA scheme would be an ideal next step for this thesis's first contribution.

The results presented in Section 5.5 are based on a post-correlation function that is computed across a correlation window of 20 chips. Future simulation can look into the use of bigger correlation window for enhanced visibility of the signal landscape in each accumulation interval.

Subsection 5.4.2 presents the improvement in detection and spoofer localization with the increase in the number of monitoring beacons. However, the GLRT network detector's performance results from a confluence of factors, which include the position geometry of the spoofer with the monitoring beacons, and the search-space discretization for the spoofer's geometric and temporal delay. Future work can provide a comprehensive analysis of the network's detection performance with respect to the above-mentioned factors, and look into a refined localization of the spoofer's position post-detection.

The autonomous SSA outlined in Chapter 5 is primarily based on symmetric difference (SD) metric, a hybrid signal quality metric that is based on both received power and correlation function distortion. Future work can look into the extraction of multiple features at different stages of single processing, such as antenna steering vector calculation, signal acquisition and tracking, and PVT calculation, to accurately characterize each signal component in the landscape [55]. Using multiple signal features for spoofer detection, in combination with joint detection across multiple epochs and over multiple beacons (outlined in Section 5.4) can drastically improve the capability of SSA.

The multipath propagation measurement campaign outlined in Chapter 6 was largely constrained within the campus ground for two reasons: 1. the use of campus Wifi for remote control of the transmitter and receiver, and 2. the ease of getting approval for outdoor experimentation. Future work can extend the measurement campaign to varied environments (e.g. suburban, and deep-urban) by setting up cellular-based remote access. In addition, one might consider the use of lower-level interfaces to the USRP with heuristics to automatically detect overruns and log them with timestamps.

Bibliography

[1] Dennis M Akos. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *Navigation, Journal of the Institute of Navigation*, 59(4):281–290, 2012.

[2] Jon M Anderson, Katherine L Carroll, Nathan P DeVilbiss, James T Gillis, Joanna C Hinks, Brady W O'Hanlon, Joseph J Rushanan, Logan Scott, and Renee A Yazdi. Chips-message robust authentication (Chimera) for GPS civilian signals. In *ION GNSS*, pages 2388–2416, 2017.

[3] Joel Barnes, Chris Rizos, Mustafa Kanli, David Small, Gavin Voigt, Nunzio Gambale, Jimmy Lamance, Terry Nunan, and Chris Reid. Indoor industrial machine guidance using Locata: A pilot study at BlueScope Steel. In *60th Annual Meeting of the US Inst. Of Navigation*, pages 533–540, 2004.

[4] Bjorn Bergman. AIS Ship Tracking Data Shows False Vessel Tracks Circling Above Point Reyes, Near San Francisco, 05 2020.

[5] Jahshan Bhatti and Todd E Humphreys. Hostile control of ships via false GPS signals: Demonstration and detection. *Navigation*, 64(1):51–66, 2017.

[6] Nuria Blanco-Delgado and Fernando D Nunes. Multipath estimation in multicorrelator GNSS receivers using the maximum likelihood principle. *IEEE Transactions on Aerospace and Electronic Systems*, 48(4):3222–3233, 2012.

[7] Daniele Borio. PANOVA tests and their application to GNSS spoofing detection. *IEEE Transactions on Aerospace and Electronic Systems*, 49(1):381–394, Jan. 2013.

[8] 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, April 2012. Institute of Navigation.

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

[10] Gianluca Caparra, Silvia Sturaro, Nicola Laurenti, and Christian 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)*, pages 1–6. IEEE, 2016.

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

[12] Koichi Chino, Dinesh Manandhar, and Ryosuke Shibasaki. Authentication technology using QZSS. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pages 367–372. IEEE, 2014.

[13] James T Curran and Matteo 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, pages 1–15, 2014.

[14] Quynh Dang. Recommendation for applications using approved hash algorithms (revised). SP 800-107, National Institute of Standards and Technology, Aug. 2007.

[15] Andrew G. Dempster and Ediz Cetin. Interference localization for satellite navigation systems. *Proceedings of the IEEE*, 104(6):1318–1326, June 2016.

[16] Fabio Dovis. *GNSS interference threats and countermeasures*. Artech House, 2015.

[17] Fabio Dovis, Musumeci Luciano, Beatrice Motella, and Emanuela Falletti. *GNSS interference threats and countermeasures*, chapter Classification of Interfering Sources and Analysis of the Effects on GNSS Receivers, pages 31–66. Artech House, 2015.

[18] Federal Communications Commission. Part 97 –Amateur Radio Service, Mar. 2018.

[19] Ignacio Fernández-Hernández, Vincent Rijmen, Gonzalo Seco-Granados, Javier Simon, Irma Rodríguez, and J David Calle. A navigation message authentication proposal for the Galileo open service. *Navigation*, 63(1):85–102, 2016.

[20] Jason Gross and Todd E Humphreys. GNSS spoofing, jamming, and multipath interference classification using a maximum-likelihood multi-tap multi-

path estimator. *Proceedings of the ION International Technical Meeting*, Jan. 2017.

[21] Jason N Gross, Cagri Kilic, and Todd E Humphreys. Maximum-likelihood power-distortion monitoring for GNSS-signal authentication. *IEEE Transactions on Aerospace and Electronic Systems*, 55(1):469–475, 2018.

[22] Peter Gutierrez. Galileo to Transmit Open Service Authentication. *Inside GNSS*, 2020.

[23] Mark Harris. Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai. *MIT Technology Review*, 11 2019.

[24] Li He, Hong Li, and Mingquan Lu. Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival. *GPS Solutions*, 23(3):78, 2019.

[25] Christopher Hegarty, Ali Odeh, Karl Shallberg, Kyle Wesson, Todd Walter, and Ken Alexander. Spoofing detection for airborne GNSS equipment. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pages 1350–1368, 2018.

[26] C.J. Hegarty. Analytical model for GNSS receiver implementation losses. *Navigation, Journal of the Institute of Navigation*, 58(1):29, 2011.

[27] Liang Heng, Daniel B Work, and Grace Xingxin Gao. Gps signal authentication from cooperative peers. *IEEE Transactions on Intelligent Transportation Systems*, 16(4):1794–1805, 2014.

[28] Todd E Humphreys. Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 49(2):1073–1090, 2013.

[29] Todd E. Humphreys. Lost in Space: How Secure Is the Future of Mobile Positioning?, 02 2016.

[30] Todd E. Humphreys. *Interference*, pages 469–503. Springer International Publishing, 2017.

[31] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W. O'Hanlon, and Paul M Kintner, Jr. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proceedings of the ION GNSS Meeting*, Savannah, GA, 2008. Institute of Navigation.

[32] Muhammad Usman Iqbal and Samsung Lim. Privacy implications of automated GPS tracking and profiling. *IEEE technology and society magazine*, 29(2):39–46, 2010.

[33] A. Jahn, S. Buonomo, M. Sforza, and E. Lutz. Narrow- and wide-band channel characterization for land mobile satellite systems: Experimental results at l-band. In *Publication: Proceedings of the Fourth International Mobile Satellite Conference (IMSC 1995)*. NASA, 1995.

[34] Ali Jafarnia Jahromi, Ali Broumandan, and Geard Lachapelle. Gnss signal authenticity verification using carrier phase measurements with multiple receivers. In *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–11. IEEE, 2016.

[35] Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[36] Andrew J. Kerns, Kyle D. Wesson, and Todd E. Humphreys. A blueprint for civil GPS navigation message authentication. In *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

[37] Faisal A Khan, Chris Rizos, and Andrew G Dempster. Novel time-sharing scheme for virtual elimination of locata-WiFi interference effects. In *Int. Symp. on GPS/GNSS*, pages 526–530, 2008.

[38] Faisal A Khan, Chris Rizos, and Andrew G Dempster. Locata performance evaluation in the presence of wide-and narrow-band interference. *Journal of Navigation*, 63(3):527, 2010.

[39] Samer Khanafseh, Naeem Roshan, Steven Langel, Fang-Cheng Chan, Mathieu Joerger, and Boris Pervan. GPS spoofing detection using RAIM with INS coupling. In *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*, pages 1232–1239. IEEE, 2014.

[40] Ronnie X.T. Kor, Peter A. Iannucci, and Todd E. Humphreys. Autonomous Signal-Situational Awareness in a Terrestrial Radionavigation System. 2021. Submitted for review.

[41] Ronnie X.T. Kor, Peter A. Iannucci, and Todd E. Humphreys. Comprehensive PNT Security for a Terrestrial Radionavigation System. *Navigation, Journal of the Institute of Navigation*, 2021. In preparation.

[42] Ronnie X.T. Kor, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys. A proposal for securing terrestrial radio-navigation systems. In *Proceedings of the ION GNSS+ Meeting*, Online, 2020.

[43] Brent M. Ledvina, William J. Bencze, Bryan Galusha, and Isaac 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.

[44] Dong-Kyeong Lee, Filip Nedelkov, Dennis Akos, and Byungwoon Park. Barometer Based GNSS Spoofing Detection. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pages 3268–3282, 2020.

[45] Young C Lee and Daniel G O'Laughlin. Performance Analysis of a Tightly Coupled GPS/Inertial System for Two Integrity Monitoring Methods 1. *Navigation*, 47(3):175–189, 2000.

[46] Andreas Lehner. *Multipath Channel Modelling for Satellite Navigation Systems*. Shaker, 2007. ISBN: 978-3-8322-6651-6.

[47] Andreas Lehner and Alexander Steingaß. Characteristics of the Land Mobile Navigation Channel for Pedestrian Applications. In *Proceedings of the GNSS 2003, European Navigation Conference*, 2003.

[48] Andreas Lehner and Alexander Steingass. A novel channel model for land mobile satellite navigation. In *Proceedings of the ION GNSS Meeting*, pages 13–16, 2005.

[49] Sherman Lo, David DeLorenzo, Per Enge, Dennis Akos, and Paul Bradley. Signal authentication. *Inside GNSS*, 0(0):30–39, Sept. 2009.

[50] Sherman C Lo and Per K Enge. Authenticating aviation augmentation system broadcasts. In *IEEE/ION Position, Location and Navigation Symposium*, pages 708–717. IEEE, 2010.

[51] Davide Margaria, Beatrice Motella, Marco Anghileri, Jean-Jacques Floch, Ignacio Fernandez-Hernandez, and Matteo Paonni. Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives. *IEEE Signal Processing Magazine*, 34(5):27–37, 2017.

[52] Emily McMilin, David S De Lorenzo, Todd Walter, Thomas H Lee, and Per 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*, pages 2233–2242. Citeseer, 2014.

[53] S Meiyappan, A Raghupathy, and G Pattabiraman. Positioning in GPS challenged locations-the NextNav terrestrial positioning constellation. *Proc. ION GNSS+ 2013*, 2013.

[54] Subbu Meiyappan, Arun Raghupathy, and Ganesh Pattabiraman. *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, volume 2, chapter Position, Navigation and Timing with Dedicated Metropolitan Beacon Systems, pages 1225–1241. Wiley-IEEE, 2020.

[55] J Merwe, Ana Nikolikj, Sebastian Kram, Ivana Lukcin, Gorjan Nadzinski, Alexander Rügamer, and Wolfgang Felber. Blind Spoofing Detection for Multi-Antenna Snapshot Receivers using Machine-Learning Techniques. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pages 3294–3312, 2020.

[56] Michael Meurer, Andriy Konovaltsev, Manuel Cuntz, and Christian 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.

[57] Paul Y. Montgomergy, Todd E. Humphreys, and Brent M. Ledvina. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna re-

ceiver defense against a portable civil GPS spoofer. In *Proceedings of the ION International Technical Meeting*, Anaheim, CA, Jan. 2009.

[58] Matthew J. Murrian, Lakshay Narula, and Todd E. Humphreys. Characterizing terrestrial GNSS interference from low earth orbit. In *Proceedings of the ION GNSS+ Meeting*. Institute of Navigation, Oct. 2019.

[59] Lakshay Narula and Todd E. Humphreys. Requirements for secure clock synchronization. *IEEE Journal of Selected Topics in Signal Processing*, 12(4):749–762, Aug. 2018.

[60] Andrew Neish, Todd Walter, and Per Enge. Quantum-resistant authentication algorithms for satellite-based augmentation systems. *Navigation*, 66(1):199–209, 2019.

[61] Andrew Neish, Todd Walter, and J David Powell. Design and analysis of a public key infrastructure for sbas data authentication. *Navigation*, 66(4):831–844, 2019.

[62] NIST. Recommendation for key management—Part I: General (revised). SP 800-57, National Institute of Standards and Technology, July 2012.

[63] B.W. O'Hanlon, M.L. Psiaki, J.A. Bhatti, and T.E. Humphreys. Real-time spoofing detection using correlation between two civil GPS receiver. In *Proceedings of the ION GNSS Meeting*, Nashville, Tennessee, 2012. Institute of Navigation.

[64] A. Perrig, R. Canetti, J.D. Tygar, and D. Song. The TESLA broadcast authentication protocol. *RSA CryptoBytes*, 5(2):2–13, 2002.

[65] Jean-Paul Poncelet and Dennis 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*, pages 1–6. IEEE, 2012.

[66] Mark Psiaki, Steven P. Powell, and Brady W. O'Hanlon. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In *Proceedings of the ION GNSS+ Meeting*, pages 2949–2991, 2013.

[67] Mark L Psiaki and Todd E Humphreys. GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, 2016.

[68] Mark L. Psiaki and Todd E. Humphreys. *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, volume 1, chapter Civilian GNSS Spoofing, Detection, and Recovery, pages 655–680. Wiley-IEEE, 2020.

[69] Mark L. Psiaki, Brady W. O'Hanlon, Steven P. Powell, Jahshan A. Bhatti, Todd E. Humphreys, and Andrew Schofield. GNSS lies, GNSS truth: Spoofing detection with two-antenna differential carrier phase. *GPS World*, 25(11):36–44, Feb. 2014.

[70] Mark L. Psiaki, Brady W. O'Hanlon, Steven P. Powell, Jahshan A. Bhatti, Kyle D. Wesson, Todd E. Humphreys, and Andrew Schofield. GNSS spoofing

detection using two-antenna differential carrier phase. In *Proceedings of the ION GNSS+ Meeting*, Tampa, FL, 2014. Institute of Navigation.

[71] M.L. Psiaki, B.W. O'Hanlon, J.A. Bhatti, D.P. Shepard, and T.E. Humphreys. GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Transactions on Aerospace and Electronic Systems*, 49(4):2250–2267, 2013.

[72] Theodore S Rappaport et al. *Wireless communications: principles and practice*, volume 2. prentice hall PTR New Jersey, 1996.

[73] Theodore S Rappaport, Scott Y Seidel, and Rajendra Singh. 900-MHz multipath propagation measurements for US digital cellular radiotelephone. *IEEE Transactions on Vehicular Technology*, 39(2):132–139, 1990.

[74] Chris Rizos, Dorota A Grejner-Brzezinska, Charles K Toth, Andrew G Dempster, Yong Li, Nonie Politi, Joel Barnes, and Hongxing Sun. A hybrid system for navigation in GPS-challenged environments: Case study. *Proceedings, ION GNSS, Savannah, Georgia, Sept*, pages 16–19, 2008.

[75] Chris Rizos, Gethin Roberts, Joel Barnes, and Nunzio Gambale. Experimental results of Locata: A high accuracy indoor positioning system. In *2010 International Conference on Indoor Positioning and Indoor Navigation*, pages 1–7. IEEE, 2010.

[76] Chris Rizos and Ling Yang. Background and recent advances in the locata terrestrial positioning and timing technology. *Sensors*, 19(8):1821, 2019.

[77] Christian Rocken and Charles Meertens. Monitoring selective availability dither frequencies and their effect on GPS data. *Bulletin géodésique*, 65(3):162–169, 1991.

[78] Akmal Rustamov, Neil Gogoi, Alex Minetto, and Fabio Dovis. Gnss Anti-Spoofing Defense Based on Cooperative Positioning. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pages 3326–3337, 2020.

[79] Logan Scott. Anti-spoofing and authenticated signal architectures for civil navigation systems. In *Proceedings of the ION GNSS Meeting*, pages 1542–1552, 2003.

[80] Logan Scott. *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, volume 1, chapter Interference: Origins, Effects, and Mitigation, pages 619–653. Wiley-IEEE, 2020.

[81] Elvino S Sousa, Vladan M Jovanovic, and Christian Daigneault. Delay spread measurements for the digital cellular channel in Toronto. *IEEE Transactions on Vehicular Technology*, 43(4):837–847, 1994.

[82] J J Spilker, Jr. *Global Positioning System: Theory and Applications*, chapter 20: Interference Effects and Mitigation Techniques, pages 717–771. American Institute of Aeronautics and Astronautics, Washington, D.C., 1996.

[83] Alexander Steingass and Andreas Lehner. Characteristics of the Land Mobile Navigation Channel for Car Applications. In *Proceedings*, 2003.

[84] Alexander Steingass and Andreas Lehner. Measuring the navigation multipath channel–a statistical analysis. In *Proceedings of the 17th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2004)*, pages 1157–1164, 2004.

[85] Alexander Steingass and Andreas Lehner. Differences in multipath propagation between urban and suburban environments. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pages 602–611, 2008.

[86] Tetsu Tanaka, Shigeru Kozono, and Akira Akeyama. Urban multipath propagation delay characteristics in mobile communications. *Electronics and Communications in Japan (Part I: Communications)*, 74(8):80–88, 1991.

[87] George L. Turin, Fred D. Clapp, Tom L. Johnston, Stephen B. Fine, and Dan Lavry. A statistical model of urban multipath propagation. *IEEE Transactions on Vehicular Technology*, VT-21(1), Feb. 1972.

[88] A. J. Van Dierendonck, Pat Fenton, and Tom Ford. Theory and performance of narrow correlator spacing in a GPS receiver. *Navigation, Journal of the Institute of Navigation*, 39(3):265–283, Fall 1992.

[89] Richard D. J. van Nee. Spread-spectrum code and carrier synchronization errors caused by multipath and interference. *IEEE Transactions on Aerospace*

and Electronic Systems, 29(4):1359–1365, 1993.

[90] Harry L. Van Trees. *Detection, Estimation, and Modulation Theory*. Wiley, 2001.

[91] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans. GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2):739–754, April 2018.

[92] Kyle D. Wesson, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *Proceedings of the ION GNSS Meeting*, Portland, OR, 2011.

[93] Chris Wullems, Oscar Pozzobon, and Kurt Kubik. Signal authentication and integrity schemes for next generation global navigation satellite systems. In *Proc. European Navigation Conference GNSS*, Munich, July 2005.

[94] Peng Xie and Mark G Petovello. Measuring GNSS multipath distributions in urban canyon environments. *IEEE Transactions on Instrumentation and Measurement*, 64(2):366–377, 2014.

[95] Chun Yang, Andrey Soloviev, Michael Veth, and Di 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*, pages 394–403, 2016.