GPS SPOOFING DETECTION FOR THE POWER GRID NETWORK VIA A MULTI-RECEIVER HIERARCHICAL ARCHITECTURE

BY

TARA MINA

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2019

Urbana, Illinois

Adviser:

Assistant Professor Grace Xingxin Gao

ABSTRACT

In the process of modernizing the North American electric power grid with the creation of the *Smart Grid*, thousands of devices called phasor measurement units (PMUs) have been deployed across the U.S. continent to continuously monitor the power grid state in real-time. Each PMU measures voltage and current phasors at its local substation, then synchronizes these measurements across the continental network using the Global Positioning System (GPS) as a common timing reference. GPS serves as an excellent timing source due to its global coverage as well as its precise, sub-microsecond level timing accuracy. However, because civilian GPS signals are unencrypted with a publicly available signal structure, any individual with the appropriate equipment can mimic these signals in order to establish a false timing solution at the PMU sites. This type of attack, commonly known as *GPS spoofing*, presents a major concern to our future power grid infrastructure. Indeed, even minor timing manipulations can cause inaccurate power flow representations and corresponding corrective measures, potentially inducing large-scale power disruptions, instability within the power grid, and/or damage to generators and other power equipment.

In this thesis, we present a multi-receiver spoofing detection algorithm for PMU devices, utilizing a hierarchical architecture framework. For the received GPS signal at each PMU station, we create conditioned signal fragments containing the military P(Y) GPS signal, which bears a binary spreading code sequence that is unavailable to civilian users and thus cannot be forged by an attacker. As a result, the military P(Y) signal establishes an encrypted signature in the background of all authentic GPS signals. The presence of the authentic signature can be verified, without knowledge of the precise bit sequence, by correlating amongst conditioned signal fragments obtained from other PMU sites in a sub-network of cross-check receivers, thereby leveraging the secure communication network available within the

power grid infrastructure. We further defend against coordinated spoofing attacks conducted against the sub-network of PMU devices by comparing condensed, representative signals generated for each sub-network within the power grid. Using real-world data recorded during a government-sponsored, live-sky spoofing event, we demonstrate that our algorithm successfully evaluates the authenticity of each receiver in a widely dispersed network.

ACKNOWLEDGMENTS

First, I would like to thank my thesis adviser, Professor Grace Gao, for her inspiring presence as well as her guidance in the research presented in this thesis. In addition to expediting my growth as a researcher through her thoughtful advisement, Professor Gao's positive spirit and enthusiasm to explore new areas always gave me excitement after our meetings and encouraged me to take risks during the master of science program. I am thoroughly grateful to have had such a remarkable adviser and mentor these past two years.

I would additionally like to thank my academic adviser, Professor Jonathan Makela, for his continuous support as well as his enthusiastic, thoroughly engaging teaching style of ECE 456: Introduction to GPS. Besides providing me with the core academic foundations of this research area, Professor Makela, through his teaching, also facilitated my growing passion and admiration for the originally unfamiliar, multi-disciplinary field of GPS navigation. To this day, I still occasionally peruse his well-crafted lecture notes to recapture past moments of curious insight and intellectual captivation.

To Professor Jade Morton at the University of Colorado Boulder, as well as Mr. Steve Taylor, I would like to thank you for helping us collect GPS data across the entire Western Hemisphere in Colorado, Ohio, Peru, and Chile.

Furthermore, thank you to my lab members: Cara Yang, Arthur Chu, Craig Babiarz, and Matthew Peretic for assisting with the experimental setup and GPS data collection at the Illinois site as well as the Western U.S. receiver spoofing site. I would also like to thank Ramya Bhamidipati in my research group for her hands-on partnership throughout this research; I thoroughly enjoyed working on this project with one of the most delightful, bright, and enthusiastic people I have ever met.

I would also like to more broadly thank all of my lab members and friends for such a memorable experience at Urbana-Champaign, including Siddharth

Tanwar, Ashwin Kanhere, Enyu Luo, Akshay Shetty, Shubhendra Chauhan, Shubh Gupta, Katherine Tsai, Pulkit Rustagi, and Prateek Ranjan. The closing of this special chapter is a bit bittersweet. But I look forward to the many exciting, unwritten chapters of our lives ahead! Thanks for all the great times along the way; it truly was a phenomenal ride.

Finally, I would like to thank my parents for their constant support and words of encouragement. Their patience throughout my childhood and unrelenting confidence in my abilities enabled me to accomplish my academic goals throughout my life.

The material in this thesis is based upon work funded by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) under contract number HSHQDC-17-C-B0025. The material in this thesis represents the views and opinions of the author and not necessarily those of the DHS.

TABLE OF CONTENTS

LIST OF FIGURES viii

LIST OF ABBREVIATIONS ix

CHAPTER 1 INTRODUCTION 1
1.1 Susceptibility of PMU Devices to GPS Spoofing 2
1.2 Feasibility of GPS Spoofing 3
1.3 Proposed GPS Spoofing Detection Strategies in Prior Literature 4
1.4 Contribution of Thesis 8
1.5 Thesis Outline 9

CHAPTER 2 BACKGROUND ON GPS 10
2.1 GPS L1 Signal Representation 10
2.2 Processing Steps Performed at GPS Receivers 12

CHAPTER 3 BACKGROUND ON GPS SPOOFING 16
3.1 GPS Jamming and Spoofing 16
3.2 Types of GPS Spoofing Attacks 17
3.3 Conducting a GPS Spoofing Attack 19

CHAPTER 4 MULTI-RECEIVER COMMUNICATION ARCHITECTURE 20
4.1 NASPInet 20
4.2 Hierarchical Architecture Framework 21
4.3 Data Format Considerations 23

CHAPTER 5 SPOOFING DETECTION ALGORITHM 26
5.1 Generation of Conditioned Signal Fragments at Each Receiver 26
5.2 Authentication within the PMU Sub-Network 28
5.3 Formation of Representative GPS Signals for the Given PMU Sub-Network 32
5.4 Evaluation of the Final Spoofing Decision 34
5.5 Detection during Meaconing 37
5.6 Detection during Data-level Spoofing 39

CHAPTER 6 EXPERIMENTATION 40
6.1 Experimental Setup 40
6.2 Examples of Cross-Correlation Plots 42
6.3 Evaluating Preliminary Spoofing Decision 45
6.4 Verifying Preliminary Spoofing Decision using Representative Signals from Other Sub-Networks 48

CHAPTER 7 CONCLUSION AND FUTURE WORK 52

REFERENCES 54

LIST OF FIGURES

1.1 Network of PMUs monitoring critical substations 1
1.2 Utilizing military GPS signal as a spoofing signature 7

2.1 Components of GPS L1 C/A and L1 P(Y) signals 11
2.2 GPS acquisition plot of two-dimensional signal search space . 13
2.3 GPS receiver tracking loops 14
2.4 Early, Prompt, and Late code replicas 15

3.1 Data-level spoofing using a nulling signal 18
3.2 Commandeering receiver tracking loops during spoofing 19

4.1 NASPInet communication architecture network 21
4.2 Proposed hierarchical architecture framework 22
4.3 High-level process diagram of spoofing detection algorithm . . 23

5.1 Authentication within a PMU sub-network 29
5.2 Final authentication step using representative signals 35

6.1 Rooftop antenna setup in Urbana, Illinois 41
6.2 Hierarchical network setup with receiver stations 42
6.3 Typical pairwise cross-correlation plots 43
6.4 Authentic cross-correlation with induced side correlations . . . 44
6.5 Evaluating preliminary spoofing statistics 45
6.6 Preliminary threshold meeting false alarm probability 47
6.7 Cumulative statistics for both sub-networks 48
6.8 Evaluating secondary spoofing statistics 49
6.9 Secondary threshold meeting false alarm probability 50
6.10 Secondary statistic for representative signals 51

LIST OF ABBREVIATIONS

AGC	Automatic Gain Control
C/A	Coarse Acquisition (civilian GPS signal)
CDMA	Code Division Multiple Access
CDMU	Central Decision-Making Unit
CSAC	Chip-Scale Atomic Clock
DoD	Department of Defense
GNSS	Global Navigation Satellites and Systems
GPS	Global Positioning System
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
MAC	Message Authentication Code
MEO	Medium Earth Orbit
NASPI	North American Synchrophasor Initiative
NMA	Navigation Message Authentication
PDC	Phasor Data Concentrator
PM	Power Monitoring
PMU	Phasor Measurement Unit
PRN	Pseudorandom Noise (Code)
SDR	Software Defined Receiver
SNR	Signal-to-Noise Ratio

SQM	Signal Quality Monitoring
SSSC	Spread Spectrum Security Codes
TESLA	Timed Efficient Streamed Loss-Tolerant Authentication
VSD	Vestigial Signal Defense

CHAPTER 1

INTRODUCTION

In Title XIII of the Energy Independence and Security Act of 2007 (EISA), the U.S. government endorsed a new, major effort to modernize the North American electric power grid with the creation of the *Smart Grid* [1]. The EISA officially defined the Smart Grid and described its key elements, including the implementation of a wide-area network of measurement devices to monitor the power grid state. Currently, this feature is largely comprised of a network of nearly 3000 phasor measurement units (PMUs), devices that measure voltage and current phasors at critical substations [2], tagging each with a precise time-stamp using GPS. A map of the widely dispersed PMU network is shown in Fig. 1.1.

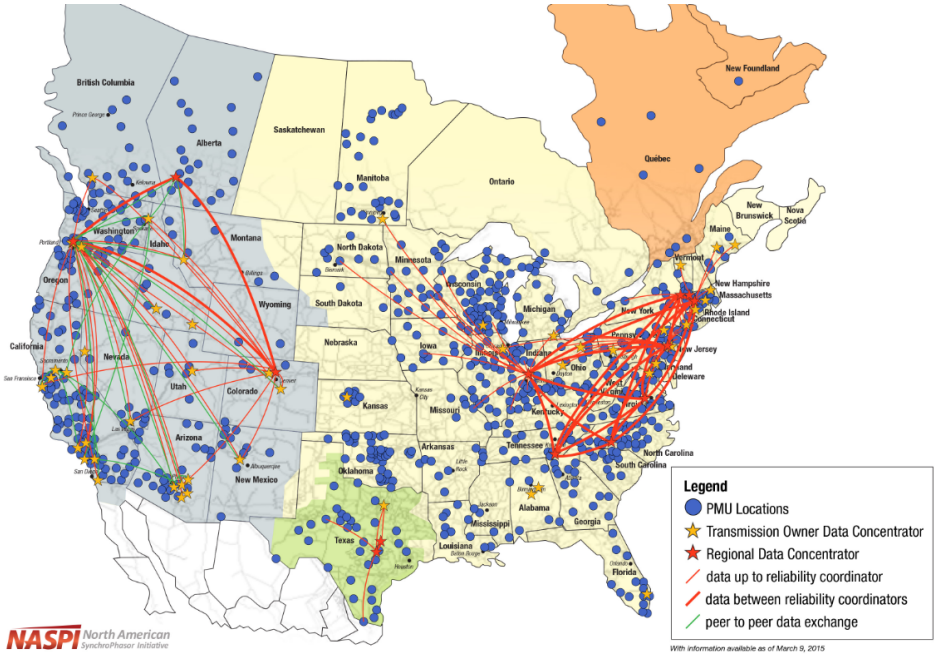


Figure 1.1: Network of PMUs monitoring critical substations [2]

However, security was not a primary design consideration of civilian GPS. Indeed, the civilian GPS signal is not only weak, with received power lev-

els on the order of 10^{-16} Watts, but it is also unencrypted, with a clearly outlined signal structure in publicly available interface specifications [3]. As a result, any individual with the right equipment can mimic the authentic GPS signals and establish a false position and/or timing solution at a victim receiver [4]. This type of attack, commonly known as *GPS spoofing*, presents a major concern to our power grid infrastructure, where even minor timing manipulations could lead to significant disruptions as discussed in Section 1.1. For the future Smart Grid, this vulnerability could be exploited to induce a false timing solution at one or more critical substations. According to the IEEE Std. C37.242-2013 [5], the timing accuracy for PMU devices must be correct to within 26 μs for a 60 Hz system, with a recommended timing accuracy on the order of 1 μs.

1.1 Susceptibility of PMU Devices to GPS Spoofing

Researchers have investigated the ability to induce false timing solutions in PMU devices via GPS spoofing [6], as well as the potential resulting effects on automatic PMU-based power control schemes within the network [7], which will become increasingly common as the power grid network undergoes modernization efforts. Indeed, timing inaccuracies significantly greater than the IEEE C37.118 standard requirement could induce a generator to trip [8]. At critical substations, the resulting additional load placed on neighboring stations could induce these generators to trip, potentially resulting in cascading failures and large-scale blackouts, similar to the Northeastern blackout of 2003 [9]. These outages are not only costly, with an estimated $6 billion for the Northeastern blackout [10], but can also be harmful to the public and possibly lethal. In fact, evaluation of the effects of the Northeastern blackout on New York City show that mortality rates increased by nearly 25% during August 2003, the month of the power outage [11].

Currently, none of the receivers incorporated within the U.S. power grid employ even basic protection against spoofing. As a result, all PMU devices are defenseless to even the simplest spoofing attacks. In this work, we propose a multi-receiver spoofing detection algorithm using a wide-area, hierarchical architecture framework. In our solution, each PMU transmits conditioned GPS signal fragments containing the encrypted military GPS signal, which

serves as a cryptographic signature present in the background of all authentic GPS signals. We then leverage the available redundancy and geographic diversity of the receivers in the power grid to compare the received signature among the network and authenticate each receiver in a coordinated manner. Finally, to validate our approach, we test our approach using recorded GPS signals during a government-sponsored, live-sky spoofing event, demonstrating the ability of our algorithm to successfully evaluate the authenticity of each receiver in a widely dispersed network.

1.2 Feasibility of GPS Spoofing

Since the invention and initial deployment of GPS, experts in the GNSS community understood that GPS spoofing was indeed technically possible, but generally considered it to be too complicated to present a realistic threat, making the menace largely hypothetical. However, the development of a portable civilian GPS spoofer and chilling demonstration of a successful attack on a common commercial receiver in 2008 [12] spurred interest from the GNSS research community. Since this study, interest in the field grew and GPS/GNSS researchers worldwide subsequently sought to characterize spoofing attacks [13] as well as develop numerous counter-measures and detection strategies. See Section 1.3 for an overview of proposed spoofing detection strategies in prior literature.

One may be eager to assuage the sudden concern for GPS spoofing by rationalizing that the portable spoofer attack demonstration in [12] was conducted by capable experts in the field. However, the threat for GPS spoofing is becoming more imminent. Programmable GPS signal simulators are readily available for purchase [14], as well as for rent at less than $1k per week [15]. Additionally, with the development of reprogrammable software defined receivers (SDR), technically capable attackers can design and perform more advanced spoofing attacks which are synchronized with the authentic GPS signal, as demonstrated in [12]. Developing the software program to conduct this type of a spoofing attack certainly requires technical propensity; however, if such a script becomes available online, any individual with a reprogrammable receiver can download the software from the Internet and run his or her own spoofing device. In fact, in 2015, software for a GPS sig-

nal simulator was publicly posted to GitHub with detailed instructions for generating a user-dened GPS signal and creating the corresponding radio-frequency signal via multiple potential SDR platforms [16].

1.3 Proposed GPS Spoofing Detection Strategies in Prior Literature

Proposed spoofing countermeasures include use of directional antennas to detect the origin of the incoming signal and comparing these measurements with the expected azimuth and elevation for each PRN [17, 18, 19]. This approach is useful for PMUs in the power grid, which have access to satellite ephemeris data from external sources and can thus immediately verify the received angle of each satellite PRN signal. However, this approach could lead to missed detections of spoofing for satellites lower in elevation and is not immune to spoofing attacks with multiple transmitters.

Angle-of-arrival techniques have also been explored using dual- or multi-antenna arrays [20] - [21] to detect carrier-phase single differences for different satellite signals. These techniques exploit the fact that the spoofing signal comes from a single transmission direction, resulting in identical carrier phase differences between antennas for each signal channel, unlike with the authentic GPS satellites, which have diverse geometric relationships between the antenna arrays, resulting in a multiplicity of received carrier phase differences. However, these angle-of-arrival techniques assume that the spoofing signal comes from a single source. In the case that the attacker uses separate transmitters for each spoofed signal, this method can no longer detect the spoofing attack using the identical received carrier phase single-differences between channels.

The Vestigial Signal Defense also provides a promising spoofing detection approach, by monitoring signal distortions in the complex correlation domain, induced by the interference between the authentic and spoofed GPS signal peaks during the onset of an attack [22]. This would be especially useful for immediate, single-receiver authentication at each station. However, missed detections could occur if the attacker also broadcasts a nulling signal to remove the vestige of the authentic signal peak. Indeed, this type of attack is challenging to execute effectively, for the spoofer must transmit

a spoofing signal that maintains precise carrier phase alignment with respect to the authentic signal received by the victim. As a result, to successfully null the authentic GPS signal, the spoofer requires centimeter-level accurate knowledge of the victim position, which certainly presents a key challenge in many navigation applications. However, this challenge becomes easier to overcome when the target is a permanent, stationary receiver, such as with receivers within the power grid network.

Techniques for spoofing detection by monitoring the received signal power from Automatic Gain Control (AGC) measurements have been proposed [23], in order to detect the increase in received power as a spoofer attempts to commandeer the receiver tracking loops. However, even a minor power ratio of 1.1 with the authentic GPS signal can reliably induce the victim receiver to track the spoofing signal [24]. As a result, such a detector may be overly sensitive to typical variations in the received signal power caused by solar and atmospheric effects.

Detection techniques have been examined which utilize both the received signal-to-noise ratio (SNR), called Signal Quality Monitoring (SQM), as well as the received power [25] to detect a spoofing attack. This technique is indeed quite promising for a single-receiver, since the SQM and Power Monitoring (PM) spoofing detection tests are complementary in which types of spoofing attacks can be detected. In particular, for spoofing attacks where the spoofer utilizes a slight power advantage with respect to the authentic signal, the PM technique is susceptible to frequent missed detections. However, the SQM test has the most powerful detection with these types of spoofing attacks, due to significant asymmetries induced in the cross-correlation function. Correspondingly, for high-power spoofing attacks, where the spoofer overpowers the authentic signal, the PM technique readily detects the spoofing attack, whereas the SQM test performs weakly due to limited distortion of the cross-correlation function caused by the authentic signal peak. However, similar to VSD, the combined PM and SQM detection approach also assumes that the spoofer cannot sufficiently null the authentic satellite signal and rely on its inevitable presence to flag degradations in the received GPS signal quality.

1.3.1 Cryptographic Authentication Techniques

Incorporating Cryptographic Authentication in Future GPS Signals

Suggestions have also been made to modify the civilian signal structure by including an encrypted sequence of bits in the navigation message for authentication [26] - [27] or by using Spread Spectrum Security Codes (SSSCs) [28] - [29]. An authentication scheme proposed for the L1C signal of the future GPS III constellation is called Chips-Message Robust Authentication (Chimera) [30], which authenticates the navigation signal using a hybrid approach between classical NMA and SSSCs. In particular, via the Chimera authentication scheme, satellites periodically create a digital signature for the navigation data message using a private key as well as the navigation message itself. Users with access to a public key can authenticate the received signature, but cannot predict the signature beforehand. Chimera additionally introduces a corresponding signature on the L1C pilot signal, by overriding or *puncturing* specific spreading code chips with bit *markers*, where the bit marker sequence and marker placement within the spreading code can be determined and verified by the receiver using the navigation message digital signature. By signing both the navigation message as well as the pilot signal, if implemented, Chimera would allow for authentication of both in-phase and quadrature-phase components of the L1C signal.

Another interesting proposed cryptographic authentication approach is called Timed Efficient Streamed Loss-Tolerant Authentication (TESLA) [31], the authentication scheme of which was originally proposed by [32] - [33] for multicast Internet applications. TESLA utilizes a chain of private keys, which can be sequentially generated using a one-way hash function $f(k_{i-1}) = k_i$. A sequence of length N private keys is first generated using the one-way function f and pre-loaded onto the satellites. The satellites then use each private key in *reverse* order (first using key k_N, then key k_{N-1}, and so on) to periodically sign the navigation message with a digital signature, called a Message Authentication Code (MAC). After digitally signing the navigation message, at a later time, the satellite also sends the corresponding private key k_i used to generate the MAC, thereby allowing the user to verify the digital signature. To verify the authenticity of the private key, the user can utilize the upcoming private key broadcast by the satellites k_{i-1}, and verify

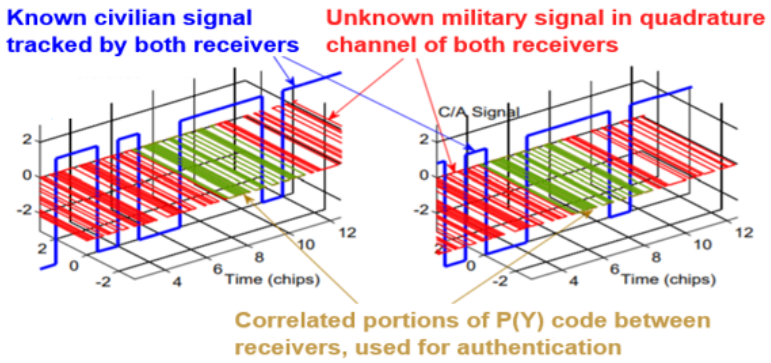


Figure 1.2: Utilizing the orthogonal encrypted military P(Y) GPS signal for spoofing detection by cross-correlation with the received signal at a trusted reference station. Figure adapted from [34].

the private keys are sequential, using the one-way function $f(k_{i-1}) = k_i$. Because f is designed to be difficult to invertible, an attacker cannot predict the correct sequence of digital keys in a computationally efficient manner.

Because the currently broadcast civilian navigation messages (L1 C/A, L2C, and L5) do not use cryptographic techniques, these proposals for modifying the broadcast satellite signals are largely targeted toward the modern L1C signal, to be first broadcast on the GPS Block III satellites and allowing for flexible message types, as well as the Galileo E1 OS signal. However, to date, these civilian authentication schemes do not currently have plans to be incorporated in the future navigation signals.

Cryptographic Techniques Leveraging the Current GPS Military Signal

Although the civilian GPS signals do not currently have any encryption available, orthogonal to the civilian GPS signal lies the military P(Y) GPS signal, which is encrypted and therefore cannot be generated by a spoofer. As a result, this signal in the received quadrature channel can be *presently* utilized as a type of signature in the background of all authentic GPS signals. Although as civilians we do not have access to the encryption key, we can verify the presence of the encrypted signal by extracting the received signal from the quadrature-phase channel and correlating against the corresponding conditioned signal sample from another cross-check receiver, as portrayed in Fig. 1.2. If both devices receive authentic GPS signals, the correlation results in a strong correlation peak due to the matching encrypted military signal. Oth-

erwise, if one receiver is spoofed, the orthogonal component of the spoofed signal lacks a correlation with the authentic P(Y) codes.

This approach of utilizing the encrypted military signal from a trusted reference station to authenticate the received GPS signal has been proposed and demonstrated in [35] - [36]. Furthermore, the 20.46 MHz encrypted military signal can be significantly under-sampled below the Nyquist rate with a narrow front-end bandwidth, resulting in an attenuated and distorted vestige of the encrypted signal, which can still be utilized as a signature for authentication between receivers. In fact, Lo et al. [35] demonstrate this technique using a 15 MHz sampling rate, and the experiments in [36] - [37] sample the signal at a rate of 5.714 MHz while additionally utilizing a narrow front-end bandwidth of 2.5 MHz. Furthermore, our research group's prior work has shown that a receiver can be authenticated for GPS spoofing by using a handful of inexpensive cross-check receivers, which may be unreliable or potentially also spoofed [38].

1.4 Contribution of Thesis

This thesis presents a multi-receiver spoofing detection approach, which leverages the widespread nature of these synchronization networks in order to collaboratively detect a GPS spoofing attack, while simultaneously authenticating all other receivers in the wide-area network. The contributions of this work can be sub-divided into the following aspects:

1. This work presents a multi-receiver hierarchical communication architecture, which authenticates the received signal at each PMU in the widely dispersed network [39, 40, 41].

2. We further defend against a coordinated spoofing attack which targets a collections of cross-check receivers by generating representative signals to compare with multiple sub-network sites, while reducing bandwidth requirements.

3. Additionally, we validate our spoofing detection approach using real-world GPS spoofing scenarios recorded during a government-sponsored, live-sky spoofing event, thereby demonstrating our algorithm can suc-

cessfully evaluate the signal authenticity at each receiver in a widely dispersed network.

1.5 Thesis Outline

The remainder of this thesis is organized in the following chapters:

- Chapter 2 provides background on the Global Positioning System (GPS) as well as processes performed at GPS receivers to acquire and track the signal to derive a position and timing solution.
- Chapter 3 describes different types of GPS spoofing attacks and outlines the steps performed by a stealthy spoofing attack which gradually commandeers the victim receiver tracking loops.
- Chapter 4 introduces our hierarchical spoofing detection architecture, provides a high-level overview of the data flow and processing steps of the algorithm, and assesses the required communication bandwidth.
- Chapter 5 details the complete multi-receiver spoofing detection algorithm, describing the method of conditioning the received signals, evaluating the signal authenticity among a sub-network of cross-check receivers, then efficiently verifying the preliminary spoofing detection by comparing signals on a larger scale, across multiple sub-networks.
- Chapter 6 presents our experimental results and our analysis on the spoofing statistics, describing our selection of the spoofing detection thresholds.
- Chapter 7 concludes this thesis and describes future research directions.

CHAPTER 2

BACKGROUND ON GPS

The Global Positioning System (GPS) was originally developed as a utility for the Department of Defense (DoD) which would continuously provide three-dimensional, global localization with high accuracy and reliability. To meet this objective, the key design engineers, Roger L. Easton, Ivan A. Getting, and Bradford W. Parkinson, developed the following key specifications for the satellite system [42]:

- Minimum number of 24 satellites in Medium Earth Orbit (MEO) (typically altitudes between $10000 - 25000$ km) for sufficient global coverage
- 6 orbital planes for inexpensive reconfiguration and station-keeping of satellites at 55° inclination
- L-band carrier frequency ($1 - 2$ GHz), since in the 1970s this frequency band was less occupied and GPS required at least 20 MHz. Additionally, frequencies below 1 GHz have significantly greater ranging error due to ionospheric refraction, while atmospheric attenuation increases at higher frequencies

Currently, GPS consists of 31 operational satellites, orbiting at an altitude of $20,200$ km above the surface of the Earth. In this thesis, we utilize the L1 GPS signal, broadcast at a carrier frequency of $f_{L1} = 1575.42$ MHz. In this frequency band, each GPS satellite broadcasts the legacy civilian signal, L1 C/A, as well as the military P(Y) signal in the orthogonal, quadrature-phase channel.

2.1 GPS L1 Signal Representation

Both the civilian and military GPS signals have 3 main components, as shown in Fig. 2.1 and outlined below:

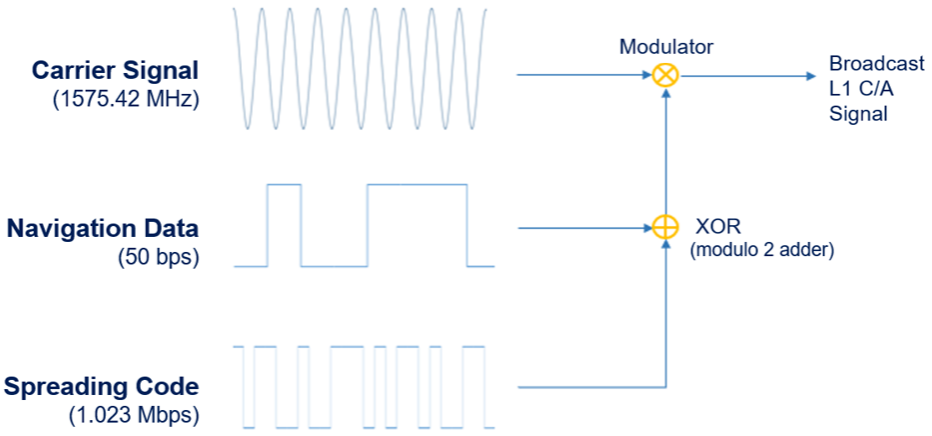


Figure 2.1: Main components of GPS L1 C/A and L1 P(Y) signals

1. *Sinusoidal carrier* - an analog, sinusoidal wave at the L1 frequency f_{L1}, represented simply by the trigonomic functions $\cos(\cdot)$ or $\sin(\cdot)$. This component modulates the navigation signal to lie in the allocated L1 frequency band

2. *Data signal* - a sequence of binary values (± 1) modulating the sinusoidal carrier. Each satellite transmits the binary signal at the leisurely pace of 50 data bits, or *chips*, per second (cps). This signal contains the navigation data, including the ephemeris for the broadcasting satellite, which allows the receiver to compute the precise satellite position. The navigation data signal is completely known, and is identical for both the civilian and military signals.

3. *Spreading code* - a high-frequency sequence of binary values modulating the combined sinusoidal and data signals. The spreading code or pseudorandom noise (PRN) code is a deterministic binary sequence unique to each GPS satellite and allows each of the 31 operational satellites to broadcast in the same frequency band without inter-signal interference through Code Division Multiple Access (CDMA).

   With knowledge of the spreading code sequence, the GPS receiver can access each satellite signal separately. Civilian users have access to the civilian spreading code, but not the military codes. As a result, the military GPS signal is encrypted and not usable for non-military users. The civilian spreading code is 1023 chips long and broadcasts at a rate

of 1.023 Mcps, thus sending a complete spreading code sequence every 1 ms, whereas the military P(Y) code broadcasts ten times faster, at 10.23 Mcps. Typical civilian GPS front-end receivers have bandwidths of about $2.0 - 10.0$ MHz, which is significantly below the Nyquist rate of the military signals. Correspondingly, the received military signal in the quadrature-phase component is significantly distorted and attenuated in power.

Mathematically, the received L1 GPS signal from satellite k, can be represented as [43]:

$$\begin{aligned} s_{L1}^k(t) =& A_C^k D^k(t) x_C^k(t) cos(2\pi(f_{L1} + f_{Dopp}^k)t + \theta^k) \\ &+ A_Y^k D^k(t) x_Y^k(t) sin(2\pi(f_{L1} + f_{Dopp}^k)t + \theta^k) \end{aligned} \tag{2.1}$$

where A_C^k and A_Y^k represent the amplitudes of the L1 C/A and P(Y) military signal from the k^{th} satellite respectively, $D^k(t)$ represents the navigation data signal, $x_C^k(t)$ and $x_Y^k(t)$ are the L1 C/A code and P(Y) encrypted military code respectively from satellite PRN k, received at a carrier frequency $(f_{L1} + f_{Dopp}^k)$, where f_{Dopp}^k is the received Doppler frequency from satellite PRN k. Finally, θ^k represents the received carrier phase at time $t = 0$.

2.2 Processing Steps Performed at GPS Receivers

To interpret the navigation data $D_k(t)$ in Eq. (2.1), the receiver must:

1. *Acquire* the GPS signals - determine which satellite signals are present and roughly estimate the received Doppler frequency and spreading code bit delay, or the *code phase* τ_{code}^k.

2. *Track* the GPS signals - continuously maintain a precise estimate of the signal parameters, including the Doppler carrier frequency f_{Dopp}^k and carrier phase θ^k as well as the spreading code phase τ_{code}^k, which provides a precise estimate of the satellite time of transmission.

During signal acquisition, the GPS receiver must search through a large *two-dimensional signal space* of potential Doppler frequencies of the received signal f_{Dopp}^k versus received lags in the spreading code sequence code phases

τ^k_{code}. The searched spreading code lags range from 0 to 1023 chips while typical ranges of searched Doppler frequencies are ±6 kHz, depending on the maximum velocity attained by the GPS receiver for the given application. For each examined Doppler frequency value and spreading code lag $\left(f^k_{Dopp}, \tau^k_{code}\right)$, the receiver generates a signal replica and correlates it with the incoming signal. In the case that the satellite signal is present with a similar Doppler frequency and code phase, a large correlation amplitude results, as graphically shown in Fig. 2.2.

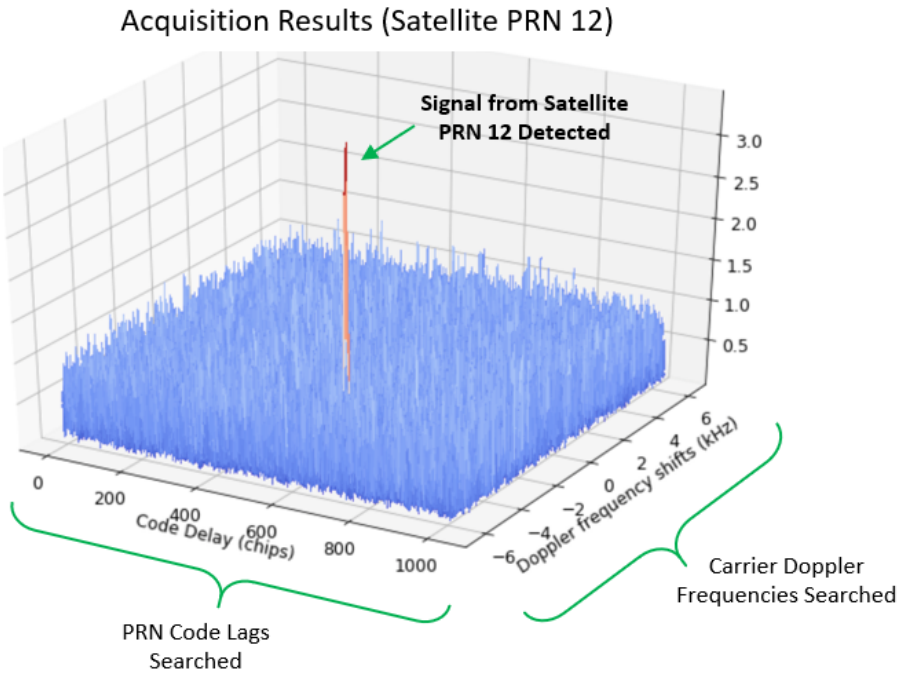


Figure 2.2: GPS acquisition plot. Each value represents the correlation between the incoming GPS signal and the signal replica having the corresponding Doppler frequency and code lag $(f^k_{Dopp}, \tau^k_{code})$ in the two-dimensional signal space. A large correlation result indicates the presence of a GPS signal, with similar Doppler frequency and code lag.

Once the receiver acquires the GPS signal from a particular satellite, it next tracks the signal and continuously maintains precise parameter estimates of the received GPS signal, including the precise carrier Doppler frequency, spreading code Doppler frequency, carrier phase, and spreading code phase (or lag). These precise estimates are required to retrieve a faithful representation of the navigation data message $D^k(t)$ as well as to obtain a precise estimate of the satellite signal time of transmission, which is necessary to

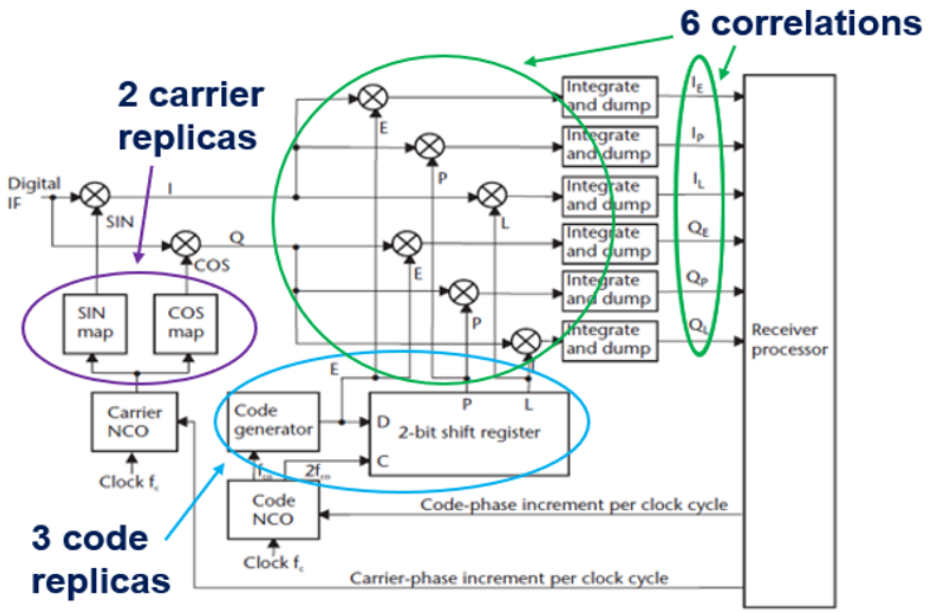


Figure 2.3: GPS signal tracking loops. The receiver tracking loops correlate the incoming signal, after down-conversion and digitization, with 6 signal replicas. The 6 replicas are generated from 2 carrier replicas, which are 90° apart in phase, modulated by 3 code replicas, which are equally spaced at $\frac{1}{2}$-chip intervals. Figure adapted from [43].

estimate the satellite range from the receiver.

While tracking a particular satellite signal, the receiver tracking loops correlate the incoming signal, after down-conversion and digitization, with 6 signal replicas, thereby performing 6 correlations, as shown in Fig. 2.3. To create the signal replicas, the receiver creates 2 carrier replicas: an in-phase and a quadrature-phase carrier replica, which are 90° apart in phase. By adjusting its carrier frequency estimate, the receiver carrier tracking loops align the in-phase carrier replica with the incoming signal, in both frequency and phase, thereby evaluating a precise estimate of the Doppler frequency f^k_{Dopp} and carrier phase θ^k for the k^{th} satellite signal.

Similarly, the receiver has 3 replicas of the satellite signal's binary spreading code. All 3 code replicas are identical binary sequences, separated temporally in equal $\frac{1}{2}$-chip intervals, and are called Early (E), Prompt (P), and Late (L). Fig. 2.4 depicts the $\frac{1}{2}$-chip temporal shift between these 3 code replicas along with the corresponding ideal correlation result below with the incoming GPS signal. By adjusting the code frequency in the delay lock loops, the receiver attempts to align the prompt code replica with the incoming signal,

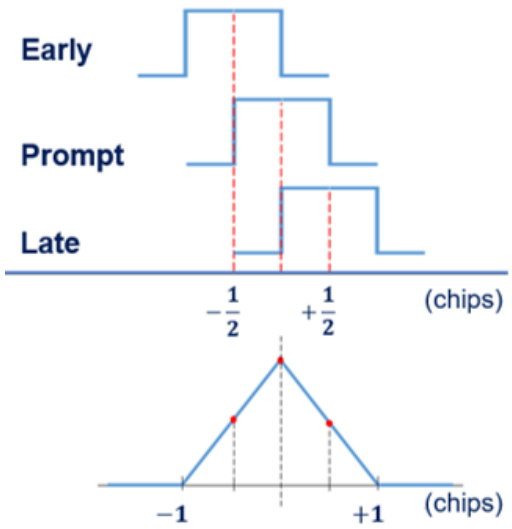


Figure 2.4: GPS signal tracking loops. The receiver tracking loops correlate the incoming signal, after down-conversion and digitization, with 6 signal replicas. The 6 replicas are generated from 2 carrier replicas, which are 90° apart in phase, modulated by 3 code replicas, which are $\frac{1}{2}$-chip apart.

resulting in the ideal correlation values shown in the triangular correlation result of Fig. 2.4. With precise alignment during scalar tracking, in addition to estimating the carrier frequency and phase, the receiver also maintains an estimate of the code frequency and code phase τ_{code}^{k} as well.

During tracking, precise signal parameter estimates are required to retrieve a faithful representation of the navigation data message, represented by $D_k(t)$ in Eq. (2.1), as well as obtain a precise estimate of the signal time of transmission, which is necessary for estimating the range of the satellite from the receiver. Once the receiver locks onto a GPS signal and begins tracking, it no longer examines the larger signal space, but rather initiates the receiver tracking loops, which continuously maintain the estimated signal parameters of the time-varying signal. If the receiver loses lock on the GPS signal, the receiver must again re-acquire the GPS signal in the two-dimensional signal space and re-instantiate the tracking loops.

CHAPTER 3

BACKGROUND ON GPS SPOOFING

The civilian GPS signal is not only weak, with received power levels on the order of 10^{-16} W, but it is also unencrypted, with a clearly outlined signal structure in publicly available interface specifications [3]. As a result, any individual with the right equipment can mimic or *spoof* the authentic GPS signals and establish a false position and/or timing solution at a victim receiver [4]. Spoofing can be performed in different ways, as outlined in Section 3.2, and more advanced spoofers can conduct an attack without raising an alarm at the victim receiver, as described in Section 3.3.

3.1 GPS Jamming and Spoofing

GPS spoofing is frequently conflated with *GPS jamming*, though spoofing is a much more sophisticated form of attack. During GPS jamming, the attacker simply broadcasts a high-powered signal in the same frequency band as GPS, such as a saw-tooth chirp signal around the GPS L1 center frequency ($f_{L1} = 1575.42$ MHz). The jamming signal thereby overpowers the satellite signals and denies the victim receiver access to the GPS navigation service. However, spoofing is much more insidious than jamming, since the victim may not even realize an attack is occurring, being tricked into trusting a counterfeit navigation solution.

3.2 Types of GPS Spoofing Attacks

3.2.1 Meaconing

During *meaconing*, also known as a *record-and-replay* attack, the attacker records an authentic GPS signal and re-broadcasts it at a later time. Before the meaconer can induce the victim receiver to track its false GPS signal, the attacker must initially force the receiver to lose track of the authentic GPS signal. This can be done by initially jamming the victim for a sustained period of time, then the attack must broadcast the recorded signal at a higher power to cause the receiver to adopt the false signal peak upon re-acquisition. For the victim receiver, this initial jamming is a telltale sign that an attacker is present and is manipulating the received signal. Furthermore, because the GPS signal is recorded, the positioning and timing solution at the victim receiver corresponds to that of the meaconer. As a result, not only does this limit the false navigation solutions possible, but in the process of performing an attack, the meaconer also reveals his own true location.

The next two types of spoofing are more sophisticated forms of attacks in that the spoofer generates the false GPS signal from scratch.

3.2.2 Data-Level Spoofing

In data-level spoofing, the spoofer provides the victim receiver with false data bits in the navigation data signal, represented as $D_k(t)$ in Eq. (2.1), which results in a false positioning and/or timing solution. To induce the victim receiver to track its navigation solution, the spoofer can steer the receiver tracking loops away from the authentic signal peak, as described in greater detail in Section 3.3. After pulling the tracking loops away from the authentic GPS signal peak, the spoofer can begin broadcasting false navigation data. Otherwise, the spoofer could additionally broadcast a phase-aligned nulling signal, also depicted in Fig. 3.1, which allows the receiver to maintain track of the authentic signal peak while flipping any desired data bits by broadcasting a matching GPS signal with opposite amplitude, at twice the signal power [13].

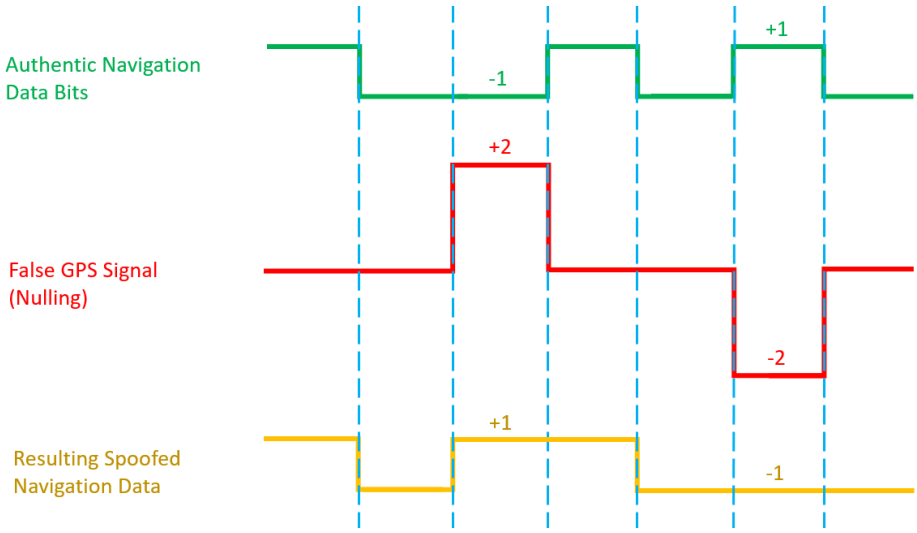


Figure 3.1: Performing data-level spoofing using a phase-aligned nulling signal. The nulling signal (in red) is twice the amplitude of the authentic GPS signals (in green), thus allowing the spoofer to flip any bit in the navigation data in order to create a counterfeit solution.

3.2.3 Signal-Level Spoofing

During a signal-level (or measurement) spoofing attack, the spoofer manipulates the navigation solution of the victim receiver by gaining control of the receiver tracking loops as described in Section 3.3, and then modifying the timing of the GPS signal peak in order to cause a false navigation solution at the victim receiver .

Considering the resources available to PMUs in the power grid network, this type of attack is the most difficult to detect for this application. In particular, the externally provided satellite ephemeris allows for detection of data-level spoofing attacks. Additionally, the access to a relatively stable backup timing source (drift rates of 1 μs every $1 - 8$ hours for an oven-controlled crystal oscillator [44]), as well as the stationary nature of the PMU receivers, with physical security protections implemented around the power grid substations [45], allows for detection of any timing discontinuities and alternate position solutions induced by meaconing attacks. As a result, this work and the experimental results primarily focus on detecting signal-level spoofing attacks, although Section 5.5 discusses an algorithm for detecting meaconing.

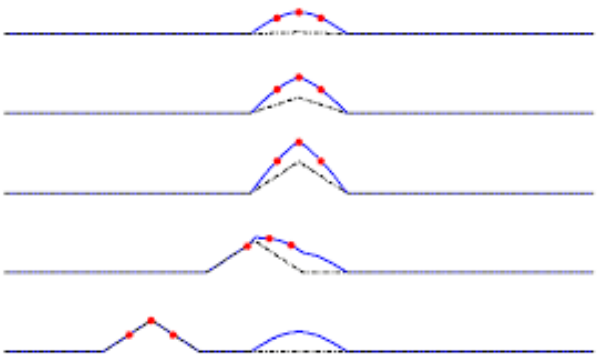


Figure 3.2: Steps performed by spoofer to drag receiver tracking loops away from the authentic GPS signal peak [13]. Red dots indicate points of reference for receiver tracking loops.

3.3 Conducting a GPS Spoofing Attack

Several research studies have sought to characterize GPS spoofing attacks [13], [46] as a first step in order to develop better detection techniques. In particular, once the attacker creates a false GPS signal according to the GPS-ICD, the spoofer must effectively induce the victim receiver to lock onto the spoofed signal. If executed properly, the spoofer can in fact do this without raising alarm at the victim receiver. In order to perform a stealthy attack, the spoofer must gradually commandeer the victim receiver tracking loops, as depicted in Fig. 3.2, and perform the following steps:

1. Send a signal which matches the authentic GPS signal received including signal parameters estimated during tracking, including the Doppler frequency f^k_{Dopp} and code lag τ^k_{code}.

2. Increase the signal power beyond that of the authentic signal. At this point, the spoofer has commandeered the tracking loops.

3. Gradually deviate the tracking loops away from the authentic GPS signal peak in the two-dimensional signal space. This can be done by gradually modifying the signal Doppler frequency f^k_{Dopp} and/or the spreading code lag τ^k_{code}.

4. Broadcast any desired, counterfeit GPS signal, now that the receiver is successfully tracking the spoofed signal.

CHAPTER 4

MULTI-RECEIVER COMMUNICATION ARCHITECTURE

Our proposed communication structure between PMU stations is through a hierarchical network architecture, with subsets of receivers organized into sub-networks, which connect to other sub-networks in a distributed manner. This architecture will utilize the future, large-scale power grid communication network. Although the protocol and structure of the communication network for the future Smart Grid have not been specified, one widely considered proposed structure was designed by the North American Synchrophasor Initiative (NASPI), and is called NASPInet. NASPI is a government-funded organization seeking to enhance the efficiency and reliability of the future, modernized power grid by installing a large-scale network of PMU monitoring stations throughout the power grid network [47]. The communication architecture proposed by NASPI for the power grid network is described in Section 4.1; however, because the future Smart Grid communication structure is yet to be decided, the hierarchical framework presented in this thesis is designed to be flexible and independent of the underlying communication network structure.

4.1 NASPInet

The North American Synchrophasor Initiative network (NASPInet) is a proposed standardized communication infrastructure designed to allow communication of PMU data throughout the power grid network in an efficient and secure manner. This architecture was designed to be decentralized as well as expandable, in order to easily incorporate more devices as the measurement network grows [48]. Fig. 4.1 shows the conceptual architecture of NASPInet.

In the NASPInet framework [49], each PMU transmits its data to a Phasor Data Concentrator (PDC) or another data collection entity, which then

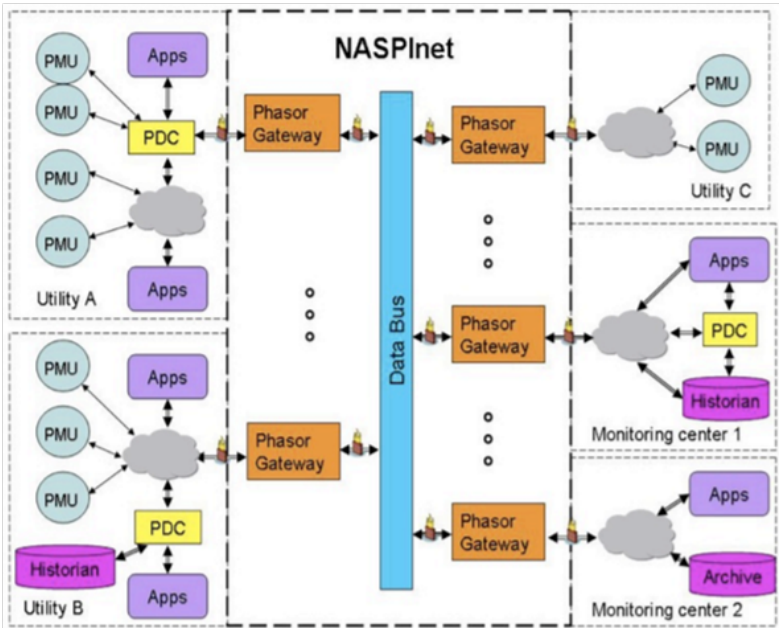


Figure 4.1: NASPInet communication architecture network [48]

sends the aggregated data to various applications, represented by the *Apps* blocks in Fig. 4.1. Applications include system visualization, fault detection, phasor-data-enhanced state estimation, as well as data archiving. Data which can be further examined for post-event analysis and for future research and development is similarly recorded for those applications as *Historical Data*.

For each utility, a Phasor Gateway unit subscribes to the PMU data within the utility. Phasor Gateways govern the secure communication of collected synchrophasor data throughout the network, which is connected via the NASPInet Data Bus [48]. NASPInet, and other interconnected communication networks for the U.S. power grid, are designed to securely transmit wide-area synchrophasor measurements in order to increase system visibility, detect stresses within the grid, and improve operations of the power grid system [50].

4.2 Hierarchical Architecture Framework

Utilizing the large-scale communication network established for the future power grid, our hierarchical architecture will be composed of a large-scale distributed network of central processing stations or central decision-making

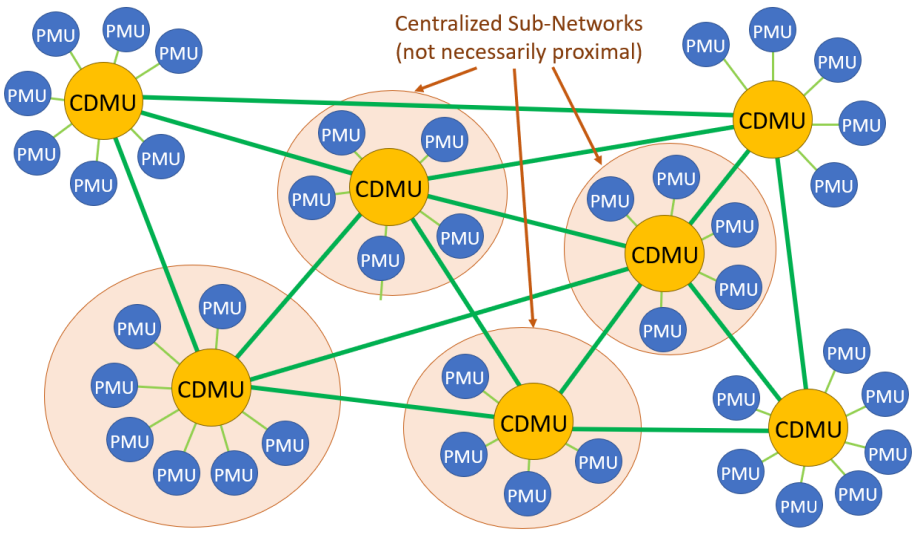


Figure 4.2: Proposed hierarchical architecture framework

units (CDMU), each of which branches out to a collection of PMU devices in a centralized manner. This hierarchical structure between the PMU devices is illustrated in Fig. 4.2. For increased reliability in spoofing detection, the PMU devices in each sub-network should ideally be widely dispersed across the power grid network, as further described in Section 6.2. The CDMU receives signal samples from all receivers in its own sub-network. To continuously authenticate the received GPS signal, conditioned signal samples must be regularly provided for each satellite PRN. See Section 5.1 for details on the signal conditioning process.

As shown in Fig. 4.3, upon receiving the GPS signal fragments from its sub-network of PMU devices, the CDMU conditions and performs pairwise cross-correlations between each pair of signal fragments, then aggregates the results to determine the preliminary spoofing decision. After comparing amongst the given sub-network in the first step, the CDMUs in contact then compare their respective signal fragments to verify the preliminary spoofing decision, particularly to detect a more sophisticated, coordinated spoofing attack against the individual sub-network.

To reduce bandwidth and processing requirements in this second step, the CDMU creates a sub-network representative signal from the GPS signals initially evaluated to be authentic within the sub-network and sends copies to other CDMUs in the distributed network. Upon receiving the representative signals from other sub-network sites, the CDMU performs a second authen-

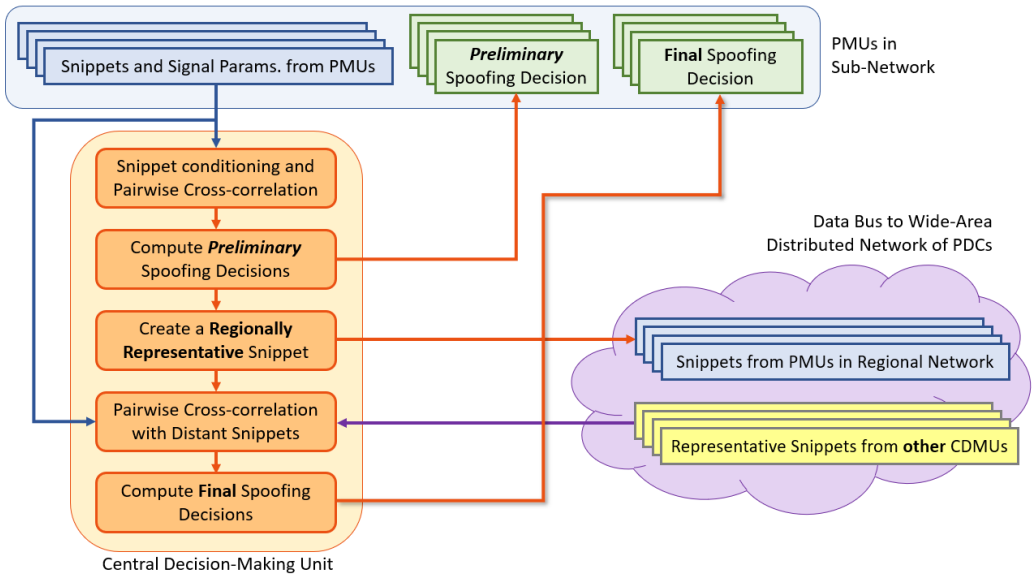


Figure 4.3: High-level process diagram of spoofing detection algorithm, focused on a single CDMU

tication step to determine the final spoofing decision, which is returned to each PMU in the individual sub-network. With this two-step hierarchy and with the generation of representative signals, we allow for a large number of received GPS signals to be compared throughout the network, while reducing on processing requirements.

4.3 Data Format Considerations

The conditioned signal fragments for each satellite PRN could be generated at each PMU, then subsequently sent to the CDMU; however, this would require a significant amount of available bandwidth. In particular, for a desired rate of signal authentication, represented by f_{check} Hz, a signal sample length of T_{snip} seconds, recorded at a sampling period of T_s seconds and a data resolution of n_{res} bits per sample, the required bandwidth W when the receiver observes N satellite PRNs can be represented as

$$W = f_{check} \cdot N \cdot \frac{T_{snip}}{T_s} \cdot n_{res} \tag{4.1}$$

By sending pre-conditioned GPS signal fragments, this would allow for less processing required at the CDMU. However, to reduce bandwidth usage and

eliminate processing requirements for participating receivers, a single raw GPS signal sample could be sent, along with the corresponding signal tracking parameters, to allow the CDMU to generate the corresponding conditioned signal fragments.

Additionally, at a particular time of transmission, the corresponding signal from each satellite PRN is received at varying times at each PMU station. Thus, to ensure the received signal samples from multiple PMU stations align over a time span of T_{snip} seconds, the PMUs must send slightly longer signal fragments. The temporal increase in sample length typically corresponds to approximately 20 ms, which is an insignificant increase in data length compared to the signal fragment lengths which typically provide strong signal peaks in our investigation. We denote this additional extension in the length of the conditioned signal as T_{ext}. Furthermore, to generate the representative signals for each sub-network to perform the second authentication step for algorithm, we must precisely align the signals from multiple PMU stations. Thus, although the signal fragments sent from each PMU can be initially coarsely aligned with respect to the transmission time of interest, a slightly longer signal sample should be sent corresponding to this margin of error.

An estimate of Doppler frequency and carrier phase is computed for each scalar tracking interval τ_{track}, leading to a total set of $\left(\frac{T_{snip}}{\tau_{track}}\right)$ signal parameters for the GPS signal fragment. As a result, the alternative format for the data sent from a PMU station to the CDMU has the following bandwidth requirement:

$$W = f_{check}\Bigg(\left[\frac{\left(T_{snip} + T_{ext} + 2\delta t_{align}\right)}{T_s} \cdot n_{res} \right] + N \cdot \left[\left(\frac{T_{snip}}{\tau_{track}}\right) \left(n_{freq} + n_{phase}\right) + n_{index} \right] \Bigg) \tag{4.2}$$

where δt_{align} represents the temporal alignment error from the desired time of transmission, and n_{freq}, n_{phase}, and n_{index} represent the data size in bits for the Doppler frequency, carrier phase, and starting indices for each satellite PRN, respectively.

In Eq. (4.2), the second additive term in the parentheses is significantly smaller than the first, largely due to the reduced number of data values required for the signal parameters, corresponding to only one set per tracking

period τ_{track}. As a result, the bandwidth requirement for this alternative data format does not significantly increase with the number of visible PRNs and is comparable to the bandwidth requirement for sending conditioned signal fragments for a single PRN at the same data resolution and authentication rate. Numerical values for the bandwidth used for our application are computed and further discussed in Section 6.1.

CHAPTER 5

SPOOFING DETECTION ALGORITHM

To continuously authenticate the received GPS signal at each PMU station, we require the signal samples to be regularly transmitted from each device to the central processing station. For each packet of transmitted data, the PMU station sends the raw GPS signal fragment, along with the estimated signal parameters computed during signal tracking for each visible satellite PRN. From these signal parameters, the CDMU must first generate a conditioned signal sample for each received satellite signal, in order to compare these conditioned signal samples for signal-level spoofing detection.

The components of the algorithm defined in this section are presented in the context of our proposed hierarchical framework. However, the steps sequentially outlined in the algorithm, including signal conditioning, generating a pairwise statistic for each pair of receivers, then aggregating the results to evaluate the cumulative spoofing statistic, can be performed in any multi-receiver application with a shared communication network.

5.1 Generation of Conditioned Signal Fragments at Each Receiver

At a particular PMU station, the received L1 GPS signal from the k^{th} satellite PRN can be represented as [43]:

$$\begin{aligned} s^k_{L1}(t) =& A^k_{C,L1} D^k(t) x^k_{C,L1}(t) cos(2\pi(f_{L1} + f^k_{Dopp})t + \theta^k_{L1}) \\ &+ A^k_{Y,L1} D^k(t) x^k_{Y,L1}(t) sin(2\pi(f_{L1} + f^k_{Dopp})t + \theta^k_{L1}) \end{aligned} \tag{5.1}$$

where $A^k_{C,L1}$ and $A^k_{Y,L1}$ represent the amplitudes of the L1 C/A and P(Y) military signal from the k^{th} satellite PRN respectively, $D^k(t)$ represents the navigation data signal, $x^k_{C,L1}(t)$ and $x^k_{Y,L1}(t)$ are the L1 C/A code and P(Y)

encrypted military code respectively from satellite PRN k, received at a carrier frequency (f_{L1}+f^k_{Dopp}), where f_{L1} is the L1 carrier frequency of 1.57542 GHz and f^k_{Dopp} is the received Doppler frequency from satellite PRN k, with the received carrier phase θ^k_{L1} at time $t = 0$.

After down-conversion by the receiver front-end to an intermediate frequency f_{IF}, the received analog signal is discretized by sampling at a rate of f_s. We denote this down-converted, discretized version of the signal as $s^k_{L1}[t]$, represented as:

$$\begin{aligned} s^k_{L1}[t] =& A^k_{C,L1} D^k[t] x^k_{C,L1}[t] cos(2\pi(f_{IF} + f^k_{Dopp})t + \theta^k_{L1}) \\ &+ A^k_{Y,L1} D^k[t] x^k_{Y,L1}[t] sin(2\pi(f_{IF} + f^k_{Dopp})t + \theta^k_{L1}) \end{aligned} \tag{5.2}$$

At this point, the receiver can determine the precise time of transmission of the received signal from satellite PRN k by using the GPS time of week and the elapsed number of C/A code chips. The receiver thus obtains a received signal sample of length T_{snip} according to this satellite time of transmission, for which the military P(Y) signal in the quadrature-phase channel should be identical and well-aligned amongst all authentic receivers.

Because the length of the signal sample T_{snip} exceeds the scalar tracking integration period τ_{track}, the PMU sends an array of the estimated Doppler frequency and carrier phase values, corresponding to the time interval the signal fragment elapses. Thus, the CDMU uses each set of signal parameters to generate a fraction of the carrier signal replica which corresponds to that particular scalar tracking time interval.

From the i^{th} scalar tracking estimates for the Doppler frequency $\hat{f}^k_{Dopp}[i]$ and carrier phase $\hat{\phi}^k[i]$ for the k^{th} received PRN, the CDMU generates a quadrature-phase replica of the corresponding carrier signal, similarly discretized to the sampling rate f_s. We assume that the 180° phase ambiguity due to the unknown navigation data bit polarity has been resolved for the received signal. From these estimates, the corresponding quadrature-phase carrier replica can be represented as [42]:

$$s^k_{replica,i}[t] = -sin\left(2\pi\left(f_{IF} + \hat{f}^k_{Dopp}[i]\right)t + \hat{\phi}^k[i]\right) \tag{5.3}$$

where $t \in \left[i \cdot \tau_{track}, (i+1) \cdot \tau_{track}\right)$ in discrete increments corresponding to the sampling period $T_s = 1/f_s$.

A total of $M = \left(\frac{T_{snip}}{\tau_{track}}\right)$ fractional quadrature-phase replica signals are generated. The CDMU then concatenates these signal segments to create the complete carrier replica of temporal length T_{snip}:

$$s^k_{replica}[t] = \left[s^k_{replica,1}[t] \ \ldots \ s^k_{replica,M}[t]\right] \tag{5.4}$$

Once this replica is generated, the CDMU wipes off the carrier signal by multiplying the down-converted, digitized L1 signal sample $s^k_{L1}[t]$ with the concatenated carrier replica from Eq. (5.4). At this point, assuming the tracking loops have converged to the received in-phase signal, the encrypted P(Y) signal lies in the quadrature-phase channel component, which the CDMU stores as the conditioned GPS signal fragment for the k^{th} visible PRN from the r^{th} PMU receiver in the given sub-network. The conditioned signal sample $m_{r,k}[t]$ for receiver r and satellite signal k can be evaluated as:

$$m_{r,k}[t] = s^k_{L1}[t] \cdot s^k_{replica}[t] \tag{5.5}$$

5.2 Authentication within the PMU Sub-Network

In this section, we outline the initial authentication step within the lower-level PMU sub-networks in the hierarchical architecture. In this sub-network authentication, as depicted in Fig. 5.1, we perform pairwise cross-correlations between each pair of receivers $\{(r_i, r_j) : i \neq j\}$ in the sub-network for each satellite signal k. From each correlation result, we evaluate the pairwise statistic $\gamma_{r_i r_j, k}$, before aggregating these statistics for each satellite PRN at a given receiver, then again aggregating across all received satellite signals, in order to determine the authenticity of the GPS signal received at the corresponding PMU station. The signals which are preliminarily determined to be authentic are then utilized to create a representative, authentic GPS signal for that PMU sub-network to be compared with other sub-networks in the hierarchical structure. Section 5.3 explains in greater detail how representative signals are created for each PMU sub-network for each satellite PRN.

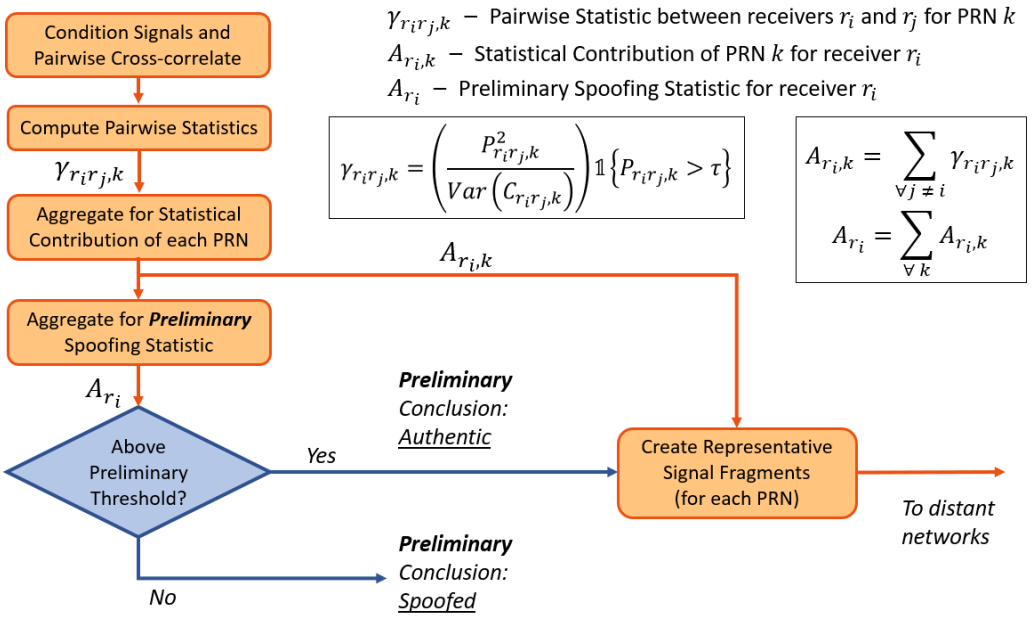


Figure 5.1: Authentication within a PMU sub-network

5.2.1 Cross-correlating between Matching PRNs

Once all signal samples from the given sub-network have been received and conditioned for a particular, desired time of transmission to authenticate, the CDMU performs pairwise cross-correlations between conditioned GPS signal fragments from matching PRNs:

$$C_{r_i r_j,k}[\tau] = \sum_{t=0}^{T_{snip}} m_{r_i,k}[t] m_{r_j,k}[t+\tau] \tag{5.6}$$

where $m_{r_i,k}$ and $m_{r_j,k}$ represent the conditioned signal fragments for receivers r_i and r_j for PRN k. From this cross-correlation, the CDMU takes the value with the largest magnitude within a central range of indices, as represented in Eq. (5.7)

$$p_{r_i r_j,k} = \max\left(C_{r_i r_j,k}[t] \cdot \mathbb{1}\left\{t \in [-\delta t_{align}, +\delta t_{align}]\right\}\right) \tag{5.7}$$

where δt_{align} corresponds to the alignment accuracy between signals from the sub-network of PMUs. The GPS signal fragments are closely aligned according to a specific satellite time of transmission, which is determined during signal tracking. Thus the alignment accuracy δt_{align} is dependent on

the quality of signal tracking at the corresponding pair of receivers, and will be correct to the nearest sample under typical scalar tracking conditions. By searching the correlation result within the narrow range of $|t| < \delta t_{align}$, we ensure detection of an authentic signal peak, if present, while also quickly seeking the signal peak by computing and checking a small number of correlation lag times.

5.2.2 Evaluating the Pairwise Statistic

As in our previous work [39], we next compute the pairwise statistic $\gamma_{r_i r_j,k}$, which represents the similarity and quality of the received quadrature-phase channels, which contain the military P(Y) codes, between the pair of receivers r_i and r_j, for satellite PRN k. :

$$\gamma_{r_i r_j,k} = w_{r_i r_j,k} \cdot B_{r_i r_j,k} \tag{5.8}$$

where $B_{r_i r_j,k}$ is a binary voting parameter, voting 1 if the correlation peak $p_{r_i r_j,k}$ lies above a pairwise spoofing threshold β_{pair}, indicating a strong correlation result with likely matching quadrature-phase signals between receivers r_i and r_j for PRN k. Similarly, if the correlation peak lies below the pairwise spoofing threshold β_{pair}, $B_{r_i r_j,k}$ votes 0, indicating poor quadrature-phase signal matching between the pair of receivers. The weighting constant $w_{r_i r_j,k}$ is defined as

$$w_{r_i r_j,k} = f_{signal}(r_i, r_j, k) \cdot f_{dist}(r_i, r_j) \tag{5.9}$$

where $f_{signal}(r_i, r_j, k) > 0$ reflects the received signal quality in the resulting pairwise correlation, with a greater signal strength corresponding to a larger weight. Similarly, $f_{dist}(r_i, r_j)$ reflects the relative distance between the two receivers in the pairwise statistic, with a greater distance corresponding to a larger weight, since receivers which are farther apart spatially are less likely to both be spoofed by the same transmitting antenna. This weighting function is positive when $i \neq j$.

In this work, we define f_{signal} to be the peak-to-noise ratio, or the ratio between the signal peak power and the noise floor power, computed from the

cross-correlation of the receiver pair:

$$f_{signal} = PNR\left(C_{r_i r_j,k}[t]\right) \tag{5.10}$$

$$= \frac{p^2_{r_i r_j,k}}{Var(C^z_{r_i r_j,k}[t])} \tag{5.11}$$

where $C^z_{r_i r_j,k}[t]$ represents the pairwise cross-correlation, with the observed main signal peak set to zero, to avoid including the large signal peak when characterizing the background noise variance.

Similarly, we define $f_{dist}(r_i, r_j)$ to be monotonically increasing as a function of the relative distance between receivers r_i and r_j with a monotonically decreasing, positive derivative. At a relative distance of 0 meters, $f_{dist}(r_i r_j)$ also equals 0 and the weight asymptotically reaches a value of 1 as the distance becomes arbitrarily large.

5.2.3 Aggregating across the Sub-Network

After evaluating the pairwise statistics, we compute the statistical contribution of PRN k to the overall preliminary spoofing statistic of each receiver in the network:

$$A_{r_i,k} = \sum_{\forall j \neq i} \gamma_{r_i r_j,k} \tag{5.12}$$

The statistical contribution of PRN k, denoted as $A_{r_i,k}$, reflects the similarity of the quadrature signal component of receiver r_i with that of other receivers in the given sub-network for PRN k.

Given that the satellite ephemerides are available via external channels, the spoofer must modify the pseudoranges from each received satellite, rather than the navigation data, in order to induce a false timing solution. Additionally, given the externally provided ephemerides as well as the well-known, stationary position of the PMUs, if the spoofer chooses to spoof only a subset of signals in view, without altering the PMU's 3D position solution, then the pseudorange residuals would be inconsistent between satellites, making the attack trivial to detect using standard RAIM techniques. Given that this initial consistency check has been performed, we thereby assume all GPS signals are consistently authentic or consistently spoofed, and thus aggre-

gate the statistical contributions of all visible satellite PRNs for receiver r_i to form its preliminary spoofing statistic:

$$A_{r_i} = \sum_{k=k_1}^{k_N} A_{r_i,k} \tag{5.13}$$

where N is the number of visible PRNs at receiver r_i and $\{k_1, \ldots, k_N\}$ is the corresponding PRN list. From the preliminary spoofing statistic, we evaluate the preliminary spoofing decision $\hat{S}_{r_i}$ by checking if A_{r_i} exceeds a threshold α_{prelim}:

$$\hat{S}_{r_i} = \mathbb{1}\{A_{r_i} \geq \alpha_{prelim}\} \tag{5.14}$$

where the threshold α_{prelim} is chosen to satisfy a desired false-alarm probability, as determined during initialization of receiver r_i where an empirical probability density function is developed under non-spoofed, authentic signal conditions. By performing this computation for all receivers in the given sub-network, we finish evaluating the preliminary spoofing decision for each PMU.

We next collect the receivers preliminarily determined to be authentic according to Eq. (5.14). Large preliminary spoofing statistics, above the threshold α_{prelim}, for this collection of receivers indicate a strong match of the quadrature signal component for the GPS signal received at these stations. This is likely due to the presence of the authentic P(Y) code in the quadrature channel of each signal, especially if the receivers are reasonably separated from each other in distance; however, similarly large preliminary statistics could also be induced during a sophisticated, coordinated spoofing attack against these receivers in the given sub-network.

5.3 Formation of Representative GPS Signals for the Given PMU Sub-Network

To determine the final spoofing decision for the preliminarily authenticated receivers, we compare the matching quadrature-phase signal received at these stations with signals from other sub-network sites, via the distributed communication network between CDMUs. Rather than sending copies of all

conditioned GPS signal fragments initially determined to be authentic, the CDMU can send one representative signal for each PRN.

This representative signal provides a condensed representation of the preliminarily authenticated signals from the given sub-network, thereby significantly reducing the bandwidth requirement for the distributed communication between CDMUs. Furthermore, the processing load at each CDMU for the second authentication step will correspondingly be reduced, leading to a shorter delay in determining the final spoofing decision for each PMU station.

5.3.1 Finely Aligning Authentic Signal Fragments

Before combining the authentic signals to create a representative signal for the sub-network, the authentic samples must be finely aligned to the nearest sample. To align the signal fragments received between a pair of receivers r_i and r_j for PRN k, we obtain the peak index of the cross-correlation between this pair of receivers, using the method described in subsection 5.2.1. The temporal shift corresponding to this index offset can be represented as:

$$\tau_{r_i r_j,k} = \frac{1}{f_s} \cdot \arg\max_t \left(C_{r_i r_j,k}[t] \cdot \mathbb{1}\{t \in [-\delta t_{align}, +\delta t_{align}]\} \right) \tag{5.15}$$

where f_s is the sampling frequency of the received signals. In this respect, we shift the GPS signal fragments from receiver r_j relative to the signal fragment from receiver r_i by the time difference $\tau_{r_i r_j,k}$, in order to align the two conditioned signals for PRN k. As discussed in Section 4.3, because the temporal shift can be as large as the worst-case alignment precision of δt_{align}, each PMU provides the CDMU with a slightly longer raw signal fragment. An additional $2\delta t_{align}$ seconds of data is transmitted to ensure a final, representative signal fragment of T_{snip} seconds can be generated for the received signal from each satellite.

This alignment process repeats for each of the other initially authenticated receivers in the given sub-network, by similarly shifting each signal fragment to align with the sample from receiver r_i. The receiver referenced for this collective signal alignment process, denoted as r_i, is chosen arbitrarily from the collection of authentic receivers. At this point, all preliminarily authenticated quadrature-phase signal fragments are mutually, finely aligned in time.

5.3.2 Generating Representative GPS Signals for a Given Sub-Network of PMU Devices

With all of the initially authenticated signal fragments collectively aligned to the nearest index, we next perform a weighted summation of these signals to generate a representative signal fragment for the sub-network of PMUs. For the k^{th} commonly received satellite PRN signal, the corresponding aligned signal fragment from each receiver r_j is weighted by the statistical contribution $A_{r_j,k}$, as defined in Eq. (5.12). This quantity $A_{r_j,k}$ represents the ability to verify the authenticity of the signal received from the k^{th} satellite PRN at receiver r_j, based on the similarity of its quadrature signal component with other receivers in the given sub-network. The weighted signals from each authenticated receiver r_j are then directly summed together and normalized to generate the representative signal sample for the local network n_i:

$$m^{rep}_{n_i,k}[t] = \frac{\sum_{\forall r_j} A_{r_j,k} m^{aligned}_{r_j,k}[t]}{\sum_{\forall r_j} A_{r_j,k}} \tag{5.16}$$

By normalizing the signal, we ensure that the representative signal $m^{rep}_{n_i,k}$ maintains the same overall signal strength as the signal fragments from individual receivers within the sub-network n_i. Additional methods of developing a P(Y) signal estimate from a collection of quadrature-phase signal samples can be utilized by extending the linear interpolation approach presented for a receiver pair in [37].

5.4 Evaluation of the Final Spoofing Decision

Once the representative signal for the sub-network has been generated for each commonly received satellite PRN, the CDMU sends copies of the representative signal to other sub-network sites via the distributed communication links. Fig. 5.2 depicts the final authentication step at the higher, sub-network level within the hierarchical framework. Once the CDMU receives representative signal samples from other sub-network sites, the CDMU then compares these representative signals from the other sub-networks with its own representative signal as well as with the original signal fragments from receivers that were preliminarily determined to be spoofed. Assuming a majority of

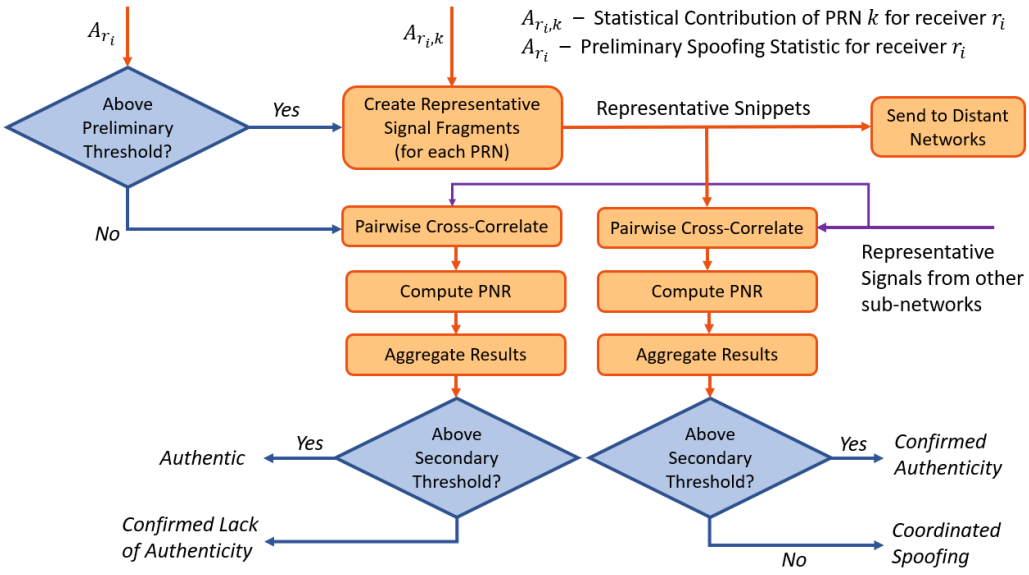


Figure 5.2: Final authentication step utilizing external, representative GPS signal fragments from other sub-network sites

the PMUs are not spoofed via a synchronized, coordinated attack, a strong match of the representative signal with the other sub-network sites confirms that these initially authenticated receivers are indeed authentic, whereas a poor signal match would lead to the conclusion that the sub-network collection of receivers have been spoofed in a coordinated manner. Similarly, with the signal from the receiver(s) initially determined to be spoofed, a strong signal match with the representative signals from the other sub-network sites would lead to the conclusion that the signal is indeed authentic. Otherwise, a poor signal match would confirm the lack of authenticity of the received signal.

It is important to note that for our algorithm we assume coordinated attacks do not scale to incorporate a majority of the PMUs in the North American continental power grid network. In such a large-scale attack, our algorithm would be unsuccessful in detection. Indeed, a widespread coordinated attack on the continental network of PMU receivers would require extensive resources, including a network of at least several hundreds of transmitters, broadcasting spoofing signals in a synchronized manner.

Thus, for the k^{th} satellite in common between the two PMU sub-networks, the CDMU cross-correlates each received, representative signal $m^{rep}_{n_j,k}[t]$ from sub-network n_j with its own representative copy, denoted as $m^{rep}_{n_i,k}[t]$, as well

as with the original signal fragments from each receiver r_q determined initially to be spoofed, denoted as $m_{r_q,k}[t]$:

$$C_{n_i n_j,k}[t] = \sum_{\tau=0}^{T_{snip}} m^{rep}_{n_i,k}[t]\ m^{rep}_{n_j,k}[t+\tau] \tag{5.17}$$

$$C_{r_q n_j,k}[t] = \sum_{\tau=0}^{T_{snip}} m_{r_q,k}[t]\ m^{rep}_{n_j,k}[t+\tau] \tag{5.18}$$

From each cross-correlation result $C_{n_i n_j,k}$ and $C_{r_q n_j,k}$, the CDMU computes the centralized signal peak using Eq. (5.7) and subsequently the peak-to-noise ratio, which can be represented as

$$\eta_{n_i n_j,k} = PNR\left(C_{n_i n_j,k}[t]\right) \tag{5.19}$$

$$\eta_{r_q n_j,k} = PNR\left(C_{r_q n_j,k}[t]\right) \tag{5.20}$$

where $PNR(\cdot)$ is defined in Eq. (5.11). The quantity $\eta_{n_i n_j,k}$ represents the quality of the signal match between the local representative signal with the representative signal from sub-network n_j for PRN k. In the same manner, $\eta_{r_q n_j,k}$ quantifies the degree of similarity between the representative signal from sub-network n_j and the signal from receiver r_q, which was initially determined to be spoofed when comparing within its sub-network of receivers. A sufficiently strong peak-to-noise ratio indicates a match with the corresponding sub-network site. Similar to the steps in subsection 5.2.3, the computed peak-to-noise ratio is aggregated for the correlation results of all received satellite PRNs and all sub-network available for comparison:

$$\tilde{B}_{n_i} = \sum_{\forall n_j \neq n_i} \sum_{\forall k} \eta_{n_i n_j,k} \tag{5.21}$$

$$\tilde{B}_{r_q} = \sum_{\forall n_j \neq n_i} \sum_{\forall k} \eta_{r_q n_j,k} \tag{5.22}$$

After aggregating across all PRNs, the CDMU smooths the secondary with a narrow moving average filter of width ν samples to reduce variability in

the final statistic:

$$B_{n_i}[t] = \frac{1}{\nu} \sum_{\tau=t-\nu}^{t} \tilde{B}_{n_i}[\tau] \tag{5.23}$$

$$B_{r_q}[t] = \frac{1}{\nu} \sum_{\tau=t-\nu}^{t} \tilde{B}_{r_q}[\tau] \tag{5.24}$$

Next, to determine the final spoofing decision S_{n_i} of the collection of preliminarily authenticated receivers, we verify the secondary cumulative statistic B_{n_i} lies above a threshold α_{PNR} chosen to satisfy a desired false-alarm probability, similar to the method of choosing the preliminary threshold α_{prelim} as described in subsection 5.2.3. The secondary cumulative statistic B_{r_q} is similarly compared with the threshold to determine the final spoofing decision S_{r_q} for each of the receivers determined initially to be spoofed, where a decision of 1 corresponds to an authentic spoofing decision and 0 corresponds to a spoofed decision:

$$S_{n_i} = \mathbb{1}\{B_{n_i} \geq \alpha_{PNR}\} \tag{5.25}$$

$$S_{r_q} = \mathbb{1}\{B_{r_q} \geq \alpha_{PNR}\} \tag{5.26}$$

5.5 Detection during Meaconing

Because true GPS signals are recorded to perform meaconing, the authentic P(Y) encrypted codes will be present in the quadrature-phase channel of the received signal. As a result, a strong correlation peak will be observed, indicating the original signal was indeed transmitted from the true GPS satellites. To detect an anomalous time-delay induced by meaconing, the GPS receiver must have access to another timing source for reference. Indeed, the PMUs in the power grid also have a backup inertial clock, which is periodically maintained by the GPS receiver to avoid long-term drift.

Through the use of Position-Information Aiding [39], we can utilize the known location of the stationary PMUs, as well as the satellite ephemeris data provided via external sources to compare the relative received times of the GPS signal between stations within the power grid network. Utilizing this methodology, we incorporate this technique in the context of this hierarchical

architecture framework.

The CDMU only needs to perform a meaconing check for receivers in the subset of PMUs n_j which has been authenticated for signal-level spoofing, as determined by evaluating the final spoofing decision S_{n_j} using Eq. (5.26). Thus to authenticate the received satellite signals for a particular time of transmission t^{Tx}, each authenticated receiver r_i sends the CDMU its estimated received time $\hat{t}^R_{r_i,k}$ for the transmitted signal from each visible satellite k. The CDMU could also send these estimates, obtained from each receiver in its own sub-network, to other sub-network sites. This would in turn provide more timing reference data, and thus increased redundancy, while using negligible additional bandwidth.

After obtaining the estimated received time from all receivers in its sub-network, the CDMU computes for each pair of receivers (r_i, r_j) the estimated difference in received times for the signal transmitted from satellite PRN k:

$$\hat{\delta}t_{r_i r_j,k} = \hat{t}^R_{r_i,k} - \hat{t}^R_{r_j,k} \tag{5.27}$$

This estimated received time difference $\hat{\delta}t_{r_i r_j,k}$ is then compared with the expected received time difference $\delta t_{r_i r_j,k}$, computed from the relative known positions of the receivers r_i and r_j as well as satellite PRN k. Additionally, the expected received time difference incorporates estimated delays due to ionospheric and tropospheric effects. Using a similar approach as with the signal-level spoofing detection algorithm, we first determine a pairwise meaconing statistic $\gamma^{meac}_{r_i r_j,k}$ between receivers r_i and r_j for PRN k:

$$\gamma^{meac}_{r_i r_j,k} = w_{r_i r_j,k} \cdot \mathbb{1}\left\{|\hat{\delta}t_{r_i r_j,k} - \delta t_{r_i r_j,k}| < \tau^R_{pair}\right\} \tag{5.28}$$

where τ^R_{pair} is the pairwise threshold for the deviation of the measured relative time delay from our computed expectation of the relative delay, and $w_{r_i r_j,k}$ is defined in Eq. (5.9). Then, for a particular receiver r_i, we similarly aggregate the pairwise statistic across all receiver pairs and visible satellites, to compute the resulting meaconing statistic $A^{meac}_{r_i}$:

$$A^{meac}_{r_i} = \sum_{k=k_1}^{k_N} \sum_{\forall j \neq i} \gamma^{meac}_{r_i r_j,k} \tag{5.29}$$

where N is the number of visible PRNs from receiver r_i, with the correspond-

ing PRN list $\{k_1, \ldots, k_N\}$. This meaconing statistic is similarly compared with a threshold to determine the meaconing decision [39].

5.6 Detection during Data-level Spoofing

During data-level spoofing, if the attacker first steers the receiver tracking loops away from the authentic signal peak, the quadrature channel of the tracked signal will no longer contain the encrypted P(Y) military signal, thereby causing our algorithm presented in Sections 5.1 - 5.4 to flag the attack. If the attacker does not manipulate the tracking loops of the receiver, and instead performs nulling to modify the navigation data bits in real-time, the encrypted P(Y) codes would indeed still lie in the quadrature channel of the tracked signal. However, because the satellite ephemeris data is provided to the PMU externally through secured communication networks, this alternate method of attack would also still be readily detected.

CHAPTER 6

EXPERIMENTATION

6.1 Experimental Setup

To verify our spoofing detection algorithm, we recorded GPS signals during a live-sky spoofing event in a western U.S. state. Simultaneously, we also recorded data at several other sites, including three sites in the United States as well as three sites in South America. Our authentic cross-checking receiver sites are listed below:

1. Urbana, IL, USA
2. Boulder, CO, USA
3. Cleveland, OH, USA
4. Lima, Peru
5. Pachon, Chile
6. Tololo, Chile

At each site, we used a sampling frequency of 2.5 MHz, which is significantly below the Nyquist rate for the 20.46 MHz bandwidth military signal. We additionally utilized a 32-bit data resolution for the spoofed station and the Illinois station, while for the other receiver sites, we used an 8-bit data resolution. Each station was equipped with a Universal Software-Defined Radio (USRP-N210), connected to a Novatel GPS antenna and triggered by a Chip-Scale Atomic Clock (CSAC). Fig. 6.1 shows our rooftop antenna setup in Urbana, Illinois, USA. The collected raw GPS data was later post-processed using our research group's object-oriented, software-defined receiver written in Python, called *PyGNSS* [51].

Figure 6.1: Rooftop antenna setup in Urbana, Illinois

For our experimentation, we used 500-ms-long signal fragments and a scalar tracking interval of 1 ms. Additionally, we represented the Doppler frequency and carrier phase signal parameters with 8-byte floats. We also used a 4-byte unsigned integer to represent the starting index for each received PRN signal within the raw GPS signal fragment. These data size parameters are defined in Section 4.3 in more detail. Thus with 6 PRNs visible, according to Eq. (4.2), the condensed data format would require less than 50 kB to represent the tracked signal parameters and about 1300 kB to represent the extended raw signal for our application, with an 8-bit data resolution. This is comparable to sending a conditioned signal fragment for a single PRN at the same data resolution, which requires 1250 kB according to Eq. (4.1).

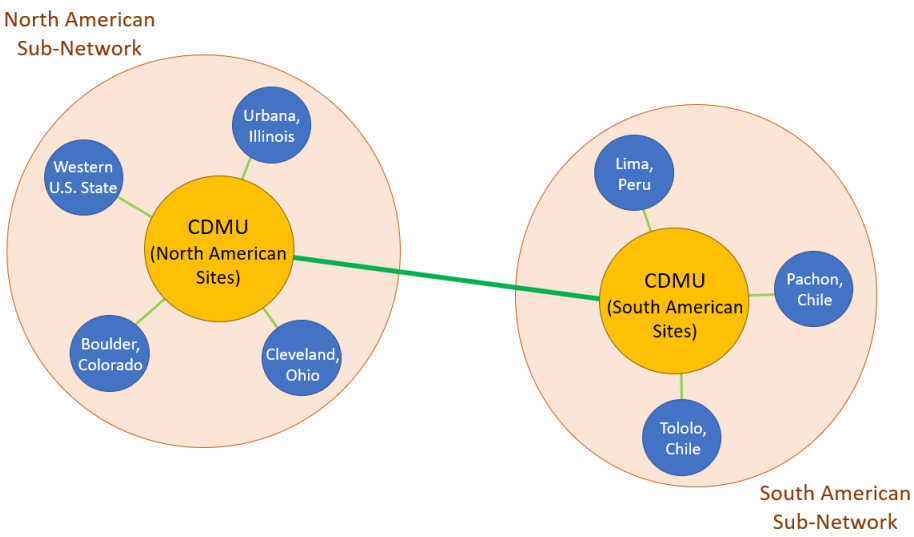


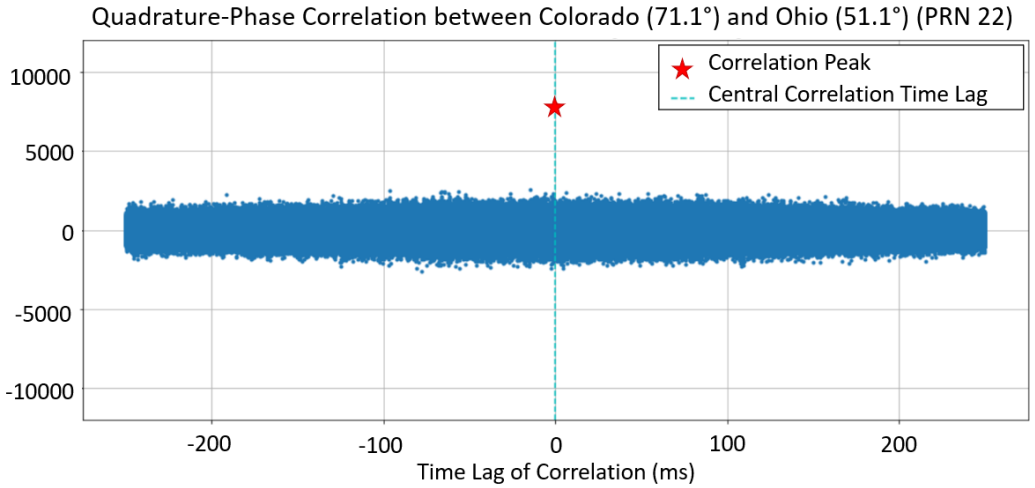
Figure 6.2: Hierarchical network setup with receiver stations

Organizing the receivers above into a hierarchical architecture as depicted in Fig. 6.2, we define the following two sub-networks: one with the North American receiver sites and another with the South American sites.

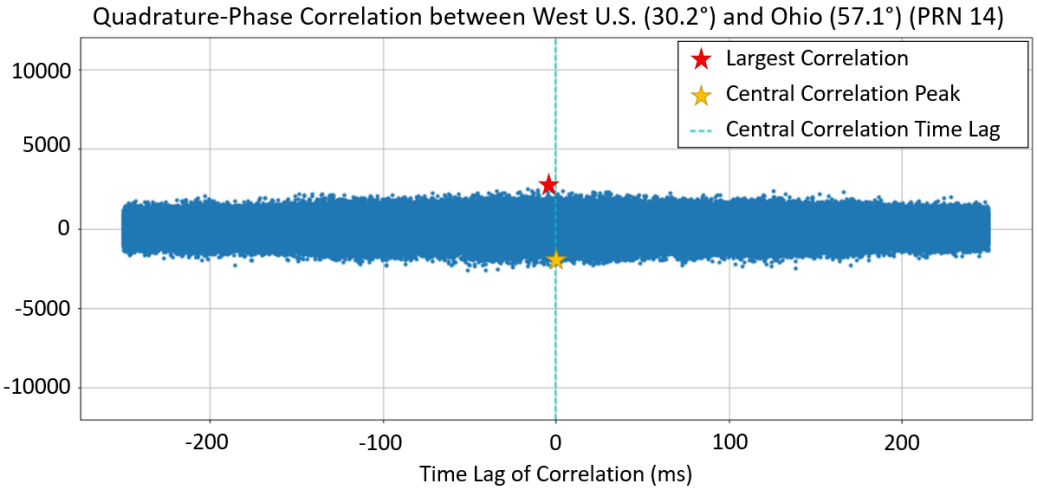
6.2 Examples of Cross-Correlation Plots

When cross-correlating conditioned signal fragments between two authentic receivers, we typically observe a single, large, centralized signal peak. Fig. 6.3a shows an example of a typical cross-correlation plot between two authentic receivers.

Within the South American sub-network, we occasionally observed side peaks in the complete cross-correlation results between the receivers in Tololo, Chile and Pachon, Chile, an example of which is shown in Fig. 6.4. By aligning the conditioned signals using the satellite time of transmission, rather than the received time and expected relative delay with respect to other PMU stations, we were able to narrowly pick out the cross-correlation peak result as shown in Fig. 6.4.



(a) Authentic conditions (between receivers in Colorado and Ohio)



(b) During spoofing (between receivers in Western U.S. and Ohio)

Figure 6.3: Typical cross-correlation plots between a pair of receivers during authentic signal conditions, between receivers in Ohio and Colorado, as well as during spoofing, between receivers in Ohio and the Western U.S. (spoofed). When both received signals are authentic, we observe a distinct, central correlation peak; otherwise, if one receiver is spoofed, we observe the lack of a correlation peak lying significantly above the noise floor.

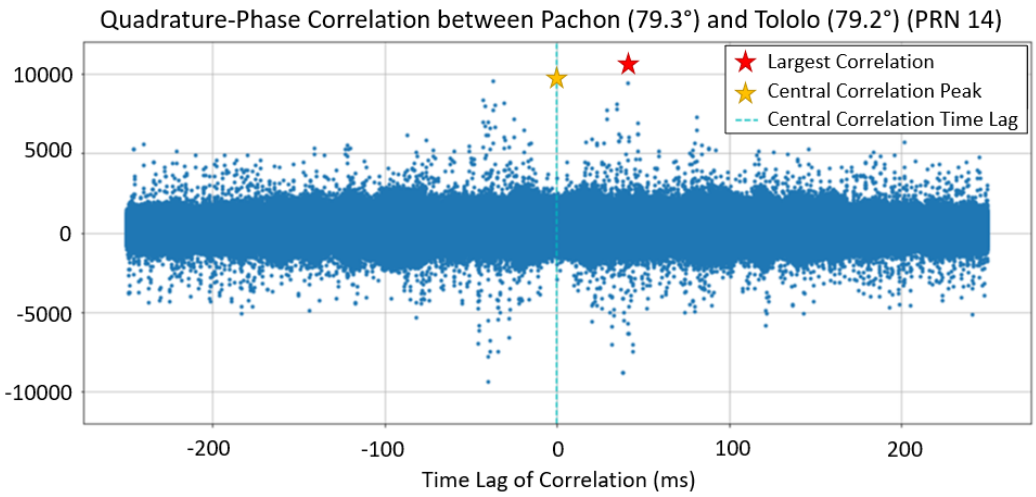
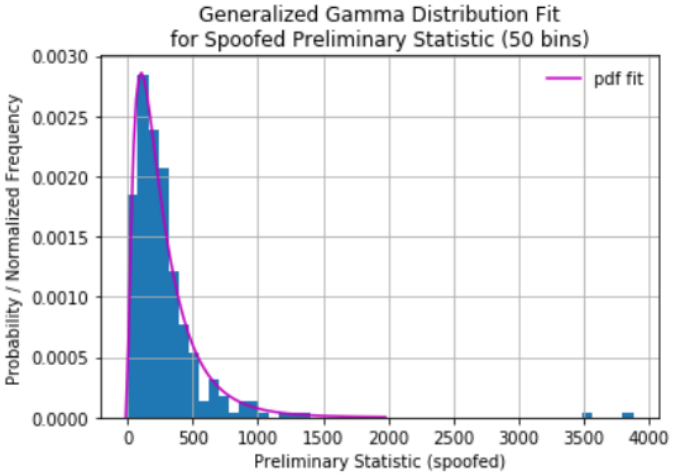


Figure 6.4: Example of authentic cross-correlation result with induced side correlations. Due to the aligned signals, according to the received time of transmission, and due to the authenticity of the two receivers, we still observe a distinct, central correlation peak. The induced side peaks are caused by the similar received Doppler frequencies of the satellite signal between the two stations, which correspondingly leads to a small difference in the residual frequencies of the two conditioned signals. To prevent these induced correlation side peaks, we require receivers in each sub-network to be well separated.

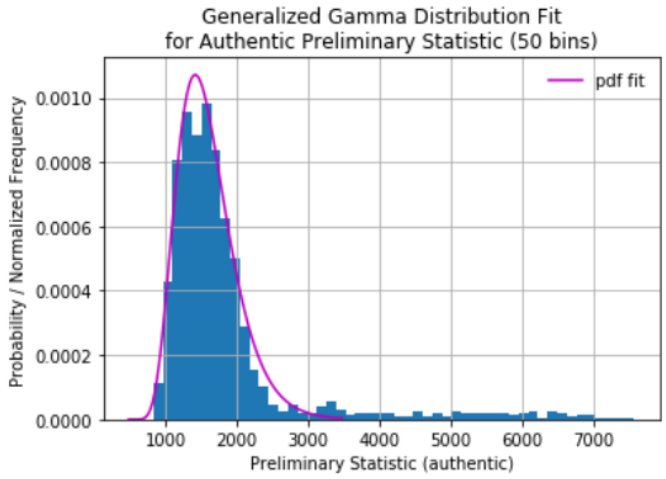
Due to the relatively close proximity of these receivers, the side correlations are likely due to similar received Doppler frequencies for the satellite signal at the two stations. In particular, if the residual frequencies in the conditioned signal are similar enough to be within the discrete Fourier transform frequency resolution f_s/N_{samp} of each other, where N_{samp} represents the number of samples in the conditioned signal fragment, the signal correlation would thereby introduce the side peaks observed in Fig. 6.4. Similar correlation effects were observed and noted by [37] between two receivers in Ithaca, New York, where the authors similarly concluded the correlations to be induced by the similar received Doppler frequencies. In [37], the authors consider and describe additional scenarios where spurious correlations could be induced between a pair of receivers.

6.3 Evaluating Preliminary Spoofing Decision

Examining 140 seconds of spoofed GPS data, with an authentication rate of 2 Hz, we computed the preliminary statistic as defined in Eq. (5.13) for each receiver in the two sub-networks. Considering the preliminary statistics from the authentic receivers, as well as from the spoofed receiver, we observe that these statistics come from two separate, right-skewed probability distributions, as plotted in Fig. 6.5.



(a) Spoofed preliminary statistics



(b) Authentic preliminary statistics

Figure 6.5: Evaluating preliminary statistics over 140 seconds of GPS data during spoofing shows authentic and spoofed preliminary statistics which come from two separate right-skewed probability distributions.

To fit the preliminary statistics with a probability distribution, we search among the family of generalized gamma distribution functions, which is a flexible probability distribution function incorporating various different families of skewed probability distributions, including the following well-known distributions: exponential, chi-squared and gamma, Weibull, and Rayleigh. The generalized gamma distribution function takes the following form:

$$f(x, \alpha, c, \beta, l) = \frac{|c| y^{c\alpha - 1} exp(-y^c)}{\gamma(\alpha)}$$
$$y = \beta(x - l) \tag{6.1}$$

where $\gamma(\cdot)$ represents the gamma function: $\gamma(\alpha) = (\alpha - 1)!$. For the authentic preliminary statistics, the distribution fit had the following characteristic parameters:

$$\alpha = 27.2, \qquad c = 0.517, \qquad \beta = 1.82, \qquad l = 486$$

whereas for the spoofed preliminary statistics, the distribution fit had parameters:

$$\alpha = 11.3 \qquad c = 0.370, \qquad \beta = 0.346, \qquad l = 0$$

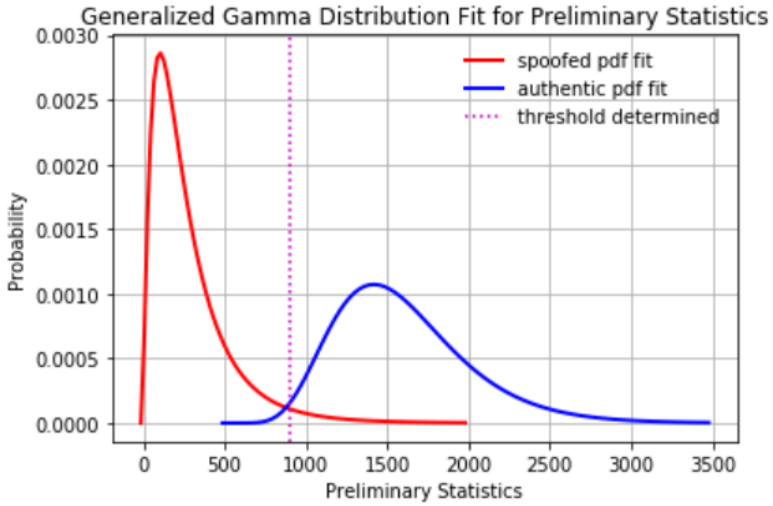
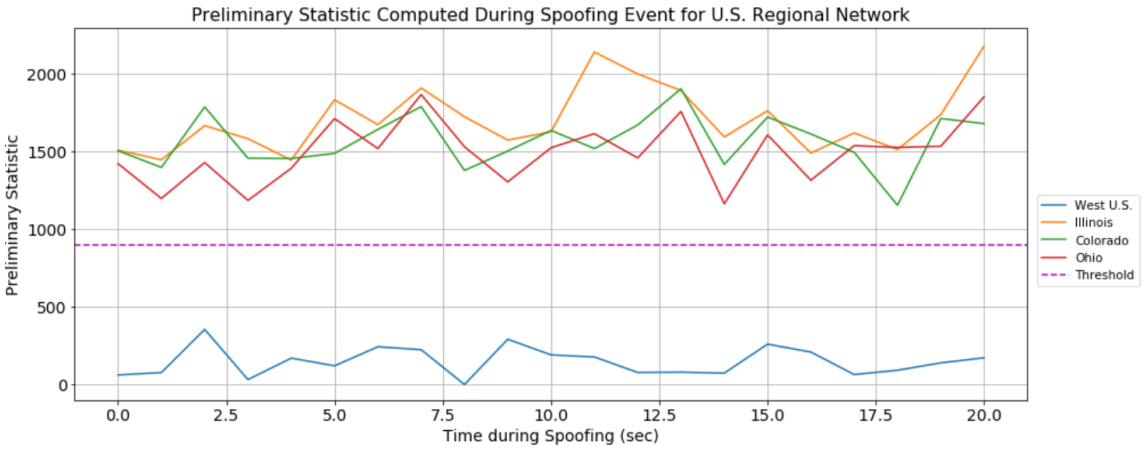


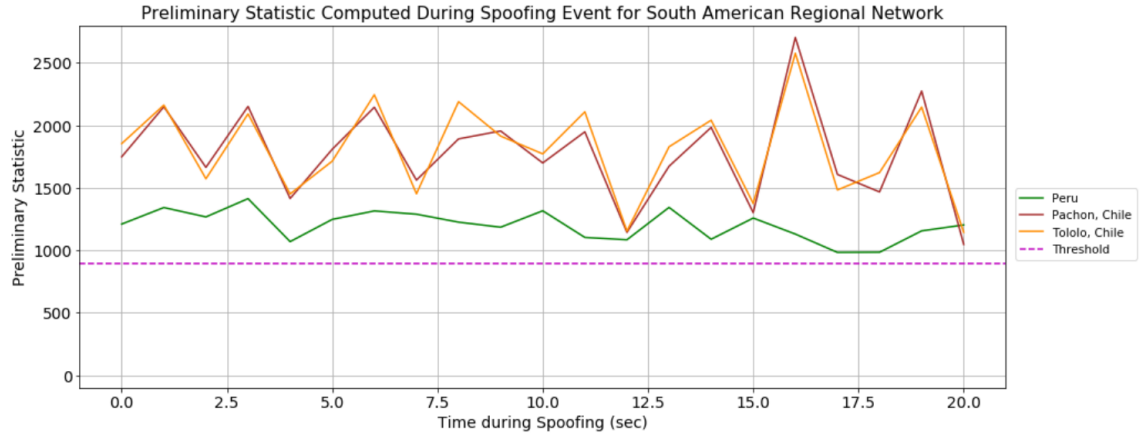
Figure 6.6: Preliminary threshold chosen to meet a specified false alarm probability, here shown for $P_F = 0.01$, with corresponding probability of missed detection of $P_M = 0.03$. If the preliminary statistic lies above the threshold, we determine the receiver is more likely to be authentic; otherwise, we conclude it is more likely to be spoofed.

Using the authentic spoofing statistic distribution, we can apply a Neyman-Pearson problem approach to correspondingly choose our preliminary and secondary thresholds given a false alarm probability rate requirement P_F^{req}. Choosing our false alarm probability to be on the order of 10^{-2} at $P_F = 0.01$, we can subsequently define the threshold, as shown in Fig. 6.6, which corresponds to a probability of missed detection of $P_M = 0.03$. Thus, if our computed preliminary statistic lies above the threshold, we conclude that the receiver is authentic; otherwise, if it lies below, we conclude that it is spoofed.

Applying our preliminary threshold on a separate, 20-second segment of data during spoofing, in Fig. 6.7a, the cumulative statistic for the western U.S. receiver in the western United States, which was spoofed, lies below the threshold by a significant margin, whereas the statistic for the authentic receivers consistently remained above. Similarly in Fig. 6.7b, for the South American receiver network, all three stations had measurements which similarly remained significantly above the threshold.



(a) North American Sub-Network



(b) South American Sub-Network

Figure 6.7: Cumulative statistic for North American and South American sub-networks. For the authentic receivers, the statistic was consistently significantly above the threshold, thus allowing for an accurate preliminary spoofing decision. In comparison, the statistic for the western U.S. receiver was consistently below the threshold, indicating a "spoofed" preliminary spoofing decision for this receiver.

6.4 Verifying Preliminary Spoofing Decision using Representative Signals from Other Sub-Networks

To verify the preliminary spoofing decisions, for each authentication time, we generate a signal fragment representative of the quadrature-phase signals obtained by the initially authenticated receivers in the North American sub-

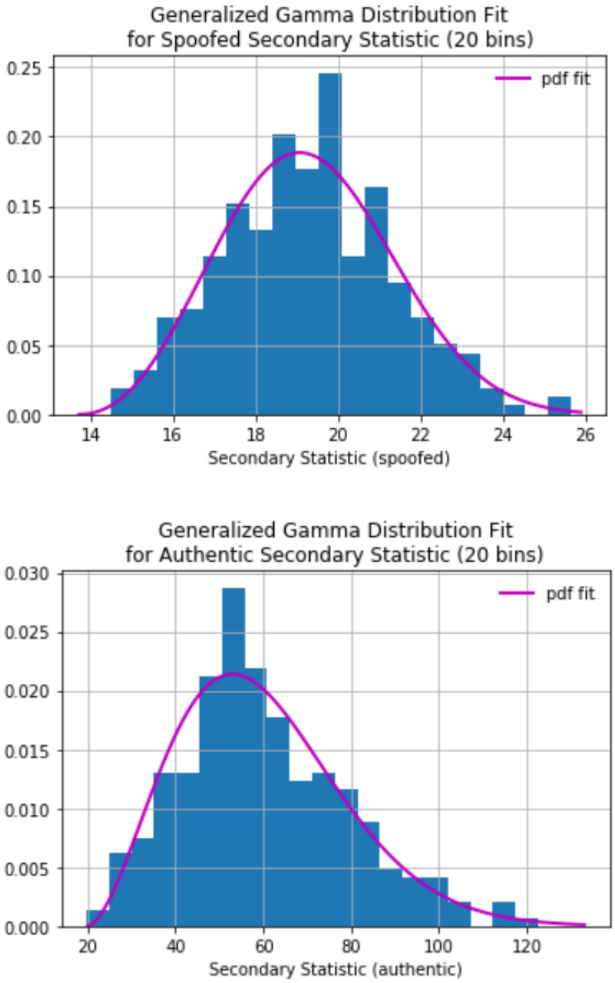


Figure 6.8: Evaluating secondary statistics over 140 seconds of GPS data during spoofing shows authentic and spoofed secondary statistics, which come from two separate right-skewed probability distributions functions.

network (Illinois, Colorado, and Ohio). Then this signal and the original spoofed signal from the western U.S. receiver are both compared with a representative signal fragment from the South American sub-network. For the secondary statistic computation, we chose our narrow filter window to be 3 samples in width. Similar to the preliminary statistic threshold determination process, we examine the same 140 seconds of spoofing data and compute the secondary statistics for both the authentic signal as well as the spoofed signal. We again observe that these statistics appear to come from two separate distributions, resembling a gamma distribution function, as plotted in Fig. 6.8.

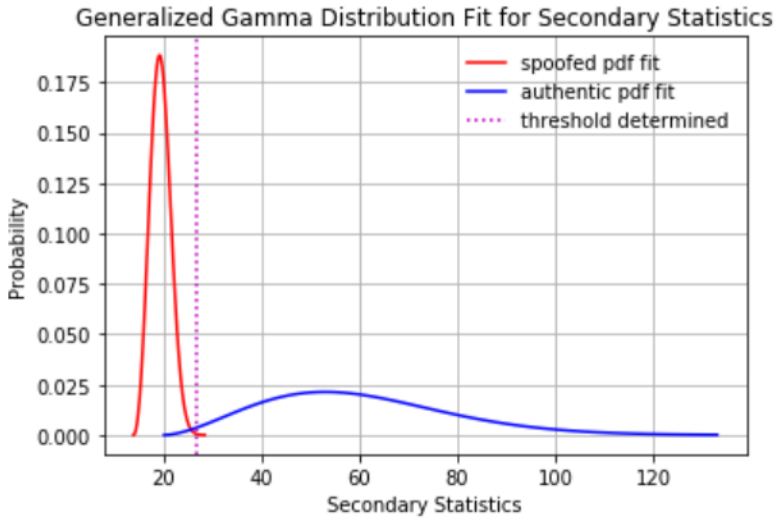


Figure 6.9: Secondary threshold chosen to meet a specified false alarm probability, here shown for $P_F = 0.01$, with the corresponding probability of missed detection of $P_M = 0.002$. If the secondary statistic lies above the threshold, we determine the GPS signal is more likely to be authentic; otherwise, we conclude it is more likely to be spoofed.

Similarly using the generalized gamma distribution for right-skewed data, with probability density function expressed in Eq. (6.1), the authentic secondary statistic had the following distribution parameters:

$$\alpha = 1.53, \qquad c = 1.74, \qquad \beta = 33.7, \qquad l = 20.0$$

whereas the distribution for the spoofed secondary statistics had parameters:

$$\alpha = 1.18 \qquad c = 2.69 \qquad \beta = 5.80 \qquad l = 13.7$$

From the fitted distribution, we similarly choose our secondary threshold according to a specified false alarm probability rate requirement, shown for $P_F = 0.01$ in Fig. 6.9, which corresponds to a missed detection rate of $P_M = 0.002$. Thus, if our computed secondary statistic lies above the threshold, we determine that the GPS signal is most likely authentic according to this probability model. Otherwise, if it lies below, we conclude that it is more likely to be spoofed. Finally, in Fig. 6.10 we apply our secondary threshold on the same 20-second segment of data during spoofing, which was separate from the data used to create the probability model. We observe that with our computed secondary statistics, by comparing with the other

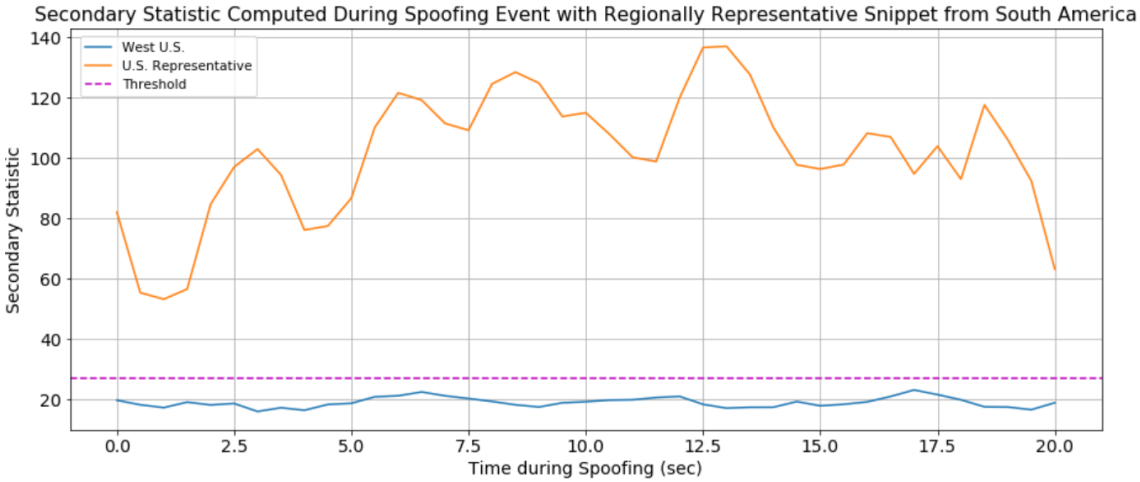


Figure 6.10: Secondary statistic for North American representative signal and western U.S. receiver signal, which was computed as the peak-to-noise ratio from correlation with the South American representative signal for PRN 26, the only common satellite signal observed between both sub-networks. We observe that this statistic was significantly above the threshold between the two representative signals, whereas for the western U.S. receiver, the statistic was significantly below the threshold, indicating a poor match with the authenticated receivers in the South American sub-network.

sub-network sites, we accurately verify the authenticity preliminarily determined for each receiver. In particular, the signal fragment representative of the quadrature-phase signal obtained by the initially authenticated receivers in the North American sub-network (Illinois, Colorado, and Ohio) generates a significant correlation with the representative signal from the South American sub-network, indicating a match with the other sub-network sites and confirming that these receivers are indeed authentic. In comparison, the GPS signal obtained at the Western U.S. receiver has a secondary statistic which lies below the threshold, indicating a poor match between this receiver with those from the South American sub-network, confirming that this receiver is indeed spoofed.

Between the North American and South American sub-networks, the receivers only observed one common PRN due to the significant separation of the two sub-networks. Despite the fact that PRN 26 is a lower elevation satellite for all receivers, we were still able to observe distinguishing secondary statistics.

CHAPTER 7

CONCLUSION AND FUTURE WORK

In this thesis, we propose a hierarchical detection framework to detect GPS spoofing amongst a network of PMUs for the future power grid. Our multi-receiver approach leverages the geographic diversity and available communication structure within the power grid network and uses the military P(Y) code as an verifiable authentic signature which cannot be forged by a spoofer due to its encryption. Our approach further defends against a more sophisticated, coordinated spoofing attack on a sub-network of cross-check receivers, while reducing bandwidth and processing requirements by using a condensed, representative signal sample to compare with other sub-networks.

We additionally test our algorithm on data collected during a government-sponsored live-sky GPS spoofing event, demonstrating that our algorithm successfully detects signal manipulation at the victim receiver, while simultaneously authenticating the other receivers in the wide-spread network.

For future work, we believe the research in this thesis can be utilized and extended to produce a *multifaceted spoofing detection* system for the power grid network. This multifaceted approach would combine multiple spoofing detection approaches, including the multi-receiver cross-verification approach discussed, in order to establish a more reliable spoofing decision for each receiver. Individual spoofing detection methods, such as clock bias and signal distortion monitoring, would be beneficial for immediate, local spoofing detection abilities as well as added redundancy, but these methods also have significant limitations with regards to the spectrum of detectable attacks. Indeed, no single method is immune to all forms of GPS spoofing; therefore, a truly effective solution requires an amalgam of techniques to form a composite detection strategy.

This research seeks to address a critical vulnerability within the United States power grid, which lacks protection against even the simplest forms of GPS spoofing attacks. As GPS, or more generally GNSS, becomes a

fundamental component of our nation's advancing critical infrastructure, we must develop and implement effective countermeasures to secure these vital sectors against malicious attacks, as well as to maintain the integrity of this key government asset used world-wide.

REFERENCES

[1] United States Congress, "Energy independence and security act (EISA) of 2007: New and enhanced FEMP responsibilities," 2009.

[2] North American Synchrophasor Initiative (NASPI), "NASPI synchrophasor starter kit," Oct. 2015.

[3] *Navstar GPS Space Segment/Navigation User Interfaces (ICD-GPS-200C with IRN-200C-004)*, Department of Defense, U.S. Government Printing Office Std., Apr. 2000.

[4] M. L. Psiaki and T. E. Humphreys, "Protecting GPS from spoofers is critical to the future of navigation," *IEEE Spectrum*, vol. 10, July 2016.

[5] *IEEE Standard for Synchrophasors for Power Systems*, IEEE Std. C37.118-2005, 2006.

[6] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domínguez-García, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3263, 2013.

[7] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[8] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Going up against time: The power grid's vulnerability to GPS spoofing attacks," *GPS World*, 2012.

[9] NERC Steering Group, "Technical analysis of the August 14, 2003, blackout: What happened, why, and what did we learn?" North American Electric Reliability Corporation (NERC), Tech. Rep., July 2004.

[10] J. R. Minkel, "The 2003 Northeast blackout - Five years later," *Scientific American*, Aug. 2008.

[11] G. B. Anderson and M. L. Bell, "Lights out: Impact of the August 2003 power outage on mortality in New York, NY," *Epidemiology*, vol. 23, no. 2, pp. 189–193, 2012.

[12] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Radionavigation laboratory conference proceedings*, 2008.

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

[14] "GPS World's 8th annual simulator buyers' guide features tools, devices, and software from leading providers," 2019. [Online]. Available: https://www.gpsworld.com/2019-simulator-buyers-guide/

[15] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann, 2015.

[16] T. Ebinuma, "Software-defined GPS signal simulator," 2015. [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[17] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-arrival assisted sequential spoofing detection and mitigation," *Proceedings of the 2016 International Technical Meeting of the Institute of Navigation*, pp. 181–192, 2016.

[18] A. P. Melikhova and I. A. Tsikin, "Angle of arrival method for global navigation satellite systems integrity monitoring," *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunication and Control Systems*, no. 1, pp. 37–48, 2015.

[19] I. A. Tsikin and A. P. Melikhova, "Optimization of angle-of-arrival GPS integrity monitoring," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer, 2015, pp. 722–728.

[20] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, and T. E. Humphreys, "GNSS spoofing detection using two-antenna differential carrier phase," in *Radionavigation Laboratory Conference Proceedings*, 2014.

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

[22] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Radionavigation Laboratory Conference Proceedings*, 2011.

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

[24] T. E. Humphreys, J. A. Bhatti, D. Shepard, and K. Wesson, "A testbed for developing and evaluating GNSS signal authentication techniques," in *Radionavigation Laboratory Conference Proceedings*, 2014.

[25] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS spoofing detection utilizing metrics from commercial receivers," in *Proceedings of the 2018 International Technical Meeting of the Institute of Navigation, Reston, VA*, 2018.

[26] D. Margaria, G. Marucco, and M. Nicola, "A first-of-a-kind spoofing detection demonstrator exploiting future Galileo E1 OS authentication," in *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. IEEE, 2016, pp. 442–450.

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

[28] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003)*, 2001, pp. 1543–1552.

[29] K. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing," *GPS World*, vol. 23, no. 1, pp. 32–39, 2012.

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

[31] J. T. Curran, M. Paonni, and J. Bishop, "Securing the open-service: A candidate navigation message authentication scheme for Galileo E1 OS," in *European Navigation Conference,(ENC-GNSS)*, 2014.

[32] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000*. IEEE, 2000, pp. 56–73.

[33] A. Perrig, D. Song, R. Canetti, J. Tygar, and B. Briscoe, "Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction," The Internet Society, Informational Memo, 2005.

[34] 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*, vol. 49, no. 4, pp. 2250–2267, 2013.

[35] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," *Inside GNSS*, vol. 4, no. 5, pp. 30–39, 2009.

[36] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," *NAVIGATION*, vol. 60, no. 4, pp. 267–278, 2013.

[37] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Radionavigation Laboratory Conference Proceedings*, 2011.

[38] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1794–1805, 2014.

[39] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing for power systems via a network of receivers for power systems," in *Proceedings of the IEEE/ION PLANS Conference*, 2018, pp. 1485 – 1491.

[40] T. Y. Mina, S. Bhamidipati, and G. X. Gao, "Detecting GPS spoofing via a multi-receiver hybrid communication network for power grid timing verification," in *Proceedings of the ION GNSS Conference*, 2018, pp. 2963–2977.

[41] T. Y. Mina, S. Bhamidipati, and G. X. Gao, "GPS spoofing detection for the power grid network using a multi-receiver hierarchical framework architecture," *NAVIGATION*, (submitted).

[42] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance (rev. 2nd edition).* Lincoln, MA: Ganga-Jamuna Press, 2006.

[43] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications Second Edition.* Artech House, 2006.

[44] NASPI Time Synchronization Task Force, "Time synchronization in the electric power system," North American Synchrophasor Initiative, Tech. Rep., 2017.

[45] *NERC Standard CIP-014-2: Physical Security*, North American Electric Reliability Corporation (NERC) Std. CIP-014-2, 2015.

[46] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*. ACM, 2011, pp. 75–86.

[47] J. E. Dagle, "North American SynchroPhasor Initiative (NASPI)," in *Proceedings of Hawaii International Conference on System Sciences*, 2008, pp. 165–168.

[48] Y. Hu, M. Donnelley, H. Tram, B. Uluski, K. Martin, M. Cioni, T. Helmer, and M. Govindarasu, *Phasor Gateway Technical Specifications for North American Synchro-Phasor Initiative Network (NASPInet)*, North American Synchrophasor initiative Std., May 2009.

[49] P. T. Myrda and K. Koellner, "NASPInet – the Internet for synchrophasors," in *43rd Hawaii International Conference on System Sciences*. IEEE, 2010, pp. 1–6.

[50] Y. Hu, M. Donnelly, H. Tram, B. Uluski, and K. Martin, *Data Bus Technical Specifications for North American Synchro-Phasor Initiative Network (NASPInet)*, North American Synchrophasor Initiative Std., 2009.

[51] E. Wycoff, Y. Ng, and G. X. Gao, "Python GNSS receiver: An object-oriented software platform suitable for multiple receivers," *GPS World*, 2015.