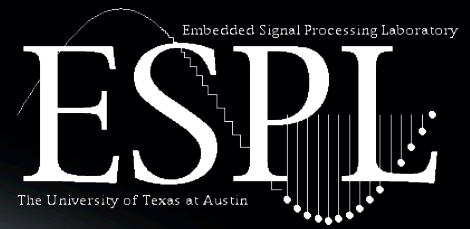




THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY




Probabilistic Secure Time Transfer: Challenges ~~and Opportunities~~ for a Sub-Millisecond World

Kyle D. Wesson, Prof. Todd E. Humphreys, Prof. Brian L. Evans
The University of Texas at Austin

UT  ECE

 Aerospace Engineering
and Engineering Mechanics

University of Texas at Austin 
Center for Space Research

 Wireless Networking &
Communications Group

Embedded Signal Processing Laboratory
ESPL
The University of Texas at Austin


THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Sources of Time and Frequency

• GPS

- 10 ns Time Accuracy
- 1×10^{-13} Frequency Stability

• WWVB

- 0.1 – 15 ms Time Accuracy
- 1×10^{-10} - 1×10^{-12} Frequency Stability

• ITS* (NTP)

- 10 ms Time Accuracy
- 1×10^{-7} Frequency Stability

*Internet Time Service

• ITS* (PTP)

- 0.1 ms Time Accuracy
- 1×10^{-9} Frequency Stability

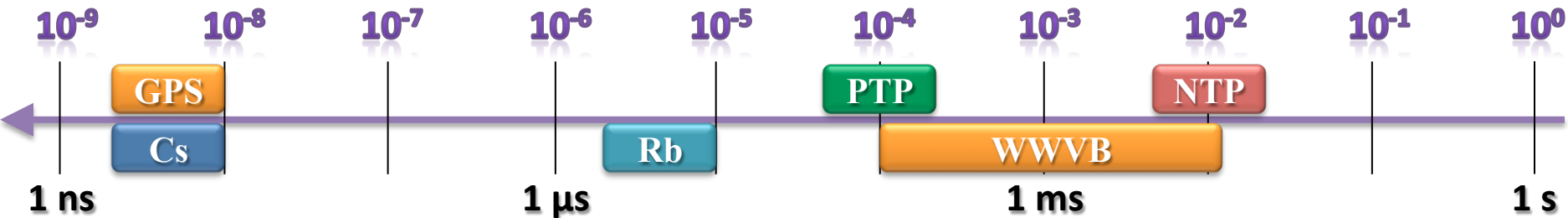
*Internet Time Service

• Cesium (Cs) Clock

- 10 ns Time Accuracy
- Cannot Recover Time independently
- 1×10^{-13} Frequency Stability

• Rubidium (Rb) Clock

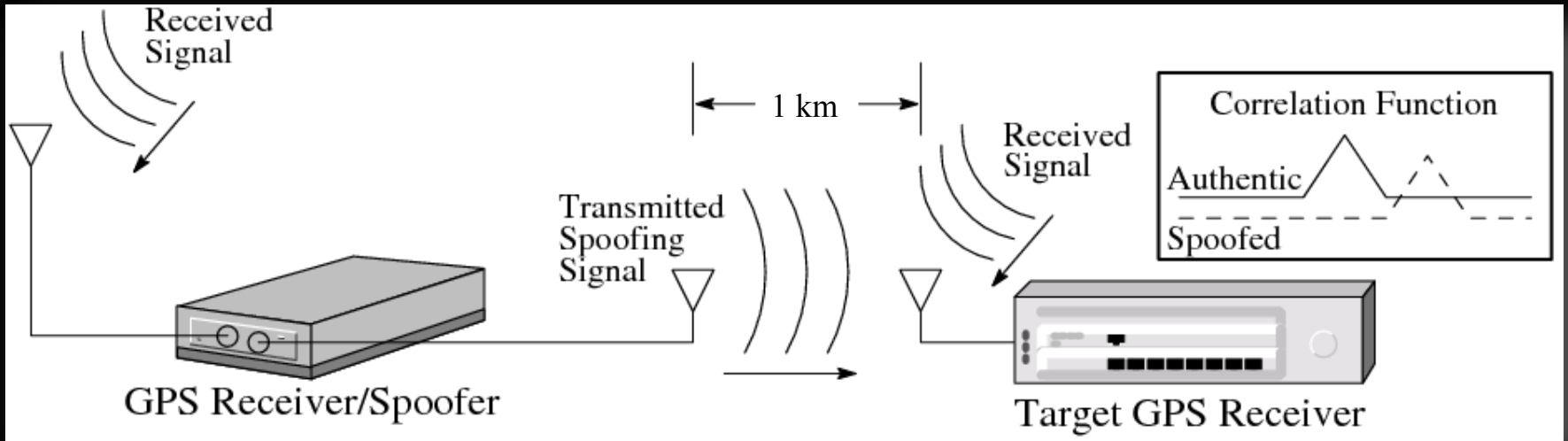
- 10 μ s Time Accuracy
- Cannot Recover Time Independently
- 5×10^{-11} Frequency Stability



| Critical Infrastructure/Key Resource Sector | Uses GPS Timing? | |
|---|------------------|----|
| | Yes | No |
| Communications Sector | X | |
| Emergency Services Sector | X | |
| Information Technology Sector | X | |
| Banking & Finance Sector | X | |
| Healthcare & Public Health Sector | X | |
| Energy/Electric Power and Oil & Natural Gas SubSector | X | |
| Nuclear Sector | X | |
| Dams Sector | X | |
| Chemical Sector | X | |
| Critical Manufacturing | X | |
| Defense Industrial Base Sectors | X | |
| Postal & Shipping Sector | X | |
| Transportation Sector | X | |
| Government Facilities Sector | X | |
| Commercial Facilities Sector | X | |
| National Monuments and Icons Sector | | X |
| Agriculture and Food Sector | | X |
| Water and Wastewater Sector | | X |

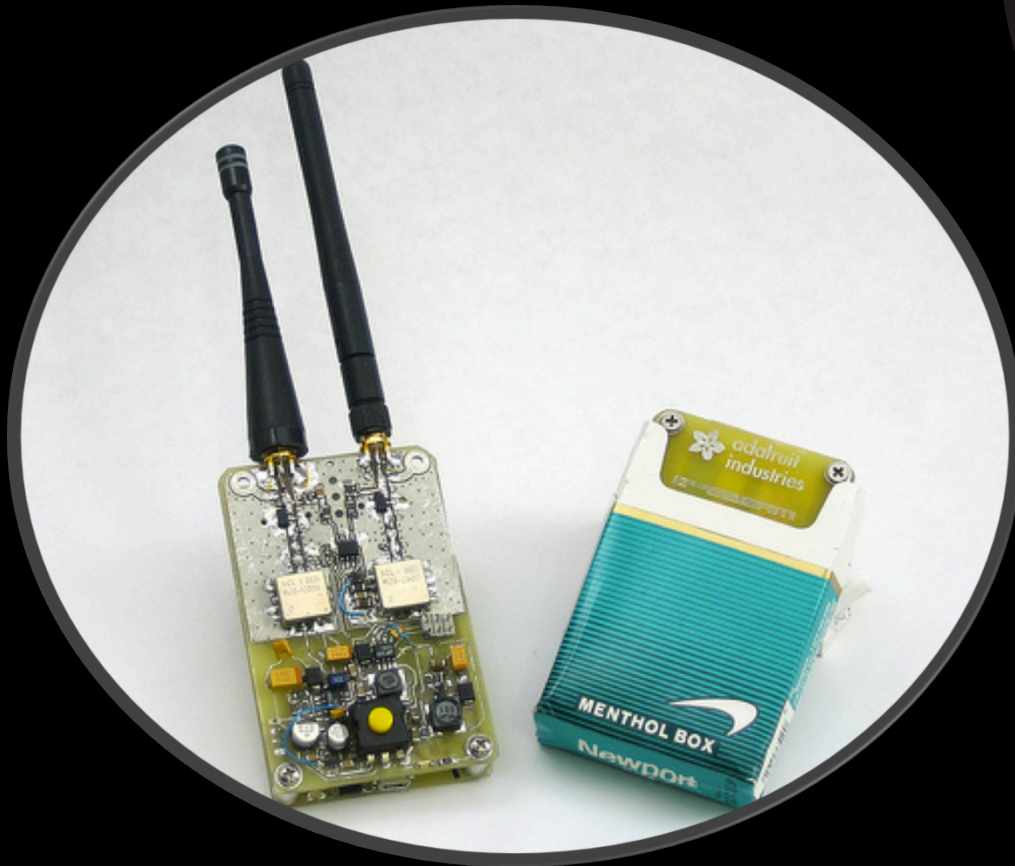
Challenges

- Can't trust civil GPS receivers to deliver secure time
 - Can't defend against a near-zero-delay meaconing attack
 - Can't verify pending leap second changes in advance
 - Can't catch a patient time saboteur by comparison with local clocks
 - Can't distinguish multipath from spoofing on dynamic platform



| | Attack | Description |
|-----------------|-------------------------------------|--|
| Jamming | Unintentional | Solar radio bursts |
| | Intentional | Denial of service via RF noise |
| Spoofing | Meaconing | Record and playback of entire RF spectrum |
| | Security Code Estimation and Replay | Estimate security code on-the-fly and playback with estimated value to defeat security enhanced GPS (not publically available) |
| | Data Bit Forgery | Alter ephemeris or leap second indicators |

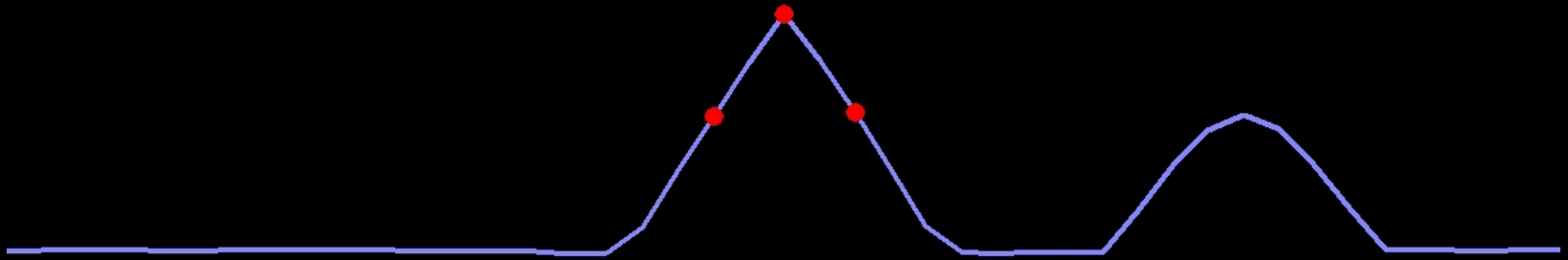
GPS Jammers



University of Texas Spoofing Testbed



GPS Spoofer



IEEE **spectrum** INSIDE TECHNOLOGY
MAGAZINE MULTIMEDIA

AEROSPACE BIOMEDICAL COMPUTING CONSUMER ELECTRONICS ENERGY

riskfactor The views expressed and do not represent o

BLOGS // THE RISK FACTOR

Commercial Drones and GPS Spoofers a Bad Mix

POSTED BY: ROBERT N. CHARETTE / MON, JUNE 25, 2012

19




Researchers at the [University of Texas at Austin Radionavigation Laboratory](#) have successfully demonstrated that a drone with an unencrypted GPS system can be taken over by a person wielding a GPS spoofing device. You can see a video accompanying a Fox News [story](#) on it, as well as a video [here](#) of an experiment conducted by the researchers, led by Professor [Todd Humphreys](#).

Drone Hijacking? That's Just the Start of GPS Troubles

By Lorenzo Franceschi-Blochieral July 6, 2012 | 6:30 am | Categories: Crime and Homeland Security, Drones

Follow @lorenzoFI

Like 271
Tweet 452
+1 43
Share 41



The University of Texas Radionavigation Laboratory drone, an Adaptive Flight Hornet Mini. Photo: Courtesy Todd Humphreys

On the evening of June 19, a group of researchers from the University of Texas successfully hijacked a civilian drone at the White Sands Missile Range in New Mexico during a test organized by the Department of Homeland Security.

FOX NEWS .com Fair & Balanced


ON AIR NOW 7pst FOX Report w/ Shepard Smith WATCH

Home Video Politics U.S. Opinion Entertainment Tech Science Health Travel

Technology Home Gadgets Military Tech

EXCLUSIVE: Drones vulnerable to terrorist hijacking, researchers say

By John Roberts / Published June 25, 2012 / FoxNews.com



A small surveillance drone flies over an Austin stadium, diligently following a series of GPS waypoints that have been programmed into its flight computer. By all appearances, the mission is routine.

Suddenly, the drone veers dramatically off course, careering eastward from its intended flight path. A few moments later, it is clear something is seriously wrong as the drone makes a hard right turn, streaking toward the south. Then, as if some phantom has given the drone a self-destruct order, it hurtles toward the ground. Just a few feet from certain

Print
Email
Share
Comments
Like 68
Tweet 27

Institutional Investor

Career Center Video Archive eBooks

Asset Management Hedge Funds & Alternatives Investors Banking & Capital Markets People

Exchanges Risk Management Technology Trading

Home > [Trading & Technology](#) > Could GPS Hackers Cause the Next Flash Crash?

20 21 22

Could GPS Hackers Cause the Next Flash Crash?

GPS attacks risk maritime disaster, trading chaos

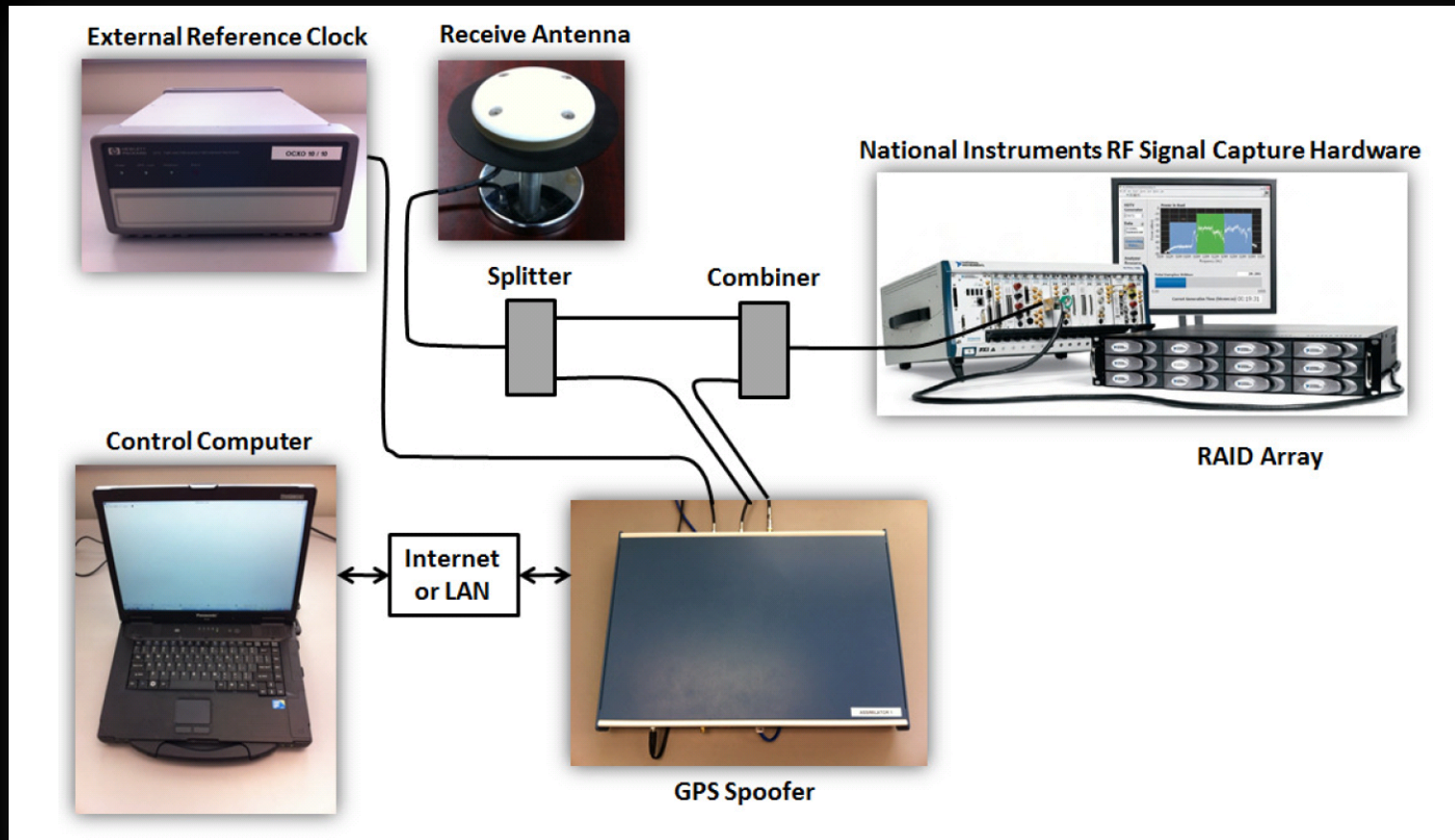
Recommend 27 people recommend this. Sign Up to see what your friends recommend.

Tue Feb 21, 2012 7:01pm EST

- * Jamming of GPS now poses real danger-experts
- * Tests show serious impact on ships in English Channel
- * GPS "spoofing" could pose serious risk to markets

Tweet 24
Share
Share this

The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques



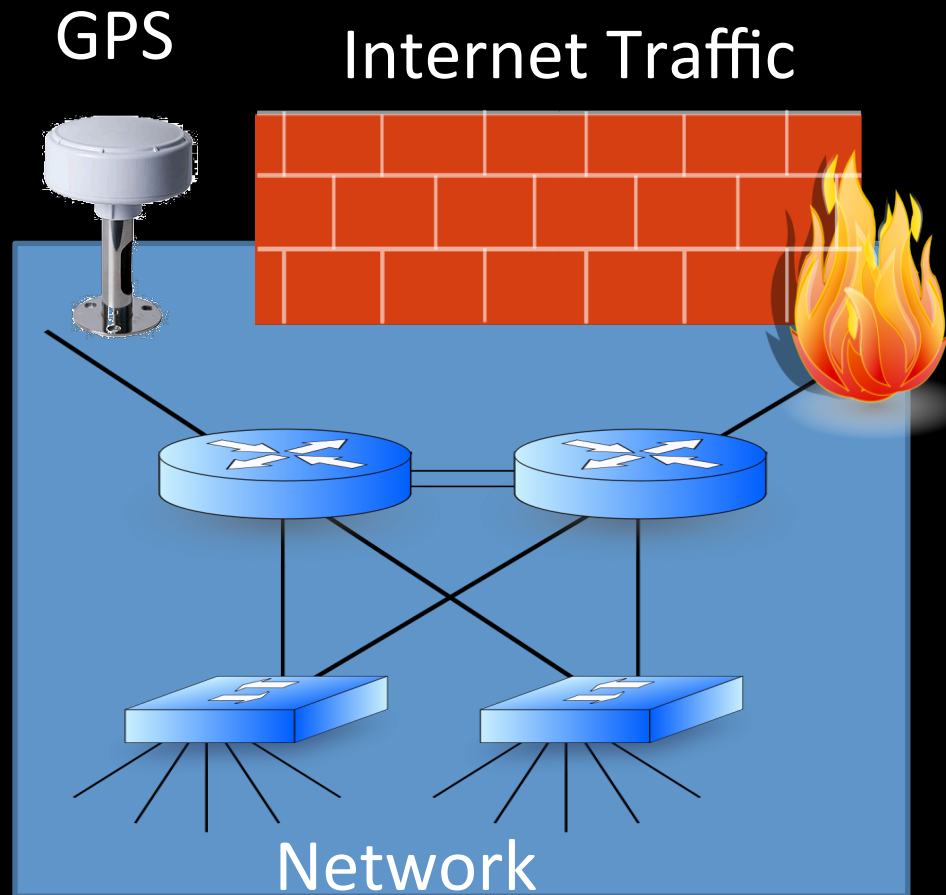
Challenges

- Can't trust civil GPS receivers to deliver secure time
 - Can't defend against a near-zero-delay meaconing attack
 - Can't verify pending leap second changes in advance
 - Can't catch a patient time saboteur by comparison with local clocks
 - Can't distinguish multipath from spoofing on dynamic platform
- Can't trust other dependent time systems

NTP/PTP Timing Attacks

| | Attack | Description |
|-----------------|----------------------|--|
| Jamming | Unintentional | Network failure |
| | Intentional | Denial of service (flood network with bogus traffic) |
| Spoofing | Delay/Replay | Man-in-the-middle rebroadcast to alter delay estimates |
| | Masquerade | Act as false grandmaster |
| | Message Modification | Modify message content |

Hybrid Cyber-Physical Attacks



Challenges

- Can't trust civil GPS receivers to deliver secure time
 - Can't defend against a near-zero-delay meaconing attack
 - Can't verify pending leap second changes in advance
 - Can't catch a patient time saboteur by comparison with local clocks
 - Can't distinguish multipath from spoofing on dynamic platform
- Can't trust other time systems
- Can't make strong guarantees: timing demands a probabilistic security model

Detection Strategy for Cryptographic GNSS Anti-Spoofing

Todd E. Humphreys

Abstract—A strategy is presented for detecting spoofing attacks against cryptographically-secured Global Navigation Satellite System (GNSS) signals. The strategy is applicable both to military Global Positioning System signals and to proposed security-enhanced civil GNSS signals, whose trustworthiness is increasingly an issue of national security. The detection strategy takes the form of a hypothesis test that accounts for the statistical profile of a replay-type spoofing attack. A performance and robustness evaluation demonstrates that the detection test is both powerful and tolerant of some uncertainty in the threat model. The test is validated by experiments conducted on a spoofing testbed.

Keywords: Cryptographic anti-spoofing, GNSS security, GNSS spoofing detection.

I. INTRODUCTION

Spoofing is no longer a concern only for military Global Positioning System (GPS) users. Spoofing attacks, in which counterfeit GPS signals are generated for the purpose of manipulating a target receiver's reported position and time, have been demonstrated with low-cost commercial equipment against a wide variety of civil GPS receivers [1], [2]. The growing dependence of critical civil infrastructure on GPS—for transportation, communication, energy distribution, and banking and finance—makes civil GPS spoofing not only an economic and safety threat but also a matter of national security [3]–[5].

Military GPS signals have long been protected against spoofing by a cryptographic anti-spoofing technique whereby a binary chipping sequence that is only predictable to authorized users modulates the GPS carrier [6]. A growing literature recommends similar techniques be applied to protect civil GPS signals [7], [8] and other Global Navigation Satellite System (GNSS) signals [9], [10]. As opposed to anti-spoofing techniques that depend on accurate inertial measurements [11] or multiple antennas [12], cryptographic spoofing defenses are attractive because they can be implemented without additional hardware. Navigation message authentication (NMA), the insertion of a public-key digital signature into the low-rate (50 Hz) civil navigation message stream, is viewed as a practical near-term approach to securing civil GNSS signals [7]–[9], [13].

For cryptographic techniques to be effective against GNSS spoofing, a proper detection test must be implemented within each secured receiver. What little has been written on this subject in the open literature has observed that spoofing can be

Authors' address: Department of Aerospace Engineering, The University of Texas at Austin, Austin TX, 78712. Email: todd.humphreys@mail.utexas.edu.

detected as a drop in the correlation power over an encrypted interval [7]. But this simple detection technique is far from optimal against an attack in which the spoofer attempts to estimate, manipulate, and replay a cryptographically-secured GNSS signal in real-time. It is especially ineffective for NMA-secured signals, which manifest no detectable drop in the standard correlation power under a replay attack. What is needed is an open and thorough statistical treatment of the spoofing detection problem for cryptographically-secured GNSS signals.

This paper makes three principal contributions. First, it develops a model for sophisticated spoofing attacks against security-enhanced GNSS signals. Second, it derives a unified near-optimal detection strategy for such attacks. The strategy is applicable to both low-rate cryptographic techniques such as NMA and high-rate techniques such as legacy military GPS Y-code encryption. Third, and contrary to a previous study [14], this paper demonstrates that with a proper detection test NMA is effective for anti-spoofing. This result is significant given the immediate need for a practical defense against civil GNSS spoofing.

II. GENERALIZED MODEL FOR SECURITY-ENHANCED GNSS SIGNALS

Consider the following model for the digital signal exiting the radio frequency (RF) front-end of a GNSS receiver:

$$Y_k = w_k c_k \cos(2\pi f_{IF} t_k + \theta_k) + N_k \quad (1)$$

Here, at sample index k , w_k is a ± 1 -valued security code with chip length T_w , c_k is a known ± 1 -valued spreading (ranging) code with chip length T_c , t_k is receiver time, f_{IF} is the intermediate value of the downmixed carrier frequency, θ_k is the beat carrier phase, and N_k is a sequence of independent, identically distributed zero-mean Gaussian noise samples with variance σ^2 that model the effects of thermal noise and interfering signals. The variance σ^2 and the unity signal amplitude imply a carrier-to-noise ratio

$$C/N_0 = \frac{1}{4\sigma^2 T_s} \quad (2)$$

where T_s is the sampling interval.

This model considers only a single GNSS signal corresponding to a unique combination of spreading code and carrier frequency. A single-signal model is appropriate because although a spoofer may generate counterfeit replicas of an entire ensemble of GNSS signals, the spoofing detection problem can be treated at the level of individual signals within the ensemble.

Practical Cryptographic Civil GPS Signal Authentication

Kyle Wesson, Mark Rothlisberger, and Todd Humphreys

Abstract—A practical technique is proposed to authenticate civil GPS signals. The technique combines cryptographic authentication of the GPS navigation message with signal timing authentication based on statistical hypothesis tests to secure civil GPS receivers against spoofing attacks. The notion of GNSS signal authentication is defined in probabilistic terms. Candidate GPS signal authentication schemes are evaluated in terms of effectiveness and practicality leading to a proposal for incorporating digital signatures into the extensible GPS civil navigation (CNAV) message. The proposal is sufficiently detailed to facilitate near-term implementation of security-hardened civil GPS.

I. INTRODUCTION

In the decade since Selective Availability was discontinued in 2000, civil technologies based on the Global Positioning System (GPS) have become ubiquitous and the GPS service has easily achieved the stated goal of the new policy regime, which is to “encourage acceptance and integration of GPS into peaceful civil, commercial, and scientific applications worldwide; and to encourage private sector investment in and use of U.S. GPS technologies and services” [1]. Also over the past decade, the concept of national security has evolved from a focus on protecting military and critical government resources to a broader ambit that includes the protection of vital elements of civilian and commercial infrastructure. Civil GPS is a critical component of the national infrastructure; hence, GPS security is a matter of national security.

In 2001, the U.S. Department of Transportation published a report assessing the vulnerability of the U.S. transportation infrastructure to disruption of civil GPS [2]. Known as the Volpe report, it highlighted the threats posed by spoofing and man-in-the-middle attacks—methods by which a victim GPS receiver is deceived into tracking counterfeit GPS signals. At the time, the open literature contained little research on such attacks and possible countermeasures. Accordingly, the report recommended further study of GPS spoofing and development of civil GPS anti-spoofing techniques. Global Navigation Satellite System (GNSS) security research over the past decade has made much progress toward this goal [3]–[11].

It is convenient to distinguish cryptographic spoofing defenses, which rely on secret keys that encrypt or digitally sign components of the broadcast signals, from non-cryptographic

Authors' addresses: Kyle Wesson, Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin TX, 78712. Email: (kyle.wesson@utexas.edu). Mark Rothlisberger, Department of Mathematics, The University of Texas at Austin, Austin, TX, 78712. Email: (mark.rothlisberger@math.utexas.edu). Todd Humphreys, Department of Aerospace Engineering, The University of Texas at Austin, Austin TX, 78712. Email: (todd.humphreys@mail.utexas.edu).

defenses, which do not depend on encryption or digital signatures. Among non-cryptographic defenses, the multi-antenna defense [10] appears to be one of the strongest, although it remains vulnerable to the coordinated spoofing attack explored in [9]. This defense requires two or more antennas spaced by an appreciable fraction of the approximately 20-cm GPS signal wavelength, which would tend to increase receiver cost, weight, and size. As a result, the multi-antenna defense is unlikely to be widely adopted by commercial GPS manufacturers. This is also true of other non-cryptographic defenses involving inertial measurement units or other hardware, which would exceed the cost, mass, or size constraints of a broad range of applications.

Cryptographic spoofing defenses are attractive because they offer significant protection against spoofing relative to the additional cost and bulk required for implementation. While it must be conceded that no anti-spoofing technique is impervious to the most sophisticated attacks, a cryptographic defense significantly raises the bar for a successful attack and can be combined with non-cryptographic spoofing defenses for better security than either category could offer separately.

Several civil GPS cryptographic spoofing defenses have been proposed whose implementation would require fundamental changes to the legacy GPS signal structure (e.g., [3], [4], [7]). These defenses are unlikely to be implemented over the next decade given the static nature of GPS signal definitions [12].

A growing literature suggests navigation message authentication (NMA) is a practical basis for civil GPS signal authentication [3], [6], [7], [13]. In NMA, the low-rate navigation message is encrypted or digitally signed, allowing a receiver to verify that the GPS Control Segment generated the data. NMA could be implemented without fundamental changes to the GPS Interface Specification by exploiting the extensibility of the modern GPS civil navigation (CNAV) messaging format. Moreover, NMA has been proposed for implementation in the European Galileo GNSS [5], [14].

Strictly speaking, NMA only authenticates the navigation message. Reference [15], which considers NMA for civil GPS anti-spoofing, recognizes this fact and further concludes that NMA is not useful for authenticating the underlying civil GPS signal. Contrary to Ref. [15], the combination of this paper and the statistical test recently developed in Ref. [16] demonstrates that NMA can in fact offer comprehensive civil GPS signal authentication if it is paired with timing authentication based on statistical hypothesis tests.

The present work offers four main contributions beyond those given in [3], [5]–[7], [13], [14]. First, it develops a

Security-Enhanced GNSS Signal Model

$$\begin{aligned} Y_k &= w_k c_k \cos(2\pi f_{IF} t_k + \theta_k) + N_k \\ &= w_k s_k + N_k \end{aligned}$$

- Security code w_k :
 - Generalization of binary modulating sequence
 - Either fully encrypted or contains periodic authentication codes
 - Unpredictable to would-be spoofer

Attacking Security-Enhanced GNSS Signals

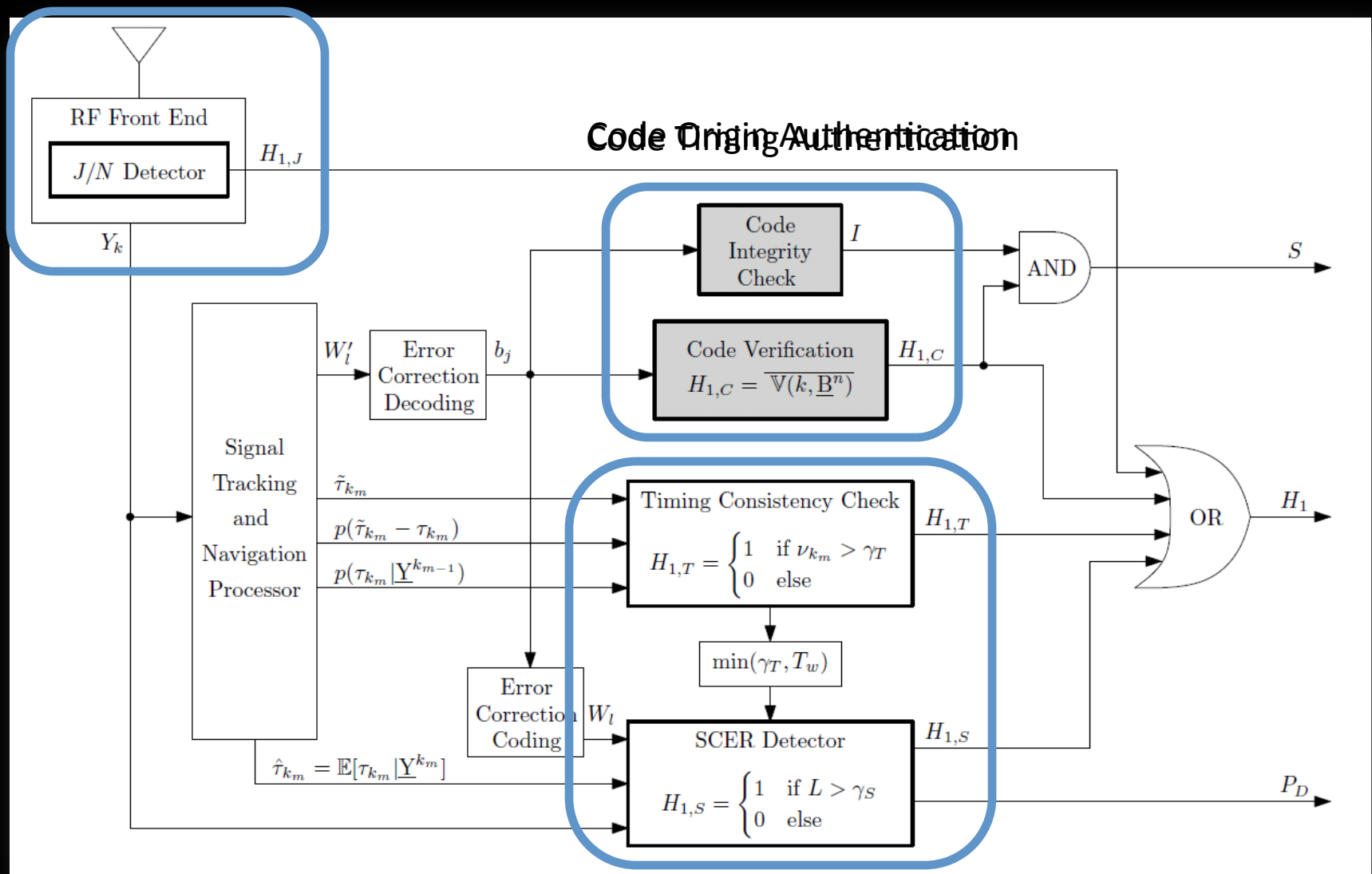
1. **Meaconing:** Spoofer records and re-broadcasts entire block of RF spectrum containing ensemble of GNSS signals

$$Y_k = \alpha w_{k-d} s_{k-d} + N_{m,k} + w_k s_k + N_k$$

2. **Security Code Estimation and Replay (SCER) Attack:** Spoofer estimates unpredictable security code chips from authentic signals on-the-fly

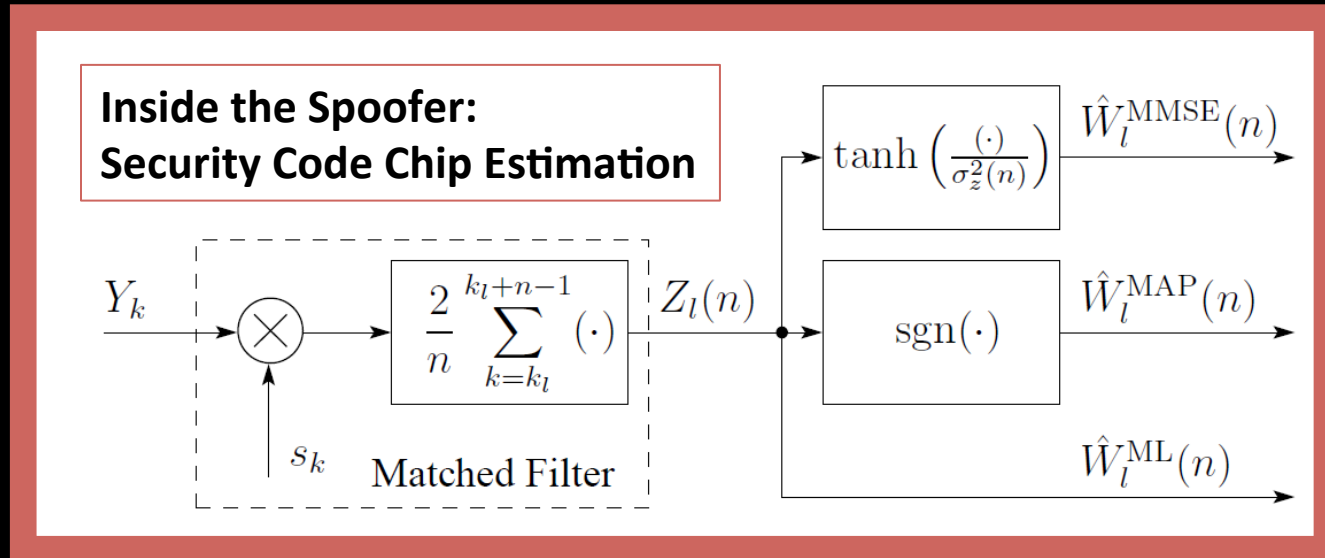
$$Y_k = \alpha \hat{w}_{k-d} s_{k-d} + w_k s_k + N_k$$

Public-Key Signal Authentication: Receiver Perspective

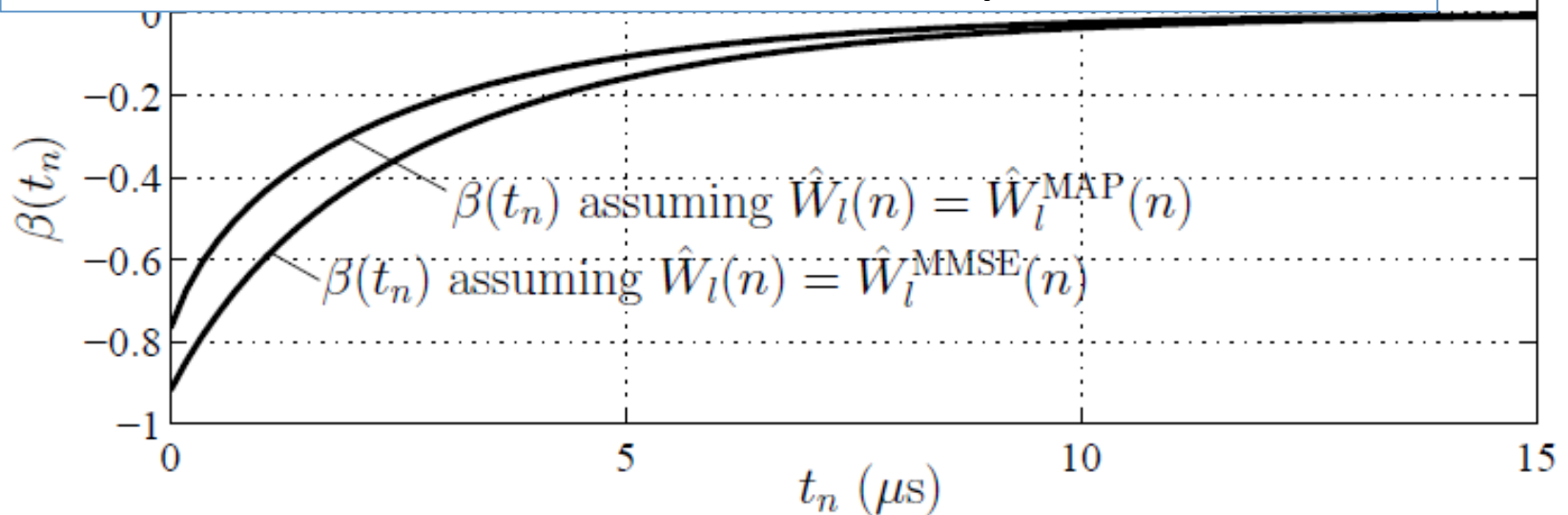


Wesson, K., Rothlisberger, M., and Humphreys, T. E., "Practical Cryptographic Civil GPS Signal Authentication," NAVIGATION: The Journal of the Institute of Navigation, 59(3):177-193.

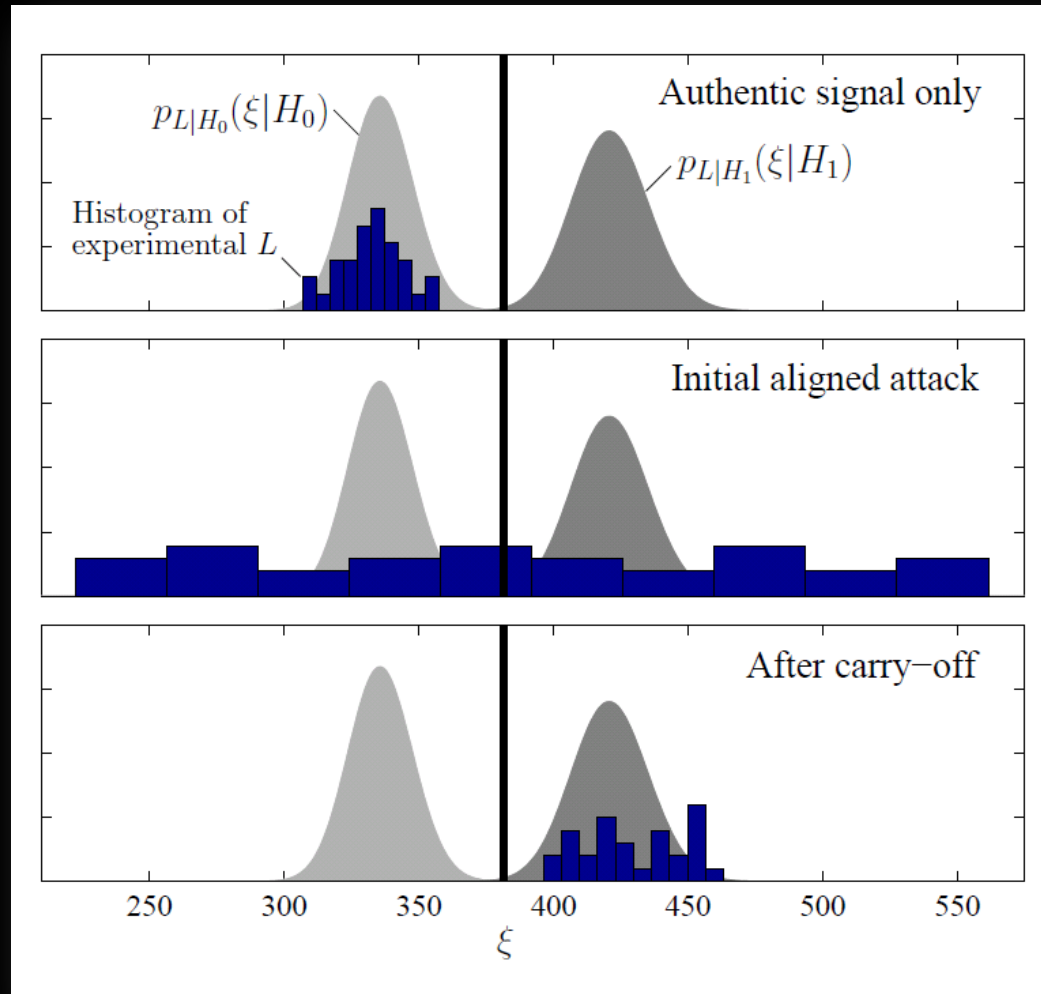
Security Code Estimation and Replay Detection



Inside the Defender: Detection Statistic Based on Specialized Correlations

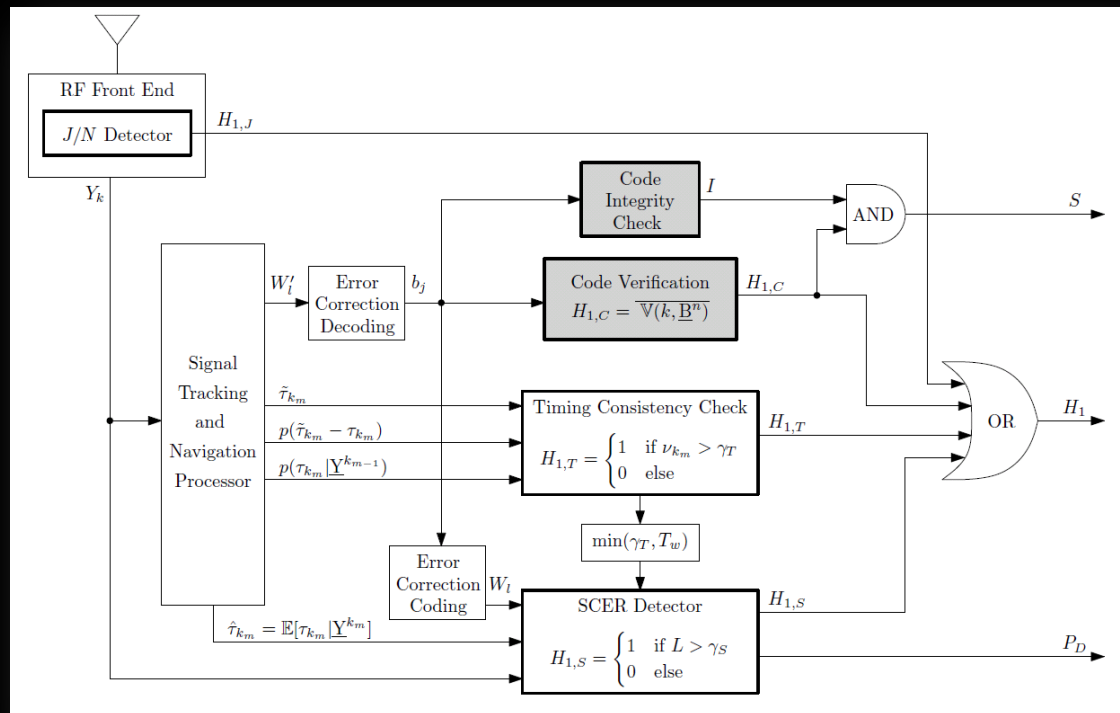


Security Code Estimation and Replay Detection: Hypothesis Testing During an Attack

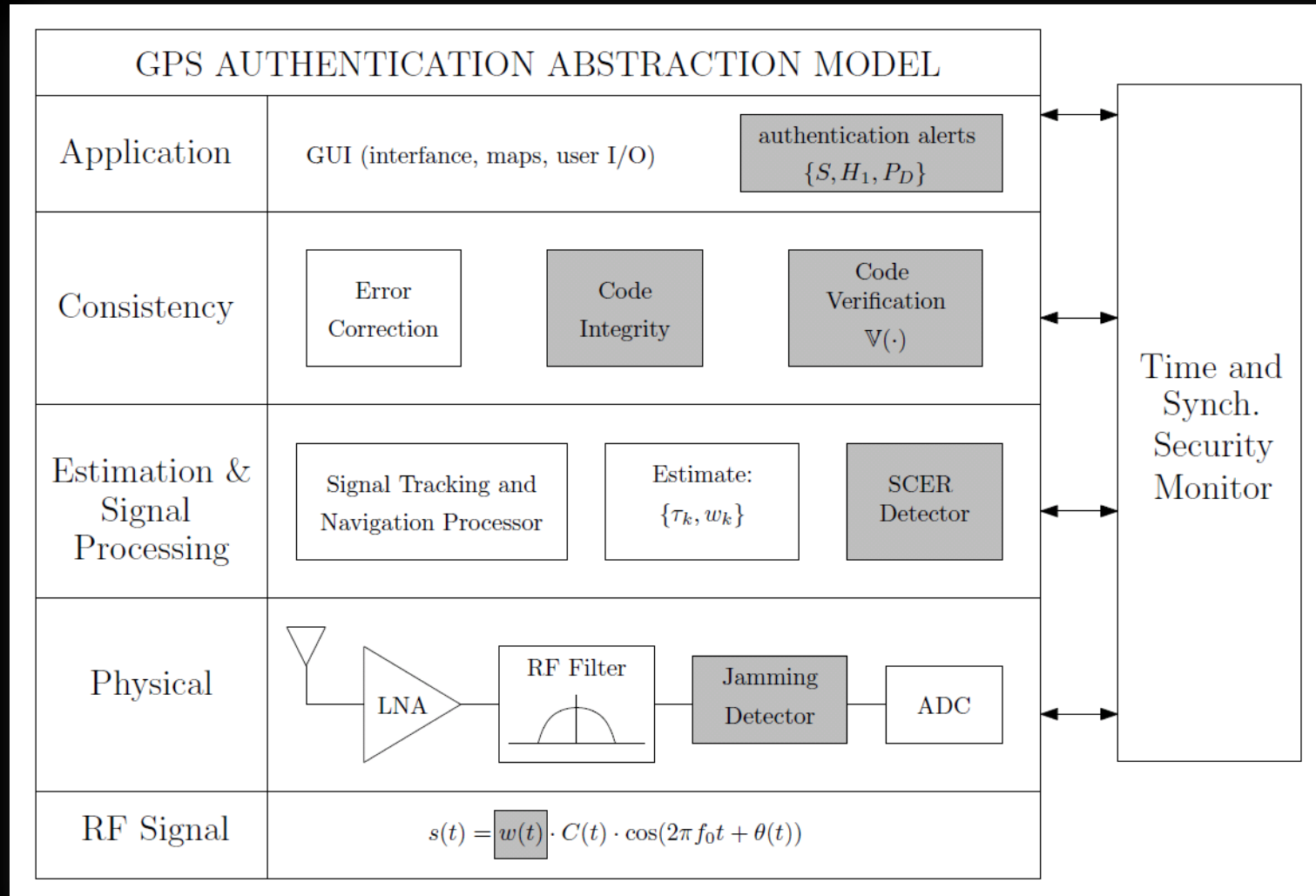


Operational Definition of GNSS Signal Authentication

- GNSS signal is declared authentic if since some trusted initialization event:
 1. logical output S has remained low, and
 2. logical output H_1 has remained low, and
 3. output P_D has remained above an acceptable threshold



What are essential elements to enable secure time transfer?



What are essential elements to enable secure time transfer?

| Layer | Description |
|-------------------|--|
| Application Level | User alerts and management |
| Consistency Level | Code verification and validation |
| Estimation Level | Security code estimation and replay attack detection |
| Physical Level | Jamming detection to detect intentional interference |
| Signal Level | Unpredictable bits or chips embedded in signal |

Challenges

- Can't trust civil GPS receivers to deliver secure time
 - Can't defend against a near-zero-delay meaconing attack
 - Can't verify pending leap second changes in advance
 - Can't catch a patient time saboteur by comparison with local clocks
 - Can't distinguish multipath from spoofing on dynamic platform
- Can't trust other time systems
- Can't make strong guarantees: timing demands a probabilistic security model