A Probabilistic Framework for GNSS Signal Timing Assurance

Kyle D. Wesson, Brian L. Evans, and Todd E. Humphreys

The University of Texas at Austin

Overview

- GNSS security is a concern because attackers can transmit spoofed signals that can deceive victim receivers.
- Our contribution is establishing necessary conditions for timing authentication of security-enhanced GNSS signals under a probabilistic framework that combines cryptographic and signal processing.

System Model

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

Security code w_k

- Generalization of binary modulating seq.
- Either fully encrypted or contains periodic authentication codes

Threat Model

Record and Playback: record and re-broadcast RF spectrum

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

Security Code Estimation and Replay (SCER) Attack: estimate security code on-the-fly without additional noise

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

Reference:

K.D. Wesson, B.L. Evans, and T.E. Humphreys (2013) "A Probabilistic Framework for Global Navigation Satellite System Signal Timing Assurance," *Asilomar SSC Conf.*

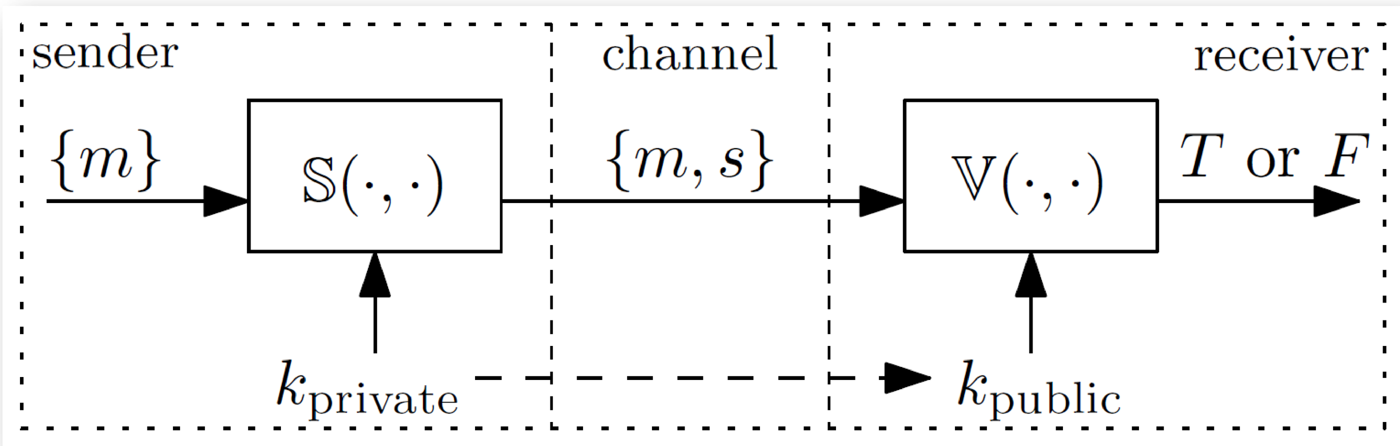
Radionavigation Lab: http://radionavlab.ae.utexas.edu

Embedded Signal Processing Lab: http://signal.ece.utexas.edu

Data Message Authentication

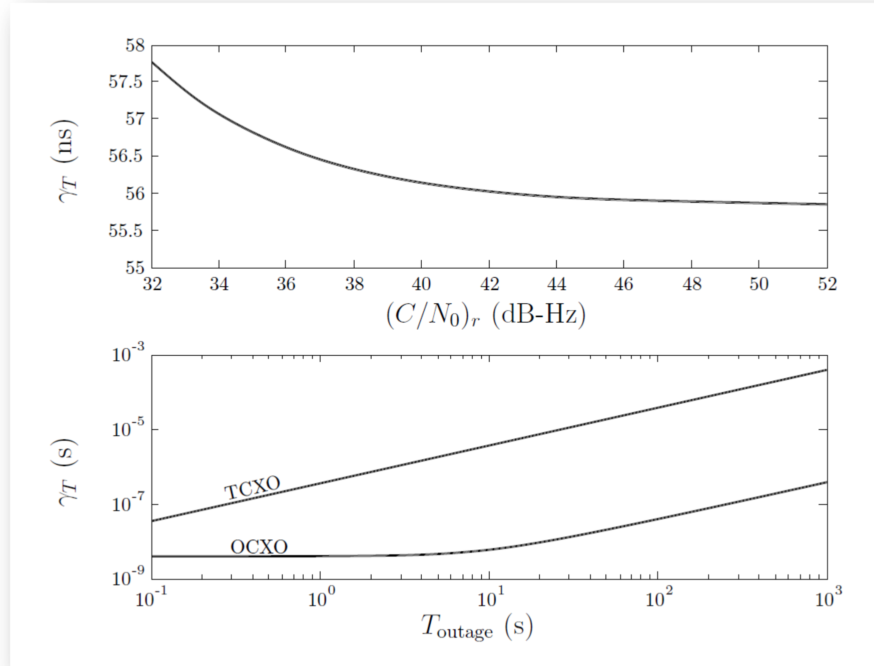
Predicated on computational infeasibility of

- performing brute-force search for secret key, or
- reversing one-way hash functions



Timing Consistency Check

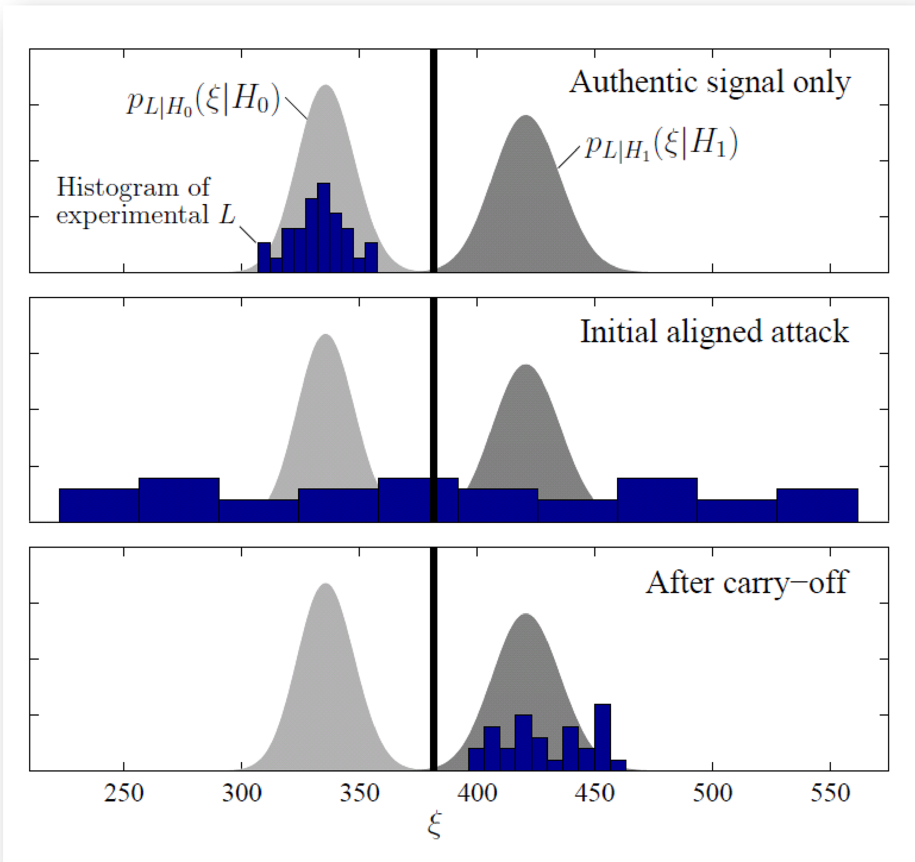
- Verifies incoming signal timing is consistent with receiver's time estimate
- Hypothesis test on difference between received and predicted code phase of spreading code



$$z = [\overline{\mathbb{V}} \wedge E, \nu, L, P_T, D]^T$$

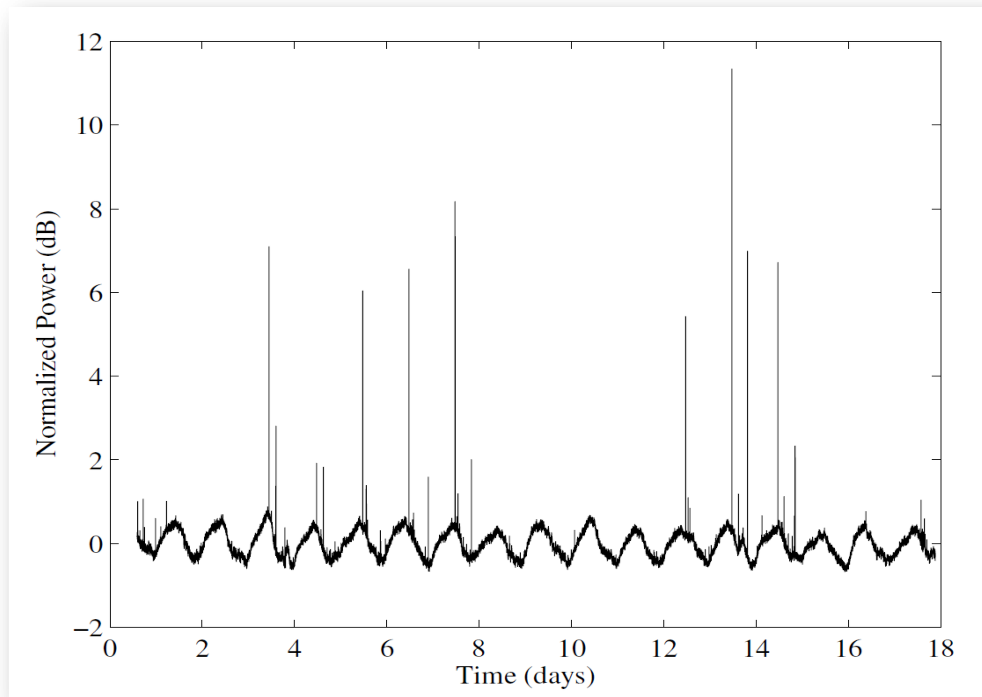
SCER Detector

- Hypothesis test at physical layer to detect if security code arrived intact and promptly
- Measures promptness and accuracy of incoming signal relative to receiver's local clock



Power Monitor

- Monitors nominal in-band power and detects when additional power is present due to spoofed signals
- Limits spoofer's power advantage



Distortion Monitor

Monitors distortions of a spoofing attack that result from interactions of authentic and spoofing signals