GPS Spoofing Detection System

Mark Psiaki & Brady O'Hanlon, Cornell Univ., Todd Humphreys & Jahshan Bhatti, Univ. of Texas at Austin

Abstract: A real-time method for detecting GPS spoofing in a narrow-bandwidth civilian GPS receiver is being developed. It is needed in order to detect malicious spoofed signals that seek to deceive a C/A-code civilian GPS receiver regarding its position or time. The ability to detect a spoofing attack is important to the reliability of systems ranging from cell-phone towers, the power grid, and commercial fishing monitors. The spoofing detector mixes and accumulates base-band quadrature channel samples from two receivers, one a secure reference receiver, and the other the defended User Equipment (UE) receiver. The resulting statistic detects the presence or absence of the encrypted P(Y) code that should be present in both signals in the absence of spoofing.

Solutions

- Use known, tracked civilian C/A code and known relationships between C/A and P(Y) code to guide correlation times and expected signal levels
- Analyze narrow-band filter power losses and distortion
- Develop signal detection statistical analysis to design reasonable accumulation intervals
- Use semi-codeless detection techniques by estimating W anti-spoofing bits in reference receiver and transmitting only those to UE
- Broadcast spoofing detection data over internet in real-time

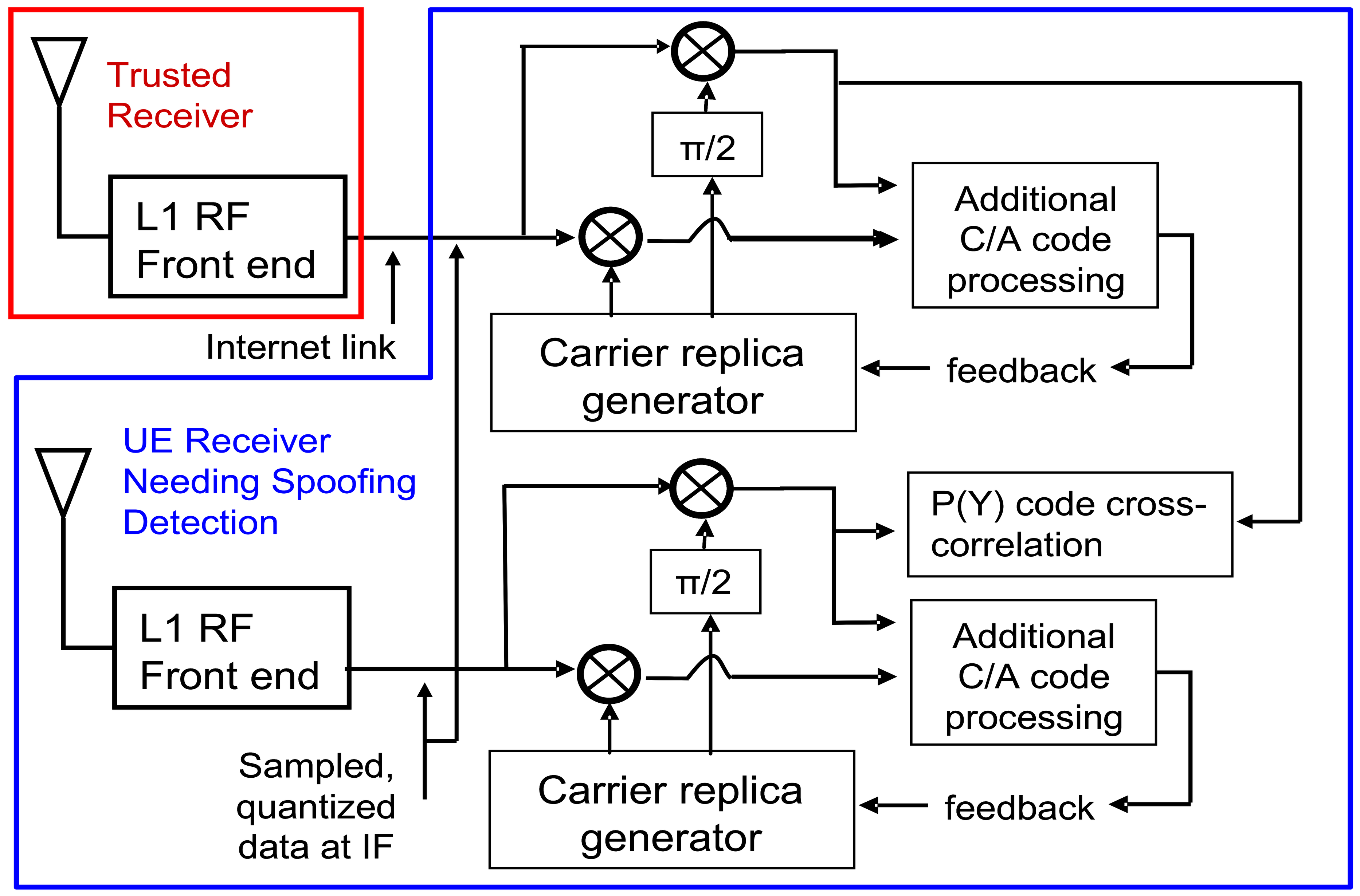

Figure 1. Spoofing detection receiver architecture.

Challenges

- Encrypted military P(Y) signal necessitates squaring operations and SNR loss
- Wide bandwidth of P(Y) code causes 75-80% power loss, further degrading SNR, and significant waveform distortions in narrow-band civilian receiver
- Bandwidth of communications link from trusted reference receiver to defended UE receiver
- Constrained real-time signal processing capabilities in low-power UE receiver

Codeless Detection Statistical Analysis

- Normalized detection statistic:

$$\gamma = \frac{\sum_{i=1}^{M} y_{rawAi}\, y_{rawBi}}{\sigma_{RFA}\sigma_{RFB}\sqrt{\frac{M}{4}\{1+2\Delta t(C/N_0)_A\}}}$$

- Predicted mean and variance absent spoofing:

$$\bar{\gamma} = 2\sqrt{\frac{T_{corr}\Delta t(C/N_0)_A(C/N_0)_B}{1+2\Delta t(C/N_0)_A}}$$

$$\sigma_\gamma = \sqrt{\frac{1+2\Delta t[(C/N_0)_A+(C/N_0)_B]}{1+2\Delta t(C/N_0)_A}}$$

- Detection threshold and probability of detection:

$$\alpha = \int_{-\infty}^{\gamma_{th}} p(\gamma\,|\,H_0)d\gamma = \int_{-\infty}^{\gamma_{th}} \mathcal{N}(\gamma;\bar{\gamma},\sigma_\gamma)d\gamma$$

$$P_{detect} = \int_{-\infty}^{\gamma_{th}} p(\gamma\,|\,H_1)d\gamma = \int_{-\infty}^{\gamma_{th}} \mathcal{N}(\gamma;0,1)d\gamma$$

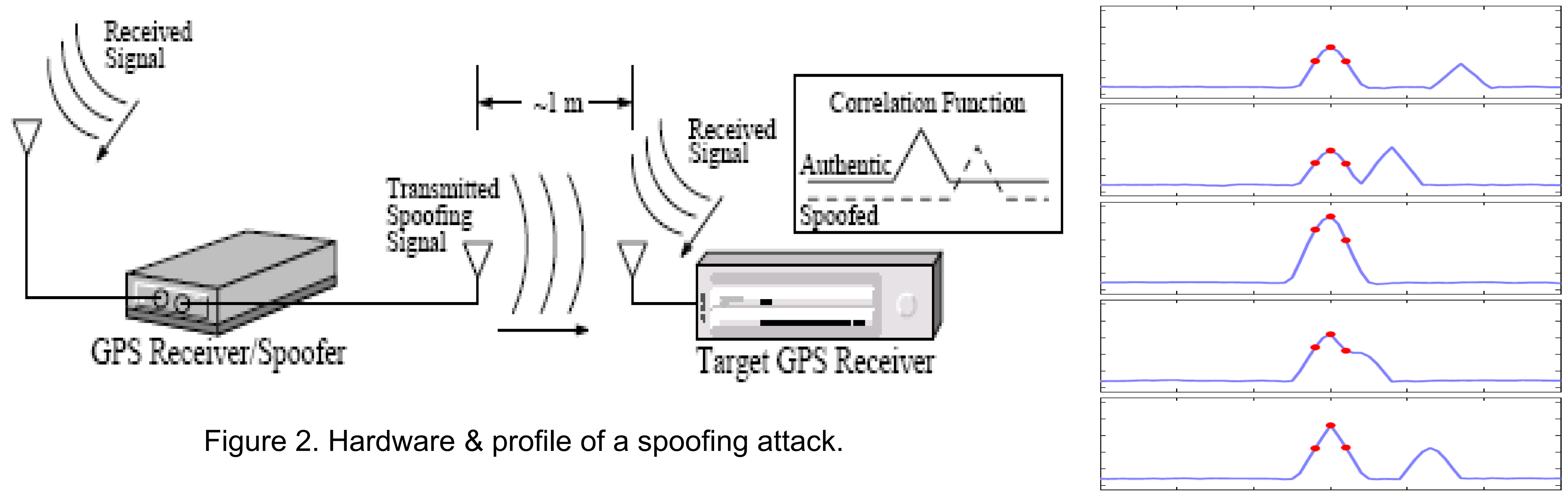

Figure 2. Hardware & profile of a spoofing attack.

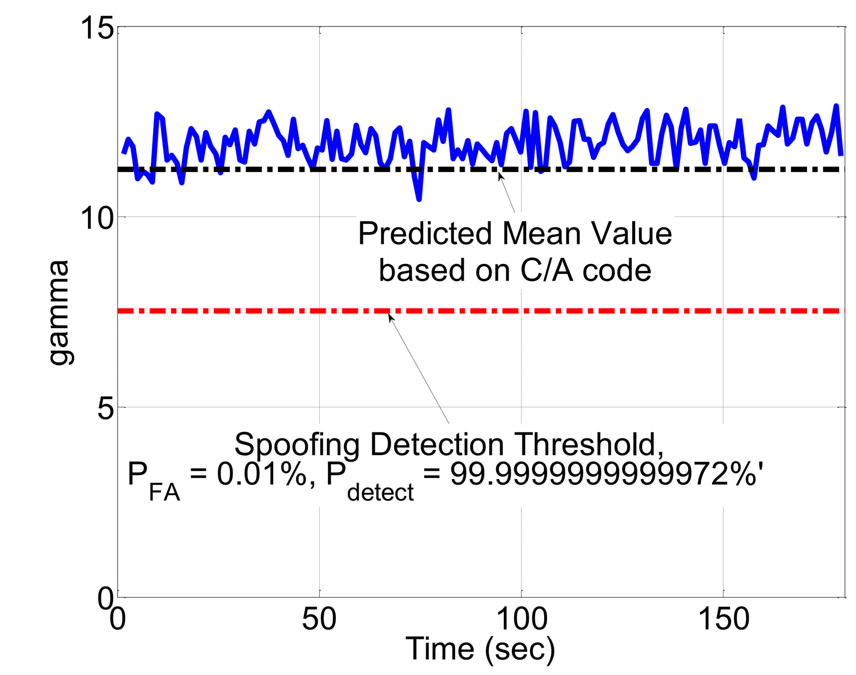

Figure 3. Codeless verification of no spoofing.

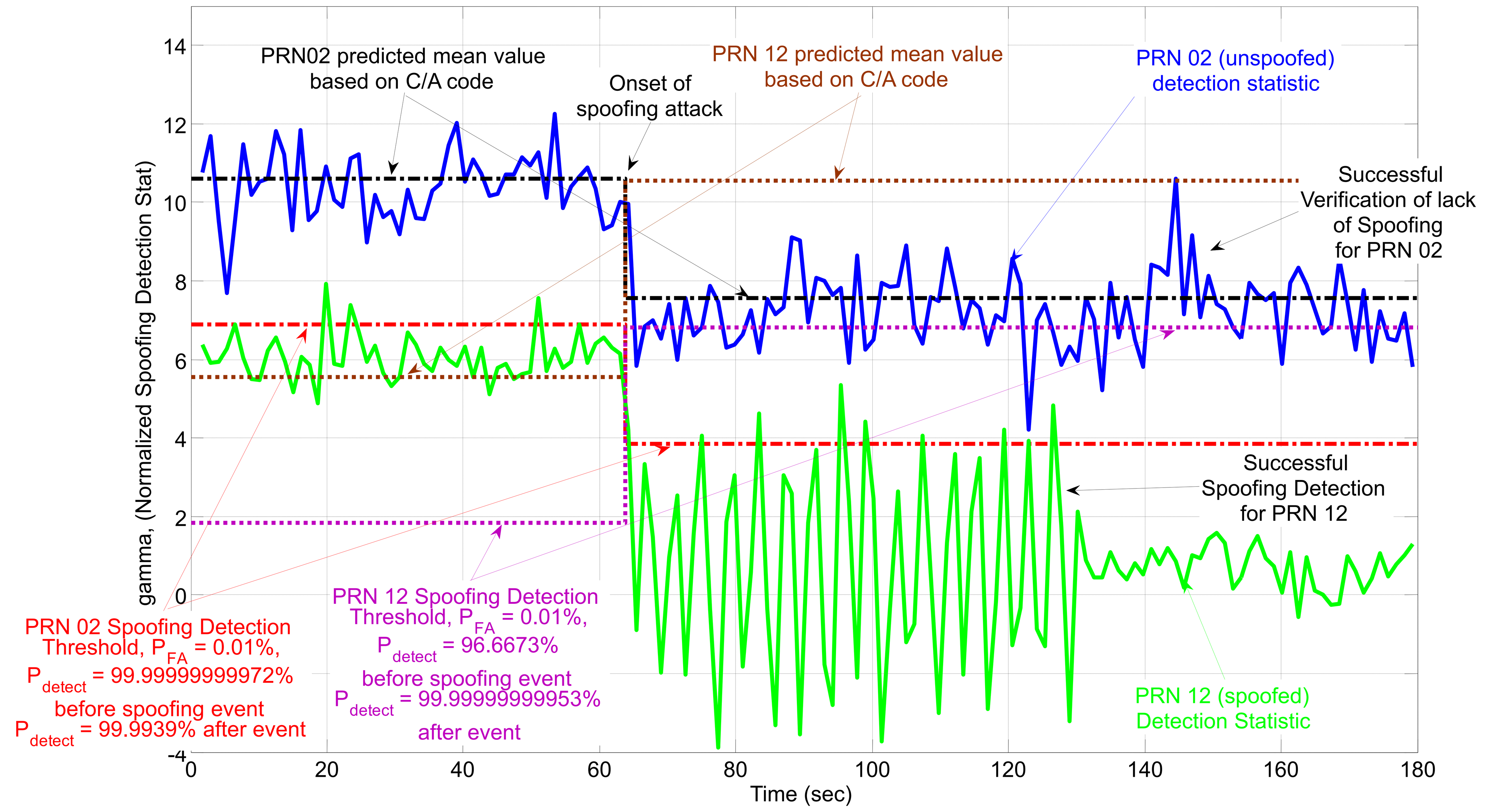

Figure 4. Codeless detection of a spoofing attack.

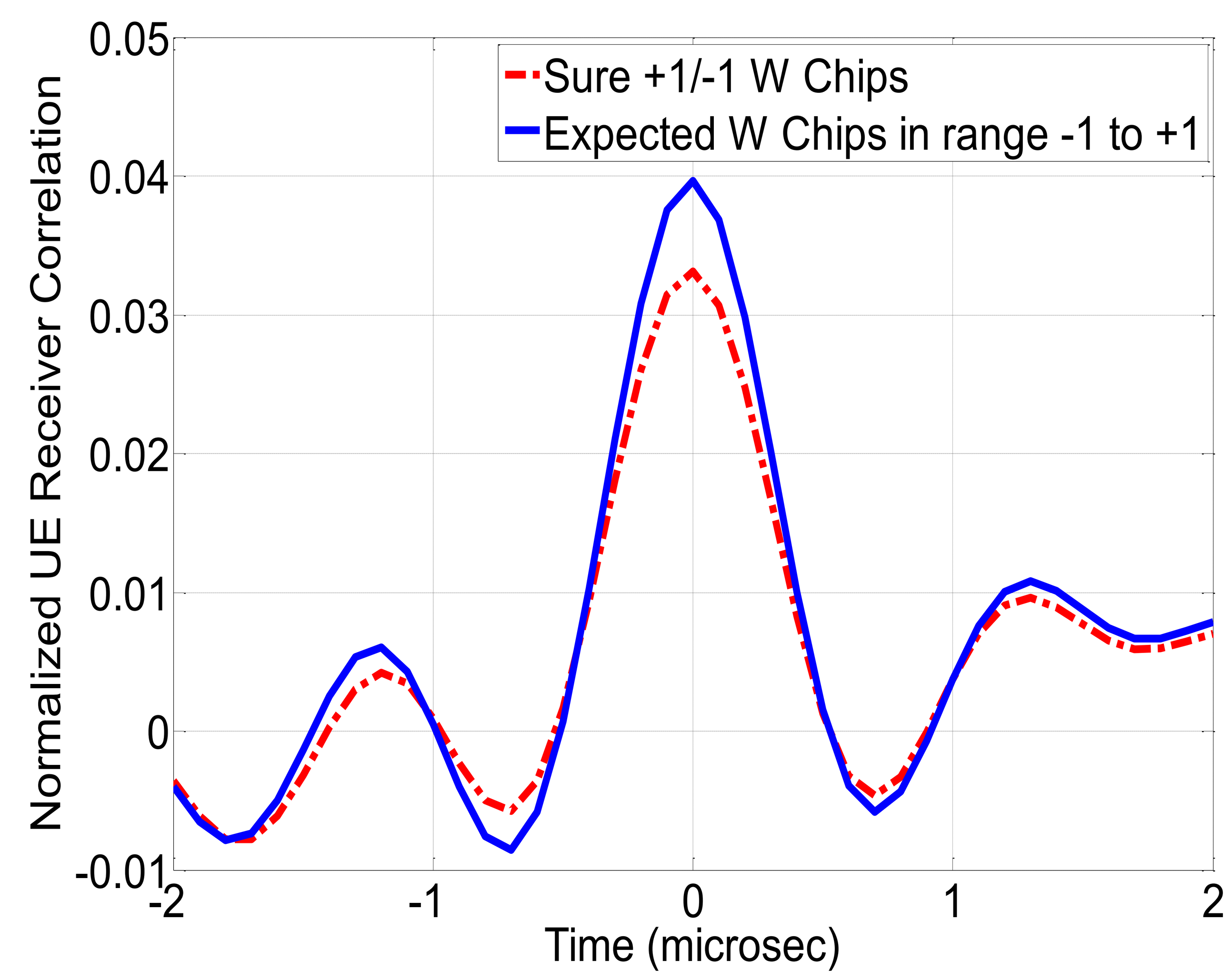

Figure 5. Comparison of 2 semi-codeless detection statistics, case of no spoofing.

Results & Conclusions

- Narrow-band-filtered P(Y) code useful for spoofing detection
  - 20-25% of P(Y) power suffices to detect spoofing
  - Spoofing detection threshold analysis requires characterization of power loss
  - W-bits semi-codeless detection requires distortion model
- Codeless & semi-codeless techniques both work
  - Successful codeless detection of real spoofing attack (first ever demonstration) with 1.2 sec detection interval
  - Semi-codeless detection intervals as short as 0.1 sec possible.
- Needed Efforts
  - Modest UE receiver modifications for after-the-fact detection
  - Significant modifications for real-time detection
  - Establishment of reference station network or intermittent after-the-fact W-bits declassification