GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase

Mark L. Psiaki  
*Sibley School of Mech. & Aero. Engr., Cornell Univ.*

Brady W. O'Hanlon & Steven P. Powell  
*School of Electrical & Computer Engr., Cornell Univ.*

Jahshan A. Bhatti, Kyle D. Wesson, & Todd E. Humphreys  
*Aero. Engr. & Engr. Mechanics, UT/Austin*

Andrew Schofield  
*Sea ID, Master of the White Rose of Drachs*

ION/GNSS+ 2014, 12 Sept. 2014
Acknowledgements

- The owner of the White Rose of Drachs lent his yacht to support the testing reported here

- The White Rose crew aided this project in many ways
Motivation:
- Detect attack by Humphreys-class spoofer on civilian GPS receiver or meaconing attack on a military receiver

Strategy:
- Exploit differences of signal arrival geometry between non-spoofed case & spoofing from a single transmitter using CDGPS/attitude-determination principles
- Develop detection statistic based on difference of fits to spoofed & non-spoofed models of single-differenced carrier-phase between 2 antennas
- Implement real-time version
- Test detection system against live-signal spoofing attacks on a superyacht during a cruise around Italy
Outline

I. Spoofing detection system architecture
II. Non-spoofed & spoofed carrier phase models
III. Detection tests with maximum likelihood optimal estimation of unknown attitude parameters
IV. Live-signal spoofing attack experiments aboard a yacht
V. Results, analyses, & discussion
VI. Summary & conclusions
VII. Future plans
Two Configurations of a 2-Antenna GNSS Spoofing Detection System

- **RF-switched-signal/single-receiver configuration**
  - GNSS patch antennas (2, mounted to ship, vehicle, or building)
  - Electronic RF Switch
  - GNSS receiver w/special PLL & spoofing detection signal processing unit

- **Two-receiver configuration**
  - RF signal A
  - GNSS receiver A
  - Antenna A beat carrier phases
  - Spoofing detection signal processing unit
  - RF signal B
  - GNSS receiver B
  - Antenna B beat carrier phases
Geometry of Non-Spoofed Case

GNSS Satellite $j$

GNSS Satellite $j-1$

GNSS Satellite $j+1$

$\hat{p}_j$

$\hat{p}_{j-1}$

$\hat{p}_{j+1}$

2-antenna spoofing detection system

Antenna A

Antenna B

$b_{BA}$
Geometry of Single-Transmitter Spoofed Case

Spoofer that transmits fake signals for GNSS satellites ..., j-1, j, j+1, ....

\( \hat{p}^{sp} \)

2-antenna spoofing detection system

Antenna A

Antenna B

\( b_{BA} \)
**Carrier Phase Models**

- **Non-spoofed case**

\[
\Delta \phi_{BA}^j = \phi_B^j - \phi_A^j \\
= -\frac{2\pi}{\lambda} (\hat{r}^j)^T A^T b_{BA} + \beta + 2\pi \Delta N_{BA}^j + n_{mpBA}^j + n_{rcvrBA}^j \\
= -\frac{2\pi \rho_{BA}}{\lambda} (\hat{r}^j)^T \hat{r}_{BA} + \beta + 2\pi \Delta N_{BA}^j + n_{mpBA}^j + n_{rcvrBA}^j
\]

- **Spoofed case**

\[
\Delta \phi_{BA}^j = -\frac{2\pi \rho_{BA}}{\lambda} (\hat{r}^{sp})^T \hat{r}_{BA} + \beta + 2\pi \Delta N_{BA}^j + n_{mpBA}^j + n_{rcvrBA}^j \\
= \beta_{sp} + 2\pi \Delta N_{BA}^j + n_{rcvrBA}^j
\]

with \( \beta_{sp} = -\frac{2\pi \rho_{BA}}{\lambda} (\hat{r}^{sp})^T \hat{r}_{BA} + \beta + n_{mpBA}^{sp} \)
Single-Differenced Carrier Phase Responses to Spoofing Attack

![Graph showing carrier phase responses to spoofing attack with different satellite PRNs and initial attack and code drag-off markers.](image)
Hypothesis Test Statistic

Non-spoofed case antenna baseline estimation

find: \( \hat{r}_a, \beta, \Delta N_{BA}^1, \ldots, \Delta N_{BA}^L \)

to minimize \( J_{nonsp}(\hat{r}_{BA}, \beta, \Delta N_{BA}^1, \ldots, \Delta N_{BA}^L) = \)

\[
\frac{1}{2} \sum_{j=1}^{L} \left[ \Delta \phi_{BA}^j + \frac{2\pi \rho_{BA}}{\lambda} (\hat{r}_{BA}^j - \beta - 2\pi \Delta N_{BA}^j) \right]^2 \]

subject to: \( (\hat{r}_a)^T \hat{r}_a = 1, \Delta N_{BA}^1 = 0, \Delta N_{BA}^j \) integer-valued for \( j = 2, \ldots, N \)

Spoofed case bias/ambiguity estimation

find: \( \beta_{sp}, \Delta N_{BA}^1, \ldots, \Delta N_{BA}^L \)

to minimize \( J_{sp}(\beta_{sp}, \Delta N_{BA}^1, \ldots, \Delta N_{BA}^L) = \frac{1}{2} \sum_{j=1}^{L} \left[ \Delta \phi_{BA}^j - \beta_{sp} - 2\pi \Delta N_{BA}^j \right]^2 \)

subject to: \( \Delta N_{BA}^1 = 0, \Delta N_{BA}^j \) integer-valued for \( j = 2, \ldots, N \)

Difference-of-fits spoofing detection test statistic

\[
\gamma = J_{sp} (\beta_{spopt}, \Delta N_{BAspopt}^1, \ldots, \Delta N_{BAspopt}^L) \]
\[
- J_{nonsp} (\hat{r}_{BAopt}, \beta_{opt}, \Delta N_{BAsopt}^1, \ldots, \Delta N_{BAsopt}^L) \]
Monte-Carlo Simulation of Spoofed & Non-Spoofed Probability Densities of Detection Statistic

Antenna Separation = 14 cm, 7 satellites, GDOP: 2.4, C/N₀: 34.12 to 49.7 dB-Hz
The Texas Lying Machine, Would-be Hijacker of the White Rose
Prototype Lie Detector, White Rose Defender

- Receiver:
  - 2 USRPs
  - 1 laptop running 2 parallel UT Austin/Cornell real-time software receivers on 2 live USRP data streams

- Spoofing detector:
  - Matlab-based detection & graphical output tic function
  - Called by real-time C receiver code & fed $\Delta \phi_{BA}$ values
Movies: Initiation of Libya Spoofing Attack & Detection

- Download a 305MByte .zip-file of videos
  (http://gps.mae.cornell.edu/libyaspoofingattack_reenactmentvideos.zip)
- Unzip in order to view two short movies
- prelibyaspoof_markleadsdiscuss_00011.mp4
  - Brief explanation of what was tested during Libya spoofing attack
- libyaspoofattack_closeupoflaptop_markbrady
  extendeddiscuss_00013_00015.mp4
  - Techie’s eye view of how spoofing detection system picked up Libya attack at its outset. Gives a “taste” of being there during the experiments
Highlights of Spoofed Trip to Libya
Detection of Attack During Libya Trip

Spoofing Det Plot (authentic >= blue dash-dot)

- Non-Spoofed Value
- Spoofed Value
- Detection Threshold

Receiver Time (sec)
Detection of More Subtle Attack

Ambiguous Detection Prior to Code Drag-Off

Spoofing Det Plot (authentic >= blue dash-dot)

Non-Spoofed Value
Spoofed Value
Detection Threshold

Receiver Time (sec)
Failed Detection of Failed Attack

Spoofing at power slightly below authentic signal?

![Graph showing ΔφBA (cycles) vs. Receiver Time (sec)]

Spoofing Det Plot (authentic >= blue dash-dot)

- Non-Spoofed Value
- Spoofed Value
- Detection Threshold

False alarm due to few Sats & poor geometry?
Comparative Histograms of RF Samples

**Authentic:** $\sigma = 7100$

**Failed Attack** $\sigma = 8200$
- Spoofing Advantage $\leq 0.9$ dB

**Successful Attack** $\sigma = 12500$
- Spoofing Advantage $\sim 7$ dB

RAW USRP I & Q Samples
Lessons Learned, Expected & Unexpected

- Initial capture & pre-drag-off is a challenge
  - Incomplete transition of differential phases (expected)
  - Difficulty of tracking thru alternating constructive & destructive interference between true & spoofed signals if spoofer power advantage not large (unexpected)

- Successful attacks not easy
  - Inexperienced spoofer operator needed to overwhelm true signals in victim receivers
  - Simple absolute power tests could have detected spoofing in these “sledgehammer” spoofing cases
Summary & Conclusions

- Developed real-time prototype of two-antenna spoofing detection
  - Exploits differing reception geometry between non-spoofed & spoofed cases: spoofing removes the natural differences between single-differenced carrier phases
  - Optimization-based data fitting leads to powerful detection tests

- Demonstrated real-time detection of live-signal spoofing attacks
  - Detections possible in 0.2 sec, depending on PLL bandwidth.
  - Tests less certain during initial capture period before code drag-off if spoofer power not much greater than authentic signal.
Future Plans

- Improve receiver tracking robustness during initial attack
- Implement real-time switched antenna version w/new PLL
- Develop additional spoofing tests for layered defense
  - Simple in-band power monitor
  - Advanced RAIM at discriminator/tracking-loop level
  - Compass continuity for 2-antenna system estimated attitude
- Improve & test methods for case of spoofing subset of signals
- Develop methods to recover true signals
  - True signals have been acquired during times of strong spoofing attack in recorded White Rose wideband data sets
- Test improvements with recorded White Rose data
- Test improvements in new live-signal tests against a subtle spoofer (requires another cruise!)