Design of a TOA-based Anti-Spoofing Method for GPS Civil Signal

Sung Lyong Cho, Mi Young Shin, Soon Lim, Dong-Hwan Hwang, Sang Jeong Lee, *Department of Electronics Engineering, Chungnam National University, Korea*
Chansik Park, *School of Electrical and Computer Engineering, Chungbuk National University, Korea*

INTRODUCTION

While the objective of jamming is the denial of the navigation service by masking GPS signals with noise, the objective of Spoofing is to convince you that you are somewhere you are not [1]. Jamming tends to aim at anyone within its coverage area whereas spoofing tends to aim at a particular victim receiver. A spoofer is likely to be designed to produce erroneous navigation solutions.

This paper designs a spoofing signal generator and anti-spoofing methods for GPS civil signal. Figure 1 shows the structure of platform for analyzing the effect of spoofing signals on the GPS receiver and the anti-spoofing performance.

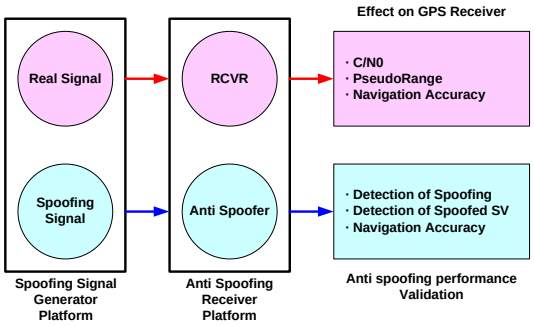

Figure 1. Structure of software platform

GENERATION OF SPOOFING SIGNAL

This paper adopts two approaches to generate spoofing signals.

(i) The spoofing method using the navigation message

Navigation massage data includes parameters for the satellite orbit, the correction information of ionospheric delay and the correction information of satellite's clock error. The changes in these parameters will be able to effect on the TOA(Time of arrival) measurements in GPS receivers.

(ii) The spoofing method using the TOA delay

The TOA delay of GPS signal results in the error of pseudo-range measurements. The pseudo-range error results in the navigation error.

DESIGN OF ANTI-SPOOFING METHODS

This paper designs two detection methods of the spoofing signals for stand alone GPS receiver : the anti-spoofing method using RAIM (Receiver Autonomous Integrity Monitoring) and the TOA-based method comparing the code and carrier phase measurement [2].

PERFORMANCE VALIDATION

Spoofing signals are generated in the form of the TOA delay with step, pulse and ramp signal in the software based spoofing signal generator. Using these signals, effects on signal acquisition and code tracking are analyzed. Finally, performance of anti-spoofing methods is also analyzed.

CONCLUSIONS

This paper has designed a GPS C/A spoofer and analyzed the effect of the spoofing signals on GPS receivers. RAIM and TOA-based anti-spoofing methods has been implemented on the software GPS receiver. The performance of anti-spoofing methods has been evaluated using the generated spoofing signals.

REFERENCES

[1] Logan Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," ION GPS/GNSS 2003, Portland, OR, 2003
[2] H. Wen, P. Yih-Ru Huang, J. Dyer, A. Archinal, J. Fagan, "Countermeasures for GPS signal Spoofing," ION GNSS 2005, September 13-16, Long Beach, California.