TECHNOLOGY

CONTACT: ipm@innovatecalgary.com • (403) 284-6400

A Novel GNSS Anti-Interference Technique using Array Processing

TECH ID #: 256.26

Background

A team of researchers from the University of Calgary's Department of Geomatics Engineering, PLAN Group, has developed an inline standalone multi-antenna system to countermeasure spoofing and jamming threats on GPS signals. Figure 1 provides an illustrative example of a spoofing scenario where a GPS receiver mounted on a vehicle is receiving both authentic and spoofing signals, where the spoofing signals are trying to induce a fake trajectory.

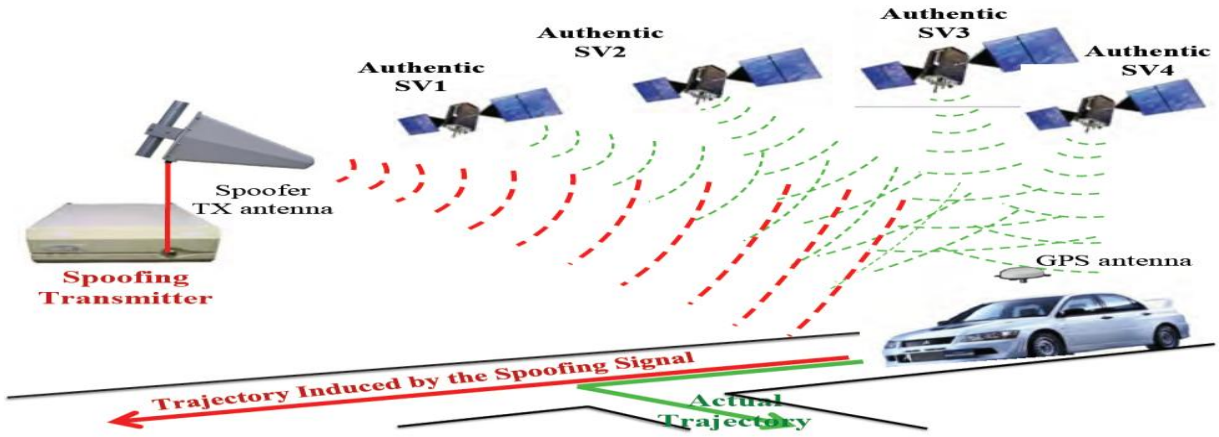

Figure 1

It is very hard to detect a spoofer since the spoofing signal is designed to have similar temporal and spectral characteristics as the authentic GPS signals. Out of several anti-spoofing methods available it is observed that spatial processing methods are the most effective anti-spoofing technique. Methods proposed previously in the literature operate after acquisition and tracking stages of a GPS receiver and they need to separately acquire and track all authentic and spoofing signals and this imposes a high computational complexity to the GPS receiver. In addition, some of these techniques depend on precise array calibration, which in turn increases the computational complexity. Moreover, most of these techniques fail in multipath environments where powerful reflections of spoofing signals are also received by the antenna array.

Unlike the above techniques, the spatial processing method developed by the PLAN Group has a very low computational complexity since it does not require separate analyses of different incident signals. This technology takes advantage of the spatial power dominancy of the spoofing signals and uses **Spatial Power Analysis** to distinguish between spoofing and authentic signals. This method can effectively reject the

incident spoofing signals and their multipath components and it does not require any antenna array calibration process. The proposed processing technique is independent of the receiver operation and as such it can be employed as a stand-alone external module at the input of conventional GPS receivers or it can be integrated inside future GPS receivers.

Area of Application

- GPS Navigation Systems

Competitive Advantages

- This technology proposes a processing method that not only has the benefits of previously proposed spatial processing anti-spoofing methods but also has much lower computational complexity.
- It provides real time operation, at very low cost and is portable.
- This system can be used as an inline unit that works independently from the GPS receiver. Therefore, there is no need to change the structure of conventional GPS receivers in order to use the proposed anti-spoofing method.
- This technology is applicable for both civilian and military signals.
- It is applicable for spoofing mitigation in multipath environments.

Stage of Development

- Several practical tests have been performed in a controlled environment with a Spirent GSS 7700 hardware simulator for generating spoofing signals. The spoofer was designed to mislead the receiver to obtain the position that was 8 miles away from the correct position. However by adding the proposed anti-spoofing module, spoofer was not able to fool the receiver and correct position was obtained. Other data collection, processing and analyses are ongoing.

Intellectual Property Status

- Patent Filed

Publications:

- Daneshmand, S., A. Jafarnia, A. Broumandan and G. Lachapelle (2011) "A Low Complexity GNSS Spoofing Mitigation Technique Using a Double Antenna Array" *GPS World magazine*, vol. 22, no. 12, December, pp. 44-46.

- Daneshmand, S., A. Jafarnia Jahromi, A. Broumandan and G. Lachapelle (2012) "A Low-Complexity In-line GPS Anti-Spoofing Method Using a Multi-Antenna Array" Accepted in ION GNSS 2012, 17-21 September, Nashville, Tennessee, 11 pages.