SPREE: A Spoofing Resistant GPS Receiver

**Summary**

GPS is a widely used system for navigation, tracking and more. Although its users all around the world extensively, its still vulnerable to spoofing attacks. The authors in this paper introduce a novel technique called SPREE to detect spoofing attacks and complex variations of spoofing such as seamless takeover attacks. SPREE presents a method to prevent spoofing attacks on GPS receivers. This method is implemented using two components called (i) Auxiliary Peak Tracker (APT) and (ii) Navigation Message Inspector (NAVI). APT works on the principles of tracking weaker signals in addition to the stronger signals and detect synchronization problems to identify fake GPS signals. NAVI inspects decoded navigation message to detect discrepancies and prevent attackers from modifying the contents of the message. According to the authors, SPREE was able to detect almost all types of GPS spoofing attacks when the paper was published.

**Strengths**

* SPREE doesn't rely on signal authentication like other countermeasures to spoofing and thereby is more reliable. Other signal authentication countermeasures are not resistant to replay attacks.
* It's evaluated against various data sets and tested in real-world scenarios. When SPREE is deployed, attackers cannot divert a ship or drones by more than 1 KM from their intended location.
* SPREE works against strong spoofing attacks as well, thereby detecting most GPS spoofing attacks including seamless takeover attacks.

**Weaknesses**

* SPREE is much more complex than the traditional GPS receiver with the introduction of APT and NAVI modules. This might increase the cost of the receivers.
* Resource utilization is high when compared to traditional GPS receivers to track correlation peaks and perform sanity checks. It will be hard to implement this in a resource sensitive receivers/ environment.
* SPREE assumes the existence of legitimate GPS signals before the start of spoofing attacks. So it may not work in factory reset or cold modes of receivers
* It's still hard to determine the peak caused by spoofing and legitimate signals, thereby making SPREE only capable of detecting spoofing attacks and not preventing them.