Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Detecting GPS Spoofing

It's easy to generate fake GPS time and location signals using widely available GPS satellite simulators. This spoofing can be detected with $15 of parts.

The Problem

Almost everybody (including most of DoD) must use the civilian Global Positioning System (GPS) signals. Unlike the military signals, these are not encrypted or authenticated, and were never intended for critical security applications. Yet civilian GPS is being used that way!

As we have demonstrated in the Vulnerability Assessment Team at Argonne National Laboratory, it is easy for an adversary to generate fake GPS signals using widely available (non-export controlled) GPS satellite signals.

The Threat of Undetected GPS Spoofing

With GPS spoofing (not jamming), an adversary can:

- Crash national utility, financial, telecommunications & computer networks that rely on GPS for critical time synchronization
- Steal cargo or nuclear material being tracked by GPS
- Install false time stamps in security videos or financial transactions
- Send emergency response vehicles to the wrong location after a terrorist attack
- Interfere with military logistics (DoD uses civilian GPS for most cargo)
- Interfere with battlefield soldiers using civilian GPS (against DoD policy, but common)
- Spoof GPS ankle bracelets used by courts
- Spoof GPS data loggers used for law enforcement and counter-intelligence

The Solution

Signals from GPS satellite simulators have artificial characteristics allowing them to be recognized as fake. These include:

- wrong time
- suspiciously low noise
- excessive signal strength
- artificial spacing of signals
- all satellites have the same signal strength
- wrong or no time variation in signal strength
- reported accelerations don't pass a sanity check

For More Information

JS Warner & RG Johnston, *The Journal of Security Administration* 25, 19-28 (2002).

JS Warner & RG Johnston, *Homeland Security Journal*, December 12, 2003.

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov