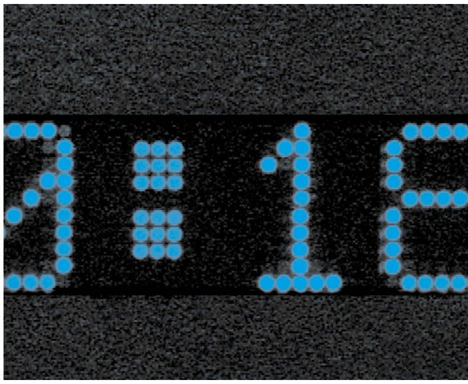
Intentional Disruption of GPS Signals – *Can it Really Affect the Telecommunications Industry?*



WHITE PAPER

Intentional Disruption of GPS Signals

Can it Really Affect the Telecommunications Industry?

Summary

The potential for denying GPS service by jamming exists and the appearance of jamming devices/techniques on the Internet and the recent tragedy of September 11 have elevated this concern within the military and civilian communities. GPS signal reception is vulnerable to disruption because of the low power of the signals. Technical improvements are currently being planned for the GPS system but are years away from implementation.

Disruption of GPS signals for civilian aviation and maritime applications could result in serious to catastrophic consequences and is therefore the subject of the vast majority of research available to date. GPS outages of as little as 30 seconds from malicious jamming in a battlefield and/or aviation situation could result in loss of life. The application of GPS for telecommunications purposes is not equivalent to aviation/maritime use for two significant reasons. The first is that telecom GPS units are stationary and second, telecom GPS units have high quality holdover oscillators. Typically, GPS receivers used in navigation applications do not use holdover oscillators.

For these reasons, telecom GPS receiver and jamming issues merit their own study. This paper will show that intentional interference by jamming will not adversely affect the telecommunications network. We will also show that the highly improbable scenario of loss of GPS service resulting from a direct attack to the satellites and/or ground stations would have limited detrimental impact on the telecommunications network.

Introduction

The Global Positioning System (GPS) is a satellite navigation system developed by the United States military to provide accurate navigation signals to any place in the world. In 1993, the GPS satellite constellation was declared operational for civilian use. Civilian use of GPS includes positioning, navigation, and timing applications.

GPS plays an important role in timing and synchronization of telecommunications networks. GPS receivers are widely used as a timing source to provide Stratum 1 accuracy because of their low cost and simple administration. GPS receivers are the first choice as the primary reference source, over transmission facility synchronization references and/or cesium beam reference clocks.

The low power of GPS signals makes them vulnerable to two types of interruptions, unintentional and intentional. Unintentional disruptions include ionospheric effects, blockage from buildings, and interference from narrow and wideband sources. Intentional disruptions are attacks by hostile interests that range from jamming and spoofing of GPS signals to disruptions of GPS ground stations and satellites.

Jamming and Spoofing

Jamming is the intentional interference of GPS signals by emitting radio frequency energy of sufficient power and with the proper characteristics to prevent receivers in the target area from tracking the GPS signals. Spoofing is the technique used to deceive an active GPS receiver to lock onto legitimate appearing false signals and then be slowly walked off the desired path such that sufficient time passes prior to the discovery of the deception.

Since operating jammers and spoofers is illegal in the United States, the only results publicly available from jamming and spoofing tests come from the military and government-sponsored laboratories for positioning and aviation applications (because of national security concerns many test results are not made public). Determining the exact distance jammed and required jamming power is difficult due to a number of factors including the type of jamming signal, the altitude of the jammer, GPS antenna pattern, geometry between the GPS antenna and the jammer, body masking loss, and receiver design. In general, these studies have concluded that:

1. An airborne jammer could potentially jam a significant geographical area

2. A single ground based jammer could **not** effectively jam over a large area because the horizon/terrain blockage acts as a significant limiter

Spoofing is more difficult to achieve than jamming and only targets individual users. As such, it is generally believed that spoofing will not likely be used. However, popular opinion would have you believe that any low skilled individual or group intent on wreaking havoc on the GPS system can do so by putting together a GPS jammer with $100 worth of parts and plans downloaded off the internet. The truth is much more complicated.

GPS jammers come in a variety of shapes, sizes, costs, and output power levels. Output power levels range from 1 W to more than 100 kW with prices ranging from $1,000 to $1 million. Stationary jammers can be more easily detected and disarmed by local law enforcement, so good jammers need to be mobile to evade detection. The amount of jamming coverage possible from a low-end 1 watt land-based jammer is extremely limited. Increasing the output to just 80 watts would require a commercially available gasoline generator to provide the needed power for more than a few hours. A 100 to 1000 watt jammer would require an SUV to transport and $100,000 to build. High end land-based or airborne jammers can cover a much wider geographic area but would require $1 million dollars or more to build.

Generally speaking, a long term GPS outage due to jamming is measured in minutes or hours, possibly days, but certainly not weeks or months. In summary:

1. Potential for denying GPS service by jamming exists
2. Long term successful jamming is very unlikely
3. Ground based jammers cannot jam a significant area due to horizon/terrain blockage limitations
4. Airborne jammers are prohibitively expensive to build and operate

Shutdown

Shutdown of the GPS system by hostile actions is highly improbable. It would require loss of a significant number of GPS satellites and/or the Operational Control Segment. Attacking these elements is very challenging and would produce an aggressive US Government response. Spare satellites are available to put in service if a small number of satellites are destroyed. A complete shutdown, as improbable as that is, would be measured in days and weeks, perhaps even months, but certainly not years.

GPS Applications for Telecommunications Network Timing

Telecommunications synchronization network standards are defined in terms of slips (loss of data) allowed per day. The objective for the network designers is no more than 4 slips per day. A well-synchronized network (for example, one that has GPS based clocks) easily beats this objective. In most current generation telecom network GPS clocks, signals from just one GPS satellite are all that is needed to steer an internal rubidium or high performance quartz oscillator. A GPS clock locked to GPS signals must meet Stratum 1 ($1X10^{-11}$) performance to be deemed functional. No slips will occur for **72 days** under Stratum 1 timing.

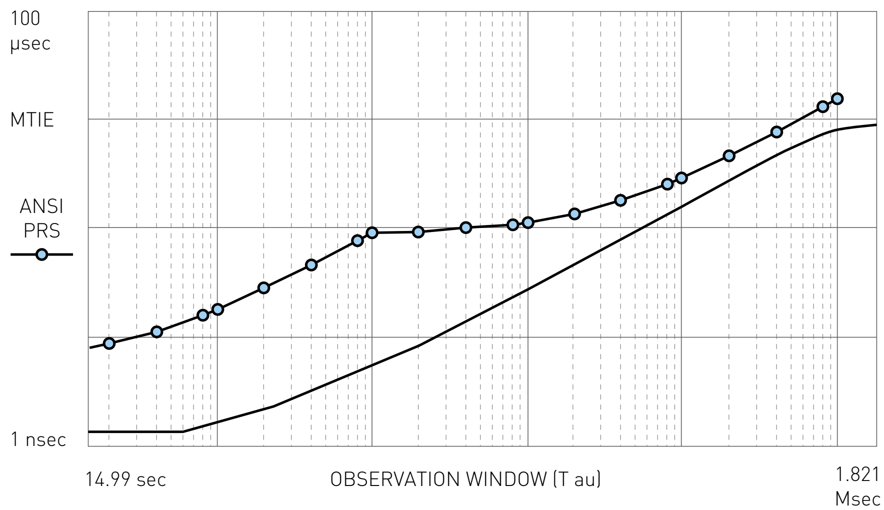


FIG.1 TimeSource 3500 Three Week PRC Quality Holdover (at 25°)

If GPS signals are interrupted such that the clock is not locked to a GPS satellite(s), as in a jamming scenario, the internal oscillator is used to maintain (holdover) the synchronization quality. A good quartz oscillator will maintain Stratum 1 holdover accuracy for several hours. On the other hand, a good rubidium oscillator will maintain Stratum 1 holdover accuracy for up to 3 weeks (see Figure 1). As long as this holdover synchronization quality is met, no slips (loss of data) will occur. If the clock continues to stay in holdover because of a very long term GPS outage, it will continue to slowly lose accuracy but not at a rate that will cause network interruptions. Recent field audit data of TimeSource 3500 clocks (Symmetricom's GPS Primary Reference Source clock with a rubidium local oscillator) in service for up to 1 year show that they will maintain a holdover accuracy such that a slip rate of 1 per day would not occur for **3 years** or more. This slip rate is still well below the 4 slips per day network objective.

Conclusion

The possibility of jamming or spoofing GPS receivers exist. However, GPS referenced clocks with holdover oscillators commonly used in telecom networks will keep those networks operational under all rationally conceived GPS jamming and disaster scenarios. Rubidium based GPS receivers add even more backup capability extending into years. More expensive cesium or backup Loran clocks are not essential for network protection. Additional GPS based clocks with adequate holdover provide a more robust timing solution than dependence on incoming synchronization reference feeds. Central offices can maintain synchronization autonomy and operability in the case of a disaster that interrupts the incoming transmission facilities carrying synchronization references.

Reference

Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, Final Report, John A. Volpe, August 29, 2001

SYMMETRICOM, INC.
2300 Orchard Parkway
San Jose, California
95131-1017
tel : 408.433.0910
fax : 408.428.7896
info@symmetricom.com
www.symmetricom.com

SYMMETRICOM EMEA
150 Wharfedale Road
Winnersh Triangle, Nr. Wokingham
Berkshire
RG41 5RB, United Kingdom
tel : 44 (0) 1189 699 799
fax : 44 (0) 1189 277 520
info@symmetricom.com

SYMMETRICOM LATIN AMERICA
1560 Sawgrass Corporate Parkway
4th Floor
Sunrise, Florida
33323
tel : 954.331.4592
fax : 954.331.4601
info@symmetricom.com

SYMMETRICOM ASIA PACIFIC
Unit 1005, Jubilee Centre
42–46 Gloucester Road
Wan Chai
Hong Kong
tel : 852.2529.7180
fax : 852.2529.7190
info@symmetricom.com