Detecting and Locating GPS Jamming

Jeffrey Coffed, Exelis Inc.  
Joseph Rolli, Exelis Inc.  
Carl Slutsky, Exelis Inc.

BIOGRAPHY

Jeff Coffed, Senior Product Marketing Manager with Exelis has product marketing responsibility for the Analytical Instruments, Precision Optics, Precision Structures and Positioning, Navigation and Timing divisions.

Joseph Rolli is a sales manager in the Positioning Navigation and Timing group at Exelis.

Carl Slutsky is the Product Manager for the Signal Sentry product line. Carl leads product strategy and development efforts and is responsible for product technology road maps and the engineering requirements for the ongoing development of the Signal Sentry product line.

ABSTRACT

The Global Positioning System (GPS) has become a ubiquitous service supporting many critical infrastructures including intelligence and law enforcement missions, transportation, financial applications, civil safety response and Department of Defense capabilities. The GPS signal is susceptible to service outages due to intentional and unintentional jamming. Recognizing this threat, Exelis set out with the objective to develop technology that identifies and locates jamming sources.

This technology provides actionable intelligence, enabling authorities to locate and mitigate the sources of interference thereby assuring safety, efficiency, and revenue. Our methodology includes combining sensors and proprietary software to enable geolocation of interference sources. The resultant data is available in the form of pin mapping of interference allowing the jamming source to be seen through an easy to use web enabled graphical user interface.

The technology has the capability to locate disruptive sources utilizing a propriety algorithm. The system’s sensors can be strategically located around high-risk areas, such as airports or utility grids, to instantaneously sense and triangulate the location of the jamming source. The server is able to identify the characteristic of the interference source and should a threat be detected and users will receive pin-point geolocation information in order to respond.

The significance of this work is to protect military, commercial and industrial systems from a diverse range of threats.

INTRODUCTION

GPS was originally developed for providing precision navigation and timing to the United States Military. However, society has rapidly developed a strong reliance on GPS information in many facets of life including transportation, communications, and financial transactions.

GPS has become an indispensable source of information with significant economic benefits, making it increasingly important that GPS data be available and reliable. GPS boosts productivity in many sectors including law enforcement, civil safety response, farming, mining, surveying, and package delivery. It is estimated more than 3.3 million jobs rely heavily on GPS in the United States, generating approximately $122.4 billion in annual economic benefits.

Future satellite designs are being prepared to improve the transmission capability and security of GPS data. However, addressing GPS information outages needs to occur now as the availability and usage of low-cost GPS jamming devices has resulted in a growing threat of GPS signal disruption and increasing the likelihood of future outages to systems that rely on GPS data. Jamming is the act of interfering with a systems capacity to lock onto the GPS signal, eliminating a user’s ability to receive the necessary information.
Addressing the security of GPS signals and preventing denial of services should be a priority. This paper focuses on GPS, its susceptibility due to jamming and technology that detects and locates sources of interference including recent field test data.

**ECONOMIC IMPACT OF GPS**

Over the past twenty years, GPS technology has transformed lifestyles and businesses with a myriad of applications across all industries and spheres of life. In addition to creating efficiencies and reducing operating costs, the adoption of GPS technology has improved safety, emergency response times, environmental quality, and has delivered many other benefits. The market for GPS has already grown into a multi-billion dollar industry with far-reaching potential.

The direct economic benefits of GPS technology on commercial users are estimated to be over $67.6 billion per year in the United States. Paul Verhoef, Program Manager for the European Union (EU) Satellite Navigation, stated that “6 to 7 percent of the European Union gross domestic product (GDP) is directly dependent on the availability of GPS.”

GPS technology creates jobs and other economic activities that spur economic growth. Studies have shown sustained productivity benefits and job creation in downstream industries and the U.S. economy as a whole. Additionally, GPS technology has created both positive direct and indirect spillover:

- 3.3 million jobs that rely on GPS technology, including 130,000 jobs in GPS manufacturing industries and 3.2 million in the downstream commercial GPS-intensive industries
- Improved public safety and national defense
- Time savings, workplace health and safety gains, job creation and reduction in emissions from fuel savings

**THE RISK AND THREAT**

Brandon Wales, Director of Homeland Infrastructure Threat and Risk Analysis Center for the Department of Homeland Security, warned in late 2011, “U.S. critical infrastructure sectors are increasingly at risk from a growing dependency on GPS for positioning, navigation, and timing services.” He stated that GPS reliance in many critical systems is either not fully understood and is often taken for granted and describes GPS as a “largely invisible utility.”

In a March 2011 Royal Academy of Engineering (RAE) report, the author, Dr. Martyn Thomas, stated, “the financial markets, for instance, rely on a globally synchronized time-stamping mechanism to ensure fair trading. Trading systems might be detecting very small differences in prices between commodities on different exchanges and buying in high volume on one and selling on the other. Since lots of people are in competition trading on different continents, for these activities to work you need to know whose order is getting in first.”

A report issued by NDP Consulting Group in June 2011 noted that the direct economic costs of full GPS disruption to commercial GPS users and GPS manufacturers are estimated to be $96 billion per year in the United States or the equivalent of 0.7 percent of the U.S. economy.

**JAMMERS**

There are people who want to interfere with GPS signals because they are engaged in smuggling, theft, or simply trying to escape tracking of their daily movements.

Jammers are devices that use radio frequency transmitters to intentionally block, jam, or interfere with lawful communications. It’s easy to jam GPS signals because they are faint — coming from satellites 13,000 miles away. Typical signal strength is around 1.5 dB (home television signals usually range from 25 to 46 dB). A small jammer (Figure 1) can disrupt the GPS signal for a mile or more.

The fact that GPS signal strength is weak is not a design flaw. These radio signals are complex and contain multiple components including time, ephemeris data, and information about the health of the satellite. To constantly produce and broadcast these signals from solar powered satellites requires a design balancing act between allocating energy, equipment and other resources. This was acknowledged by Colonel Bernard Gruber — former Commander of the GPS Directorate, Space and Missile Systems Center, Air Force Space Command, Los Angeles Air Force Base — in an interview from the July 13, 2013 edition of Inside GNSS, “by design, GNSS signals are weak and vulnerable to intentional and unintentional interference.”
One example of unintentional jamming was noted when every day for almost ten minutes near the London Stock Exchange, someone was blocking GPS signals. Navigation systems in cars stopped operating and time stamps on financial trades were affected. It was determined that the culprit was a delivery driver hiding from his management.\textsuperscript{11}

GPS jammers are being used by criminals to hide the fact they are driving stolen cars or by commercial drivers to conceal they are driving for dangerously long hours. It has been reported that a 500 meter shield is created around a vehicle that uses a simple jamming device plugged into a cigarette lighter. Within that shielded area, other GPS devices are left inoperable. For example, airplane safety and other technology is unintentionally disrupted when an exhausted taxi cab driver wants to take a break and plugs in a GPS jammer to avoid detection.

U.S. LAWS GOVERNING JAMMERS

Federal law prohibits the operation, marketing, or sale of any type of jamming equipment. Indication that jammers are becoming increasingly problematic is indicated by a recent statement issued by the Enforcement Bureau of the Federal Communications Commission (FCC):

In recent years, the number of websites offering “cell jammers” or similar devices designed to block communications and create a “quiet zone” in vehicles, schools, theaters, restaurants, and other places, has increased substantially. While these devices are marketed under different names, such as signal blockers, GPS jammers, or text stoppers, they have the same purpose. We remind and warn consumers that it is a violation of federal law to use a cell jammer or similar devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi. Despite some marketers’ claims, consumers cannot legally use jammers within the United States, nor can retailers lawfully sell them.\textsuperscript{12}

Despite the prohibition of obtaining a signal jammer, GPS jammers can be ordered easily via the Internet (see Figure 1). It is insufficient and misleading for manufacturers and retailers to simply include a disclaimer on their websites or in promotional material that the consumer bears sole for complying with all legal obligations regarding signal jammers. The manufacturer or retailer is breaking the law by responsibility offering the device for sale to U.S. consumers. GPS jamming devices are also prohibited in Canada and Australia. In other areas, such as the United Kingdom, GPS jammers are illegal for civilians to use, but not to purchase.

![Portable Cell Phone GPS Jammer]

**Figure 1** – Jamming technology is readily available

THE RISK IS REAL

Both the motive and the means to jam or render GPS capabilities useless are clearly evident in our society. Whether intentional or inadvertent, jamming GPS signals poses a significant risk to our daily lives, with potentially larger, long standing impacts. Some examples that highlight the real risk of GPS jamming have been reported and are summarized below.

In January 2007, GPS services were significantly disrupted throughout San Diego, California (Figure 2). Air-traffic controllers at the San Diego Airport noticed that their system for tracking incoming planes was malfunctioning; Naval Medical Center emergency pagers stopped working; and the harbor traffic-management system used for guiding boats failed. Additionally, cell phones users found they had no signal and bank customers trying to withdraw cash from Automated Teller Machines (ATMs) were refused.

![GPS Jammer Effect]

**Figure 2** – Impact of a drill was significant in San Diego

It took three days to find an explanation for this mysterious event: two Navy ships in the San Diego harbor had been conducting a training exercise when...
technicians jammed radio signals. Unwittingly, they also blocked GPS signals across a broad swath of the city.

In August 2013, the FCC fined a Readington, New Jersey, man nearly $32,000 after concluding he interfered with Newark Liberty International Airport’s satellite-based tracking system by using an illegal GPS jamming device in his pickup truck to hide from his employer. The signals emanating from the vehicle blocked the reception of GPS signals used by the air traffic control system and potentially put travelers in danger.

In another incident in late 2009, engineers noticed that satellite-positioning receivers for a new navigation aid at the airport would lose signal during certain times of the day. The Federal Aviation Administration (FAA) investigated the problem and after two months discovered that a local truck driver had installed an inexpensive jammer in his vehicle. The driver was using the jammer to prevent his employer from tracking his movements. When he passed the airport area in his daily routine, the airports systems would temporarily fail.

**TAKING ACTION**

Most do not realize how much of our infrastructure is dependent upon GPS signals and information. Industries around the world utilize GPS for a variety of applications that effect everyday life.

GPS jamming is an increasing worldwide problem. The first and best step to take is to pursue technologies that can detect and locate GPS jammers.

Exelis, Inc., has developed technology that detects sources of intentional and unintentional interference to GPS signals and provides actionable intelligence. We leveraged our signal domain knowledge of the global navigation satellite system to develop Signal Sentry technology. This solution enables geolocation of interference sources and provides visualization tools to support timely and effective actionable intelligence in GPS denied and contested environments.

Signal Sentry 1000 system sensors can be strategically located around high-risk areas, such as marine ports or utility grids, to instantaneously sense and triangulate the location of jamming sources. The server is able to identify the characteristics of each interference source separately and should a threat be detected, users would receive pin-point geolocation information in order to respond.

**SIGNAL SENTRY TECHNOLOGY**

Signal Sentry is Interference, Detection and Geolocation system developed to detect and locate the position of GPS interference. The overall system is defined to monitor GPS signals, detect interference to those signals and locate the source. The detection process will attempt to geolocate the interferers using arrayed sensors.

An array of sensors can be deployed for sensitive and high value entities such as infrastructure installations. Examples of infrastructure include airports, railroads, chemical plants, electric power plants and grids, cargo ports, wireless communication systems and financial transfer centers. The sensors will connect to servers that will assimilate the sensor data and provide suitable operator interfaces.

This section details some of the reports and features of the Signal Sentry 1000 solution and is intended to provide an understanding of its capabilities.

Signal Sentry 1000 is based on a Server/Client model. The user accesses Signal Sentry using a Web Browser and a URL specific to the user’s system. Signal Sentry will work with Firefox, Chrome and Internet Explorer. The user is required to login (figure 3) before accessing the system.

![Figure 3: Signal Sentry Login Prompt](image)

The home page is displayed when a user logs into the system. Sensors are displayed on a map as triangles with colors reflecting status (see Table 1) and interferers are displayed as red stars or as error ellipses.

A user can see the current status of the system. Selecting the Status button will display the definition of the status as described below. The System Health indicator shows status of the Signal Sentry system as a whole. System health levels include the following:

- **Initializing**: Not all sensors are registered, but no sensors have failed
- **Checking IQ and Awaiting Fixes**: All sensors are registered, but some are waiting for a GPS fix or results from an initial IQ check
Healthy

All sensors are registered and fully operational

Degraded

Some sensors have faults, and the system is operating in a degraded mode meaning interferer geolocations are less accurate

No Geolocation Updates

Not enough healthy sensors to perform interferer geolocation updates

Selecting the Sensors button on the interface brings the user to the web page that lists all the sensors associated with this system. A description of each column follows in the table where the sensor icon on the map is a triangle where the color corresponds to a state as described below.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Unregistered" /></td>
<td>Unregistered</td>
</tr>
<tr>
<td><img src="icon" alt="Registered but Still Initializing" /></td>
<td>Registered but Still Initializing</td>
</tr>
<tr>
<td><img src="icon" alt="Registered, Still Initializing and Event Occurring" /></td>
<td>Registered, Still Initializing and Event Occurring</td>
</tr>
<tr>
<td><img src="icon" alt="Connected, Registered and Fully Initialized" /></td>
<td>Connected, Registered and Fully Initialized</td>
</tr>
<tr>
<td><img src="icon" alt="Connected, Registered, Fully Initialized and Event Occurring" /></td>
<td>Connected, Registered, Fully Initialized and Event Occurring</td>
</tr>
<tr>
<td><img src="icon" alt="Communication Problem" /></td>
<td>Communication Problem</td>
</tr>
<tr>
<td><img src="icon" alt="Communication Problem and Event Occurring" /></td>
<td>Communication Problem and Event Occurring</td>
</tr>
<tr>
<td><img src="icon" alt="Communication Problem and Not Able to Send Event Data" /></td>
<td>Communication Problem and Not Able to Send Event Data</td>
</tr>
<tr>
<td><img src="icon" alt="Communication Problem, Not Able to Send Event Data and Event is Occurring" /></td>
<td>Communication Problem, Not Able to Send Event Data and Event is Occurring</td>
</tr>
</tbody>
</table>

Table 1: Sensor Icon Descriptions

Interferers are seen on the map (Figure 4) in History mode and they are displayed as red stars or error ellipses.

The Signal Sentry web page lists all the Interferers stored in the database with their start and end times (Figure 5). The user can manipulate the list by changing the minimum duration of the event to be displayed as well as if the interferer had been geolocated or not or both.

Modifying the duration of the interferer to display does not affect the real-time display of interferers. All interferers will be displayed in real time regardless of duration since it’s not possible to know how long the event will last when it starts.

If an interference event was less than a minute long it may not have a geolocation entry on the map so it will be listed in the Interferers list but since no geolocation occurred there will not be a corresponding icon for it on the map. It will be included in the Interference Event Frequency Chart.

There is also an Interference Event Frequency Chart that is a valuable tool for forensically evaluating the occurrence of Interferers. The viewer can adjust the following:

- **Resolution** – Time of Day, Day of Week, Day of Week AND Time of Day or by Timeline
- **Minimum Interference Duration** – only events longer than a user-define amount will be displayed
- **Geolocated/Not Geolocated** – display only events that have been or have not been geolocated or both. Some interference events may not have been geolocated because of the short duration of the event or not enough sensors detecting it
- **Date Range** – From/To Date allows the user to display data for a specific time range. The user can use the format MM/DD/YYYY HH:MM:SS (24 hour clock or 12 hour clock with AM or PM after time)
**Time of Day** – Limit the time of day to displayed with the From and To Time of Day fields

The chart (figure 6) displays the interference events as circles where the size of the circle represents the number of events that occurred at that day of the week and time. When dots are selected on the chart, a map is displayed below the chart showing the geographic location of the interference events. More than one dot can be selected at a time. This allows a user to find correlations in time and space to discover if events occur at specific locations at certain times of the day and/or days of the week.

![Interferer Frequency Chart](image)

**Figure 6: Interferer Frequency Chart**

The various Timeline Charts (figure 7) display the number of interference events for a time range. What data is displayed can be adjusted as in the previous chart.

![Timeline Interferer Frequency Chart](image)

**Figure 7: Timeline Interferer Frequency Chart**

There are also charts that display number of interferer events for Time of Day (figure 8) and another chart for the Day of the Week (figure 9) for both 1 hour and 15 minute increments.

![Interferer Frequency Chart for Time of Day](image)

**Figure 8: Interferer Frequency Chart for Time of Day**

The user can select the interferer on the map to get more information about the interferer.

Selecting the interferer on the map and then the details button on the popup brings up the Interferer Details page (figure 10). The Interferer Details page displays a map with the Interferer displayed. The slider bars on the bottom define the start and end time of what is displayed on the map. In addition, there is a Signal to Noise Ratio (SNR) Data chart that displays the SNR data for the time range of the interferer for each sensor/satellite (PRN) combination.

![Interferer Details](image)

**Figure 10: Interferer Details**

Users can sign up for interferer alerts to be sent to their email (figure 11) or phone by text (figure 12).
TESTING

Signal Sentry 1000 was deployed and tested during GPS jamming trials that occurred at Sennybridge, United Kingdom, in August 2014. Signal Sentry 1000 was able to detect and geolocate stationary and moving jammers in both open and obstructed environments.

The trials were managed and administered by the Defense Science and Technology Laboratory (DSTL) and authorized by MoD Joint Spectrum Authority. Commercial off-the-shelf jamming devices were measured and where necessary modified to conform to the spectrum and bandwidth allowed. Commercial devices were modified under screened room conditions to ensure that they did not transmit at powers or frequencies not authorized by the clearance.

Testing ranged from stationary jammers to jammers placed in cars driving through open fields and built-up areas at speeds of up to 50 mph.

Signal Sentry 1000 utilized the jamming trials as an opportunity to test the geolocation capacity of the system in a real world setting and the results are outlined in this section. Signal Sentry 1000 successfully detected and located all GPS jamming during the trials.

JAMMER DESCRIPTION

There were two Jammers utilized during the trials, 150mW and .5W. The jammers that were used to disrupt the GPS L1CA code that operates at 1575.42 MHz. The following information characterizes each jammer.

150MW JAMMER: The physical form of the jammer and the waveform for the jammer is shown in Figure 13.

.5W Jammer: The output characteristics were measured on a Booton average power meter. The waveform for the jammer is shown in Figure 14.

OPEN FIELD TEST RESULTS

An open field test was constructed in order to observe the ability of Signal Sentry 1000 to geolocate jamming in an area with no obstructions. The test included static jammers and dynamic jammers. Five waypoints along the road were surveyed prior to the test using a Garmin, handheld GPS receiver. Six waypoints were surveyed for the purpose of evaluating location accuracy (figure 15). The following is some of the details about the testing:

- August 7, 2014
- Line Site – Open Field Testing
- Jammer – 150 mW wideband
- 6 Waypoints
- Size of Area – 320m x 444m

The overall average accuracy error was 17.25 meters.

OPEN FIELD RESULTS WITH JAMMER IN A CAR

![Figure 14: .5w jammer waveform](image)

![Figure 15: Open Field Static Jammer Locations](image)

<table>
<thead>
<tr>
<th>Waypoint</th>
<th>Accuracy Error (m)</th>
<th>Number of Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>39.7</td>
<td>37</td>
</tr>
<tr>
<td>B</td>
<td>13.0</td>
<td>35</td>
</tr>
<tr>
<td>C</td>
<td>10.8</td>
<td>116</td>
</tr>
<tr>
<td>D</td>
<td>10.7</td>
<td>32</td>
</tr>
<tr>
<td>E</td>
<td>12.1</td>
<td>67</td>
</tr>
</tbody>
</table>

Table 2: Open Field Static Accuracy
In these tests, the jammer was driven in a car on the road through the sensor field. Car was driven at 25 mph (Figure 16 left) north to south then 50 mph (Figure 16 Right) south to north along the road. Cars in the north parking lot caused multipath errors when jammer came in contact with that area.

The overall average accuracy error for 25 mph and 50 mph dynamic tracking was 10 meters.

**Figure 16:** Image on left illustrates jammer locations at 35 mph. Image on right represents jammer at 50 mph

**OBSTRUCTED AREA TEST RESULTS**

An obstructed area test was constructed in order to observe the ability of Signal Sentry 1000 to geolocate a jamming in an area with obstructions (to simulate an urban environment). An area in Sennybridge called a FIBUA (Fighting in Built-up Areas) was utilized to test both stationary and dynamic jammers. Seven waypoints were surveyed for the purpose of evaluating location accuracy. Info/Assumptions:

- August 8, 2014
- Jammer – 150 mW & .5W wideband
- 7 Waypoints
- Size of Area – 176m x 253m

**URBAN AREA STATIONARY JAMMER RESULTS**

The results with the 150mW jammer held stationary at the waypoints are as follows:

<table>
<thead>
<tr>
<th>Waypoint</th>
<th>Accuracy Error</th>
<th>Number of Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>14.1</td>
<td>117</td>
</tr>
<tr>
<td>B</td>
<td>38.9</td>
<td>42</td>
</tr>
<tr>
<td>C</td>
<td>25.0</td>
<td>49</td>
</tr>
<tr>
<td>D</td>
<td>17.8</td>
<td>53</td>
</tr>
<tr>
<td>E</td>
<td>16.1</td>
<td>104</td>
</tr>
<tr>
<td>F</td>
<td>12.6</td>
<td>80</td>
</tr>
<tr>
<td>G</td>
<td>14.0</td>
<td>117</td>
</tr>
</tbody>
</table>

*Table 3: Urban Static Accuracy*

Figure 17 provides a graphical view of the jammer position in relation to the waypoints. The overall average accuracy error is 21.40 meters.

**URBAN AREA RESULTS WITH JAMMER IN A CAR**

In these tests, the jammer was driven in a car on the road through the sensor field.

The car was driven at approximately 20 mph (Figure 18) in a clockwise direction using a .5W jammer. There were two routes driven shown in yellow (path 1) and orange (path 2). The overall average accuracy error for approximately 20 mph dynamic tracking was 50 meters.

**SUMMARY**

GPS is a ubiquitous “utility” that supports critical infrastructure including: law enforcement, transportation, communications, and financial transactions, just to name a few. It has become a vital source of information with significant economic benefit. For example, more than 3.3 million U.S. jobs are estimated to rely heavily on GPS. It is paramount that GPS is reliable, available and secure.
GPS is susceptible to service outages due to intentional and unintentional jamming. To maintain critical infrastructure, proactive measures must be taken to eliminate GPS outages. Detection and tracking is the best and first step to take as the availability and usage of low-cost GPS jamming devices has resulted in an increased threat of GPS signal disruption. Addressing the security of GPS signals and preventing denial of service should be a priority.

Exelis clearly understands the threat of signal disruption and the economic, safety, and security implications that disruptions can cause. Signal Sentry 1000 enables authorities to locate with pin-point accuracy the sources of interference thereby assuring safety, efficiency, and revenue.

Recent worldwide events demonstrate that GPS is susceptible to service outages due to intentional and unintentional jamming. Therefore, is becoming increasingly important to pursue technologies that can detect and locate GPS jammers. However, due to the fact that operating a jammer is illegal and could cause havoc it is difficult to verify these technologies in a controlled, but real world environment.

Exelis developed Signal Sentry 1000 to detect and locate GPS interference sources. The product was deployed and tested during GPS jamming trials that occurred at Sennybridge, United Kingdom in August 2014. The test data clearly indicates that Signal Sentry 1000 is capable of detecting and locating interference sources and can provide real time actionable intelligence for responders to respond to the scene of potential threats.

To find out more, please visit the Exelis Signal Sentry® 1000 website at: www.exelisinc.com/signalsentry.

ACKNOWLEDGMENTS

This document is not subject to the controls of the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR).

REFERENCES

1. PR Newswire, “Study Shows Interference with GPS Poses Major Threat to U.S. Economy” (June 22, 2011)

2. Pham, Nam D., “The Economic Benefits of Commercial GPS Use in the U.S. and the Costs of Potential Disruption” (NDP Consulting, June 2011)

3. Cameron, Alan, “Galileo from the Top: Interview with the EC’s Paul Verhoef” (GPS World, November 20, 2011)


5. Ibid


7. Thomas, Dr. Martyn, “GPS vulnerability to hacking,” Engineering and Technology Magazine, April 15, 2011


