

Perspectives — June 2008

The JLOC system will automatically take in reports of higher than normal signal levels in the GPS band and lower than normal signal/noise ratio, indicating the presence of a GPS threat. JLOC uses such reports to determine in aggregate the regions where interference is occurring. The next level is to geolocate the source of the interference extremely precisely.

Jun 24, 2008

By: [Alan Cameron](#)

Threats to GPS

Here's yet another way to measure the success of GPS: by the efforts to negate it. While unintentional jamming continues to rise, intentional jamming by both foreign military forces and at-home miscreants of various stripes also has shown increased vigor in the past six months. I'll relate here recent instances of intentional jamming on each side of the border, and briefly outline one initiative mounted by the National Geospatial Intelligence Agency (NGA) to counteract it.

North Korea Jammers

A South Korean media source, the *Chosun Ilbo*, reported in late May that North Korea has been attempting to export a device capable of jamming GPS signals, copied from a Russian unit, to Middle East countries including Iran and Syria. When the Iraq War began in 2003, the Iraqi Army reportedly used a Russian-made GPS jamming system to attempt to disrupt the U.S. military's guided weapons systems such as the Joint Direct Attack Munition (JDAM), a GPS-based bomb-guidance system, and long-range air-to-ground GPS-guided Tomahawk cruise missiles.

The Russian systems deployed by Iraq during the Gulf War were quickly disabled by U.S. military targeting. Undeterred, the North Korean knock-off supposedly offers similar goods at a lower price. South Korean military authorities are deeply concerned that the device could create havoc at home if war broke out along the ever-tense border between the two Koreas. The South Korean army will have accumulated 900 JDAMs in its arsenal by 2012.

China Jammers

In November 2007, a report surfaced that China had deployed special vans equipped with sophisticated electronics designed to jam GPS signals. At that time, U.S. intelligence officials were reportedly uncertain exactly how capable the Chinese jammers were versus U.S. munitions, but were monitoring the situation carefully, and watching for moves to export the technology to Chinese customers such as Iran. Although they had located and destroyed the Russian systems in Iraq with relative ease, Pentagon officials are concerned that they may not yet be able to deal as effectively with the Chinese jammers.

A source familiar with U.S. military efforts confirmed "the information is accurate and the situation has not improved. This is one of the reasons for more GPS signals at different frequencies and why signal strength and anti-jam efforts are top priority with the GPS Wing

currently."

China's People's Liberation Army Air Force reportedly possesses its own long-range cruise missiles equipped with GPS sensors. While China's Beidou GNSS system, reputed to have a core military component, remains far from complete, such GPS munitions, coupled with any Chinese capability, partial or whole, localized or regional, to jam GPS signals at will, constitutes a major concern for the Pentagon. Such operations could critically affect the U.S. Seventh Fleet in the Pacific and its effectiveness as a deterrent in a crisis over Taiwan – or in actual combat should it come to that.

The Domestic Variety

Meanwhile, several Internet sites offer small, localized GPS jammers for sale in the U.S. domestic market. These include a "GPS Blocker" with an advertised 10-meter to 20-meter range for roughly \$200. "Just plug into a standard cigarette lighter with 12 V for power," says the web page, "and it will automatically protect you from any GPS tracking on and within your vehicle. This is a popular item with sales personnel and delivery drivers, who wish to take lunch or make a personal stop outside of their territory or route."

On May 28, the Federal Communications Commission (FCC) issued a citation to David Steele Enterprises of Newport Beach, Calif., for marketing in the United States unauthorized radio frequency devices in violation of the Communications Act of 1934, specifically a GPS jammer imported – ironically – from Taiwan. The company admitted selling 67 GPS Jammers between December 5, 2007, and May 16, 2008. The FCC stated that the main purpose of the jammer device – blocking or interfering with radio communications – is clearly prohibited, and threatened fines of up to \$11,000 per device sold.

Hacker sites also publish instructions for a "do-it-yourself GPS jammer that can have a range of up to several hundred feet. Keep in mind this is not an easy hack; a bachelor's in electrical engineering seems like a prerequisite." The parts can be obtained at shopping-mall electronics retailers.

The Counter-Jamming Effort

The [Innovation column by Phil Ward in the June issue of *GPS World*](#) magazine "Interference Head-Up: Receiver Techniques for Detecting and Characterizing RFI," presented receivers with the capability to sense jamming-to-noise power (J/N) in the front-end. It has been suggested that a system of such receivers, distributed among already installed cell towers across the country, could constitute a monitoring network to detect and locate by triangulation any jamming sources.

The National Geospatial Intelligence Agency (NGA) has just such a system in early build-out. The JLOC system described here will automatically take in such reports from GPS sensors and use them to determine in aggregate regions where interference is occurring. The next level is to geolocate the source of the interference extremely precisely.

While manufacturers continue to improve the tolerance of their GPS products to interference, the NGA has focused on an alternative means to counter the threat of GPS interference and jamming. In 2007, the GPS Jammer Location (JLOC) Master Station went into operation at the NGA's Monitor Station Network Control Center (MSNCC). Joedy Saffel, the JLOC program manager at NGA explained, "The JLOC system is designed to monitor for GPS threats and provide alerts to military users in the field when a threat is detected." The web-based system allows military users to set up subscriptions where they can identify the area over which they would like to receive alerts. The JLOC software client military users can download from the JLOC Master Station to run in their Falcon View mission planning systems. This allows them to view the affected area of degradation based on known GPS threats.

Collate Reports

Though many details of the JLOC system operation cannot be released, Jim Dalrymple, JLOC lead at Navsys Corp., explains some of its principles of operation. "Modern GPS receivers include the capability to detect GPS interference and can provide reports showing higher than normal signal levels in the GPS band and lower than normal signal/noise ratio. This condition indicates the presence of a GPS threat. The JLOC system allows networked GPS receivers to send reports to the JLOC Master Station of detected interference, acting as JLOC sensors. The JLOC Master Station is designed to collate these reports to provide near real-time situational awareness on GPS threats to military users." Bruce Bockius, who supports JLOC Master Station operations, indicated that thousands of JLOC sensor reports are now being received daily.

Testing during the GPS Jamfest conducted regularly by the 746th Test Squadron has proven the JLOC system operation under elaborate jamming scenarios. Saffel explained: "By providing the warfighter tools situational awareness on the GPS threats and their predicted effects on military operations, they are able to plan their missions accordingly and also develop tactics to counter the threats where appropriate."

Alison Brown, president and CEO of Navsys, commented on potential JLOC system evolution. "Navsys designed the JLOC system to accept GPS sensor feeds from a variety of different sources. As more GPS equipment is able to provide JLOC sensor reports, the ability to detect and geolocate GPS threats will improve and the areas of JLOC coverage will increase." She gave as an example of a type of inexpensive JLOC sensor the company's Tidget product, which can be installed as a geolocation device and as a jammer or interference monitor. "Under a Navsys R&D project we have shown that networks of these types of inexpensive JLOC sensors could be used by a future version of the JLOC Master Station to provide pinpoint locations in near real time of even large fields of GPS interference sources."

The Department of Homeland Security developed an Interference Detection and Mitigation Plan to coordinate domestic capabilities to identify and mitigate sources of interference to GPS and its augmentations. Details of this plan will be released soon.

Tattle Tales

With the criticality of GPS and future GNSS systems to the infrastructure of the United States and many other nations, it is equally critical that mechanisms are developed to protect access to the GPS system. One vision for the future, proposed by Brown, is to make every networked GPS receiver a "tattle-tale" on its local GPS RF environment.

"One threat sensor report to the JLOC system could just indicate a particular receiver having a bad day. When we get large numbers of the JLOC sensor reports indicating a problem, though, that is pretty clearly indicating a real GPS threat. As more GPS receivers are embedded into communications networks, we could have the potential to receive JLOC reports from a very large number of sensors.

"Some might see this as a Big Brother view on protecting the GPS environment, but as Smokey the Bear might say, 'Only *you* can prevent GPS interference.'"