New technologies deployed to counter the threat of GPS jamming

Eurekalert!

The first profile of the perpetrators of GPS jamming on British roads will be presented today alongside research results that confirm it is these small device, available online for as little as £30, rather extreme solar weather, which poses the greatest threat to navigation and timing signals in the UK.

Presenters at GNSS Vulnerabilities 2013: Countering the Threat, held at the UK's National Physical Laboratory, will also demonstrate a series of new technologies including intelligent receivers and radio-based backups that will protect against the impact of these jammers.

Bob Cockshott, Director of Position, Navigation and Timing at the ICT Knowledge Transfer Network and organiser of the conference says: "Our more complete understanding of the risks posed to GNSS systems is bringing forward new mitigation technologies and approaches. There is no one solution that fits all. Instead we need to combine the right protection and back-up technologies with legal reforms which punish the ownership and use of these jammers, and finally advise government and industry on new commercial and civil policies that will reduce the incentive to jam in the first place."

Understanding the threat

The latest figures on GPS jammer use on British roads comes from the Technology Strategy Board funded SENTINEL Project and its new suite of detectors which includes one deployed close to a busy airport that has been logging as many as 10 interference events per day. Concerns have been raised in the past around the potential impact of jamming on air traffic control systems and aviation landing technology.

This data also provides a profile of the likely sources of this jamming. The interference profile with marked peaks during the week and a dearth of hits at the weekend strongly indicate it is human activity which is the primary cause rather than natural sources of interference such as the effects of space weather. More specifically, marked peaks during the times of rush hour traffic suggest the main users of jammers are commercial drivers of company vehicles rather than organised criminal gangs who have been caught with jammers in lorry hijackings.

Charles Curry, founder of Chronos Technology, and a leader of the project says: Over the past four months our sensors near this airport have detected nearly 100 events on Mondays, but this falls to less than 30 on a Sunday. The pattern of behaviour suggests it is likely to be civilian sourced jamming and most likely the evasion of tracking within commercial vehicles for moonlighting activities or for

other non-work purposes. More broadly we are also seeing an overall increase in interference incidence which is worrying at a time when GPS is being thrust upon people more and more with GPS tracked car insurances, company vehicle tracking, criminal tagging or asset tracking. The SENTINEL project can now quickly deploy small test networks to organisations with critical infrastructure dependent on GPS signals so they can quantify the problem for themselves and take the appropriate action to counter the threat."

The danger of these jammers is confirmed by new results presented today from the STAVOG project, which developed state of art interference simulations using Spirent, a UK based simulator manufacturer. These mimic the various threats to GNSS signal covering both extreme solar weather and the latest illegal jamming devices available online. In partnership with the General Lighthouse Authorities, STAVOG then tested these interference simulations on a variety of marine grade receivers used in most big commercial shipping vessels and found:

- Despite simulating intense solar activity, the perceived threat from solar weather only resulted in minor signal interference and no complete outages for any of the tested marine receivers
- In contrast even the cheapest jammers resulted in complete outages across all receivers currently on the market. Some were jammed without the users even knowing and continued to give out inaccurate results, potentially leaving shipping at risk of grounding or collision.

Dr. Chaz Dixon, Project Manager of STAVOG says: "The results from the simulated solar storms were unexpectedly dull. Concerns over the impact of space weather on the most precise use of GPS such as offshore oil operations are legitimate, but our testing proved that modern receivers cope remarkably well with even high levels of disturbance. Instead the real danger seems to come from illegal jammers which other studies have shown are increasingly common. Even the cheapest ones available online can cause complete outages of the receiver signal. It is in anticipation of this threat that we will be making this service available for any GPS users to understand and protect themselves against the vulnerabilities in their positioning and timing systems."

Mitigation technologies

- The General Lighthouse Authorities will announce details of the first demonstration of a new type of jamming-proof receiving system for the shipping industry to take advantage of the recently unveiled back-up eLoran radio-navigation signal for the world's busiest shipping lanes in the Dover Strait. The receiving system is the first in the world to switch automatically and seamlessly to eLoran should the GPS signal be lost. It will be demonstrated on board the GLA vessel Galatea on several excursions from Harwich, starting on 25 February, during which its GPS navigation system will be jammed.
- Raytheon will outline how the modernisation and miniaturisation of

controlled reception patterns antennas (CRPA) technology, within the military domain, can have application into the non-military arena. CRPA systems have been used in military application for many years but are only now available at the reduced cost, size and power consumption which makes them applicable to civil operations, particularly those of high critically such as in aircraft positioning and landing. In aviation there is some concern over the increasing use of Global Navigation Satellite Systems (GNSS) as a critical component of systems such as ADS-B for en-route and airfield operations, coupled with the increasing recognition that GNSS vulnerability needs to be tackled in the non-military domain, Raytheon will discuss how the investment in military technology may benefit the civil community.

- Mike Jones, Senior Consultant Engineer at Roke Manor Research, will discuss the barriers to wider adoption of military anti-jam technology, and preview a new miniaturised anti-jamming product aimed at critical infrastructure, security and civilian markets. In addition, the accurate geolocation of jamming sources will be discussed, with technology offered to enable monitoring, enforcement and prosecution of GNSS spectrum offences.

Source: http://www.eurekalert.org/pub_releases/2013-02/npl-ntd021113.php [1]

Source URL (retrieved on *12/09/2013 - 12:53pm*):
http://www.ecnmag.com/news/2013/02/new-technologies-deployed-counter-threat-gps-jamming?qt-video_of_the_day=0

Links:
[1] http://www.eurekalert.org/pub_releases/2013-02/npl-ntd021113.php