URSI AP-RASC, Sydney, Australia, 17-22 August 2025

Cyber Vulnerabilities in GNSS-Enabled Systems

Andrew G Dempster*(1), Peter Johnson(1), and Arash Shaghaghi(1)
(1) University of New South Wales, NSW, Australia 2052, e-mail: a.dempster@unsw.edu.au

For over a decade, it has been known that GNSS is essential to all critical infrastructure sectors of the economy. Vulnerability of GNSS systems is thus a serious issue, with serious economic consequences if not addressed.

Historically, significant effort has been invested in research into jamming and spoofing of GNSS systems, as the low signal levels received from the satellites are easily overcome by attacks of this kind. This research has led to receivers being made more resilient to this kind of attack, but it only deals with one channel: the satellite to receiver channel.

The critical infrastructure that relies on GNSS uses GNSS-enabled systems that have many communications channels and many storage locations, each of which is vulnerable to attack, generally in ways that are not addressed by the body of research dedicated to jamming and spoofing.

This presentation reports on a study that examines many of these GNSS-enabled systems, identifying where vulnerabilities lie. The study is as comprehensive in the coverage of these systems at block diagram level. It then drills down in one system to demonstrate how cyber security discipline can be brought to analyse these systems for vulnerability to attack. Although the type of attack can be described in language common to many cyber physical systems, the methodology of how such attacks can succeed relies on GNSS subject matter expertise.

The system chosen as the exemplar is Australia's Space Based Augmentation System (SBAS): SouthPAN. Each of the well-known types of cyber attack are examined and evaluated in terms of whether they apply in such a case. Several vulnerabilities are identified which have not before been discussed in the public domain. The resulting implications for other GNSS-enabled systems are then discussed.