Chapter 13
GNSS Vulnerability: A Taxonomy

Andrew G. Dempster
University of New South Wales, Australia

ABSTRACT

This chapter examines sources of global navigation satellite system (GNSS) vulnerability, identifying the broad range of topics that comes under this heading, and cites some key references in each category area. GNSS vulnerability has been a very productive area for GNSS researchers in recent years and this chapter sets out to be a comprehensive review of the different ways that the operation of GNSS can be degraded by outside influences, from the high (system) to the low (receiver component) level.

INTRODUCTION

Satellite navigation systems are vulnerable to interference of various kinds. This interference has a range of effects and there is a range of remedies available to receiver designers and users. This chapter aims to summarize and provide a taxonomy of the state of knowledge of all sources of satellite navigation vulnerability.

Global Navigation Satellite Systems (GNSS) have been implemented or are being implemented by the US (Global Positioning System – GPS), the USSR, and later Russia (Glonass), Europe (Galileo) and China (Beidou/Compass). Regional Navigation Satellite Systems (RNSS) are being implemented by China (Beidou/Compass has regional elements), Japan (Quasi-Zenith Satellite System – QZSS) and India (Indian Regional Navigation Satellite System – IRNSS). Additionally, there are Space-Based Augmentation System (SBAS) satellites that carry navigation payloads that “look like” satellites from other systems, GPS in particular. One thing all these systems have in common is that their received power on the surface of the earth is very weak. For instance, the civilian GPS signal, L1 C/A has a specified minimum received power on the earth’s surface of -158.5 dBW which requires an equivalent isotropic radiated power (EIRP) of 26.8 dBW, or power into the antenna of 21.9W (Kaplan, 2006). In other words, about 20W of power is transmitted over 20,000 – 26,000 kilometers. These extremely weak signals can still be used for navigation, as the common in-car navigator proves to the layman. However, their low...
levels mean that, despite being controlled by strong and stable entities (in the case of GPS for instance, the US military), they are still vulnerable.

This chapter aims to outline the types of vulnerability experienced by GNSS systems and signals.

**SOURCES OF GNSS VULNERABILITY**

The categories of vulnerability are shown in Figure 1, with arrows indicating a breakdown of more general categories into lower level categories. Figure 1 does not indicate the overall structure of the chapter, because the highest level of Figure 1 includes vulnerabilities to systems that use and augment GNSS. However, it is important here to acknowledge that these vulnerabilities exist, and are important to users and integrators of GNSS systems. Augmentation systems such as space-based augmentation systems (SBAS), continuously operating reference station (CORS) networks, real-time kinematic (RTK) systems, differential GPS (DGPS), and assisted GPS (AGPS) all have vulnerabilities of their own, but are not considered further here. Similarly, systems that integrate GPS can suffer where reported GPS positions can be intercepted and modified (spoofed) (Hackett, 2015). This type of vulnerability is also not considered further here.

We first consider the three segments of a GNSS system: the space segment, the control segment and the user segment. When speaking about GNSS vulnerability, most people think only of signal interference in the user segment. This will be dealt with in a later section. Here we consider the control and space segments.

*Figure 1. High-level Categories of where GNSS vulnerability can occur. In other words, vulnerabilities occur at system and segment levels, as well as the better known examples at lower levels. The box at the bottom right is expanded further in Figure 2.*
Related Content

Cognitive Radio Networks: IEEE 802.22 Standards
[www.igi-global.com/chapter/cognitive-radio-networks/210267?camid=4v1a](www.igi-global.com/chapter/cognitive-radio-networks/210267?camid=4v1a)

Mobile Technology Adoption in the Supply Chain
[www.igi-global.com/chapter/mobile-technology-adoption-supply-chain/58856?camid=4v1a](www.igi-global.com/chapter/mobile-technology-adoption-supply-chain/58856?camid=4v1a)

Microsystems for Wireless Sensor Networks with Biomedical Applications
[www.igi-global.com/chapter/microsystems-wireless-sensor-networks-biomedical/58841?camid=4v1a](www.igi-global.com/chapter/microsystems-wireless-sensor-networks-biomedical/58841?camid=4v1a)

Distributed Space-Time Block Coding for Amplify-and-Forward Cooperative Networks
[www.igi-global.com/chapter/distributed-space-time-block-coding/36551?camid=4v1a](www.igi-global.com/chapter/distributed-space-time-block-coding/36551?camid=4v1a)