Chapter 3
Interference and Spoofing: New Challenges for Satellite Navigation Receivers

Fabio Dovis
Politecnico di Torino, Italy

Luciano Musumeci
Politecnico di Torino, Italy

Nicola Linty
Politecnico di Torino, Italy

Marco Pini
Istituto Superiore Mario Boella, Italy

ABSTRACT
This chapter deals with one of the major concerns for reliable use of Global Navigation Satellite Systems (GNSS), providing a description of intentional and unintentional threats, such as interference, jamming, and spoofing. Despite the fact that these phenomena have been studied since the early stages of Global Positioning System (GPS), they were mainly addressed for military applications of GNSS. However, a wide range of recent civil applications related to user safety or featuring financial implications would be deeply affected by interfering or spoofing signals intentionally created. For such a reason, added value processing algorithms are being studied and designed in order to embed in the receiver an interference reporting capability so that they can monitor and possibly mitigate interference events.

INTRODUCTION
Global Navigation Satellite Systems (GNSS) are communication infrastructures enabling a generic user to compute position, velocity and time at its current location anywhere on the Earth, processing the signals transmitted from a constellation of satellites and performing a trilateration with respect to the satellites taken as reference points. One of the main characteristics of GNSS signals is the low signal power level reaching a receiving antenna on the ground. Despite of the weakness of the signals, the spread spectrum nature of the transmission allows navigation receivers to recover timing information and to compute the user’s position by exploiting the gain obtained at the output of the correlation block (Enge & Misra, 2006).

Among all the different error sources that can potentially corrupt satellite navigation waveforms, such as errors introduced by ionospheric and tropospheric propagation, obsolete satellites ephemeris, errors due to satellites clocks, Radio Frequency

DOI: 10.4018/978-1-4666-6034-2.ch003
Interference and Spoofing

Interference (RFI) is particularly harmful since, in some cases, it cannot be mitigated by the correlation process. In fact, even if the correlation process is theoretically able to mitigate the presence of nuisances in the bandwidth of interest, a real limitation can be the finite dynamic range of the receiver front-end (Motella, Savasta, Margaria, & Dovis, 2009).

The presence of undesired RFI and other channel impairments can result in degraded navigation accuracy or, in severe cases, in a complete loss of signal tracking. It is also to be considered that the number of electromagnetic sources that are candidate to become unintentional interferers for GNSS signals is large. There is in fact an increasing number of systems that we depend on in daily life that rely on the transmission of Radio Frequency (RF) energy in the L-band or close to it (Kaplan & Hegarty, 2005). Depending on the spectral and power features of the interfering sources they can affect the performance of GNSS receivers (CEPT, 2002).

Furthermore, GNSS threats include intentional attacks aiming at deceiving the target receiver. Recalling that GNSS bandwidths are protected and that signal radiation on frequency bands allocated to radio navigation is not legal, the transmission of false GNSS-like signals, usually known as RF spoofing, may become quite dangerous also for civil use of GNSS, as the number of applications increases.

An example of application that can be severely damaged by jamming or spoofing attacks are the new Pay As You Drive (PAYD) systems, in which costs of motor insurance depend on the type of vehicle used and are measured against time, distance and place. PAYD insurance usually involves an on-board unit equipped with a GNSS receiver able to collect and transmit data related to the vehicle’s use to an operational center: the device can measures how safely the vehicle is being driven in terms of speed, type of road, driving time and distance. GNSS is a key component in this segment and also it enables additional services, like the last estimated position in case of a distress call after an accident (European emergency call) or for tracking a stolen vehicle. This application, taken as example, demonstrates that RF spoofing is a potential risk leading to frauds towards insurances. The driver might want to take advantages providing false positions to the service provider (e.g. pretending he is driving on a different road, parking in a different park slot, etc.). In this case, we refer to self-spoofing (or limpet spoofing), since the target receiver is owned by the attacker. Although RF spoofing in the road sector seems just a research curiosity, the problem can be real in the future years, since the market for insurance telematics is now approaching its maturity phase. In 2010, the telematics-enabled services market was worth in Europe an estimated of approximately 5 b€, or 4% of the whole European motor insurance market, estimating 2 million users worldwide (PTOLEMUS Consulting Group, 2012).

The scope of this chapter is to provide an updated overview of both the traditional and the most advanced techniques currently under investigation for unintentional interference, jamming and spoofing detection, in order to implement user alerts and, possibly, to mitigate their effects on the receiver performance.

In the first part of the Chapter the different threats are considered and described in details, providing a general classification. Then, an overview of techniques for detection and mitigation of interference and jamming is presented, along with some mathematical details and examples, showing their features and performance. To conclude a brief note on the complexity tradeoff is given and the future research directions are outlined.

**BACKGROUND: THREATS CLASSIFICATION**

GNSS receivers’ interference can be divided in unintentional and intentional. Intentional interference includes jamming, meaconing and different
Related Content

Round-trip Engineering UML Class Models and Java Models: A Real-world Use Case for Bidirectional Transformations with QVT-R
[www.irma-international.org/article/round-trip-engineering-uml-class-models-and-java-models/170520/](www.irma-international.org/article/round-trip-engineering-uml-class-models-and-java-models/170520/)

Iterative Knowledge Based Embedded Systems Development Framework
[www.irma-international.org/chapter/iterative-knowledge-based-embedded-systems/50442/](www.irma-international.org/chapter/iterative-knowledge-based-embedded-systems/50442/)

Migration Goals and Risk Management in Cloud Computing: A Review of State of the Art and Survey Results on Practitioners

2-SQUARE: A Web-Based Enhancement of SQUARE Privacy and Security Requirements Engineering
[www.irma-international.org/article/square-web-based-enhancement-square/77617/](www.irma-international.org/article/square-web-based-enhancement-square/77617/)

A Study on the Intention to Adopt Third Generation (3G) Wireless Service on a Small Community with Unique Culture: The Use of Hofstede Cultural Dimensions in Predicting the Interaction between Culture and the Technology Acceptance Model on Guam
[www.irma-international.org/article/a-study-on-the-intention-to-adopt-third-generation-3g-wireless-service-on-a-small-community-with-unique-culture/89388/](www.irma-international.org/article/a-study-on-the-intention-to-adopt-third-generation-3g-wireless-service-on-a-small-community-with-unique-culture/89388/)