Application of Computer Modelling in Adaptive Compensation of Interferences on Global Navigation Satellite Systems

Valerian Shvets
National Aviation University, Ukraine

Svitlana Ilnytska
National Aviation University, Ukraine

Oleksandr Kutsenko
National Aviation University, Ukraine

EXECUTIVE SUMMARY

Modern society is characterized by the increased use of global navigation satellite systems (GNSS), which is inseparably linked with the interference immunity ensurance. The most effective way to protect against interferences is an introduction into the receiver structure of adaptive interference compensators. However, the most of proposed methods have been designed for radiolocation and communication and use a priori information about the transmitted signal. Since as structure of GNSS signal differs from the radar and communication systems, GNSS does not know the time-frequency structure of the useful signal in advance, which excludes the possibility of using a number of widely known methods. In this chapter, the authors propose a method, which does not use a priori information about a useful signal, and a new direct method for calculating the inverse correlation matrix of interference in adaptive antennas of interferences compensators.

ANALYSIS OF GLOBAL NAVIGATION SATELLITE SYSTEMS VULNERABILITIES

Modern society is characterized by the increased use of Positioning, Navigation, and Timing (PNT) services, which provide the basis for the effective functioning of many industries. In particular, PNT is an essential part of modern transportation systems, digital systems, telecommunications systems, command and control of precision weapons. The main suppliers (providers) of PNT services are Global Navigation Satellite Systems (GNSS), which are presented now by Global Positioning System (GPS, USA) (Federal Aviation Administration [FAA], 2013 a, 2013 b), GLObal NAvigation Satellite System (GLONASS, Russia) (Russian Institute of Space Device Engineering, 2008). The European Community sets up its own GALILEO system and China sets up BeiDow system for these purposes. GNSS provides with the data, using which one can determine the position of any user in space with an accuracy of one meter and by time with the accuracy of dozens and units of nanoseconds in any point of the globe and near-Earth space at any given time and in any weather.

After the first years of the intensive development and implementation of satellite navigation and time technologies, the more thorough analysis of the use of GNSS as the sole source of coordinate-time information, and more sober approach to the prospects of using GNSS begins. First, this is due to the GNSS vulnerability under the influence of unintentional and intentional interferences. The vulnerability of civilian GNSS receivers had been known for a long time (Littlepage, 1998; Pinker, Walker and Smith, 1998; Lyusin et.al., 1998; Ward, 1994; Gilmore, 1998; Key, 1995; Bond, 1998), but receiver manufacturers and their users rarely consider it. Only when the US Department of Defense has intensified its activities related to the use of GPS in the military environment (NAVWAR), it became apparent that deliberate interferences to the civilian receivers should be taken into account as an important factor. Military testings conducted in the New York (United States) (Forssel and Olsen, 2003) area have shown, that a number of receivers installed on board of civil aviation aircrafts have lost the ability to track GPS signals (due to severe drops in the carrier-to-noise ratio of several GPS satellites' L1 C/A code) at the approach phase at the International Newark Liberty Airport (NJ, USA). After an investigation by the FAA, it was discovered that a truck driver had installed a low-cost PPD on his vehicle (Colby et al., 1997).

The analysis of transport systems based on the use of GPS signals was carried out by (Winer, et al., 1996), (Wallis, 1999; Colby, 1997), (Report of the Commission to Assess United States National Security Space Management and Organization, 2001), (Corrigan, 1999). One of the most important and relevant reports on the research in this area was the Volpe Center Report on GPS vulnerability (John, 2001), which concluded that the GPS system, like other radio navigation systems, was vulnerable to unintended and intentional interferences and that such interference was a threat to security and can have serious consequences for the economy and the environment. The report concludes that the growing use of GPS in civilian infrastructure makes it an increasingly attractive target for hostile actions by individuals and groups. At the same time, the commercial availability of equipment for interference was detected (Forssel and Olsen, 2003; Rodgers, 1991).

Thus, the GNSS vulnerability under the influence of unintentional and intentional interference is now a generally known fact. This vulnerability equally applies to all systems: GPS, GLONASS, GALILEO and BeiDow, since as the principles of their construction and frequency ranges are quite close. Currently, the radio navigation community is actively discussing the vulnerability of GNSS and the search for back-up systems. In this regard, it is necessary to analyze the main sources of unintentional interferences, possible ways of setting up the intentional interference for consumer's equipment of GNSS and the prospects for improving the reliability of coordinate and time information under interference influence.