STUDY OF ATTACKS ON SATELLITE NAVIGATION SYSTEM RECEIVERS

Teodor Mitrea[1], Vlad Vasile[1], Monica Borda[1], Corina Nafornita[2] and Alexandru Romaniuc[3]
[1] Communications Department, Technical University of Cluj-Napoca, Cluj-Napoca, Romania
[2] Communications Department, Politehnica University of Timişoara, Timişoara, Romania
[3] Communications Department, Land Forces Academy, Sibiu, Romania
tmitrea@mapn.ro, vladut.vasile@yahoo.com, monica.borda@com.utcluj.ro, corina.nafornita@upt.ro, romaniuc_alexandrugabriel@yahoo.com

***Abstract* — Nowadays, there are many important areas in which the positioning information provided by the satellite navigation systems is used, systems whose development has accelerated in recent years. Due to this pace, it seems that the measures to ensure the security of these systems have lagged behind. This article presents the results of various tests that targeted the security of the receivers of the most used commercial satellite navigation systems - those of smart phones and cars and how these receivers behave in the event of spoofing attacks.**

Keywords — GPS; satellite; navigation; attack; security

I. INTRODUCTION

Satellite navigation is a technique by which a user can determine his position based on measuring the distance between the orbiting satellites around the Earth and the receiver of the navigation system. Basically, to determine its position, the navigation equipment uses the triangulation principle. It receives from each of the satellites in the field of vision information about their position, as well as periodic timing signals used to determine the propagation time of the signal from the satellite to the receiver. When the propagation time is known, the distance between the satellite and the navigation equipment can be calculated by approximating that the signal speed is constant. Furthermore, each satellite transmits the so-called ephemeris - information about its own position at any given time.

Theoretically, the position can be determined using data from three satellites, but in practice it requires a fourth satellite to estimate another unknown - the time error of the navigation system, because the receiver's clock does not have the required time accuracy. Obviously, the more satellites are in the area of visibility, the more accurate the position estimation becomes. The estimation of the distance between the satellite and the user is based on the measurement of the propagation time of the signal. The accuracy of these measurements is influenced by the following sources of errors [1]: satellite clock, signal distortion, satellite-positioning errors, and influence of the ionosphere and troposphere, reflections, thermal noise, interference and receiver type.

In addition, the navigation signal has a very low power level at the reception, being very affected by the ambient noise and the interference with other signals. Regarding the influence of the ionosphere and the troposphere, the magnitude of the errors caused depends on the solar activity and the elevation of the satellite.

This paper presents the results of a study that carried out various tests aimed at the security of the receivers of the most used commercial satellite navigation systems - the navigation systems incorporated in the smartphones and the navigation systems for cars (car navigators). Specifically, the way in which these receivers behave in the case of spoofing attacks was studied.

The paper is organized as follows. In Section 2, the important aspects regarding the security of satellite navigation systems are highlighted, and in Section 3 the tests performed for the evaluation of the way in which common satellite navigation receivers behave in the case of spoofing attacks are presented. The paper ends with the conclusions resulting from these tests and it was found that the measures to ensure the security of these systems or, at least, the protection against spoofing attacks, are not at the same level with the development of the capabilities of these devices.

II. ASPECTS REGARDING THE SECURITY OF SATELLITE NAVIGATION SYSTEMS

A. Global Positioning System Background

Currently, the best known GNSS (Global Navigation Satellite System) is GPS (Global Positioning System) a system that uses a constellation of 32 satellites orbiting the Earth [2], transmitting signals that allow users to determine their position anywhere on the planet. The first satellite of this system was launched in 1978 and became fully operational in 1995. The system offers two different positioning services: SPS (Standard Positioning Service), using a signal transmitted in the L1 band (1575.42 MHz) and PPS (Precise Positioning Service) using two signals in the L1 (1575.42 MHz) and L2 (1227.6 MHz) bands. The satellites launched in orbit since 2005, also emit in the L5 band (1176.45 MHz), this signal being interoperable with those emitted by other navigation systems (European, Japanese and Indian).

GPS mainly uses BPSK (Binary Phase-Shift Keying) and BOC (Binary Offset Carrier) modulation, the signal having at the receiver level a power of approximately -158 dBW. Some satellites transmit several BPSK streams at the same frequency

978-1-7281-5611-8/20/$31.00 ©2020 IEEE

in quadrature, in a form of quadrature amplitude modulation (QAM).

GPS is not the only navigation satellite system: the Russian Federation owns GLONASS (GLObal NAvigation Satellite System), the Galileo system is a product of the collaboration between European Space Agency and European Commission, while China has its own navigation system called BeiDou [3].

B. Satellite navigation systems security background

Nowadays, there are important areas such as transports, finances, communications, agriculture, emergency services and many others that use the information transmitted through GNSS, and the security of these systems is becoming an increasing issue. In order to discuss about satellite navigation systems vulnerabilities two important peculiarities of navigation signals are to be taken into consideration: the very low signal strength and the fact that the structure and characteristics of the GPS signals are well known.

Generally, attacks on navigation systems fall into two broad categories: signal jamming and signal spoofing. Although they do not cause major damage to the satellite navigation system as such, because the target is not represented by its components, but by the calculated location solution, they can have severe effects on critical national infrastructures and many other systems. In fact, signal jamming is a relatively simple process by which a signal is emitted at the same frequency transmitted by the satellites of the navigation systems, so that the receiver can no longer separate the navigation signal. On the other hand, spoofing involves deceiving the tracking device so as to believe that it is in another location and even at another time, by issuing signals that mimic the authentic ones, but contain the information inserted by the attacker.

Currently, there are numerous studies in the field of spoofing attacks on navigation signals and, due to the fact that the security of satellite navigation systems is a topical issue, solutions are still being sought for the defense against these types of attacks. In the same manner, satellite navigation can also be used for destructive purposes. For example, guided drone attacks can be carried out via satellite navigation systems.

Due to this fact, there are also studies exploring ways in which a spoofing attack can be used, for example to control and capture a drone with hostile intentions [4]. Therefore the fact that the structure and characteristics of navigation signals represent public information creates the premises for the relatively easy development of spoofing attacks on receivers used by navigation systems worldwide.

At present, there are numerous studies and reports that indicate the development of GNSS spoofing attacks around the world [5], [6].

III. Approach Overview

The aim of this paper is to bring to the forefront the security of satellite navigation systems and specifically, the way in which common satellite navigation receivers behave in the case of spoofing attacks. The safety of the satellite navigation systems receivers was tested in a legal framework, in specific laboratory conditions to avoid possible interference and the used frequency bands were monitored permanently, in the immediate vicinity of the transmitters.

A. GPS spoofing attacks overview

Because GPS is the most widely used navigation system globally, the tests on the security of the receivers of the navigation systems were performed by emitting counterfeit signals on the 1575.42 MHz frequency (L1 band of GPS).

The following equipment was used for the performed tests: laptops with common technical characteristics and a Linux distribution as operating system; several smartphones with various operating systems with built-in navigation systems and car navigation systems (from older generations, but also from the latest generation); Software Defined Radio equipment (RTL-SDR, HackRF One); equipment for spectral analysis of signals (Spectran 5).

As far as smartphones are concerned, a wide range has been used, with navigation software that used information from one or more GNSS, different operating systems with different versions, over 50 such devices being used in the performed tests.

To carry out the spoofing attacks, files containing navigation data were used and modified such that, upon receiving the information contained in them, the navigation system indicates a location desired by the attacker.

An open-source software application was modified to meet the purpose of the test and was used to process navigation information. The information thus modified was transmitted using HackRF One, an SDR (Software Defined Radio) platform, compatible with many software applications and extensions. The proposed approach is schematically illustrated in Fig. 1.

The software application was used in static working mode, compiling a fixed position given by latitude and longitude coordinates. Thus, the attacker can indicate a location he wants directly through the command line.

Compiling the files, containing the navigation data with the coordinates for which a false GPS signal is desired, is performed at the command line by calling a library consisting of a series of files built in the C++ programming language.

These files contain algorithms that perform the compilation of the input files having as output a binary file. In the following, a GNU Radio Companion project was developed [7], as illustrated in Fig. 2, to indicate the emission flow graph of the previously compiled binary file, but also to perform time/spectral analysis in the time and frequency domains, especially for monitoring the emitted counterfeited GSP signals.

The diagram illustrated in Fig. 2 contains a source block in which the file to be transmitted is uploaded and from which the bit string will be retrieved. In the continuation of the source we find a block of modulation of the signal.

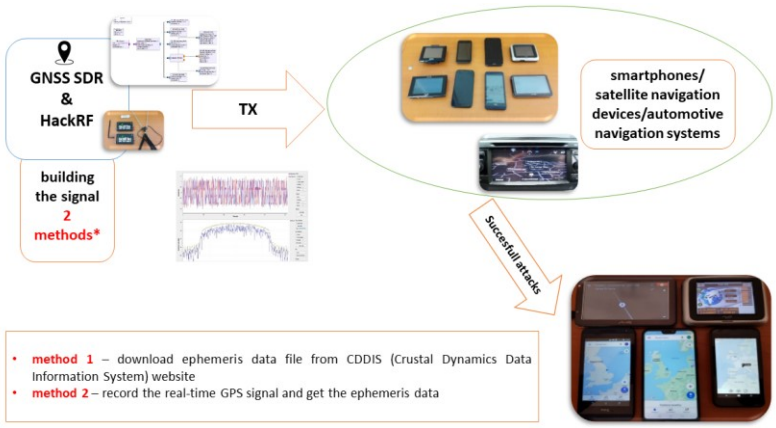

Fig. 1 Test setup.

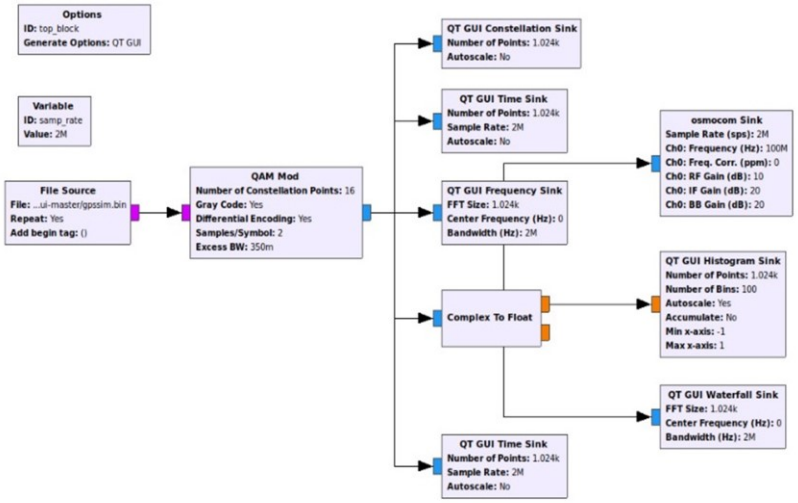

Fig. 2 Emmision diagram using GNU Radio Companion.

B. GPS spoofing attacks scenarios

For the first set of tests, in the case of smartphones that allowed advanced configurations for the location settings, all additional options were deactivated, or, as the case may be, the location method that uses only GPS information was chosen.

When the counterfeit signals were issued, almost all the tested systems indicated the location chosen by the attacker. The only exceptions were iPhone smartphones that had iOS 13 operating system versions. Although, regarding these smartphones, the attack did not have the effect desired by the attacker, the navigation system became unusable, because it was not possible to locate the position or it provided incorrect location information (other than those desired by the attacker).

The test was repeated, choosing other locations around the Earth, the result being the same: the position indicated was the one chosen by the attacker.

For the second set of tests, the advanced settings for smartphones that had such options on the menu were changed. This time, location settings were chosen so that the devices use other available information: information from mobile networks, wireless networks and also Bluetooth devices.

For this test set, the additional settings were activated one at a time, not simultaneously. After changing the available options, the tests were repeated following the same steps as in the initial set of tests.

IPhone smartphones that had iOS 13 operating system versions were no longer used for these tests, as they do not have advanced localization options.

The results obtained were the same as the initial ones, after emission with the counterfeit message, the navigation devices changing their position and indicating the location desired by the attacker.

The tests were also repeated, choosing other locations around the Earth, the result being the same: the position

indicated was the one chosen by the attacker, so the attack was successful. An example of localization is illustrated in Fig. 3.

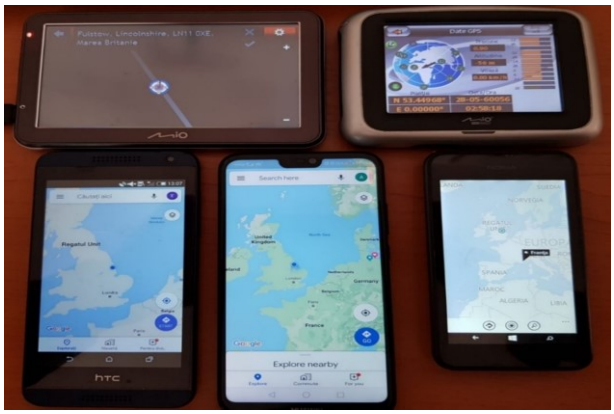

Fig. 3 Example of localization within set 2 of tests.

For the third set of tests, the advanced settings for smartphones that had such options on the menu were changed again. This time, location settings were chosen so that the devices use all available information: navigation signals, information from mobile networks, wireless networks, Bluetooth devices, as illustrated in Fig. 4.

Fig. 4 Configuring locating method – advanced settings.

These settings are most commonly found on mobile devices. When first using the embedded navigation systems, the user is usually asked if he wants to improve the location accuracy and in most situations he accepts. At that point the device sets the advanced options in this mode.

Similar to the previous test set, iPhone smartphones that had iOS 13 operating system versions were excluded from this test set.

The tests were repeated following the same steps as the initial set of tests, under these new conditions. The navigation devices have changed their position and indicated the location desired by the attacker, so the attack was successful, as illustrated in Fig. 5.

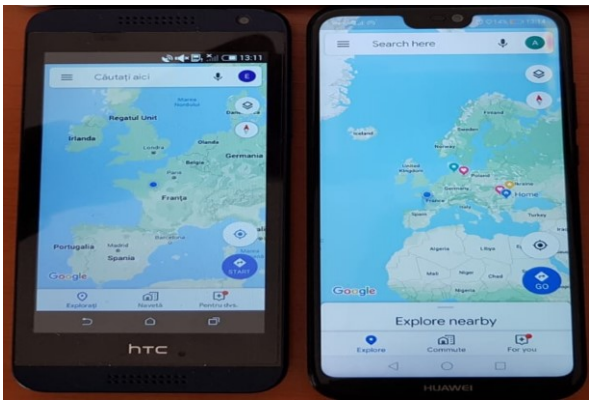

Fig. 5 Example of localization within set 3 of tests.

In these first three sets of tests, the output of the counterfeit signal was performed in a laboratory where there was no authentic signal of the navigation systems, using very low power level signals. This level is similar to the power level of authentic GNSS signals at the receiver level of the navigation system (-158 dBW).

Using the results obtained in these first sets of tests, in the fourth set of tests we aimed to use two SDR transmitters:

- one of the laptops together with an SDR transmitter was used to emit location signals using the same power level as in the previous tests, thus simulating the situation where the receivers of the navigation systems would receive a genuine signal; this signal was issued throughout the tests;
- the second laptop, with another SDR transmitter was used to simulate the attack, after the navigation systems were located.

In a first phase, the second transmitter was used to transmit signals with the same power level as the first transmitter. In this situation, as expected, most devices failed to locate. In the second phase of this test set, the signal strength of the second transmitter was increased.

After increasing the signal strength, most of the tested devices changed their location indications, displaying the position desired by the attacker. However, there were exceptions, some of the devices indicating the loss of the location signal. IPhone smartphones with iOS version 13 behaved the same as in the first set of tests.

For the last set of tests, a “bucket” type work area was arranged in the outer space: a test area in which the emitted signals could not propagate horizontally outside this boundary, but which was not covered. In this way, the satellite navigation system receivers received authentic positioning signals from the satellites in the area of visibility. In this set of tests, the devices were allowed to position themselves using authentic signals, after which counterfeit signals were issued. Initially, it was emitted with a low power level. Under these conditions, most navigation systems have changed their position, indicating the location desired by the attacker.

When using a higher power level of the counterfeit signal, the same results were obtained as for the initial test set: all the systems used for testing indicated the position chosen by the attacker, the only exceptions being the iPhone smartphones with iOS operating system version 13. Their behavior was also similar to that of the tests performed initially. Unlike the previous set of tests, these were the only exceptions reported, with no other devices indicating loss of localization signal. Within this last set of tests, due to the simulation conditions, some navigation systems incorporated in the on-board equipment of some cars could be included.

As the number of navigation systems of this type included in the tests is small, the results may not be considered relevant, but it should be noted that, in their case, the tested devices indicated the location desired by the attacker.

IV. CONCLUSIONS

As a result of these various tests, it was found that the measures to ensure the security of common satellite navigation receivers or, at least, the protection against spoofing attacks, are not at the same level with the development of the capabilities of these devices.

After performing several types of tests, as outlined in Table I, it was concluded that these devices, with very few exceptions, are vulnerable to spoofing attacks. Using commercial equipment, cheap and simple to procure, the necessary premises have been created to emit counterfeit GPS signals. When issuing these counterfeit signals in several types of tests, after a relatively short time, which varied slightly from device to device, in which the receivers of the navigation systems made the acquisition of signals, almost all the tested systems indicated the location chosen by the attacker.

TABLE I. Summary of the tests.

Test ID	SDR nodes	Devices	Location method	Location
T01	1	smartphones, satellite navigation devices	GPS only	Lab/indoor
T02	1	smartphones, satellite navigation devices	GPS + other sources (one at a time)	Lab/indoor
T03	1	smartphones, satellite navigation devices	GPS + all other available sources	Lab/indoor
T04	2	smartphones, satellite navigation devices	GPS + all other available sources	Lab/indoor
T05	1	smartphones, satellite navigation devices, automotive navigation systems	GPS + all other available sources	Training field/ outdoor

It should be noted that the only devices that failed to respond to the counterfeit signals by positioning in the location desired by the attacker were devices with a very recent version of the operating system belonging to a single manufacturer. Moreover, even in the case of these exceptions, the attacks carried out resulted in a malfunction of the navigation system.

Although the test aimed only to change the location of the tested systems, some of them also indicated changes in the displayed time. This phenomenon was mainly encountered in car navigators, which is explained by the fact that those systems are built in such a way as to adjust their clock using the information transmitted by the satellites of the navigation systems.

However, it is important to note that a significant part of the tested devices was represented by latest generation smartphones that could use navigation information from several satellite navigation systems (GPS, GLONASS, Galileo, BeiDou). Even if a series of tests were performed under the conditions in which the tested navigation systems had also authentic navigation signals at the reception, location settings were chosen so that the devices use other available information (from mobile networks, wireless networks) and the counterfeit signals were only emitted at the frequency of 1575.42 MHz (GPS L1 band / Galileo E1 band) with the format of GPS messages, these multi-constellation devices behaved similar to those that used for positioning only GPS signals. This leads to the conclusion that the software used by the manufacturers of multi-constellation devices uses as a high-priority information the signal received from GPS satellites.

On the other hand, satellite navigation can be used for destructive purposes and, in those situations; such a spoofing system can be really useful in defending against GPS-guided weapons.

REFERENCES

[1] P. J. G. Teunissen, O. Montenbruck (Eds.), “Springer Handbook of Global Navigation Satellite Systems” 2017.

[2] USA Department of Defense, “Global Positioning System SPS Performance Standard”, 4th Edition, September 2008.

[3] Vlad-Cosmin Vasile, Corina Nafornita, Monica Borda, “Comparative Study of Satellite Navigation Systems”, International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, November, 2018.

[4] A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing”, University of Texas at Austin, 2014.

[5] C4ADS, “Above Us Only Stars - Exposing GPS Spoofing in Russia and Syria”, April, 2019.

[6] David Duchet, Gerhard BERZ, “GNSS RFI Mitigation: International Efforts to Protect Aviation”, 58th Civil GPS Service Interface Committee Meeting, Miami, September 2018.

[7] Y. Pei, H. Chen and B. Pei, "Implementation of GPS Software Receiver Based on GNU Radio", Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), Xuzhou, 2018, pp. 1-3.

[8] S. Lo, Y. H. Chen, D. Akos, B. Cotts, and D. Miralles, “Test of Crowdsourced Smartphones Measurements to Detect GNSS Spoofing and Other Disruptions,” Proceedings of the 2019 International Technical Meeting of The Institute of Navigation, Feb. 2019.

[9] P. Dabove and V. Di Pietra, “Single-Baseline RTK Positioning Using Dual-Frequency GNSS Receivers Inside Smartphones,” Sensors, vol. 19, no. 19, p. 4302, Oct. 2019.