DOI: 10.26552/tac.C.2023.1.8

GNSS Spoofing – Advanced Mechanisms of Detection

Vojtech Šimák[1], Jozef Šedo[2]

[1]Department of Control and Information Systems, Faculty of Electrical Engineering and Information Technologies, University of Žilina, Univerzitná 1, 01026, Žilina, Slovakia
[2]Department of Mechatronics and Electronics, Faculty of Electrical Engineering and Information Technologies, University of Žilina, Univerzitná 1, 01026, Žilina, Slovakia

Abstract GNSS spoofing is a technique used to deceive Global Navigation Satellite Systems (GNSS) receivers by broadcasting fake signals that appear to be genuine. To detect GNSS spoofing, a receiver can use various techniques such as monitoring signal strength, cross-checking data from multiple satellites, comparing the signal characteristics with the expected patterns, and analyzing the timing and location information. Advanced detection methods may use machine learning algorithms to identify anomalies and patterns in the signal data. In addition, the use of encrypted signals and multiple frequency bands can make spoofing more difficult, and the implementation of spoofing-resistant hardware and software can further enhance detection capabilities. In this article various techniques of manipulation and detection of spoofing and experiments are described. There is no 100% method for spoofing detection.

Keywords GNSS, Spoofing, Jamming, Detection

JEL L63, L93, R41

1. Introduction

GNSS jamming is common illegal attack on availability of these services. Many systems are affected during jamming attack (navigation, emergency services, road, train, aircraft, ship transport, army, telecommunications etc.). Jamming is used by for example car thieves avoiding localization systems gain and transmit the correct position. GNSS jamming devices are cheap and available on internet market. Besides jamming, spoofing is more complex attack on integrity of these services. Nowadays GNSS chips are equipped with basic spoofing detection. During spoofing a wrong position is transmitted to receivers. This article will deal with more complex manner of spoofing detection.

Global Navigation Satellite System (GNSS) technology has become an integral part of our daily lives. It is used in various applications, such as navigation, transportation, and time synchronization [1] and [6]. However, the widespread use of GNSS technology has also made it vulnerable to attacks, such as spoofing. Spoofing is a type of attack where a malicious entity broadcasts a signal to deceive GNSS receivers. In this article, we will discuss the concept of GNSS spoofing, its effects, and the techniques used to prevent it.

The concept of GNSS spoofing involves broadcasting a signal that is intended to deceive a GNSS receiver. This can be done by generating a signal that is like the signal broadcast by GNSS satellites. The spoofing signal can be stronger than the genuine signal, causing the receiver to lock onto the spoofed signal. Once the receiver is locked onto the spoofed signal, the attacker can manipulate the receiver's output, causing it to provide incorrect information to the user.

The effects of GNSS spoofing can be severe. In transportation, it can cause accidents by manipulating the location of vehicles. In aviation, it can cause a plane to deviate from its course, leading to a crash. In maritime navigation, it can cause ships to run aground or collide with each other. Spoofing can also be used to manipulate time synchronization, causing errors in financial transactions and communication systems..

2. Basic spoofing detection

All modern GNSS receivers are equipped with basic spoofing detection algorithms. This is called as “receivers autonomous integrity monitoring” (RAIM). This is based on several features of spoofing signal. These properties could be divided into basic groups:

- **Based on time synchronization**. The time difference between GNSS time and spoofing signal time could be evaluated as spoofing presence. Based on authors experiments, if receiver starts with real signal and then receives spoofing signal, the signal is recognized as spoofing. The same applies vice versa. Some receivers are equipped with (Chip-Scale Atomic Clock) CSAC. Once synchronized, the receiving unit has increased capabilities of time comparison.
- **Stepwise changes in satellite position**. Satellites position is used in receiver for computation of receiver’s

position. This could not swap instantly from one position to another.

- **Multiple GNSS services**. Nowadays receivers have multiple receiving units for GPS, GLONASS, Beidou and Galileo. Since the data from one service differs from another two or three, it could be evaluated as a spoofing attack.

2.1. Manner of detection

For example Ublox 8 chips are capable to detect some spoofing attempts. The sentence UBX-NAV-STATUS gives under "flags2" the "spoofDetState" the information about spoofing attempts to fool the receiver. The mechanism is the data consistency check within one epoch. If the receiver is aligned to a genuine satellite signal, the spoofing attempt must be very sophisticated (the receiver detects stepwise changes in satellite position and timing). If the receiver has possibilities of multiple GNSS services, the spoofing detection works. If the receiver has only a single service and the receiver wakes up to an already spoofing polluted area, and the signal is consistent, there is no chance to detect the falsified signal.

3. The Experiment

We performed this experiment in the laboratory of the Department of Multimedia and Information and Communication Technologies. (setup at Figure 1) Used equipment was a Spirent GSS6700 GNSS simulator.

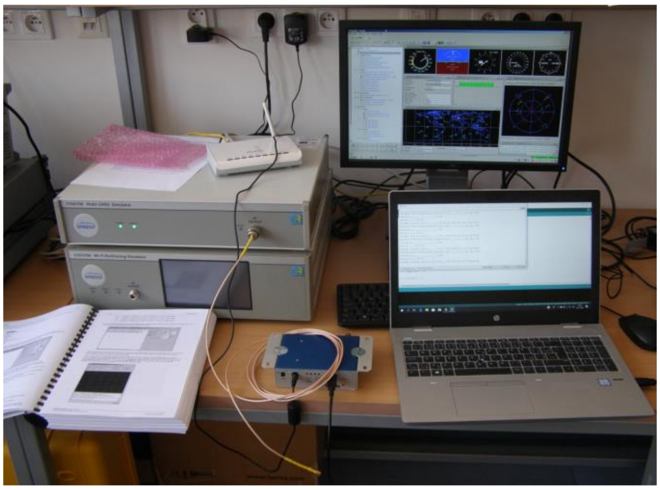

Figure 1. Setup for GPS spoofing experiment, for safety reasons the output of the generator is connected directly with the receiver, not radiating the signal.

With the help of this device, it is possible to simulate the civil part of navigation services and create a signal that would be received by the antenna in the case of a simulated trajectory. This simulator allows us to simulate different signal levels from in-dividual satellites, simulate any time, latitude, longitude, altitude, etc. For safety reasons, the receiver was directly connected to the simulator by a coaxial cable, to avoid leakage (signal transmission) and influence (spoofing) of other receivers. The device GPS Trimble Condor (70291-15) was used as the receiver. The receiver is connected to a computer that records messages composed of NMEA protocol sentences. The Spirent simulator enables the simulation of various signal changes, in this experiment we set a flight at an altitude of 500 m.a.s.l. towards the east at a speed of 50 m/s (180 km/h).

Example of a message received via the antenna (real GPS):

```
$GPGGA,070030.000,4912.1532,N,01845.3512,E,1,8,1.03,415.4,M,42.1,M,,*57
$GPGSA,A,3,16,29,05,31,26,25,20,21,,,,,1.65,1.03,1.29*01
$GPGSV,3,1,10,21,83,183,18,26,68,254,30,16,49,302,16,29,36,087,30*75
$GPGSV,3,2,10,20,27,163,24,27,17,282,,05,13,036,27,31,12,216,33*74
$GPGSV,3,3,10,25,07,148,27,10,05,176,*74
$GPRMC,070030.000,A,4912.1532,N,01845.3512,E,0.04,113.18,200100,3.3,E,A*0A
```

Example of a message received from the simulator (spoofed GPS) evaluated as correct:

```
$GPGGA,001053.000,4913.0010,N,01911.5073,E,1,7,1.18,459.6,M,42.0,M,,*5B
$GPGSA,A,3,10,29,23,02,13,04,24,,,,,,1.46,1.18,1.75*03
$GPGSV,3,1,11,02,81,328,45,04,50,084,44,10,39,217,44,13,31,066,44*7A
$GPGSV,3,2,11,23,17,039,43,29,12,313,43,24,06,274,43,12,,,44*49
$GPGSV,3,3,11,05,,,44,30,,,44,17,,,42*7F
$GPRMC,001053.000,A,4913.0010,N,01911.5073,E,97.19,90.01,200100,3.9,E,A*01
```

Example of a message received from the simulator (spoofed GPS) evaluated as incorrect:

```
$GPGGA,071839.000,,,,,0,1,,,M,,M,,*4D
$GPGSA,A,1,,,,,,,,,,,,,,,*1E
$GPGSV,3,1,10,21,85,103,,26,66,232,,16,56,295,,20,35,160,*78
$GPGSV,3,2,10,29,29,093,,27,24,286,,10,12,175,,05,08,032,43*76
$GPGSV,3,3,10,31,06,212,,15,01,095,*74
$GPRMC,071839.000,V,,,,,2.78,136.87,200100,3.3,E,N*27
```

3.1. Real GNSS spoofing attack

This incident was recorded in Black Sea in 22nd of June 2017 [2] and [3]. Several GPS receivers on a ship showed the same location on a land and evaluated it as true position signal (Figure 2).

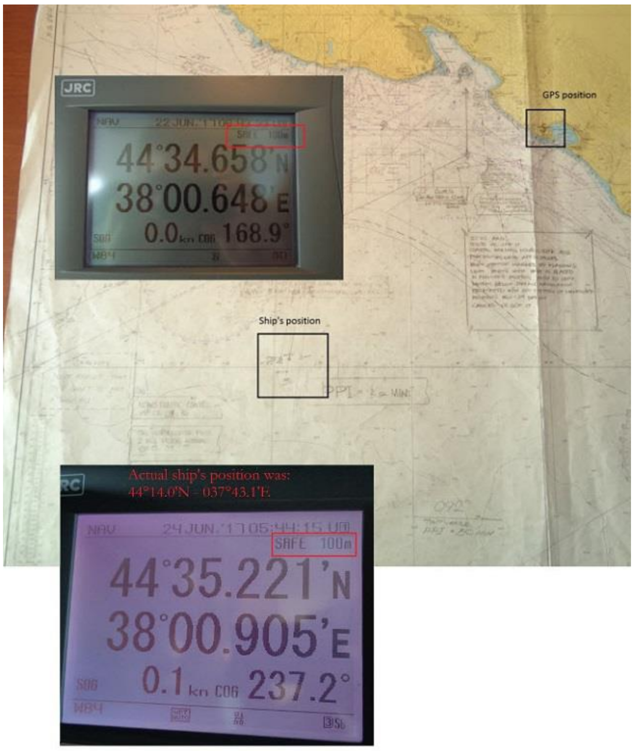

Figure 2. The example of real spoofing attack. [2]

4. Advanced spoofing detection

More complex receivers equipped with multiple antennas could apply spatial filtering for jamming or spoofing signal [4]. Relying only at GNSS signal from one point receiver the spoofing detection methods are exhausted. There are available other methods to detect abnormality in received GNSS signal leading to conclusion that the receiver is under spoofing attack:

- **Mathematical model of possible movement**. If there is movement outside the expected parameters, the received signal could be evaluated as falsified. Some NMEA sentences also contain velocity and direction information. Depending on vehicle type the behaviour scheme could be created. For ex-ample, train could not undergo acceleration exceeding some limits (ordinary train could not accelerate in 4 seconds to 100 km/h).
- **Data fusion** of GNSS with INS, GSM, barometric altimeter, odometer… This system calculates its position and speed. If a vehicle receives vertical climb from GNSS and altimeter data remains still, its suspicious. If a vehicle receives movement and INS doesn't undergo any acceleration, it's also suspicious.
- **Sensor network**. If sensor nodes are sharing its position between each other and they have another location, then it's possible to detect a spoofing attack. Example of such a sensor network is Waze application (Figure 3). Sensor nodes are sharing its position in real time. In the case of spoofing attack, all nodes in certain area will send the same location (what is impossible). Even jamming attack will be possible to detect, in the case that all nodes in area affected by jammer will lose their position simultaneously.

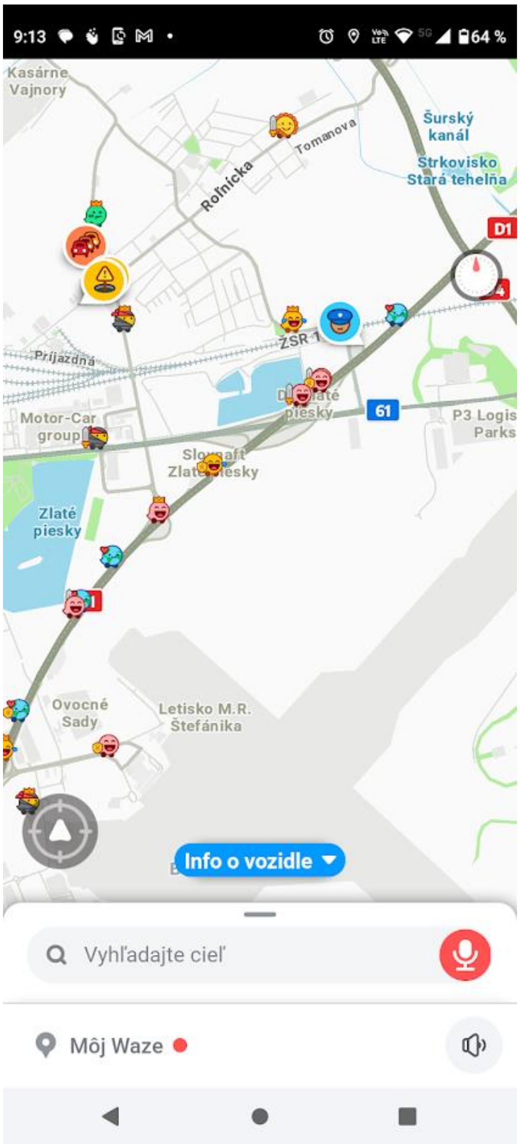

Figure 3. The example of sensor network application Waze

5. Conclusions

In conclusion, GNSS spoofing is a serious threat to the widespread use of GNSS technology. The effects of spoofing can be severe, causing accidents and errors in financial transactions and communication systems. However, there are several techniques that can be used to prevent GNSS spoofing, including signal authentication, multi-constellation receivers, and spatial filtering. By using these techniques, we can ensure the safety and reliability of GNSS technology in various applications.

ACKNOWLEDGEMENTS

"This publication was realized with support of Operational Program Integrated Infrastructure 2014 - 2020 of the project: Innovative Solutions for Propulsion, Power and Safety Components of Transport Vehicles, code ITMS 313011V334, co-financed by the European Regional Development Fund".

EUROPEAN UNION
European Regional Development Fund
OP Integrated Infrastructure 2014 – 2020

MINISTRY
OF TRANSPORT
AND CONSTRUCTION
OF THE SLOVAK REPUBLIC

REFERENCES

[1] Yousuf, S. Kadri, M. B. Sensor fusion of INS, odometer and GPS for robot localization. [online]. Malaysia : Bandar Hilir, 2016. pp 118 - 123. [cit. 2019-10-07] ISBN 978-1-5090-1181-0. URL: <https://ieeexplore.ieee.org/document/7920715> .

[2] Goward, D. Mass GPS Spoofing Attack in Black Sea? [online] 2017 [cit. 2019-10-07] URL <https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea>

[3] Jones, M. Spoofing in the Black Sea: What really happened? [online] 2017 [cit. 2019-10-07] URL <https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>

[4] Jones, M. Anti-jam technology: Demystifying the CRPA [online] 2017 [cit. 2019-10-07] URL: <https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/>

[5] Šimák, V. at al. GNSS vs. INS behavior and position data processing In: Technical computing Prague 2017 [elektronický zdroj] : sborník příspěvků 23. ročníku konference : Praha, November 8, 2017. - ISSN 2336-1662. - Prague: University of chemistry and technology, 2017. - ISBN 978-80-7592-002-7. - CD-ROM, [3] s.

[6] Aftatah, M. Lahrech, A. Abounada, A. Soulhi, A. GPS/INS/Odometer Data Fusion for Land Vehicle Localization in GPS Denied Environment In: Modern Applied Science; Vol. 11, No. 1; 2017 ISSN 1913-1844 E-ISSN 1913-1852 Published by Canadian Center of Science and Education, [online] 2017 [cit. 2019-10-08] URL: <https://pdfs.semanticscholar.org/4778/a2e85effdb4e0cf875b40e377efec0d94332.pdf>