XVI Jornadas de Ingeniería Telemática

JITEL 2023

La Salle – Universitat Ramon Llull

Actas de las XVI Jornadas
de Ingeniería Telemática
(JITEL 2023),
Barcelona (España),
8-10 de noviembre de 2023.

ISBN

Server-Side GNSS Spoofing Detection Challenges for Vehicle Tracking Applications

José Jesús Sánchez Gómez, Isaac Agudo.
Departamento de Lenguajes y Ciencias de la Computación,
Universidad de Málaga (UMA)
sanchezg@uma.es, isaac@lcc.uma.es

This paper focuses on the risks linked to the Global Navigation Satellite System (GNSS) and introduces a scenario involving a data-transmitting device connected to a cloud-based service. We explore potential attackers and the diverse attacks possible during the communication and data-processing stages of the scenario. Additionally, we categorize current detection methods based on the information they employ to detect spoofing attacks and discuss their limitations concerning Server-Side detection. Ultimately, we propose solutions and future lines of work to mitigate these problems.

***Keywords*—GNSS Spoofing, Location Spoofing, Server Verification, Security**

I. Introduction

Currently there are numerous satellite-based navigation systems that provide services to users. Although people commonly use the term GPS (Global Positioning System) to refer to all systems able to determine the location of a device, this usage is incorrect. GPS refers to the U.S. Global Positioning System, which was first developed by the United States Government in the 1970s [1]. The accurate term used to refer to the collection of systems to determine different location parameters is GNSS (Global Navigation Satellite System). This encompasses different systems, such as the U.S. GPS, the European Galileo System, the Russian GLONASS (GLObal NAvigation Satellite System) or the Chinese BDS (Beidou Navigation Satellite System), among others [2].

GNSS reception modules are commercially available for purchase. These modules come in a wide range of prices, and while more affordable options provide basic positioning and navigation functionalities, higher-end, more expensive modules offer enhanced features and greater accuracy. These modules can be integrated into various systems and applications, enabling a wide range of functionalities and being used for tasks such as obtaining accurate time synchronization or determining the precise location of the system itself. This location information can then be utilized by a variety of applications. For instance, in the case of vehicular navigation systems, the accurate positioning data obtained from these modules enables drivers to receive turn-by-turn directions, real-time traffic updates, and optimized route suggestions. Additionally, competitive applications like Strava use location information to allow users to track and analyze their performance in activities such as running or cycling, facilitating the comparison of results with others.

The widespread adoption of GNSS reception modules has led to an increasing number of companies using vehicle tracking for various purposes. For example, fleet management has significantly benefited from the integration of GNSS modules, not only in terms of real-time monitoring and control but also by enabling businesses to impose restrictions on vehicle usage. With the advanced capabilities of GNSS modules, companies can implement several policies and regulations, such as the enforcement of time-based restrictions or geofenced areas in order to restrict vehicle access to certain zones or regions. Insurance companies also leverage GNSS reception modules to offer pay-as-you-drive insurance programs. By tracking vehicles' location and driving behavior, insurers can assess risks more accurately and provide personalized plans. Safe driving habits can be rewarded with lower premiums, incentivizing responsible behavior on the road.

In 2021, the revenues of the GNSS market exceeded €200 billion. It is expected that by the next decade, GNSS-related revenues will reach €500 billion, with more than 10 billion GNSS devices in use [3]. The potential advantages gained from carrying out these attacks have motivated malicious actors to engage in GPS attack due to the relative ease with which such attacks can be executed.

The following section provides an overview of the architecture of a location-based service while also outlining the potential attackers to the system. Subsequent to this characterization, a range of possible attacks that can be carried out are addressed. Section III furnishes a comprehensive insight into various spoofing detection mechanisms, categorizing them based on the data used to detect an attack and addressing their limitations. Lastly, section IV presents a conclusion about the detection methods and briefly presents future lines of work.

II. SYSTEM TOPOLOGY AND SECURITY CONCERNS

The typical data flow in a cloud-based service using GNSS is as shown in Fig. 1. Satellites broadcast information to all potential receptors. Then, the receivers compute and send its location to the server in order to get some service, e.g. Weather information.

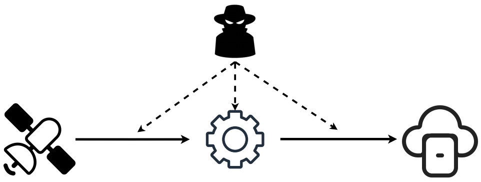

Fig. 1. Location-Based Architecture.

In this flow there are three critical steps:

- **GNSS signal**. The GNSS signal is broadcasted over the air. Since these signals are emitted without making use of any authentication method, these are vulnerable to spoofing attacks as described in the next subsection.
- **Vehicle processing.** The signal received from the satellites is processed by the in-vehicle device in order to determine the location of the vehicle. If the device is compromised, the computed location could be modified.
- **Server reception.** After computing its location, the device transmits it to the server. If this connection is not secure, the transmitted data being sent could be compromised.

Considering these steps, we can focus on the possible types of attacks depending on the attacker:

- **External.** An external attacker would have no access to the device itself. Consequently, attacks carried out by this type of attacker must target the GNSS signal received by the device.
- **Internal.** An internal attacker, e.g. the user of the device, would have physical access to the device, being able to act on all three steps described.

The next subsections outline various potential attacks depending on the attacker.

A. External malicious

The GNSS system makes use of different constellations of medium earth orbit satellites. Reception modules are capable to track satellites from different constellations, which means that different GNSS systems can be jointly used [2]. GNSS satellites make use of accurate atomic clocks to transmit signals to Earth. These signals are used by GNSS receivers to estimate the distance to the satellite by measuring the TOA (time of arrival) of the signal. In order to achieve that, both the satellites and the receiver clocks must be synchronized [4]. The exact position of each of the satellites of the GNSS system is included in the Ephemeris, a set of data periodically broadcasted by satellites or posted on Internet. These can be used by receivers in order to obtain information about the satellites that are in their line of sight. While the accuracy and availability of the system have significantly evolved since its inception, the implementation of publicly-available integrity methods is only beginning to take shape. GNSS systems offer different services, some being authenticated e.g. GPS PPS (Precise Positioning Service) or Galileo PRS (Public Regulated Service). However, the authenticated services are encrypted, being the access to these services limited to the military or authorized government personnel. The first public-authenticated GNSS service has been deployed by Galileo OSNMA (Galileo Open Service Navigation Message Authentication) and has just started this year (2023). The system uses the TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol to broadcast authentication data. Nevertheless, although this system solves the integrity problems of the GNSS system, at the moment there are few GNSS modules supporting this technology. The U.S. GPS system is also developing its own authentication system: Chimera.

GNSS satellites typically transmit signals at a power level of around 44 dBm. However, due to considerable distance between the satellites and the Earth's surface, which exceeds 20km, the power received at the Earth surface reaches approximately -130dBm considering a clear view of the sky [2]. The weak power of the received signal exposes the system to signal spoofing attacks, which can be easily executed using SDRs (Software-Defined Radios) or similar devices. For instance, Markgraf showcased at OsmoCon the utilization of a modified €5 USB to VGA card that was capable of executing such attacks [5]. This serves as evidence of the system's susceptibilities and emphasizes that performing these attacks does not necessarily require a significant budget. Additionally, there is well-documented Open-Source software available for generating fake GNSS messages [6].

Attacks against UAVs, boats and vehicular systems are well documented. Academics have demonstrated that it is possible to perform these kind of attacks [7]–[9]. In real situations, attackers were able to modify the estimated location of all cars in a motor show [10] or spoof the location of several boats in the black sea[11].

Although most of these attacks can be solved using signal authentication methods, it has been demonstrated that the system would still be vulnerable to relay attacks [12], which consist on capturing real traces in a location, in order to relay them to the victim receiver.

B. Internal

The user of the device containing the GNSS receiver module can also be regarded as an attacker. This attacker would benefit from the attack's possible consequences, such as overriding Geo-Fences or emulating driving behaviours. An internal attacker could launch an attack to the

GNSS signal, the same way as an external attacker would. An example of this situation could involve a user with a sealed device, unable to access it to alter its hardware or software. When an external attacker executes an attack on the GNSS signal, all of the devices in an area are affected, since the attack signal must cover a wide area to affect the attacked device. In contrast to this, an internal attacker would not need to affect other devices, since the target device would be close enough to emit the signal solely to itself.

If an internal attacker gains access to the device, they could modify the software of the device to manipulate the computed parameters or alter the data sent to the server. Additionally, this attacker could change the legitimate location data provider to a compromised one. For example, in the context of attacking the Pokemon Go application, it was common to utilize the Android developer API, which enables the emulation of the device's location. Similarly, data obtained from various sensors could be emulated or manipulated using similar techniques.

III. OVERVIEW OF SPOOFING DETECTION MECHANISMS

In the previous section, we described the scenario under examination within the automotive environment. This scenario encompasses two data flows intrinsic to providing the client location to the server. One of these flows pertains to the GNSS signals that the GNSS receiver obtains, while the other pertains one to the location data-sets that are sent to the server.

Various researchers have developed methods to detect spoofing attacks. We classify these detection methods in Fig. 2, based on the parameters and data used to detect GPS spoofing attacks. Despite the extensive documentation on these types of attacks, most of them consider an external attacker, who would focus on GNSS Signal Spoofing, whereby the signal broadcasted by the satellites is overridden by the signal transmitted by the attacker. Nonetheless, in our scenario, we also consider the possibility of an internal attacker who might target the data transmitted to the server instead of the GNSS signal.

Methods based only in GNSS use the received parameters from the GNSS receiver, such as the PDOP (position dilution of precision) or the physical characteristics of the received signal such as its SNR (signal-noise ratio) and power. These methods have been proven to work, obtaining a detection percentage of almost 99%, as described in [13]. Several implementations have been developed in the latest years, using ML (Machine Learning) and neural networks, evaluating the correlation and variation of the different parameters [14].

Despite these methods have been proved to work on the client side in most cases, its feasibility when deployed on the server side is not demonstrated. These would require the client to send the received GNSS traces and parameters to the server in order for it to verify them. Since we consider that the client is able to send illicit traces to the server, the traces could be generated by the client, emulating the correlations and expected variations of the parameters, in order for the algorithm running on the server-side to not detect the spoofing. In addition, despite these attacks have been proven to work in simple scenarios, attackers using multiple well-located antennas are able to bypass the security system.

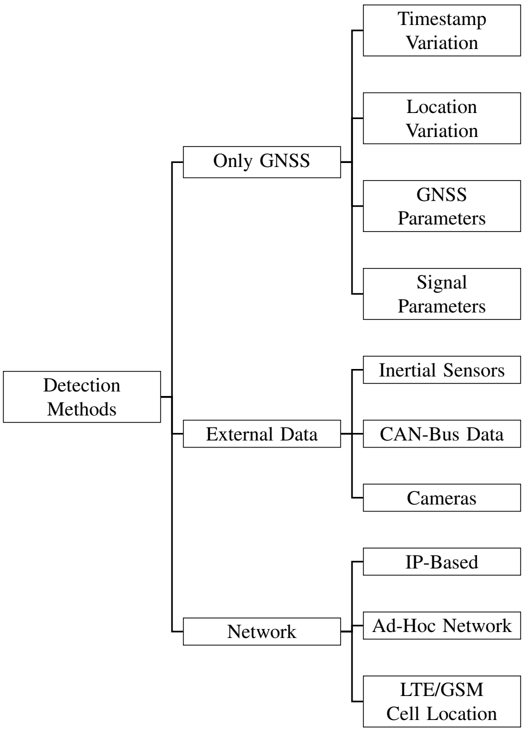

Fig. 2. Spoofing Detection Methods depending on the method used

Systems using external data, such as inertial sensors or obtained CAN-BUS data from the vehicle share a common objective: utilize this data to estimate the path followed by the vehicle, obtaining the possible turns, speed and distance traveled. Then, these estimates are compared to the data obtained using the GNSS module to verify its authenticity. Additionally, the integration of cameras allows to use ML for the same purposes. For example, captured frames can be compared with globally available images, allowing the server to verify the location. These methods induce higher complexity to the security system, thereby increasing the difficulty of a successful attack. As a way for the server to verify the location, these data-sets must be transmitted to the server. However, this leads to on a increase on the required bandwidth and processing power, in order for the server to run the mentioned verification methods. Despite that, determined attackers could attempt to generate synthetic sensor data or manipulated images in order to bypass the system.

Finally, we can consider systems that use network-obtained parameters in order to validate the location. Despite the diversity and limitations of the methods in this category, they are well-suited for a server-based verification. Some of these methods require the server use the IP of the client or the localization of the cell tower the device is connected to estimate the position of the client. However, the primary drawback of these methods lies in the range of possible locations, since each LTE cell tower typically covers a radius of up to 3km, while a GSM tower can theoretically cover up to 15km [15]. Additionally, methods employing ad-hoc network facilitate communication among clients, enabling the comparison of received signal characteristics to detect attackers. The received parameters can be sent to the server, enabling it to compare the parameters obtained from the different clients to identify a client which is sending discrepancies in order to the determine if the reported location is genuine. Moreover, Ad-hoc networks can be utilized to enable clients to verify the location of each others, being able to report compromised devices to the server. These network-based methods may require to be combined with any of the others mentioned above in order to present a feasible solution.

IV. CONCLUSIONS AND FUTURE WORK

Detecting Location Spoofing on the server side proposes some challenges to overcome.

As already mentioned in Section III, there are many works on how to prevent GNSS signal spoofing. We have also mentioned the risk of compromised on-board devices, either by an external attacker or the user itself in order to circumvent access restrictions in location-based services.

Some solutions in this area focus on sensor fusion technologies, but the emerging use of AI to generate deep fakes in other fields makes feasible the possibility of an attacker using these tools to generate artificial data from sensors that would seem real.

A promising line of work in this area is the use of HSM (Hardware Secure Module) to offload GNSS information processing from the GNSS signals to a trusted element in the car, avoiding being tampered by an attacker: for example, the DRACONAV project aims to develop a secure GNSS module able to detect attacks using multi-constellation, a secure MCU and motion sensors, being able to deliver signed data . A combination of such module with OSNMA or Chimera would be a nice approach to a feasible solution. Another interesting research topic is the use of complex ML algorithms to detect synthetic traces received on the server using previous training data. Additionally, the data received from different clients and the network can be analyzed to identify the discrepancies produced by an attack.

V. ACKNOWLEDGEMENTS

This work is part of the research project SECUREDGE (Security Services Platform for the Protection of Edge Scenarios), with PID2019-110565RB-I00, funded by AEI/10.13039/501100011033.

REFERENCES

[1] NASA. "Global positioning system history." T. May, Ed. (Oct. 27, 2012), [Online]. Available: https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html (visited on 05/17/2023).

[2] E. Kaplan and C. J. Hegarty, *Understanding GPS/GNSS : Principles and Applications, Third Edition, Principles and Applications, Third Edition*. Artech House Publishers, 2017.

[3] EUSPA: European Union Agency for the Space Programme, "Euspa eo and gnss market report," 2022. [Online]. Available: https://www.euspa.europa.eu/2022-market-report.

[4] J. L. B. Valero, N. G. Villen, and R. C. Romá, *GNSS GPS, Galileo, Glonass, Beidou. Fundamentos y métodos de posicionamiento*. Universitat Politècnica de València, 2019.

[5] S. Markgraf. "Osmo-fl2k." (2018), [Online]. Available: https://osmocom.org/projects/osmo-fl2k/wiki/Osmo-fl2k (visited on 05/18/2023).

[6] T. Ebinuma, *Gps-sdr-sim*, https://github.com/osqzss/gps-sdr-sim.

[7] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto, "Capture of UAVs Through GPS Spoofing Using Low-Cost SDR Platforms," *Wireless Personal Communications*, vol. 115, Dec. 2020.

[8] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *NAVIGATION*, vol. 64, no. 1, pp. 51–66, 2017.

[9] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[10] J. Torchinsky. "There's something very weird going on with cars' gps systems at the geneva motor show." (Mar. 8, 2019), [Online]. Available: https://jalopnik.com/theres-something-very-weird-going-on-with-cars-gps-syst-1833138071 (visited on 05/18/2023).

[11] H. Lied. "Gps freaking out? maybe you're too close to putin." (Sep. 18, 2017), [Online]. Available: https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/ (visited on 05/18/2023).

[12] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan, "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals," arXiv, Tech. Rep., Nov. 2022.

[13] T. T. Khoei, S. Ismail, and N. Kaabouch, "Dynamic selection techniques for detecting GPS spoofing attacks on UAVs," *Sensors*, vol. 22, no. 2, p. 662, Jan. 2022.

[14] M. Nayfeh, Y. Li, K. A. Shamaileh, V. Devabhaktuni, and N. Kaabouch, "Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification," *Computers' Security*, vol. 126, Mar. 2023.

[15] P. K. Sharma, D. Sharma, and A. Gupta, "Cell coverage area and link budget calculations in LTE system," *Indian Journal of Science and Technology*, vol. 9, no. S1, Dec. 2016.