A Forensic Analysis of GNSS Spoofing Attacks on Autonomous Vehicles

Tobias Reichel*, Mathias Gerstner†, Leo Schiller†, Andreas Attenberger*, Rudolf Hackenberg†, Klara Dolloš *
*Central Office for Information Technology in the Security Sector
Munich, Germany
e-mail: {tobias.reichel, | andreas.attenberger, | klara.dolos}@zitis.bund.de
†Dept. Informatics and Mathematics, OTH Regensburg
Regensburg, Germany
e-mail: {mathias.gerstner, | leo.schiller, | rudolf.hackenberg}@oth-regensburg.de

***Abstract*—Global Navigation Satellite Systems (GNSSs) are essential for modern technology, enabling precise geographic positioning in aviation, maritime shipping, and automotive systems. In the future, their role will be even more critical for autonomous vehicles, which rely on accurate localization for navigation and decision-making. However, the increasing connectivity of autonomous vehicles exposes them to cyber threats, including GNSS spoofing attacks, which manipulate location data to mislead onboard systems. As reliance on GNSS grows, so does the risk posed by spoofing attacks, making it a critical security concern. This paper describes GNSS spoofing attacks on autonomous vehicles, focusing on their detection both during and after an attack. Furthermore, we analyze data storage strategies to facilitate effective forensic analysis. We highlight the importance of position, signal, and camera data, which should be preserved to ensure a comprehensive forensic investigation. Finally, we suggest a simulation setup that enables studying which data could be used for a forensic investigation. Additionally, we examine established data frameworks and decide whether they are suitable for detecting GNSS spoofing attacks.**

Keywords-GNSS; autonomous driving; forensic; spoofing

I. Introduction

The ability to determine the geographical location of a device has become an indispensable technology in modern society, finding applications across a wide range of domains. From navigation to resource optimization, location-tracking systems have transformed how individuals and industries operate. Modern mobile phones, for example, enable users to effortlessly navigate unfamiliar locations, access detailed information about their surroundings, and plan their routes efficiently. This constant availability of location data has not only simplified everyday tasks, but has also revolutionized critical sectors such as transportation, logistics, and emergency response [1].

In the transportation industry, precise location tracking has proven to be a cornerstone of operational efficiency and safety. Maritime vessels can optimize their routes to minimize fuel consumption and travel time, while aircraft rely on accurate positioning systems to maintain safe distances between one another and ensure effective coordination in airspace [2]. For cars, location awareness has made traditional paper maps and co-driver navigation obsolete. Instead, Global Navigation Satellite System (GNSS), which encompasses multiple satellite navigation systems, including Global Positioning System (GPS), Galileo, Global Navigation Satellite System (GLONASS) and BeiDou, and related technologies have paved the way for advanced navigation systems, ultimately fostering the evolution of autonomous vehicles [3]. Modern cars increasingly incorporate features aligned with Society of Automotive Engineers (SAE) J3016 autonomy level 3 standards, where the vehicle can control driving in specific conditions, such as on highways. However, these systems still require the driver to take over when requested by the vehicle [4].

Although these advances have brought convenience and efficiency, they have also introduced critical vulnerabilities, particularly in the realm of GNSS-reliant systems. Attacks targeting GNSS receivers in autonomous or semi-autonomous vehicles can compromise their ability to accurately determine a location, potentially leading to catastrophic outcomes, such as collisions or operational failures [5]. These attacks are typically classified into two main categories: jamming and spoofing [6].

GNSS jamming and spoofing, while not new phenomena [7], remain significant threats due to their potential to exploit the dependency of modern systems on precise location data [8]. Jamming involves transmitting high-power interference signals across a wide frequency spectrum, including those used by navigation satellites, effectively disrupting the receiver's ability to interpret legitimate signals [9]. Spoofing, on the other hand, relies on generating and transmitting counterfeit satellite signals to deceive GNSS receivers into calculating an incorrect location. When executed skillfully, spoofing can mislead even sophisticated systems, causing them to accept falsified positions as accurate [10][11].

The motivations behind such attacks are diverse, ranging from malicious intent to sabotage and theft. A conceivable scenario involves targeting a high-profile individual, such as a politician on the way to an important event. By deploying a jamming device, attackers could immobilize the vehicle, potentially preventing the individual from reaching their destination on time. In addition, advances in vehicular technology, such as the Tire Pressure Monitor Sensors (TPMSs), provide attackers with tools to identify specific vehicles [12]. This capability allows for highly targeted attacks, where a jamming or spoofing signal is activated only when the intended vehicle

passes by.

The increasing reliance on GNSS systems in critical applications underscores the importance of addressing their vulnerabilities. Understanding the mechanisms and implications of GNSS jamming and spoofing is crucial to develop robust countermeasures that can safeguard the functionality and safety of location-dependent technologies. Additionally, forensic analysis is crucial in examining such attacks after the event, enabling a deeper understanding of methods, impact, and potential attribution to specific actors.

This paper is divided into four main sections. First, we discuss the state of the art and related work in Section II. The fundamentals of GNSS jamming and spoofing are introduced in Section III, outlining key attack methods and their impact on autonomous navigation. Next, we propose a simulation using CARLA [13] and Autoware© [14], replicating realistic spoofing scenarios to analyze attack dynamics and detection challenges in Section IV. Finally, we discuss what is the expected outcome for the simulated data in Section V and comparing it to some established data frameworks, aiming to reconstruct spoofing incidents and extract forensic markers. This methodology is designed to be transferable to real vehicle data in future research, strengthening GNSS-based navigation security.

II. Related Work

GNSS spoofing attacks pose a significant threat to autonomous vehicles, as they can manipulate positioning data and mislead navigation systems. Several of the following studies have addressed the detection and mitigation of such attacks. Bhatti and Humphreys demonstrated how GNSS spoofing could be used to gain hostile control over ships, effectively altering their navigation routes without immediate detection. Their study highlights the broader implications of GNSS deception across various transportation domains, including autonomous vehicles [15].

Further research has focused on spoofing detection methodologies. Dasgupta *et al.* [16] propose a prediction-based GNSS spoofing detection approach using Long Short-Term Memory (LSTM) models to identify anomalies in vehicle position estimates. Similarly, Liu *et al.* [17] assesses the impact of GNSS spoofing on integrated navigation systems by analyzing error covariance in Kalman filtering. A broader survey of spoofing techniques and countermeasures is provided in [18], categorizing current anti-spoofing technologies. In addition, hybrid sensor fusion methods, as demonstrated in [19], integrate GNSS with Inertial Measurement Units (IMUs) and vehicle odometry to detect inconsistencies caused by spoofing attempts.

Recent work [20] explores stealthy "slow-drift" GNSS spoofing attacks in urban environments, highlighting the difficulty of detection when position deviations occur gradually. To improve resilience, [21] presents a physics-based anomaly detection framework, GPS-Intrusion Detection System (IDS), which monitors vehicular behavior to identify spoofing attacks in real time. Furthermore, Radoš et al. provide a comprehensive survey of GNSS jamming and spoofing detection methods, discussing the latest advancements, including machine learning-based approaches for early detection [6].

There are many forensic frameworks [22]–[25] that describe which data should be stored and how it can be preserved for further investigations. Additionally, there are many forensic concepts that define which data is generally relevant for forensic purposes [26]–[28]. Most of them characterize location data as very relevant. In regard to conventional GNSS spoofing detection, in the frameworks for autonomous vehicles, comprehensive data is available to cross-validate the GNSS spoofing. According to Law Enforcement Agencies (LEA), the Event Data Recorder (EDR) plays a central role. The EDR typically has triggers from, for example, a crash or airbag sensor to persist the data. Usually, the last 5 seconds of vehicle speed, steering angle and others will be saved permanently [29]. Caused by the fact that this data is not sufficient for investigations in situations with automated driving functions [30], the conception of a Data Storage System for Automated Driving (DSSAD) is given, where, additionally, data from the driver assistant systems is saved [31]. Data used by an IDS to detect GNSS spoofing in real-time is also relevant for forensic analysis [21]. Due to the non-availability of some data in post-mortem analysis and the difficulty obtaining some data in vehicles, another approach for GNSS spoofing detection must be developed, or volatile data, such as signal strength of satellite signals, must be made available similar to the work in [32] where camera footage is implemented into the EDR.

III. Background and Fundamentals

For a forensic analysis, it is important to understand and document which data points were created and how they were received. In the case of GNSS, it is important to notice that the received signals and their properties depend on, e.g., topology, atmospheric conditions, reflections and it is not feasible to focus on just one of the factors and determine if an attack has occurred [33].

A. How GNSS Works: Principles and Mechanisms

Satellite-based positioning relies on trilateration, where a receiver calculates its location by measuring distances from navigation satellites [34]. Clock synchronization is crucial, as any deviation introduces errors, necessitating additional correction methods.

To determine an accurate three-dimensional position, at least four satellites are required. Three satellites provide an intersection of three spheres, which theoretically yields two possible solutions: one in space and one on Earth's surface. The fourth satellite is necessary to account for timing errors inherent in the receiver's internal clock, ensuring precise positioning by correcting discrepancies in signal travel time. Without this fourth satellite, accurate location determination would be significantly hindered due to clock inaccuracies.

The distance is derived from the travel time of the signal, which in turn is calculated by comparing the relevant send and

receive timestamps. This means that perfectly synchronized clocks are required to achieve the highest degree of precision. In practice, it is not unusual that the clocks are not synced as close to one another as desired. Therefore, a pseudo range is being introduced into the system, which has a geometric range and error term. This pseudo-range is based on the clock error and is simply added. This uncertainty complicates the equation in such a way that one needs at least four satellites -the fourth satellite for calculating the time error- to achieve sufficient position accuracy [34].

Determining one's precise location is important, but understanding the current speed of movement is equally crucial. This can be achieved through the Doppler shift, as the signal frequency is proportionally shifted in response to the speed of the receiver [35].

There exist multiple satellite systems. The first operational system, known as Navy Navigation Satellite System (NNSS) or Transit, was decommissioned in 1996. Some older systems, such as the Russian Tsikada from 1974, are still operational but are rarely used in modern society due to their limited positioning accuracy. The oldest widely used system is GPS, developed by the U.S. Army. It was later made accessible for civilian use, but without military-grade security features. Other systems include Global Navigation Satellite System (GLONASS), the Russian alternative to GPS; Galileo, the European navigation network; and BeiDou, which is a Chinese system. These systems operate as down link systems, meaning they use one-way communication from satellites to Earth. [33]

B. The Concept of GNSS Spoofing

Long believed impossible or hard to achieve, GNSS spoofing became reality in 2008, when Humphreys *et al.* demonstrated feasibility under laboratory conditions [36]. Since then, it has become more widespread and bigger attacks have been noticed.

GNSS spoofing is realized by transmitting counterfeit signals that are stronger than the signals from GNSS satellites. Thus, a receiver discards the true signals and computes an incorrect position and timing information. The process is illustrated in Figure 1. There are different possible attacks with a GNSS spoofer. In this paper, we copy the notation and names from sprint [37]. The first possible attack is meaconing, where original GNSS signals are replayed. The attack is successful if the receiver believes the replayed signal instead of the actual satellite signal. The second attack is the code carrier attack, where the GNSS signal is replicated, and the authentic signal is mimicked before adding power and changing the signal. The third attack is the navigation data attack, where the code carrier signal is left intact, but the navigation message will be faked and therefore a denial of service is achieved. The fourth attack is application-level spoofing, which is a man-in-the-middle attack. And the last attack is a multi-method attack, where any number of aforementioned attacks are combined to create a complex attack. Not each attack can be applied successfully on all systems. It depends on the technical capabilities and vulnerabilities of the receiver and vehicle.

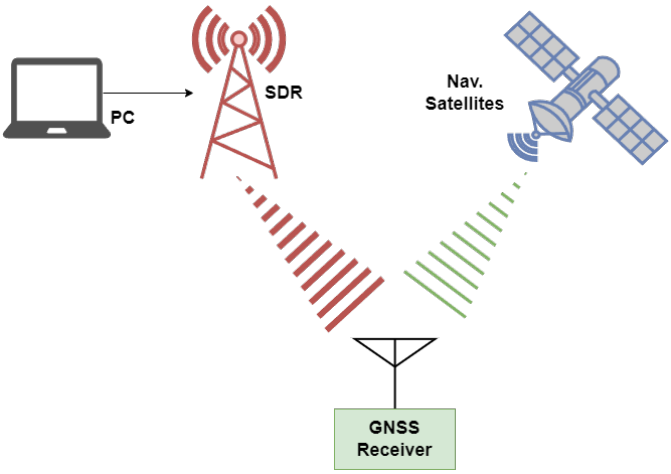

Figure 1. Illustration of GNSS spoofing: The SDR device overpowers satellite signals, deceiving the GNSS receiver with false location data.

It is often helpful to know which receiver is being used and in which state it is. The four distinct states, a receiver can be in, are cold start, warm start, hot or assisted start and reacquisition. While in the state of a cold start, the receiver just starts and has no information. With the warm start, the receiver has the approximated time and position. And with the hot start, the time and last position are known [38]. On the other hand, the reacquisition is not a usual start position, but indicates whether one or more signals from satellites are lost. This can occur naturally, for example in a tunnel, or unnaturally by jamming the frequency of GNSS.

C. Anti Spoofing Mechanisms

There are multiple methods to detect and avoid a GNSS spoofing signal [39] [40]. The simplest to implement is while the receiver has a warm or hot start, which involves obtaining a fix on satellite signals, to verify the location, speed of the vehicle and received timestamps for plausibility. There should be no major sudden jumps in each data type. Another simple solution is to check the authentication of the satellite message. This is not secure for currently deployed systems, as their structure is open knowledge. However, other GNSS systems, which aim to improve security, are in development [41]. By including features from the United States (US) military GPS, an encrypted authentication is being developed as an alternative way for positioning like cell ID.

As spoofing attacks pose significant risks to security-sensitive applications, the development of robust anti-spoofing mechanisms is crucial. Various anti-spoofing methods have recently been developed [6][42][43]. Signal processing-based techniques include correlation peak monitoring, which identifies distortions in the correlation function caused by spoofed signals, and power-based monitoring, which detects anomalies in the Carrier-to-Noise Ratio (C/N0) and Automatic Gain Control (AGC) values that often indicate spoofing attempts [6]. Another approach is to analyze the direction of the arriving signals, which differentiates spoofed signals from legitimate GNSS signals due to their different origins [44].

Data-driven approaches leverage Artificial Intelligence (AI) and Machine Learning (ML) techniques. Supervised learning algorithms classify authentic versus spoofed signals, while deep learning methods extract features from raw signal data for improved detection [45]. Radio Frequency Fingerprinting (RFF) can further enhance security by identifying unique signal characteristics such as phase noise and Doppler shifts[46].

Cryptographic and authentication techniques provide an additional layer of protection. Navigation Message Authentication (NMA) integrates digital signatures into GNSS signals, to ensure data integrity [41].

A promising direction for anti-spoofing involves integrating multiple detection methods. Hybrid approaches that combine signal processing, machine learning, and cryptographic authentication enhance robustness against evolving spoofing threats [6].

D. Digital Automotive Forensics

The digital automotive forensics is a part of the IT-forensics; especially the post-mortem analysis will be examined here. This means that live data is unavailable and only the data which is stored on a device may be used. The Federal Office for Information Security (BSI) gives a six point plan for a standard forensic investigation: strategic preparation, operational preparation, data collection, investigation, data analysis and documentation [26]. The European Network of Forensic Science Institutes (ENFSI) also describes first to validate and test the data with complex examinations [27]. The relevance of data depends on the specific use case. Those are typically given by the organization, which is interested in the investigation and in the technical implementation [47]. For Original Equipment Manufacturers (OEMs), it will often be sufficient to have some sort of hint for a technical conclusion. For the LEAs or insurance provider, where the evidence will be validated in court, it is much more important to have reliable data on the sequence of the event and especially information for attribution. For this, data that can be cross-validated is highly useful. Therefore, data that originates from just one source is considered circumstantial evidence. An example is the National Marine Electronics Association (NMEA) data, which cannot be validated using another data source. With regard to the case where all assistant driving data is acquired, it will be possible to detect the GNSS spoofing by cross-validation. There is a difference between the forensic analysis of stored data in the vehicle and real-time spoofing detection, such as cross-validation of the location provided by a cell tower and the GNSS sensor. Even with possible cross-validation methods, such as visual identification, computing everything in real-time would be challenging. However, in case of an incident, the data could be retrieved and validated.

This can lead to a significant overhead, especially if the dataset is large, distributed across multiple locations, difficult to obtain and unsorted. This is why a forensic framework is necessary. We will consider the data that would be provided by the established forensic framework AVGuard [24] and the legally mandatory or soon to be legally mandatory data storage systems EDR [29] and DSSAD [31]. The forensic framework AVGuard will save the following data: camera Frame per Second (FPS), Light Detection and Ranging (LiDAR)PointCount, GPSFreq, cars, pedestrians, trafficLights, roadsigns, laneDetectionConfidence, undefindedObjects, landmarks,Finite State Machine (FSM), acceleration, brake and steering angle. In the data point FSM it is for example recorded if the vehicle is turning or following a lane. The EDR will save the change in longitudinal velocity, the vehicle speed, the engine throttle, the service brake, the ignition cycle, the drivers safety belt status, the status of the frontal airbag warning lamp, the time of the frontal airbag deployment, if it is a multi event the number of the event and the time to the previous event [48]. The DSSAD is still at the conceptual stage. However it is likely that it will record the state of the Autonomous Driving (AD) system, the transition demand, the human driver take-overs, the minimum risk maneuvers and respective data timestamps [49].

IV. Outline of a GNSS Spoofing Attack Simulation

Since we aim to control all simulation parameters, we propose a simple scenario. For example, an autonomous vehicle is driving on a road with several intersections coming up. According to the users navigation settings, the vehicle is supposed to turn at the second intersection. However, due to a GNSS spoofing attack, the vehicle is being misled into turning early, at the first intersection, instead. Using a real vehicle and executing a successful spoofing attack is not feasible with reasonable resources, and we do not intend to develop a GNSS spoofing attack for state-of-the-art vehicles. Furthermore, for testing purposes of GNSS attacks, a license from the government is needed. Another possibility is conducting testing in a shielded environment. This is feasible but holds some complications, caused by the fact that there is interference with the real world. An alternative is testing with a simulator, which is much easier because the signals can be synchronized in a more straightforward manner [37]. Since our aim is to detect such an attack and conduct a successful forensic investigation, we simply need the resulting digital traces. For this, we expect that a simulation provides us with sufficient data quality for now. Ultimately, we plan to validate our developed workflow on real world data.

The scenario of an autonomous vehicle being misled to an earlier intersection could be simulated using a combination of CARLA [13] and Autoware© [14]. The simulated vehicle in CARLA should be spawned with a camera, two LiDARs sensors, one in the front and one in the back, a GNSS, IMU, lane invasion and a collision sensor. This sensor data will be sent by the Autoware CARLA bridge [50] to Autoware universe, where it can be processed and the vehicle in CARLA will be steered by the control commands of Autoware.

To simulate the signal strength of a GNSS signal, one can produce data in the NMEA 0183 standard [51][52] with help of gps-sdr-sim-realtime by GitHub user gym-487 [53] (Figure 2). This can be used to produce In-Phase and Quadrature (I/Q) data for the true position, called good signal, and the wrong position, called spoofed signal. For spoofing purposes, one has

to combine the good and the spoofed signal. This should be done, for example in gnu radio [54], in such way that the spoofed signal is substantially stronger than the good signal. One can reinterpret the signals by GNSS-SDR [55], which provides the full NMEA data. This could be used to see how many satellites are in sight and how fast the vehicle is.

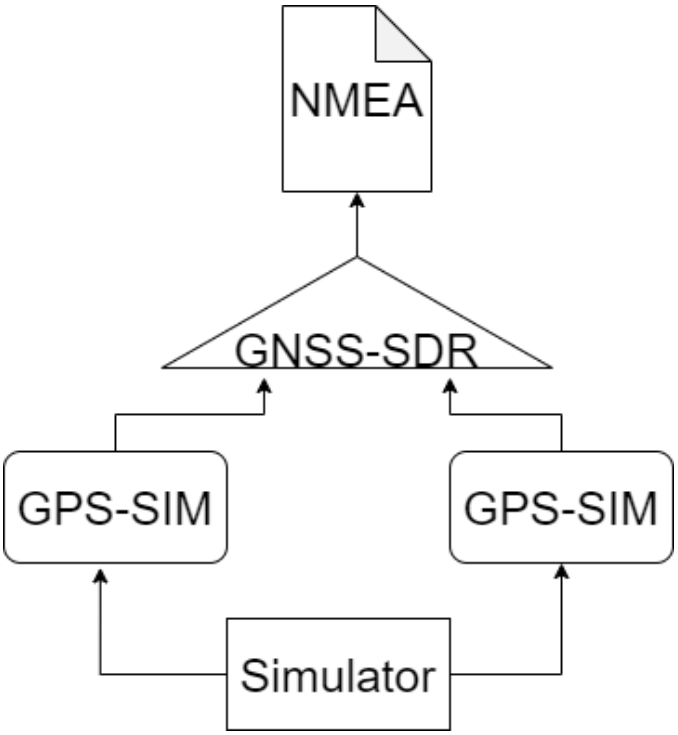

Figure 2. Simulation of GPS signal data

In order to understand the influence of external factors, this scenario should be simulated several times with varying input parameters. The simulation could vary in the following three different manners. The spoofed signal should be varied in the speed with which it is redirected from the original signal. The surroundings should change for easy and hard orientation, and the speed of the target vehicle should be changed.

These simulations will generate data in the vehicle that can be used for incident detection by the IDS as well as for forensics. Importantly, forensics will only be possible if the data is made available by an augmented EDR, DSSAD, the IDS or an elaborated forensic information system. In order to show the relevance of the full GNSS data, it is useful to imagine two different starting points:

1) One investigation with only the location information from the GNSS signal available and
2) another investigation with the full information of the GNSS signal such as signal strength, number of satellites etc.

The second case 2 has already been described in literature and in Subsection III-C. There are many plausibility checks, like changes in speed or C/N0 and AGC values, [6] which uncover such an attack. This data is required to be available for a post-mortem analysis as well, especially after an unclear event. For case 1 it is still possible to compute the GNSS-based speed and compare it to the data given by the speedometer of the vehicle. This plausibility check will likely not have the necessary strength since the GNSS-based speed is calculated on few locations only. Few data points of the GNSS signal and calculated speed will cause high uncertainty, e.g., in terms of wide confidence intervals preventing a test against the speedometer being positive.

To test this hypothesis, we want to generate data similar to the data displayed in the Figure 3. This data is calculated from the GNSS-based speed of the simulated vehicle under the assumption it is locked onto the spoofer, i.e., it ignores all data from the satellites. We can extract the speedometer data from CARLA and can generate the speed data by the real GNSS location and by the spoofed one. We validated this approach by implementing the GPS data creation. For this, we simply used two different GPS sensors, which drifted 10 meters apart over a timespan of 300 seconds. We set the first as the input for the true location and the second for the spoofed location and used the gps-sdr-sim-realtime setup as described and visualized in Figure 2.

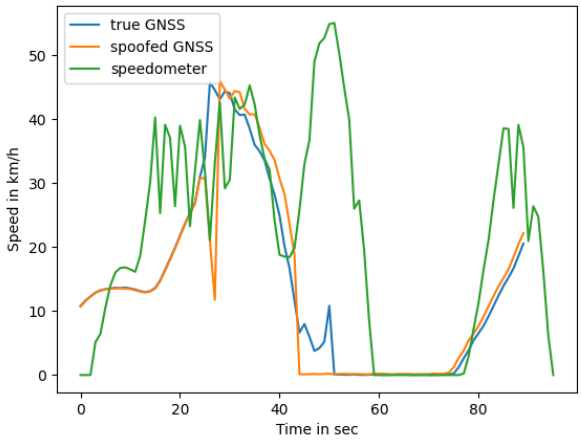

Figure 3. Velocity by GNSS and Speedometer

In this first exemplary simulation, one can see that the speed calculated based on the good GNSS signal also typically lacks behind the speed measured within the vehicle and does not reflect fast changes. And, for our study most interestingly, the spoofed and original GNSS-based speeds are apparently indistinguishable and therefore not viable for GNSS spoofing detection.

V. Discussion

We expect from our simulations that the speed given by GNSS will not significantly differ from the actual speed of the vehicle, and it is thereby not possible to detect GNSS spoofing without additional data. However, caused by the stronger signals that are necessary for GNSS spoofing, in the simulation data a higher number of stronger satellite signals

is expected. If the signal strength is recorded, this can aid in detecting an attack. Additionally, we want to consider other sources of information beyond GNSS signals for the in-situ detection as well as the post-mortem analysis of a GNSS spoofing attack. This allows for more elaborate plausibility checks. One option could be to identify street intersections using camera sensor data and AI. This could give a rough estimate of the location of the vehicle in a given street map.

In the currently established forensic frameworks of AVGuard [24] and the data recorders EDR [29], and DSSAD [31], different types of data are stored. AVGuard [24] will store enough data to have some possible ways to cross-validate GNSS signals. One could test if the acceleration, traffic light and roadsigns could be used for cross-validation. For GPS related data, only the GPS frequency is saved. We do not think any spoofing attack could be detected in that way. The frequency only depends on the band, i.e. one frequency of the GNSS signal. In the simulation, we focused on just the GPS L1 band, which is around 1575.42 MHz. This limitation is not an issue, because the bands are independent. In the future, this should still be tested.

The EDR [29] will only record data in the case of an emergency, i.e., when the airbag gets deployed. In regard to an IDS, like in [21], the data that can be retrieved, is constrained by what is saved. Typically, one wants at least the route data or the satellite data for detecting GNSS spoofing. In contrast, the EDR saves only the vehicle's speed as only parameter for GNSS spoofing detection indicated in [56]. Even if the vehicle crash is caused by a GNSS spoofing attack, in the data recorded by the EDR this would not be recognizable, because no route information or other data associated with GNSS is saved.

Similarly for the DSSAD, which is mandated by United Nations Economic Commission for Europe (UNECE)s United Nations (UN)-R157 [31], there will be data saved regarding the Advanced Driver Assistant Systems (ADASs). The proposal for a DSSAD is not completed yet, so we can only make assumptions about which data might be stored. Interesting data for our use case could be the state of the autonomous driving mode and if the vehicle detected some malicious attacker, which requires the vehicle driver to take over. Both the legally and soon to be legally mandatory data recorders, EDR and DSSAD, are only going to save data in a 5 to 30 seconds interval. Additionally, no data that is typically used in GNSS spoofing detections is recorded.

Looking at the data storage systems, we see the importance of reliable data. Not all data points are interesting, but in the case of autonomous vehicles, attacks like GNSS spoofing should be easily detectable. In the current state this is not the case and one should record more data associated with GNSS. This could include NMEA or other localization data. In the real world there are many ways to identify the location of a vehicle, for example through cell tower ID [57], 3D maps [58] or object detection through Radio Detection and Ranging (Radar) and LiDAR [59].

To conclude which data points are relevant, we will set up a simulation as described above. The simulation will generate data that enables us to analyze the impact of a GNSS spoofing attack on an autonomous vehicle. By evaluating the results, we aim to determine whether our hypothesis is correct, i.e. that current data storage in EDR and DSSAD is insufficient. The findings will help assess whether additional data points are necessary to improve both forensic analysis of such attacks and the security measures used against them.

VI. Conclusion

By evaluating the EDR, DSSAD and AVGuard, we concluded that they will not provide enough data to identify GNSS spoofing attacks. Subsequently, a larger forensic framework needs to be defined, in which sensor data, like images or point clouds going to be saved for a specific period. To determine which data is relevant, we proposed a simulation setup. We plan to expand on this and subsequently publish an analysis of the simulated data. o validate the data from the simulation, we plan to conduct real-world driving tests using a GNSS receiver. These tests will include baseline measurements as well as scenarios where the receiver is intentionally disrupted. The disruptions will be introduced by covering the antenna with metal objects or injecting corrupt signals via a wire to simulate jamming and spoofing. We expect these tests to provide deeper insights into the specific navigation parameters relevant to forensic analysis. We have looked at a very specific case, where the GNSS spoofing worked every time. This should be improved in two different ways. First, the case needs to be closer to the real world, which is more complex and presents further challenges that need to be addressed. For further testing, hardware that more closely replicates real-world complexities should be deployed. On the other hand, there should be more disruptive factors in the simulation like different vehicles, more visible input to clarify the position and different maps, where the angle of the intersections do not line up perfectly. Additionally, it would be interesting to investigate anti spoofing mechanisms. If spoofing is prevented, it would still be possible to detect whether the vehicle has been attacked.

Acknowledgment

The authors would like to thank Conrad Meyer and Dr. Tabea Rosenkranz from the Central Office for Information Technology in the Security Sector (ZITiS). This work was supported by the project 'Digital Forensics in IT Systems (DiForIT)', funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK).

References

[1] Fortune Business Insights, "Globaler Markt für Navigationssatellitensysteme (GNSS) [Global Market for Navigation Satellite Systems (GNSS)]", Jan. 27, 2025, [Online]. Available: https://www.fortunebusinessinsights.com/de/globaler-markt-f-r-navigationssatellitensysteme-gnss-103433 (visited on 02/14/2025).

[2] D. Verma, B. Singh, and F. Zahidi, "Management of GPS Tracking Systems in Transportation", in Mar. 2024, pp. 251–263, ISBN: 978-981-97-0514-6. DOI: 10.1007/978-981-97-0515-3_11.

[3] M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds., *Autonomous Driving*, en. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, ISBN: 978-3-662-48845-4 978-3-662-48847-8. DOI: 10.1007/978-3-662-48847-8.

[4] SAE, "SAE Levels of Driving Automation Refined for Clarity and International Audience", 2021, [Online]. Available: https://www.sae.org/site/blog/sae-j3016-update (visited on 01/28/2025).

[5] M. Shabbir, M. Kamal, Z. Ullah, and M. M. Khan, "Securing Autonomous Vehicles Against GPS Spoofing Attacks: A Deep Learning Approach", *IEEE Access*, vol. 11, pp. 105 513–105 526, 2023. DOI: 10.1109/ACCESS.2023.3319514.

[6] K. Rado, M. Brki, and D. Begui, "Recent Advances on Jamming and Spoofing Detection in GNSS", *Sensors*, vol. 24, no. 13, p. 4210, Jun. 2024, ISSN: 1424-8220. DOI: 10.3390/s24134210.

[7] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks", in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, Y. Chen, G. Danezis, and V. Shmatikov, Eds., New York, NY, USA: ACM, 2011, pp. 75–86, ISBN: 978-1-4503-0948-6. DOI: 10.1145/2046707.2046719.

[8] "GNSS Jamming and Spoofing Are a Daily Occurrence", [Online]. Available: https://www.eetimes.eu/gnss-jamming-and-spoofing-are-a-daily-occurrence/ (visited on 02/21/2025).

[9] T. Morong, P. Puricer, and P. Ková, "Study of the GNSS Jamming in Real Environment", *International Journal of Electronics and Telecommunications*, vol. 65, pp. 65–70, Feb. 2019. DOI: 10.24425/ijet.2019.126284.

[10] M. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, "Generalized Likelihood Ratio Test for GNSS Spoofing Detection in Devices With IMU", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3496–3509, 2021. DOI: 10.1109/TIFS.2021.3083414.

[11] S. Islam *et al.*, "Impact Analysis of Spoofing on Different-grade GNSS Receivers", in *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2023, pp. 492–499. DOI: 10.1109/PLANS53410.2023.10139934.

[12] C. Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester*. San Francisco: No Starch Press, 2016, ISBN: 978-1-59327-770-3.

[13] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, *Carla: An Open Urban Driving Simulator*, 2017. arXiv: 1711.03938.

[14] A. Foundation, "Autoware: Open-Source Software for Autonomous Driving", [Online]. Available: https://github.com/autowarefoundation/autoware (visited on 01/31/2025).

[15] J. Bhatti and E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection", pp. 51–66, 2016. DOI: https://doi.org/10.1002/navi.183.

[16] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "Prediction-Based GNSS Spoofing Attack Detection for Autonomous Vehicles", 2020, Publisher: arXiv. DOI: 10.48550/ARXIV.2010.11722.

[17] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System", *Sensors*, vol. 18, no. 5, p. 1433, May 2018, ISSN: 1424-8220. DOI: 10.3390/s18051433.

[18] L. Meng, L. Yang, W. Yang, and L. Zhang, "A Survey of GNSS Spoofing and Anti-Spoofing Technology", *Remote Sensing*, vol. 14, no. 19, p. 4826, 2022, ISSN: 2072-4292. DOI: 10.3390/rs14194826.

[19] A. Broumandan and G. Lachapelle, "Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation", *Sensors*, vol. 18, no. 5, p. 1305, Apr. 2018, ISSN: 1424-8220. DOI: 10.3390/s18051305.

[20] S. Dasgupta, A. Ahmed, M. Rahman, and T. N. Bandi, *Unveiling the Stealthy Threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling the Resilience*, Version Number: 1, 2024. DOI: 10.48550/ARXIV.2401.01394.

[21] M. M. Abrar *et al.*, *GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous Vehicles*, Version Number: 2, 2024. DOI: 10.48550/ARXIV.2405.08359.

[22] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles", *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50–57, 2018, ISSN: 0163-6804. DOI: 10.1109/MCOM.2018.1800137.

[23] S. Lee, W. Choi, H. J. Jo, and D. H. Lee, "T-Box: A Forensics-Enabled Trusted Automotive Data Recording Method", *IEEE access : practical innovations, open solutions*, vol. 7, pp. 49 738–49 755, 2019. DOI: 10.1109/ACCESS.2019.2910865.

[24] M. A. Hoque and R. Hasan, "AVGuard: A Forensic Investigation Framework for Autonomous Vehicles", in *ICC 2021 - IEEE International Conference on Communications*, Piscataway, NJ: IEEE, 2021, pp. 1–6, ISBN: 978-1-7281-7122-7. DOI: 10.1109/ICC42927.2021.9500652.

[25] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV)", in *2017 IEEE 2nd International Congress on Internet of Things*, M. Parashar, Ed., Piscataway, NJ: IEEE, 2017, pp. 25–32, ISBN: 978-1-5386-2011-3. DOI: 10.1109/IEEE.ICIOT.2017.13.

[26] Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security], *Leitfaden IT-Forensik [Guide to IT-Forensics]*, 2011.

[27] ENFSI, *Best Practice Manual for the Forensic Examination of Digital Technology*, 2015.

[28] L. Ahmeti, K. Dolos, C. Meyer, A. Attenberger, and R. Hackenberg, "A Forensic Approach to Handle Autonomous Transportation Incidents within Gaia-X", *CLOUD COMPUTING 2024*, p. 51, 2024.

[29] Event Data Recorder Committee, "Event Data Recorder", DOI: 10.4271/J1698_202303.

[30] K. Böhm, T. Kubjatko, D. Paula, and H.-G. Schweiger, "New Developments on EDR (Event Data Recorder) for Automated Vehicles", *Open Engineering*, vol. 10, pp. 140–146, Mar. 2020. DOI: 10.1515/eng-2020-0007.

[31] "UN Regulation No 157 Uniform Provisions Concerning the Approval of Vehicles with Regards to Automated Lane Keeping Systems", *Official Journal L 82*, no. 82, pp. 75–137, 2021.

[32] K. Böhm, T. Kubjatko, D. Paula, and H.-G. Schweiger, "New Developments on EDR (Event Data Recorder) for Automated Vehicles", *Open Engineering*, vol. 10, no. 1, pp. 140–146, 2020. DOI: doi:10.1515/eng-2020-0007.

[33] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS: Global Navigation Satellite Systems - GPS, Glonass, Galileo, and More*. Wien and NewYork: Springer, 2008, ISBN: 978-3-211-73012-6. DOI: 10.1007/978-3-211-73017-1.

[34] Y. S. Simamora, N. F. Rachmach, M. Y. Rizqon, K. A. Suseno, and M. N. Hilmi, "Revisiting Trilateration Method Based on Time-of-Flight Measurements for Navigation", *Jurnal Riset Multidisiplin dan Inovasi Teknologi*, vol. 2, no. 01, pp. 207–214, Dec. 2023, ISSN: 3024-8582, 3024-9546. DOI: 10.59653/jimat.v2i01.432.

[35] A. Angrisano, G. Cappello, S. Gaglione, and C. Gioia, "Velocity Estimation Using Time-Differenced Carrier Phase and Doppler Shift with Different Grades of Devices: From Smartphones to Professional Receivers", *Algorithms*, vol. 17, no. 1, 2024, ISSN: 1999-4893. DOI: 10.3390/a17010002.

[36] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer", in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314–2325.

[37] spirent, "GNSS Signal Spoofing: How to Evaluate the Risks to Safety-Critical and Liability-Critical Systems", *DWP0014 Issue 1-00*, 2020.

[38] R. Goudenove, *Understanding GNSS Receiver Start Modes: Cold, Warm, Hot, Direct*, Nov. 2024.

[39] D.-K. Lee *et al.*, "Detection of GNSS Spoofing using NMEA Messages", in *Proceedings of the European Navigation Conference (ENC)*, Dresden, Germany, 2020, pp. 1–10.

[40] Y.-S. Lee, J. S. Yeom, and B. C. Jung, "A Novel Array Antenna-Based GNSS Spoofing Detection and Mitigation Technique", in *Proceedings of the 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 8, 2023, pp. 489–492.

[41] I. Fernández-Hernández *et al.*, "A Navigation Message Authentication Proposal for the Galileo Open Service", *NAVIGATION*, vol. 63, no. 1, pp. 85–102, 2016. DOI: https://doi.org/10.1002/navi.125.

[42] L. Meng, L. Yang, W. Yang, and L. Zhang, "A Survey of GNSS Spoofing and Anti-Spoofing Technology", en, *Remote Sens. (Basel)*, vol. 14, no. 19, p. 4826, Sep. 2022.

[43] P. Papadimitratos and A. Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures", *IEEE MILCOM*,

[44] M. C. Esswein and M. L. Psiaki, "Classification of Authentic and Spoofed GNSS Signals Using a Calibrated Antenna Array", en, *Navigation (Wash.)*, vol. 72, no. 1, navi.675, Jan. 2025.

[45] P. Borhani-Darian, H. Li, P. Wu, and P. Closas, "Detecting GNSS Spoofing Using Deep Learning", en, *EURASIP J. Adv. Signal Process.*, vol. 2024, no. 1, Jan. 2024.

[46] R. Morales-Ferre, W. Wang, A. Sanz-Abia, and E.-S. Lohan, "7Identifying GNSS Signals Based on Their Radio Frequency (RF) Features-A Dataset with GNSS Raw Signals Based on Roof Antennas and Spectracom Generator", *Data*, vol. 2020,

[47] A. Cockburn, *Writing Effective Use Cases* (The Agile Software Development Series), 24. print. Boston: Addison-Wesley, 2012, 270 pp., ISBN: 978-0-201-70225-5.

[48] "EVENT DATA RECORDERS", 2006, [Online]. Available: https://www.ecfr.gov/current/title-49/part-563 (visited on 02/14/2025).

[49] "Data Storage System for Automated Driving", 2019, [Online]. Available: https://wiki.unece.org/download/attachments/87621710/EDR-DSSAD-01-08%20%28CLEPA-OICA%29%20DSSAD%20first%20draft%20for%20discussion%20based%20on%20GRVA-02-21.pdf?api=v2 (visited on 02/14/2025).

[50] G. Kaljavesi, T. Kerbl, T. Betz, K. Mitkovskii, and F. Diermeyer, "Carla-Autoware-Bridge: Facilitating Autonomous Driving Research with a Unified Framework for Simulation and Module Development", 2024.

[51] N. M. E. Association, "NMEA 0183 Version 4.10", 2013, [Online]. Available: https://www.nmea.org/nmea-0183.html (visited on 03/12/2025).

[52] G. Baddeley, "GPS - NMEA Sentence Information", 2001, [Online]. Available: https://aprs.gids.nl/nmea/ (visited on 01/28/2025).

[53] T. Ebinuma, *Gps-sdr-sim-realtime*, GitHub-Repository, 2017.

[54] G. R. Project, "Gnu Radio", [Online]. Available: https://www.gnuradio.org (visited on 01/29/2025).

[55] C. Fernandez-Prades, C. Aviles, L. Estove, J. Arribas, and P. Closas, "Design Patterns for GNSS Software Receivers", in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Netherlands: IEEE, Dec. 2010, pp. 1–8, ISBN: 978-1-4244-8740-0. DOI: 10.1109/NAVITEC.2010.5707981.

[56] Electronic Code of Federal Regulations (eCFR), "Event Data Recorders", 2025, [Online]. Available: https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-563 (visited on 01/29/2025).

[57] S. Saleh, A. S. El-Wakeel, S. Sorour, and A. Noureldin, "Evaluation of 5G Cell Densification for Autonomous Vehicles Positioning in Urban Settings", in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2021, pp. 1–6. DOI: 10.1109/ICCSPA49915.2021.9385733.

[58] A. Khoche, M. K. Wozniak, D. Duberg, and P. Jensfelt, "Semantic 3D Grid Maps for Autonomous Driving", in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, 2022, pp. 2681–2688. DOI: 10.1109/ITSC55140.2022.9922537.

[59] J. Koci, N. Jovii, and V. Drndarevi, "Sensors and Sensor Fusion in Autonomous Vehicles", in *2018 26th Telecommunications Forum (FOR)*, Nov. 2018, pp. 420–425. DOI: 10.1109/FOR.2018.8612054.