PNT Cyber Resilience: a Lab2Live Observer Based Approach

Report 1

GNSS Resilience and Identified Vulnerabilities

Elijah Adegoke, Matthew Bradbury, Erik Kampert,
Matthew Higgins, Tim Watson, Paul Jennings,
Colin Ford, Guy Buesnel and Steve Hickling

April 2020

WMG
THE UNIVERSITY OF WARWICK

spirent™
Promise. Assured.

Research Undertaken By

Research Supported By

Research Funded By

Cite this document as:

E. Adegoke, M. Bradbury, E. Kampert, M. Higgins, T. Watson, P. Jennings, C. Ford, G. Buesnel, and S. Hickling. PNT Cyber Resilience: a Lab2Live Observer Based Approach, Report 1: GNSS Resilience and Identified Vulnerabilities. Technical Report 1, University of Warwick, Coventry, UK, April 2020. Version 1.0

Executive Summary

The use of global navigation satellite systems (GNSS) such as GPS and Galileo are vital sources of positioning, navigation and timing (PNT) information for vehicles. This information is of critical importance for connected autonomous vehicles (CAVs) due to their dependence on this information for localisation, route planning and situational awareness. A downside to solely relying on GNSS for PNT is that the signal strength arriving from navigation satellites in space is weak and currently there is no authentication included in the civilian GNSS adopted in the automotive industry. This means that cyber-attacks against the GNSS signal via jamming or spoofing are attractive to adversaries due to the potentially high impact they can achieve.

This report reviews the vulnerabilities of GNSS services for CAVs (a summary is shown in Figure 1), as well as detection and mitigating techniques, summarises the opinions on PNT cyber testing sourced from a select group of experts, and finishes with a description of the associated lab-based and real-world feasibility study and proposed research methodology.

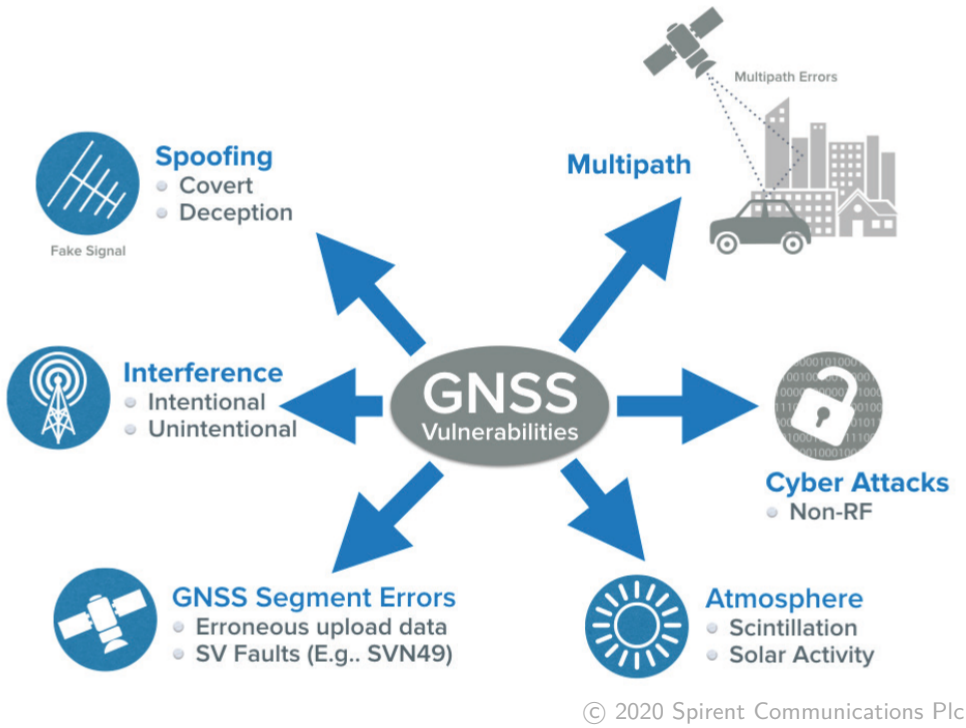


Figure 1: Range of typical GNSS vulnerabilities

Aim

The aim of this report is to identify the methods to create and test cyber-physical and software architectures, with a specific focus on CAV PNT systems. As will be explained in detail, the ideal PNT cyber resilience testing method for CAVs is based on a Lab2Live approach, spanning the full test continuum, from simulation to emulation, to tests on intelligent vehicles inside a dedicated lab, to real-world environment testing on autonomously-driving vehicles.

Lessons Learnt

Our literature review supports the broad classification of threats to CAV's GNSS receivers into the categories jamming and spoofing, where jamming denies access to GNSS-provided PNT information and spoofing presents incorrect and altered PNT information. Jamming is often easier to perform and detect compared to spoofing, but can be harder to mitigate. Amongst the various aims for spoofing attacks are: providing an incorrect position to a receiver, providing an incorrect time to the receiver, altering route planning decisions, and maliciously crafting data contents to attack the receiver's software. These attacks can be performed using commercially available devices, so it is important that PNT and CAV manufacturers, as well as CAM service providers utilise a combination of techniques to detect and mitigate these threats.

- Vehicles and the infrastructure they interact with are dependent on GNSS to supply positioning, navigation and timing information.
- Vehicles using GNSS for PNT are vulnerable to jamming, spoofing and software attacks.
- Actual attacks have been observed along these attack vectors for a variety of motivations (e.g., privacy, financial gain, terrorism, geopolitics and accidental).
- Fast pace of technology evolution means adversaries gain new capabilities quickly. An example of this are software defined radios (SDRs), which are comparatively cheap devices that facilitate performing RF transmissions, such as GNSS spoofing.

Detecting jamming attacks can be fairly straightforward as the receiver loses its GNSS fix. Spoofing detection can be more difficult to detect if the threat actor has the required technical knowledge and is in close proximity to the target receiver. It is thus essential that GNSS manufacturers continue to invest in joint jamming and spoofing detection mechanisms for GNSS chipsets. With respect to CAM service providers, an overlay detection layer can also be included in the system design for increased robustness of autonomous vehicles. Although both theory- and practice-focused literature exists on developing mitigations for attacks against any PNT system, there is no individual panacea. Hence, a combination of mitigation techniques should be applied, developed such that their interaction results in correct functioning of the PNT system. A deeper understanding of the practical ability for these attack-withstanding techniques is required, necessitating testing in lab-based and real-world environments, in which the capabilities of adversaries can be replicated.

Detection

- Jamming and spoofing can be detected using a wide range of techniques. Most of them are based on detection theory or hypothesis testing of measured observables or parameters available at the PNT device's level.
- Detection of jamming is the easier task, as spoofing attacks can be subtle and *indirect*. An example of an indirect attack can be a spoofing or software attack directed at the navigation service, whereby a preferred route is spoofed with excessive vehicular traffic.
- Whereas different techniques exist, PNT systems in CAVs need to adopt the combination of multiple techniques for robust threat detection.

Mitigation

- Mitigating techniques are generally based on adopting multiple independent positioning methods or algorithms.

- GNSSs including authentication information (e.g., via digital signatures or message authentication codes (MAC)) mitigate some spoofing threats, but it is not a panacea.
- For any given countermeasure(s), the sensor fusion framework in CAVs should be able to exclude or de-weight faulty measurement observables.

Community Experience

The acquired knowledge and conclusions drawn from the literature review are supported by the interviewed range of independent, GNSS and automotive cyber-security experts. All participants highlighted that jamming, spoofing and timing attacks are practical for an attacker to perform and can lead to severe impacts on a CAV. Participants with an automotive and PNT expertise supported their opinion with personal observations of the impact of attacks, and those with a cyber-security expertise highlighted the need for facilities to perform the testing. The latter experts also raised the importance of the context in which a CAV system operates, in determining an attacker's motivations and attack techniques. Amongst others, further consensus exists on dealing with threats to CAV PNT cyber-security as a high priority matter, the need to develop a common and consistent methodology for assessing PNT cyber-security risks, and a need to consider the impact of sensor fusion on testing attacks and developing mitigations. Moreover, it was stressed that the responsible disclosure of incidents and discovered PNT vulnerabilities is essential in the commercial sector, especially for safety and liability-critical applications such as CAV. In addition, a potential risk was seen in manufacturers expecting a certain level of performance from the devices they procure, and thus do not test them for resilience and robustness themselves. Hence, there is room for greater co-ordination/co-operation between agencies and industry. Reflecting the range of opinions given by all survey participants, if Zenzic could lead and accommodate a future public round table involving CAV PNT system cyber-security stakeholders from industry, government, academia, regulators and institutes, this would be very beneficial to all parties, also addressing their differences in focus and motivate the need for further collaborations between them. Further detailed specifications for CAV PNT testbeds and recommendations based on the outcomes of these interviews are made in Report 2 [2].

- Attacks focusing on jamming, spoofing and timing are all credible with some experts having observed these attacks in-person.
- Which threat to focus resources on developing mitigations depends, on the context in which a vehicle will be attacked.
- Other PNT sources need to be fused with GNSS to mitigate attacks on either type of sensor.
- There is a need to monitor systems for threats and responsibly disclose these incidents.
- Mitigations need to consider the complexity of a CAV being part of a system-of-systems due to interactions with other vehicles, road-side infrastructure and other services.

Testing

The practical feasibility study that has been carried out in the course of this project follows WMG's Intelligent Vehicles research team's view on achieving CAV adoption through the learning from a continuum of simulation, testing, trials, and early deployment. Computer-based simulations provide a first input on parameters and their ranges of interest, as well as hard- and software requirements for physical experiments on the device or vehicle of interest. Lab-based

work in a closed environment supports the control of most external parameters, allowing for high reproducibility and potential programmable repeatability of tests. Moreover, a lab provides a safe environment in which controlled scenarios can be investigated, in particular the corner-case scenarios that are unpractical or impossible to carry out in the real-world. Finally, live tests and measurements are required for guaranteeing a device's level of operation under real-world conditions, whilst experiencing real noise and interference for all sensors that interact with the device and might be affected by them. Figure 2 shows researchers performing experiments with two different pieces of equipment to test jamming and spoofing attacks.

© 2020 WMG

(a) Mobile jamming set-up

© 2020 WMG

(b) Mobile spoofing set-up

Figure 2: Researchers preparing the equipment for live, real-world tests at Wellesbourne Campus

Our lab-based jamming and spoofing tests on various GNSS receivers informed us about the model-dependent, purpose-specific metric sensitivities. This fed into the development of model-independent, black box research methodologies, as would be used in a cyber-physical testing facility when certain detailed component-level information might neither be disclosed nor otherwise available. Typical investigated parameters during the attacks on the GNSS receiver or complete CAV system were the signal power of the in-view satellite vehicles (SV), the number of visible SVs, and the time-to-first-fix (TTFF) when signals were intentionally or partly interrupted. Moreover, using a state-of-the-art PNT Attack Emulator (PNTAE), lab-based spoofing tests that involved the generation of corrupt GNSS data, such as SV clock bias and health, and tests that generated either static or dynamic false positions were successfully carried out. The research methodology was then adjusted to align with real-world, live-sky conditions, in which a black box CAV system was attacked in a dedicated testing area. Generalising the live results, led us to conclude that real-world testing on a CAV-system can result in distinctively different observations than those made in a lab environment. This can be understood through the influence of the GNSS implementation in the CAV's operating system and potential sensor fusion algorithms, e.g. including the inertial navigation system; cameras and radar, on the associated decision-making processes.

Because of the versatility of PNT attack scenarios, for both the lab-based and live testing labour-intense work needs to be carried out in order to scan the full parameter space of interest, in order to provide a reliable and detailed conclusion on a GNSS receiver's or CAV's PNT cyber resilience, which was beyond the scope of this project. Most importantly, **this project has shown that the chosen Lab2Live methodological approach, starting with lab-based testing on isolated GNSS-receivers and finishing with real-world tests on a black box CAV, provides the complimentary and comprehensive results that are required to evaluate a system's PNT cyber resilience**.

Acknowledgements

This research was supported by Innovate UK [Grant No. 133896].

Project Team

- Dr Matthew Higgins (PI, University of Warwick)
- Prof Tim Watson (CoI, University of Warwick)
- Prof Paul Jennings (CoI, University of Warwick)
- Dr Matthew Bradbury (Researcher, University of Warwick)
- Dr Elijah Adegoke (Research-CoI, University of Warwick)
- Dr Erik Kampert (Research-CoI, University of Warwick)
- Jasmine Zidan (PhD student, University of Warwick)
- Steve Hickling (Spirent Communications Plc)
- Colin Ford (Spirent Communications Plc)
- Guy Buesnel (Spirent Communications Plc)
- Mark Hunter (Spirent Communications Plc)

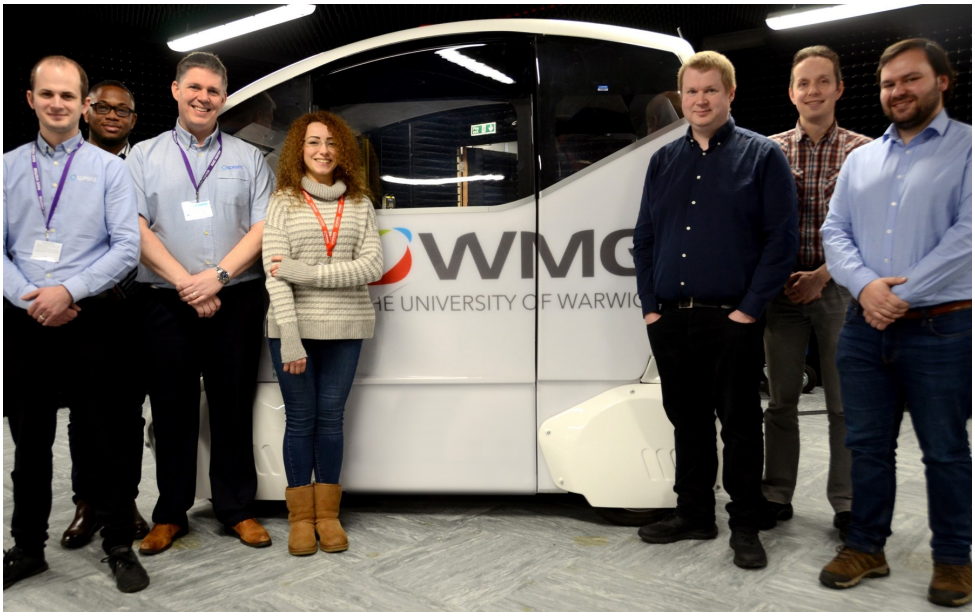


Figure 3: PNT Cyber Attack Resilience Project's Technical Team

Additional Acknowledgements

We would also like to thank the following colleagues for their assistance during this project:

- Dr Jakes Groenewald (CAM Testing Facilities Lead Engineer, University of Warwick)
- Harry Chan (VUT Safety Driver and Graduate Trainee Engineer, University of Warwick)
- Lee-Rose Jordan (Project Manager, University of Warwick)
- Daniel Martin (Spirent Communications Plc)
- Francesca Filippi (Spirent Communications Plc)
- Akis Drosinos (Spirent Communications Plc)

Project Team's Related Publications

- E. Adegoke, J. Zidan, E. Kampert, C. R. Ford, S. A. Birrell, and M. D. Higgins. Infrastructure Wi-Fi for connected autonomous vehicle positioning: A review of the state-of-the-art. *Vehicular Communications*, 20:100185, December 2019. ISSN 2214-2096. doi:10.1016/j.vehcom.2019.100185
- C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello. A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. *Applied Sciences*, 9(23):5101, November 2019. ISSN 2076-3417. doi:10.3390/app9235101
- J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins. GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. *IEEE Access*, pages 1–1, 2020. ISSN 2169-3536. doi:10.1109/ACCESS.2020.2973759

Most Relevant References

- C. Whitty and M. Walport. *Satellite-derived Time and Position: A Study of Critical Dependencies*. London, UK, 30th January 2018. URL `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf`
- M. Pattinson, S. Lee, Z. Bhuiyan, S. Thombre, V. Manikundalam, and S. Hill. Draft Standards for Receiver Testing Against Threats. Technical Report D4.2, STRIKE3, November 2017. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D42_Test_Standards_v2.0.pdf`. Issue 2.0

Contents

List of Tables xi

List of Figures xi

Abbreviations xii

1 Introduction 1
- 1.1 Project Methodology . . . 1
- 1.2 Global Navigation Satellite Systems . . . 2
  - 1.2.1 GNSS Operating Principle . . . 2
  - 1.2.2 GNSS Vulnerabilities . . . 4
- 1.3 Application of GNSS . . . 5
- 1.4 Scope of Threats . . . 5
- 1.5 Adversaries . . . 6
  - 1.5.1 Goals and Motivations . . . 7
  - 1.5.2 Resources and Knowledge . . . 9
  - 1.5.3 Presence . . . 9
  - 1.5.4 Tactics, Techniques, and Procedures . . . 10
  - 1.5.5 Summary . . . 10

2 PNT Attacks on CAM Systems 11
- 2.1 Jamming: Methods and Techniques . . . 11
- 2.2 Spoofing: Methods and Techniques . . . 12
  - 2.2.1 Meaconing Replay Spoofer . . . 12
  - 2.2.2 Self-Consistent Spoofer . . . 12
  - 2.2.3 Nulling Spoofer . . . 13
  - 2.2.4 Multiple Phase-Locked Receiver-Spoofer . . . 13
- 2.3 Software Attacks . . . 13
  - 2.3.1 GNSS Receiver Firmware/Operating System . . . 13
  - 2.3.2 GNSS Receiver Data Manipulation . . . 14
  - 2.3.3 Application Data Consumption . . . 14
- 2.4 Conclusion . . . 15

3 Threat Detection 16
- 3.1 GNSS Jamming Detection . . . 16
  - 3.1.1 AGC Monitoring . . . 16
  - 3.1.2 Digital Signal Processing/Spectral Monitoring . . . 17
  - 3.1.3 Post Correlation-Based Monitoring . . . 17
- 3.2 GNSS Spoofing Detection . . . 17
  - 3.2.1 Position Solution and Navigation level . . . 17
  - 3.2.2 Signal Processing Level . . . 18
  - 3.2.3 Multipronged Spoofing Detection . . . 18
- 3.3 Conclusions . . . 18

4 Threat Mitigation **19**
4.1 GNSS Jamming Mitigation . . . 19
4.1.1 External Aiding — Inertial Systems . . . 19
4.1.2 Antenna-Based (Spatial Filtering) . . . 19
4.1.3 Signal Conditioning (Time-Frequency) . . . 20
4.1.4 Receiver-Based — Vector Tracking . . . 20
4.2 GNSS Spoofing Mitigation . . . 20
4.2.1 Position Solution and Navigation Level . . . 21
4.2.2 Signal Processing Level . . . 21
4.2.3 Data Bit Level Cryptographic Approaches . . . 21
4.3 Software Attack Mitigation . . . 22
4.3.1 Impracticality of Exhaustive Testing . . . 22
4.4 Conclusions . . . 23

5 Community Experience **24**
5.1 PNT Experts . . . 24
5.2 Cyber-security Experts . . . 28
5.3 Conclusions . . . 32

6 Lab2Live Attack Emulation and Testing **34**
6.1 Legality . . . 34
6.2 Test Methods and Devices . . . 35
6.2.1 PNT Attack Emulator (Spirent) . . . 35
6.2.2 Vector Signal Generator and Signal and Spectrum Analyser (Rohde & Schwarz) . . . 36
6.2.3 Uninterruptible Power Supply . . . 37
6.2.4 Receivers under Test . . . 37
6.3 Lab-based Jamming Tests . . . 37
6.3.1 TTFF for Jamming with CW Jamming . . . 38
6.3.2 Sensitivity & Satellite Visibility with CW Jamming . . . 38
6.4 Lab-based Spoofing and Emulation Tests . . . 39
6.4.1 Tests with Corrupt GNSS NAV Data . . . 39
6.4.2 Tests with False Position . . . 43
6.5 Real-World, Live-Sky Tests . . . 43
6.6 Practicality and Realism of Testing . . . 46
6.7 Conclusions . . . 47

7 Conclusions **48**
7.1 Findings and Discussion . . . 48
7.2 Future Work . . . 49
7.2.1 Incentivise Non-GNSS Position and Timing Sources . . . 49
7.2.2 Infrastructure . . . 49
7.2.3 Potential Future Testing and Research Activities . . . 49
7.2.4 WMG and Spirent . . . 50

A Spirent Interviews **51**
A.1 Spirent PNT Cyber Security Round Table One Interview Guidelines . . . 51
A.1.1 Guidance to the participants . . . 51
A.1.2 Core Interview Guideline . . . 51
A.1.3 Background, Context and Prompting . . . 51
A.1.4 Follow-on Discussion on Actors . . . 52

A.1.5 Follow-on Discussions 52
A.1.6 Follow-on Closing general discussion 53

B Warwick Interviews **54**
B.1 Prompting Questions 54

Bibliography **56**

List of Tables

1.1 GNSS frequencies and minimum received power [8] 3

4.1 Obtaining security properties via different techniques 22

6.1 Test receiver mapping 37
6.2 TTFF CW jamming test performance 38
6.3 Base values for the different receivers tested 39
6.4 Summary of FZC jamming and receiver sensitivity (Field) 46

List of Figures

1 Range of typical GNSS vulnerabilities ii
2 Researchers preparing the equipment for live, real-world tests at Wellesbourne Campus v
3 PNT Cyber Attack Resilience Project's Technical Team vi

1.1 Satellite Constellations with number of satellites in parentheses 2
1.2 Illustration of a 3-anchor trilateration 4
1.3 Block diagram of a typical GNSS receiver (adapted from [9]) 5

2.1 Meaconing replay spoofer rebroadcasting valid GPS signal after a time delay. . . 12
2.2 Illustration of a self-consistent spoofing attack (adapted from [10]). 13
2.3 GPS Subframes L1 C/A navigation message 14

4.1 Generic architecture for GNSS/INS integration (adapted from [11]) 20

6.1 Positioning, Navigation and Timing Attack Emulator 35
6.2 Representative FZC-waveform characteristics 36
6.3 Signal generating and analysing devices used during jamming tests 36
6.4 Receiver-C behaviour under low CW jamming power (J/S = 20 dB) 38
6.5 SimGEN GPS signal source showing Clock Error Parameters 39
6.6 SimGEN GPS signal source showing satellite upload information 40
6.7 Effect of clock bias on position 41
6.8 Observation table of receiver under test 42
6.9 Effect of spoofing signal power 44
6.10 Effect of a spoofed location 45
6.11 VUT testing performed at Wellesbourne 46

Abbreviations

Notation	Description
A/D	Analog to Digital
AGC	Automatic Gain Control
BOC	Binary Offset Carrier
C/A	Coarse Acquisition
CAM	Connected and Automated Mobility
CAV	Connected and Autonomous Vehicle
CDMA	Code Division Multiple Access
CNI	Critical National Infrastructure
CORS	Continuously Operating Reference Station
DoS	Denial-of-Service
EM	Electromagnetic
FAT	File Allocation Table
FDMA	Frequency Division Multiple Access
FMEA	Failure Mode and Effects Analysis
FPGA	Field-programmable Gate Array
FZC	Frank–Zadoff–Chu
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSA	European GNSS Agency
IF	Intermediate Frequency
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ISM	Industrial, Scientific and Medical
ITS	Intelligent Transportation System
LoS	Line-of-Sight
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NLoS	Non Line-of-Sight
NMEA	National Marine Electronics Association
NTP	Network Time Protocol
NTRIP	Network Transport of RTCM via Internet Protocol
OEM	Original Equipment Manufacturer
OS-NMA	Open Service Navigation Message Authentication
P	Precise
PKI	Public Key Infrastructure
PNT	Positioning, Navigation and Timing
PNTAE	Positioning, Navigation and Timing Attack Emulator
PPD	Personal Privacy Device
PRN	Pseudorandom Noise
PSD	Power Spectral Density
PVT	Positioning, Velocity and Timing
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
RFI	Radio Frequency Interference
SDL	Security Development Lifecycle
SDR	Software Defined Radio
SV	Satellite Vehicle
TETRA	Terrestrial Trunked Radio
TOA	Time-of-Arrival
TTFF	Time To First Fix
TTPs	Tactics, Techniques and Procedures
USRP	Universal Software Radio Peripheral
VSG	Vector Signal Generator
VUT	Vehicle Under Test
WI-FI	IEEE 802.11
WLAN	Wireless Local Area Network

1 Introduction

Global Satellite Navigation Systems (GNSSs) such as GPS, GLONASS, Galileo and BeiDou provide a wide range of devices access to accurate position (error $\leq 7.8\,\mathrm{m}$ for GPS [12], accuracy within 4.9 m observed in practise [13]) and timing information (error $\leq 40\,\mathrm{ns}$ for GPS [12]). Both position and timing are critical for a wide range of use cases including autonomous and non-autonomous vehicles. Existing vehicles are using GNSS data to facilitate satellite navigation recommendations and future autonomous applications will extend to sharing this information [14] to avoid collisions [15], support emergency response via eCall [16], and facilitate novel applications such as autonomous formation of platoons [17]. Timing will also be critical as autonomous vehicles will not just need to know where to execute tasks, but also when. Expensive time synchronisation protocols can be avoided if GNSS can be relied upon to provide an accurate timing source [18]. The high reliance of critical functions of an autonomous vehicle on the position and timing information supplied to it by GNSSs, makes attacking that input appealing to adversaries. GNSS jamming [19], spoofing [20], others [21], and combinations of these threats [22] are recognised as potential serious threats to systems that rely on position and timing.

In this document we will present a summary of the threat actors who might perform attacks against GNSS-equipped vehicle systems and a summary of the jamming, spoofing and software attacks that can be performed against a GNSS receiver. This report will focus on threats to GNSS receivers in a vehicular context due to the high impact that GNSS attacks can have on transportation systems.

The remainder of this chapter will describe GNSSs at a high level, uses for their applications, and the threats that can be encountered when using GNSS. This chapter will also describe the methodology used to analyse the impact of GNSS threats. Chapter 2 presents a detailed description of these threats, for each of which the detection and mitigation techniques for these threats are described in Chapter 3 and Chapter 4 respectively. The results of interviews with experts to understand the importance of testing and developing mitigations for these threats is presented in Chapter 5. The practical testing performed in this project is described in Chapter 6, including the results of the testing. Finally, Chapter 7 summarises our findings, and presents guidelines and recommendations based on these findings with the aim to improve the resilience of connected and automated mobility (CAM) solutions that require GNSS by improved cyber-security testing.

1.1 Project Methodology

In order to identify methods to create and test cyber-physical and software architectures, with a specific focus on CAV PNT systems, we have followed below project methodology:

1. Survey literature to identify (i) threats, (ii) methods to detect threats, and (iii) techniques to mitigate these threats.

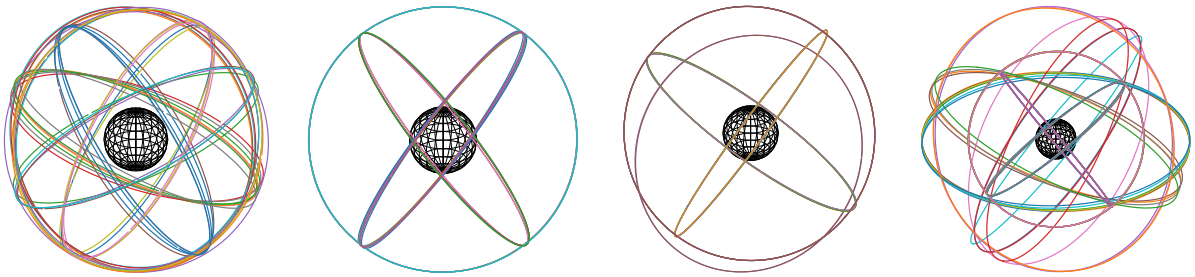
2. Ask relevant experts to provide input on which identified threats are high-priority and how a testbed should be designed to evaluate CAM system's resilience to these threats.

3. Perform a feasibility study by attacking GNSS receivers throughout the full test continuum, starting in the lab and finishing with live scenario tests, in order to understand how these testing environments complement each other, and to develop an optimised black box research methodology for the vast range of PNT attack scenarios.

4. Summarise this information and obtained experience to present recommendations for a new cyber test facility in [2].

This methodology led to the conclusion that the ideal PNT cyber resilience testing method for CAVs is based on a Lab2Live approach, spanning the full test continuum, from simulation to emulation, to tests on intelligent vehicles inside a dedicated lab, to real-world environment testing on autonomously-driving vehicles.

1.2 Global Navigation Satellite Systems



(a) GPS (31) (b) GLONASS (25) (c) Galileo (26) (d) BeiDou (48)

Figure 1.1: Satellite Constellations with number of satellites in parentheses

A GNSS constellation is made up of three segments: (i) space, (ii) ground and (iii) user [9]. The space segment is composed of a defined number of satellites within a constellation (as shown in Figure 1.1 for 4 major GNSS systems) and ground stations that are responsible for monitoring performance and health of the satellites in that constellation. In addition, the ground station is also responsible for time synchronisation. The user segment encompasses devices that receive GNSS signals sent by the space segment and use them to calculate their position and the current time. In the electromagnetic (EM) spectrum, GNSS operates as microwaves with frequencies ranging from 1151 to 1610 MHz. The frequency allocations for the American, Russian, European and Chinese GNSSs are presented in Table 1.1.

Multiple access in all GNSS constellations is based on spread spectrum technology via code division multiple access (CDMA), with the exception of GLONASS which uses frequency division multiple access (FDMA). In CDMA-based GNSS, signals are modulated by a pseudorandom noise (PRN) code that is unique to each satellite vehicle (SV). This allows all satellites to share the same frequency resource. For radio transmission to user devices on earth to occur, the signals from the SVs needs to be upconverted using modulation techniques such as binary phase shift keying (BPSK) or variations of binary offset carrier (BoC) modulation. The modulated signals from the SVs typically contain the satellite's location (ephemeris data), transmission time and additional information for estimating the time and position of the user [23].

1.2.1 GNSS Operating Principle

In this subsection, a basic explanation of how a GNSS receiver computes its position and timing information is presented. GNSS signals transmitted on any given band (as shown in Table 1.1) are made up of a radio frequency (RF) carrier, data waveform, and PRN. With respect to the PRN/spreading codes, there are two types:

- C/A (Coarse Acquisition) code: This PRN has no security measures and it is typically adopted in civilian applications such as CAVs and CAM.

GNSS	Band	Centre frequency (MHz)	Minimum received power (dBm)
GPS	L1	1575.420	-128.5 (C/A-code), -127 (L1C)
	L2	1227.600	-130 (IIR-M/IIF), -128.5 (III)
	L5	1176.450	-124.9 (IIF), -124 (III)
GLONASS	L1OF	1598.0625 to 1605.375	−131
	L2OF	1242.9375 to 1248.625	−137
	L1OC	1600.995	tbd 2023–25 for GLONASS V
	L2OC	1248.060	tbd 2023–25 for GLONASS V
	L3OC	1202.025	tbd 2023–25 for GLONASS V
Galileo	E1	1575.420	−127
	E6	1278.750	−125
	E5	1191.795	−125
	E5b	1207.140	−125
	E5a	1176.450	−125
BeiDou	B1	1561.098	−133
	B2	1207.140	−133
	B3	1268.520	−133

Table 1.1: GNSS frequencies and minimum received power [8]

- P (Precise) code: This PRN is encrypted and adopted in military applications.

The process of computing a positioning, velocity and timing (PVT) solution comprises of three stages [24]:

1. Acquisition
2. Tracking & Correlation
3. Navigation Message Decoding

At the acquisition stage, the receiver scans for live-sky signals in view. Thereafter, it obtains an estimate of the time-of-arrival (ToA) of corresponding satellites in view. For this process to occur, the receiver needs to generate local replicas of the satellite PRN codes. A correlation peak occurs when the local replica aligns with the satellite signal. At the tracking phase, further alignment is carried out and the incoming signal is correlated with replica codes for early, late and prompt correlators. At this stage, the receiver is now able to demodulate the transmitted navigation message [9, 24, 25]. The pseudorange (ρ^k) to each satellite can be geometrically calculated using Equation (1.1), where (x, y, z) are the user coordinates to be determined, (x^k, y^k, z^k) are the coordinates of the kth satellite and δb is the clock bias (in meters). Since GNSS systems are based on ToA ranging techniques, the distance can be inferred using the propagation time of the radio wave between the transmitter/initiator and the receiver/responder. In order to estimate a receiver location, multilateration is employed to different anchors (or satellites in GNSS) as illustrated in Figure 1.2. Ideally, the circles drawn from the distance to each satellite (radius) will intersect. However, due to ranging and timing errors, a cross section area results from the intersection. Consequently, the user coordinates and clock bias is obtained by solving the pseudorange equation iteratively[1]. In Figure 1.3, a generic block diagram of a GNSS receiver

[1]An in-depth explanation of the operating principle is out of the scope of this report. Readers can obtain detailed information on the operating principle from [9, 26].

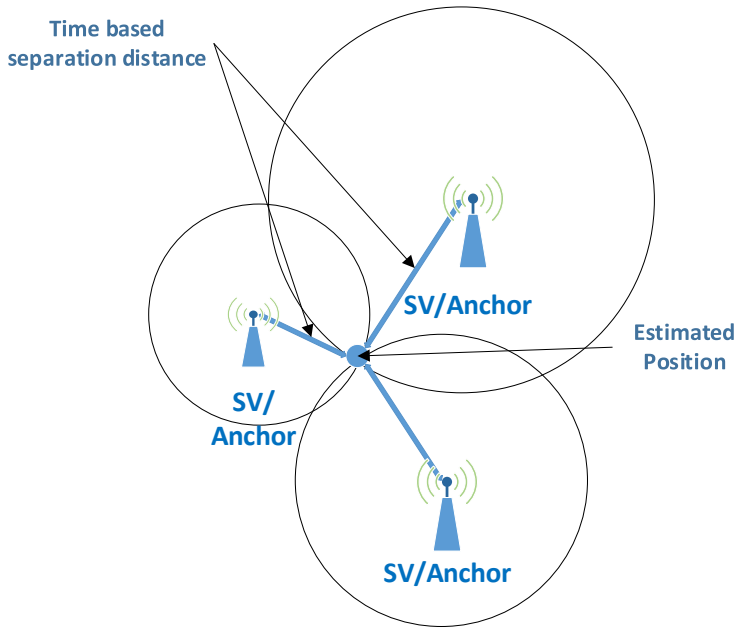


Figure 1.2: Illustration of a 3-anchor trilateration

is presented, which illustrates the signal flow across stages as the receiver computes a PVT solution.

$$\begin{aligned} \rho^1 &= \sqrt{(x^1 - x)^2 + (y^1 - y)^2 + (z^1 - z)^2} + \delta b \\ \rho^2 &= \sqrt{(x^2 - x)^2 + (y^2 - y)^2 + (z^2 - z)^2} + \delta b \\ &\vdots \\ \rho^k &= \sqrt{(x^k - x)^2 + (y^k - y)^2 + (z^k - z)^2} + \delta b \end{aligned} \tag{1.1}$$

1.2.2 GNSS Vulnerabilities

Whereas GNSS is widely used across various industries for positioning, navigation and timing (PNT)[2] services with acceptable accuracy, the performance of a GNSS receiver in certain environments (such as urban canyons) is severely impaired [27, 28]. This is due to RF propagation effects. Within the space segment, signal modulation faults, clock errors as well as space storms [29] can affect the performance of a GNSS receiver. In general, GNSS signal vulnerabilities can be grouped as [5]:

- Physical degradations: These effects are mostly due to multipath or non line-of-sight (NLoS) propagation. Since GNSS receivers require a line-of-sight (LoS) link to SVs in view, multipath and NLoS propagation alter the correlation function. This in turn results into inconsistent pseudorange measurements, C/N_0[3] fluctuations and polarisation changes. In addition, ionospheric scintillation, which results in fading and signal power loss, can also be regarded as physical degradation.

- Unintentional and intentional threats: Unintentional interference to GNSS receivers can occur from EM effects such as multipath propagation or from other wireless communication

[2]Without loss of generality, PNT and PVT are used interchangeably in this report.

[3]This parameter characterises the signal strength of the GNSS signal at the receiver front end as well as the lock of the carrier and tracking loops [30].

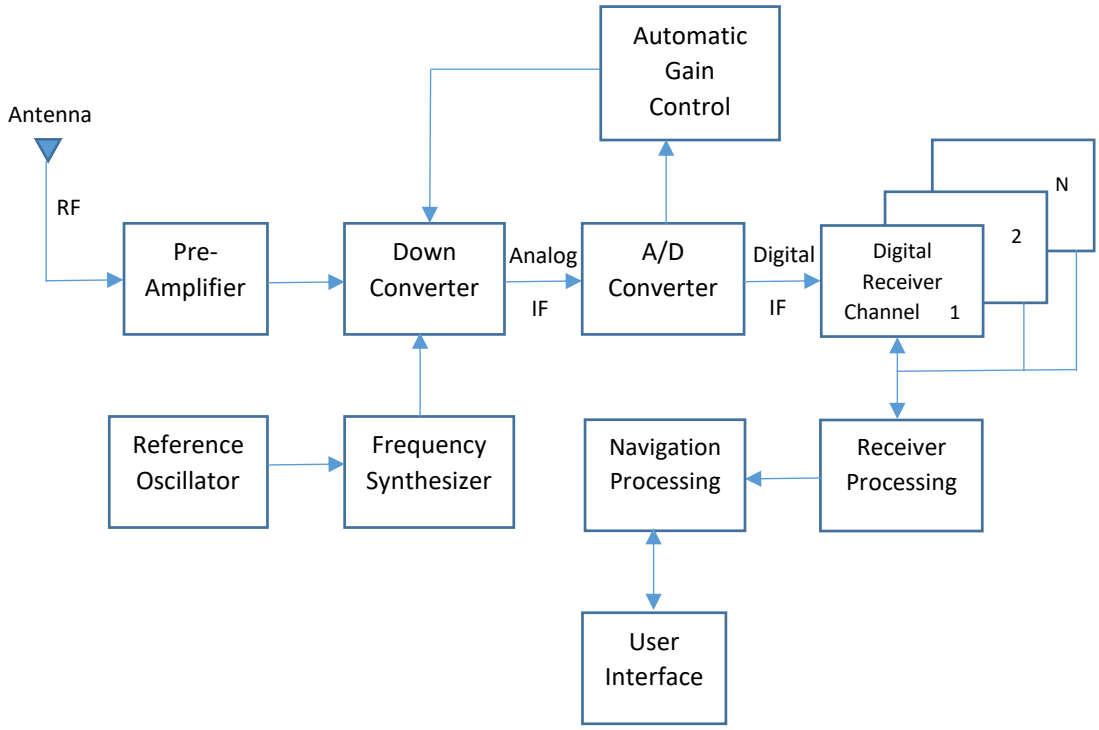


Figure 1.3: Block diagram of a typical GNSS receiver (adapted from [9])

technologies. Intentional threats can also result from RF devices. In addition, PNT/GNSS receivers can be open to cyber attack. In the academic literature, the most relevant cyber attacks are spoofing-based attacks, which are discussed in Chapter 2.

1.3 Application of GNSS

GNSS-provided information is used in many sectors, as highlighted in [6]. Areas include aspects of a country's critical national infrastructure, such as: telecommunications, maritime, finance, energy, food (including supply chain management), and transport (including emergency services). Both position and timing information are required from GNSS by these sectors, however, for many, the timing information is often more critical. For example accurate and high-precision timing information is required by: financial services to facilitate trading, telecommunications to correctly time slot communication channels, the energy sector to control frequency and voltage, and emergency services for the terrestrial trunked radio (TETRA) network that is used when cellular communications are unavailable.

The European GNSS agency (GSA) GNSS Market Report predicts that the road sector will make up 55% of the GNSS market from 2019–2029 [31]. For transportation, both location and timing are required to facilitate vehicle routing. A loss of GNSS will not only impact passenger vehicles, but also manufacturing and agriculture supply chains. As autonomous vehicles are expected to be deployed in the near future, a loss of GNSS could impact the safety of these systems as well as its functionality. Therefore, due to the large market size and potential impacts, the transport sector needs to be evaluated for resilience against a GNSS attack.

1.4 Scope of Threats

In this section we will detail the scope of threats against PNT systems that we consider in this report. A large number of potential attacks exist that could potentially prevent access to or

cause incorrect position and timing information contained within a GNSS signal. In this report we only consider attacks and mitigations for the unrestricted GNSS signals, due to the impact on a wide range of systems that depend on PNT from these signals. We do not examine the impact of attacks on the encrypted GNSS signals for restricted use.

In this report we focus on threats to vehicular GNSS receiver systems, specifically focusing on RF threats. This is due to the ease with which RF threats can be performed and high impact that can be gained from performing them. These threats include jamming to cause a denial-of-service (DoS), which prevents a vehicle from having access to the position and timing information contained within the GNSS signals. The second threat is spoofing the GNSS signal such that a receiver could believe it is located at a different position, or is made to believe that the reported time is different to the current time. We also consider attacks on the software of GNSS receivers via the data contained within the GNSS signal. Such attacks can potentially escalate and cause a DoS due to incorrect handling of malicious data [21].

As this work focuses on RF threats, there are several classes of threats that we do not consider in this report but do form part of the threat landscape of GNSS. However, several of these threats will lead to a similar impact as RF-based threats, meaning that mitigations for the RF-based threats will also be able to be applied to these non-RF-based threats.

This report does not consider the impact of space weather [32], direct physical attacks (such as anti-satellite weapons) [33], or cyber attacks against satellites [34]. We assume that GNSS satellites function correctly and within their specifications (e.g., transmit signal power is within the required range). The impacts of these threats will either prevent a GNSS signal from being transmitted or interfere with the transmission of the signal. Detection of these events will differ to RF-based threats, however, these impacts may be mitigated by the same techniques used to mitigate jamming-based DoS and spoofing-based signal manipulation.

Other threats considered as out-of-scope include physical attacks on GNSS receivers, attacks on internal vehicle systems (via the CAN bus [35]) such as the GNSS receiver or internal vehicle timing sources, and attacks on other vehicle sensors [36], with which the position and timing of a vehicle can be manipulated. However, they involve different detection and mitigation approaches and the testing strategies will need to be considered separately to RF-based attacks on GNSS receivers.

1.5 Adversaries

In order to understand what RF-based GNSS attacks to focus mitigation development on, it is first important to understand who the GNSS threat actors are. Multiple dimensions exist to evaluate GNSS threat actors, which include:

Goals What is the threat actor trying to achieve?

Motivations Why is the threat actor trying to achieve their goals?

Resources What equipment/tools/finance/personnel/etc. does the threat actor have?

Knowledge What information does the adversary have? How does this impact the way in which they perform GNSS attacks?

Presence Where is the adversary (or their equipment) located? What is their mobility?

Tactics, Techniques, and Procedures (TTPs) Is the attack likely to be slow and silent, requiring persistence on the system, or quick and noisy? How will attacks likely be conducted?

Understanding the threat actors via these classifications informs the types of attack, i.e. the threat actors capabilities that a system needs to mitigate. Threats with the highest likelihood and impact on a system should be prioritised and mitigations implemented first.

1.5.1 Goals and Motivations

In this section, multiple examples of GNSS attacks will be examined by identifying the goals and motivations behind them, with the focus on adversaries considering vehicular systems.

Personal Privacy

Adversaries can perform GNSS jamming for their own privacy. This is typically against employer-installed devices [37] used to "defeat the fleet tracking devices in company cars and trucks" [38, Slide 4]. Jamming devices sold for personal privacy are cheap and easy to obtain [39]. A typical example of accidental jamming by a personal privacy device (PPD) was at the London Stock Exchange in July 2013, where GPS signals were unavailable for about 10 minutes each day [40].

Financial Gain

An adversary may jam GNSS in order to "defeat attempts to document road use for taxes" [38, Slide 4]. Other uses may be to prevent pay-as-you-go insurance from accurately detecting the distance travelled thus reducing the cost of insuring a vehicle [41].

Theft

GNSS jamming and spoofing can be used to facilitate the theft of vehicles [42]. "Jammers [overwhelm] anti-theft measures on cars" [38, Slide 4] in order to disable tracking systems that allow the owner or police to locate the stolen vehicle [39]. These jammers often do not only block GNSS signals, but also key fobs used to unlock doors and other frequencies, such as those used by wireless CCTV cameras [6, p.20–21].

Other approaches than GNSS spoofing can also impact navigation. One recent example was how 99 smartphones transported down a road led to Google Maps reporting a traffic jam when the street was clear [43]. In this instance the reporting of many GNSS-obtained positions to a service led to the impact on vehicles.

Terrorism, Destabilisation and Chaos

GNSS jamming and spoofing may be performed as part of terrorist acts [44] which aim to cause chaos among a population. Goals of an adversary could include: reducing effectiveness of emergency services, economic disruption, reducing safety of the targeted group, and to reduce confidence in a government. An adversary would aim to achieve high a impact from attacks performed under this kind of motivation.

Geopolitics

Nations creating their own GNSS are primarily led by geopolitical concerns, as managing their own system allows access to restricted signals with higher tolerance to spoofing due to its encryption. As an impact of leaving the EU, the UK's plans do not include access to the encrypted Public Regulated Service (PRS) provided by Galileo [45]. However, in [46, §3.F(135)], the EU's position is that continued access to the PRS is a possibility. Due to the evolving nature of the negotiations there is still uncertainty regarding the UK's use of Galileo. This potentially reduces the UK's resilience to GNSS threats depending on the outcome of the negotiations

between the UK and EU. Non-critical systems will still have access to the unencrypted signals, meaning vehicles can still receive and process Galileo-provided position and time information.

In a report by C4ADS [47], instances of GNSS spoofing and jamming were investigated across Russia. A number of use cases were uncovered including: (i) protection of VIPs via GNSS spoofing, (ii) protection of strategic facilities for national defence via GNSS spoofing, and (iii) use of GNSS spoofing in combat. It is possible that some of these actions led to navigation issues for civilian owned vehicles in St. Petersburg [48]. Other instances of nation-state cyber warfare has been reported to have impacted civilian vehicles. In 2012, North Korea produced GPS jamming signals that impacted commercial flights, ships and vehicle navigation [49]. A similar incident also occurred in 2016 [50] where North Korea jammed GNSS signals in border regions.

Impact Navigation

An adversary may wish to impact the navigation of target vehicles. This is typically motivated by other motivations, such as theft or financial gain. Manipulation of navigation is typically performed via GNSS spoofing in order to re-position a vehicle. Some of the goals when impacting navigation would be to [51, 52]:

- Direct a target to an incorrect destination.
- Direct a target to a correct destination via an incorrect way point (delay).
- Direct a target to a dangerous situation, e.g., incorrect direction on road.

Escalation Aims

An adversary may perform one kind of attack that is easier to do and less impactful, to cause a situation that is more impactful, in essence escalating their capabilities. For example, by intentionally jamming or spoofing GNSS, 802.11p V2X communication can be impacted [53, § 3.7.1], such as by causing a DoS due to the equipment not being able to transmit. This is caused by GNSS jamming or spoofing either denying the V2X communication equipment access to accurate timing information, or providing incorrect timing information.

Indirectly related to vehicular systems, many aspects of critical national infrastructure (CNI) depend on timing (and sometimes position) information supplied by GNSS [6]. Threat actors may attack one aspect of the CNI in order to obtain impacts on other aspects, such as transportation.

Accidental

Not all threat actors will intentionally be perpetrating threats and are instead exposing systems to attack due to issues such as misconfiguration of the system. For instance, a GNSS repeater at Hannover Airport, Germany was incorrectly configured leading to unintentional spoofing [54] in 2012. A second case of accidental impact was when a PPD was used inside Newark Liberty International Airport, NJ, USA. Intermittent jamming caused by the PPD impacted the functioning of the airport's systems. Although this was unintended, due to the device's mobility and transmit power it was able to [55]. The STRIKE3 project also observed a number of GNSS jamming events at sites near both airports and motorways in the UK [56, p.39] indicating that such accidental events remain very relevant.

Accidental leakage of signals from a GNSS simulator caused a variety of issues at the ION GNSS+ 2017 Conference [57]. The spoofing source had no antenna attached, but still managed to have a large impact, likely due to the fact that it was an indoor event without view of live-sky. This spoofing of GNSS should have been mitigated by a number of additional verification sources, such as Assisted GPS from the carrier network and Wi-Fi access points, but it appeared that too much trust was placed in GNSS signals.

Unknown

There have been a variety of incidents where the effects of spoofing were observed, but the motivations for attacking GNSS were unclear. One example observed in Shanghai, was the spoofing of the location of ships as if they were rotating in a circle [58]. It was theorised that spoofing was potentially being performed to obscure ships that were ferrying illegal goods. A second example is the spoofing of position and time of vehicles at the Geneva International Motor Show 2019 [59]. As the spoofing was intermittent, the organisers were unable to find the origin of the spoofed signal. It is possible that this was another instance of an unintentional attack, similar to the one performed at ION GNSS+ in 2017.

1.5.2 Resources and Knowledge

In order to perform jamming, spoofing and software attacks on GNSS receivers, adversaries will require sufficient equipment to broadcast on the same frequency as one or more GNSSs. For attacks on mobile receivers, this attack equipment most likely needs to be portable and battery-powered. Adversaries will also require knowledge of the vulnerabilities of commercial GNSS receivers, knowledge on how to operate jamming and spoofing equipment, and more advanced adversaries will have knowledge about how to mitigate their potential for detection.

Jamming Equipment

Jamming in the real world as discussed in this report is majorly carried out as unintentional jamming. In such scenario, GNSS/PNT devices within the effective range of a jammer are affected momentarily. Whereas this occurs at relatively low power levels in the transportation industry, jammers with high transmit power have the potential to affect PNT receivers within a wider coverage area.

Spoofing Equipment

At the core of custom GNSS spoofing equipment is typically a software defined radio (SDR) such as a HackRF One, BladeRF or universal software radio peripheral (USRP). An SDR facilitates transmitting and receiving signals across a wide range of the RF spectrum, because components that are typically implemented in hardware are implemented using software instead. This implementation is often accelerated using a field-programmable gate array (FPGA) instead of running on a general purpose processor. Using SDRs for GNSS spoofing has been effectively demonstrated multiple times [52, 60]. The source code for SDR-based GPS simulators is available online for free [61]. In [52] the total cost of equipment to create a GNSS spoofer was $223, meaning that the financial barriers to performing the spoofing attacks that this hardware is capable of are low.

1.5.3 Presence

It is important to consider the presence of an adversary, including if they are mobile. This to both understand where an adversary is and the impact that this has (e.g., strength of jamming signal) and also the feasibility of performing an attack. A stationary spoofer has a limited area in which it can attack a mobile vehicle, but the potential tracking of that vehicle is simpler than for a mobile spoofer. In order to achieve a greater impact, an adversary may use multiple transmitters to obtain a distributed presence, either by jamming a larger area simultaneously or better facilitating spoofing.

1.5.4 Tactics, Techniques, and Procedures

The final dimension to consider are the tactics, techniques and procedures (TTPs) used by an adversary. The National Institute of Standards and Technology special publication (NIST SP) 800-150 defines TTPs as the behaviour of an attacker, where tactics refer to a high-level description of the adversary's behaviour, techniques provide a more detailed description in context of a tactic, and procedures give an even more detailed description in the context of a technique [62, p. 31]. These will include details such as how an attack will likely be conducted. The first *T* of the TTPs of an adversary is sometimes defined as the *Tools* an adversary uses, however, this has been covered in Section 1.5.2 by the equipment required to perform these attacks.

The duration and detectability of an attack is an important consideration of the adversary's TTPs. Is an attack likely to be slow and stealthy, or quick and noisy? Many of the GNSS threats observed, have been executed over a short period of time. For most of the jamming threats observed by the STRIKE3 project [56], the duration of the attack was short, which was likely due to jammers being installed inside vehicles. However, performing a spoofing attack over a longer period of time can lead to greater impacts [63], because there is more time for an adversary to slowly shift the location or time of the target. A jamming attack over a longer period of time also has the potential to create greater disruption as there is a longer time until the system recovers or regains access to GNSS-provided information. These longer-duration attacks will require a persistent adversary that can maintain an attack on the system.

1.5.5 Summary

Adversaries can have a wide range of capabilities and different motivations that lead to attacks being performed. It is important to understand whom a system needs to be defended against, in order to prioritise effort testing and developing mitigations. The adversary definitions should not be based on the point-of-view of system defenders, because the scope of threats investigated tends to be reduced. Therefore, effective red teaming (where a team in an organisation emulates a potential attack [64, p. 101]) is necessary to present a credible, creative, and useful adversary definition and analysis of system vulnerabilities.

2 PNT Attacks on CAM Systems

In this chapter we present a high-level viewpoint of attacks against PNT systems of CAM systems. Here we focus on three main classes of threats against GNSS receivers, as per the scope defined in Section 1.4: (i) jamming — which denies the GNSS receivers access to position and timing information supplied by one or more GNSSs, (ii) spoofing — which presents false position and timing information to GNSS receivers, and (iii) software attacks — affecting the firmware running on GNSS receivers.

2.1 Jamming: Methods and Techniques

Given that the signal strength of GNSS signals on earth is quite weak, between -122 to $-132\,\text{dBm}$ [8, 20, 37, 65], when compared to typical strength of $-85\,\text{dBm}$[1] for wireless local area network (WLAN)/Wi-Fi communication, GNSS signals can be easily masked by other wireless communication signals. While GNSS is fairly robust to noise due to spread spectrum technology, radio frequency interference (RFI) from wireless communications systems will continue to increase with growth of the wireless communication sector [66]. This can result into erroneous PVT solutions. Apart from the positioning solution, jamming affects GNSS receivers across different stages. At the receiver front-end, jamming can alter the output of the automatic gain control (AGC) and cause saturation effects [67]. At the acquisition stage, jamming can result into erroneous estimates of Doppler shift and code delay. With respect to tracking, jamming can result into an increased bit error rate (BER) as well as impairment in data decoding [67].

From a cyber-security point of view, threat actors relating to jamming can either be unintentional or intentional. In most of the scenarios involving unintentional jamming, a PPD interferes with the intended receiver as well as nearby devices. The operation of these PPDs/jammers consequently leads to impaired performance of GNSS receivers within range. With respect to intentional jamming, jamming can be grouped into different categories [37]. In [65], jamming was classified based on the bandwidth occupied by the transmitted signal, the adopted classification was:

- Continuous wave (CW) jamming: This refers to unmodulated jamming signals occupying a maximum bandwidth of 100 kHz.
- Narrowband (NB) jamming: This encompasses interference signals with bandwidths between 1 MHz and the C/A code bandwidth (± 1.023 MHz)
- Wideband (WB) jamming: This refers to signals with a ± 10.23 MHz bandwidth.

A more compact classification was presented in [37], with jamming signals classified as:

- CW jammers: Similar to those presented in [65].
- Chirp jammers: This refers to jamming devices that transmit WB or NB signals. These signals can either be saw-tooth functions or frequency bursts. In the academic literature, these type of jammers are more common.

From a perspective of commercially available devices, jammers can also be classified as follows [68]:

[1] This represents the typical minimum required power for receiver operation. The exact value varies with original equipment manufacturer (OEM).

- Group 1: Cigarette lighter jammers — Transmit on L1, for in-vehicle use via cigarette lighter socket. Linear frequency modulation, different frequency ranges and sweep rates. Mean transmit power L1: 0.1 to 23 mW (2 to 50 MHz).
- Group 2: SMA-battery jammers — Transmit on L1 and possibly L2. Linear frequency modulation, different frequency ranges and sweep rates. Mean transmit power L1: 0 to 642 mW, L2: 27 to 482 mW (2 to 50 MHz).
- Group 3: Non-SMA-battery jammers — Transmit on L1 and L2. Mean transmit power L1: 0 to 5 mW, L2: 0 to 8 mW (2 to 50 MHz).

While most cases of intentional jamming result in a DoS attack, jamming with intermediate power values can be malicious and difficult to detect. This approach adopts a power level that is significant enough to introduce impairments in the receiver, but below a power level that causes the receiver to lose lock to authentic signals [67]. Other approaches may focus only on jamming critical aspects of the GNSS message or preventing effective decoding of the remainder of the message [19].

2.2 Spoofing: Methods and Techniques

In comparison to jamming which adopts a brute force approach, spoofing attacks adopt a sophisticated approach in taking control of a PNT device. Critical immobile infrastructure such as power grids and slow moving targets such as cruise ships are vulnerable targets [20, 27, 69]. In the field, carrying out spoofing attacks can be quite complicated, especially with moving targets such as CAVs. However, with the development of SDR communications, it is envisaged that the threat actor's ability to perform spoofing will evolve. In order for an attacker to spoof an intended target, the spoofer requires accurate information about the target's location, and, if mobile, its speed [20, 27, 69].

2.2.1 Meaconing Replay Spoofer

This approach represents the simplest form of spoofing attacks. In a meaconing replay spoofer, the attacker simply records authentic GNSS signals and plays back the recorded signals with a time delay [20] and sufficient transmit power as illustrated in Figure 2.1.

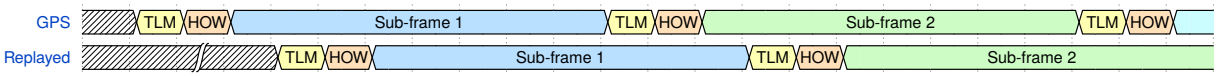


Figure 2.1: Meaconing replay spoofer rebroadcasting valid GPS signal after a time delay.

The time delay introduced can be associated with the signal processing at the replay spoofer as well as the signal propagation time to the target [69]. In this type of attack, the position solution computed by the target device is that of the spoofer. This attack is less likely to occur with encrypted GNSS (such as military GPS), as an encryption key is required for predicting the spreading codes [69].

2.2.2 Self-Consistent Spoofer

A self-consistent or portable receiver-spoofer, depicted in Figure 2.2, has been assembled by researchers using commercially available hardware and open software [10], and, according to the academic literature, poses a long-term threat [69]. In a self-consistent spoofer, the carrier and code phases of the spoofed signals are designed to vary in a similar way as authentic signals. The self-consistent spoofer thereby needs to be aware of its geometry relative to the target receiver [69].

Provided that the spoofer has accurate position information of the target, a scenario is created whereby the spoofed and authentic signals are aligned in code-phase/carrier-phase and Doppler. The target device can be attacked either through a jam and spoof approach, or a subtle approach whereby the amplitude of the aligned spoofed signal is gradually increased until the target receiver locks on to the spoofed signal. In a jam and spoof approach, jamming is carried out first and the receiver is now more likely to lock onto the high-power spoofed signal [10, 69]. This is because the receiver goes into acquisition mode due to the noise introduced by the jammer [27]. In order for a spoofer to carry out this attack, it needs to be in proximity of the target receiver. This allows the spoofer to receive the same authentic GNSS signals as that of the target receiver.

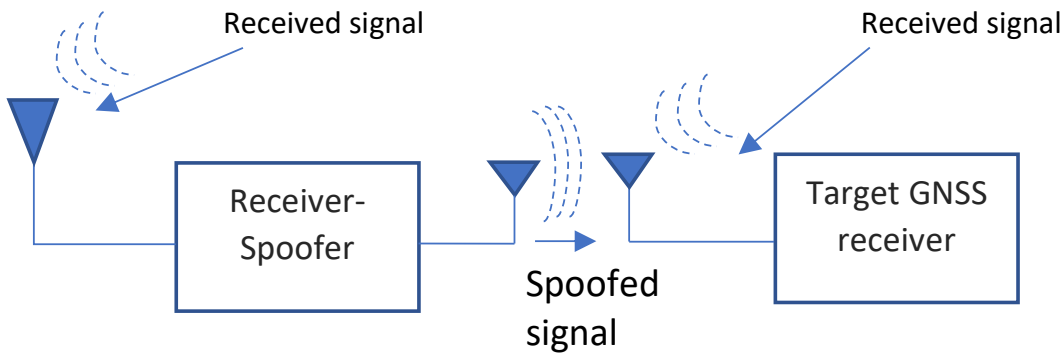


Figure 2.2: Illustration of a self-consistent spoofing attack (adapted from [10]).

2.2.3 Nulling Spoofer

In this type of attack, the spoofer transmits two sets of signals towards the target. The first signal represents false signals that can cause the target to deduce false positions, and the second represent a nulling signal that effectively cancels out the authentic signals [69]. This approach requires advanced signal processing, as both carrier-phase alignment and a calibration of external physical parameters is required [69].

2.2.4 Multiple Phase-Locked Receiver-Spoofer

This type of attack requires multiple portable receiver spoofers with multiple transmit and receive antennas. While this attack is less likely to occur due to its complex nature and the requirement for precise position information of the target, these spoofers can be designed to share a common reference clock and wireless link. This presents a scenario whereby mitigation strategies against the self-consistent spoofer may fail [10].

2.3 Software Attacks

When considering the threats to GNSS, it is important to consider that GNSS receivers execute software that is influenced by the data contained within a GNSS signal. This software processes the data that is sent by GNSS satellites and uses it to calculate a position and timing fix. If the data sent is incorrect or contains invalid values, then the software may react incorrectly if it does not perform sufficient validation of the supplied values.

2.3.1 GNSS Receiver Firmware/Operating System

When a GNSS receiver has decoded a GNSS signal there will be software processing of this data. This software will either form part of the firmware of the receiver, or will run within an

Operating System running on the receiver. A typical task is the conversion of the data into a format to be consumed by clients, such as NMEA 0183 [70].

Several GNSS receiving devices are Linux-based [21] and are therefore potentially vulnerable to the same threats as general purpose Linux deployments. In [21, § 5.2] the authors were able to gain root access to three of the GPS receivers being tested. However, these attacks required physical access via Ethernet, USB, or SD cards in order to attack the system. Obtaining a privilege escalation via the GNSS data stream is highly unlikely due to the restrictive format of the data.

2.3.2 GNSS Receiver Data Manipulation

	1	2	3 4 5 6 7 8 9 10
Subframe 1	TLM	HOW	Timing Correction Information
Subframe 2	TLM	HOW	Ephemeris Parameters (including $\sqrt{A}$)
Subframe 3	TLM	HOW	Ephemeris Parameters (including Ω_0, $\dot{\Omega}$)
Subframe 4	TLM	HOW	Navigation Message
Subframe 5	TLM	HOW	Navigation Message

Figure 2.3: GPS Subframes L1 C/A navigation message

An attacker could manipulate the data in the navigation message of a GNSS signal. In [21, § 5.1] the authors set the semi-major axis $\sqrt{A}$ to 0, a value that indicates to the receiver that the transmitting satellite is at the centre of the Earth. The majority of the tested GNSS receivers rejected the invalid data, however, one GNSS receiver was caught in a crash loop leading to DoS. It was speculated that this was caused by a division-by-zero error that kept recurring because the invalid data had been cached locally.

The authors also successfully performed two attacks on the time information contained within the GNSS data. The first one involved adjusting the Week Number Field to the next week once the ephemeris expired. After that week number was accepted, the week number could then be changed to any value in its 10 bit range. The second attack involved abusing the week number rollover that naturally occurs every 19.7 years due to its 10 bit field length. The authors then alternated between setting all 10 bits high, setting only low bits (1–5) and setting only mid bits (8–9). The authors found that one device did not correctly check if the rollover could validly be occurring, leading to large time jumps of about 20 years each time the attack was successful.

2.3.3 Application Data Consumption

When considering software impacts, it is not just important to consider the software on a GNSS receiver, but also the impact of the output from a GNSS receiver to applications consuming that information. Due to the various applications that can depend on PNT information supplied by GNSS, there are many possible ways in which these applications can be influenced by missing or incorrect information. Below are a few examples of potential attacks on the software system via spoofed or jammed GNSS signals. As this report focuses on threats through signals from GNSS satellites that are spoofed or jammed, these threats are a limited selection, with possible escalated impact on other vehicular systems.

Vehicle Routing

An adversary manipulating the route taken [51] via spoofing or jamming of the vehicle's position, would have a major impact for vehicles. If an attacker is able to deny access to location or timing

information, then a vehicle may be unable to autonomously plan a route and execute that plan. If an attacker is able to spoof the location or timing information, then an undesired route may be taken to an incorrect destination, or actions may be taken at incorrect times leading to a vehicle to deviate from a safe route [71].

System Timing

The timing information supplied by GNSS is crucial for multiple applications, as the exact moment a task is performed can be important to it being performed correctly. If timing information is manipulated, then a CAV may take actions at incorrect times, leading to unsafe situations. Other aspects of a vehicle's system could be impacted by an adversary manipulating the GNSS time, for example, large time jumps in the spoofed GNSS signal could lead to the overflow of timestamps stored in a small fixed-width timestamp, e.g., in file allocation table (FAT) file systems using 7 bit or 32 bit to represent time which could potentially overflow [21, § 5.3].

Escalation via Dissemination

Systems that do not directly rely on GNSS to obtain accurate timing information, can use other services to obtain accurate timing. Two potential services that can be used to obtain accurate timing information are the Network Time Protocol (NTP) [72] and those using Network Transport of RTCM via Internet Protocol/Continuously Operating Reference Station (NTRIP/CORS) [73] to stream GNSS data over networks. If the receivers, which are the source of the data sent via NTRIP/CORS, are spoofed, a dissemination of this incorrect information will occur [21, § 5.3]. NTP Stratum-1 servers can also use GNSS as a timing source. If that input is attacked, then applications that rely on NTP will be impacted [21, § 5.3].

2.4 Conclusion

In general, threats to GNSS receivers can be broadly classified into two categories: jamming and spoofing, where jamming denies access to GNSS-provided PNT information and spoofing presents incorrect and altered PNT information. Jamming is often easier to perform and detect compared to spoofing, but can be harder to mitigate. Spoofing attacks can be performed in order to achieve different aims such as providing an incorrect position to a receiver, providing an incorrect time to the receiver, altering route planning decisions, and maliciously crafting data contents to attack the receiver's software. These attacks can typically be performed in practice using commercially available devices, so it is important that PNT and CAV manufacturers as well as CAM service providers utilise a combination of techniques to detect and mitigate these threats. In subsequent chapters, a high level description of detection and mitigation techniques adopted in the academic literature are discussed.

3 Threat Detection

In this chapter we present a summary of the detection methods for jamming and spoofing of GNSS signals. Before considering mitigations, it is often necessary to focus on detecting that an attack is underway. Therefore, it is important that robust mechanisms are available to detect GNSS jamming and spoofing.

3.1 GNSS Jamming Detection

The process of detecting a jamming attack is analogous to binary hypothesis testing as shown in Equation (3.1) [67][1].

$$\begin{aligned} H_0 &: \text{absence of jamming interference} \\ H_1 &: \text{presence of jamming interference} \end{aligned} \tag{3.1}$$

This detection problem can be mathematically formulated as:

$$\begin{aligned} H_0 &: y_n = s_{IF}[n] + w[n] && \text{for } n = 0, 1, \ldots, N-1 \\ H_1 &: y_n = s_{IF}[n] + vq[n] + w[n] && \text{for } n = 0, 1, \ldots, N-1 \end{aligned} \tag{3.2}$$

where y_n is the satellite signal sequence obtained from the receiver front-end, $s_{IF}[n]$ is the digital sequence of the downconverted signal at the intermediate frequency (IF), $q[n]$ is the IF digital sequence of the jamming signal, $w[n]$ is noise, and v is an amplitude factor [67]. With respect to the academic literature, the detection problem is typically solved by:

1. Evaluating N samples of the received signal to obtain a test statistic
2. A comparison check with a predefined threshold. This threshold can be determined using classical detection theory or the sequential probability ratio test.

In this report, jamming detection techniques are categorised into: AGC monitoring; digital signal processing/spectral monitoring (DSP/SM); and post correlation-based monitoring [27, 67].

3.1.1 AGC Monitoring

By principle of operation, the AGC adapts its gain depending on the amplitude/power of the received signals. As a jamming detector, the AGC count (g_{AGC}) has been adopted in the literature as a means for selecting the alternate hypothesis (H_1) [74, 75, 76]. Detecting the presence of a jammer using the AGC is carried out by evaluating N samples of g_{AGC} and declaring H_1 when the count is below a threshold (T_h) [67].

$$g_{AGC} < T_h \qquad \text{for } n = 0, 1, \ldots, N-1 \tag{3.3}$$

AGC monitoring techniques can also be implemented using a control logic or look-up-table for selecting the gain of the AGC. In like manner, the receiver compares the power at the output of the analogue to digital converter (A/C) with a predefined reference value [27]. The challenge associated with this approach is the characterisation of the threshold [67].

[1] This can also be adopted in spoofing detection, where the interference is a spoofed satellite signal.

3.1.2 Digital Signal Processing/Spectral Monitoring

These techniques are implemented at the output of the receiver RF front-end. By examining a block of digital samples from the RF front-end, DSP-based detection methods can estimate the frequency components of the incoming samples, compare them with an estimate of the expected power spectral density (PSD) and indicate an early warning if an attack is detected [27, 67]. Most spectral estimation techniques adopted in the academic literature are either based on the frequency-domain methods, such as fast Fourier transform, or time-frequency methods, like the short-time Fourier transform [27, 67]. Nonetheless, time-domain techniques have been adopted as shown in [74, 77]. In time-domain spectral monitoring, the received signal stream is modelled as a random process or assumed to follow a Gaussian distribution. In the presence of a jamming attack, the probability density function of the digital samples deviates from this norm and H_1 can be declared. Other complex methods such as wavelet transforms and quadratic time-frequency representations have also been reported. However, these methods introduce additional computational requirements for increased detection accuracy [27, 67].

3.1.3 Post Correlation-Based Monitoring

In post correlation-based techniques, jamming detection is carried out by inspecting observables such as the C/N_0, which is obtainable from most GNSS receivers. This parameter can be defined as:

$$\frac{C}{N_0} = \frac{C}{N_0 + \alpha J} \tag{3.4}$$

where C is the received signal power, N_0 is the spectral noise density, J is the received jamming power and α is the spectral separation coefficient that accounts for filtering in the GNSS receiver. In the event of a jamming attack, C/N_0 is overestimated by the receiver [67] and the C/N_0 observable reduces. With respect to this observable, the system designer can choose to [67]:

- use individual C/N_0 from specific satellites, generate a statistic and make a decision;
- use a combined approach whereby joint C/N_0 from all tracked satellites is evaluated to generate a statistic and make a decision.

3.2 GNSS Spoofing Detection

Spoofing detection techniques have been categorised differently, as shown in [20, 27, 69, 78]. In this report, the classification presented in [78] has been adopted for detection as well as mitigation, as will be shown in Chapter 4.

3.2.1 Position Solution and Navigation level

This method evaluates the position solution obtained from the GNSS receiver with independent sources such as inertial navigation systems (INSs) [79], Wi-Fi or cellular networks. In the event of an attack, the position estimate from the GNSS receiver will not be consistent with other sources. With respect to urban locations, Wi-Fi networks are becoming ubiquitous and can be opportunistically used for CAV positioning. A recent survey by the authors of this report on how Wi-Fi networks have been adopted in CAV positioning can be found in [3]. It is noteworthy that these wireless networks have inferior accuracy when compared to GNSS, however, they can be used to define confidence regions within which the PVT/PNT solution (obtained from a GNSS receiver) can be evaluated [78]. In addition, INS accumulates positioning errors and can be inefficient at detecting a position drift induced by a spoofing attack [20].

3.2.2 Signal Processing Level

Signal processing methods like signal quality monitoring (SQM) have been adopted in the academic literature for detecting spoofing attacks [80, 81]. This technique is based on the Neyman-Pearson (NP) detection theory, whereby distortions in the correlation peaks can be identified. In order to use this method, metrics that characterise the signal, such as the Delta test and Ratio test, can be evaluated against a predefined threshold. A combination of these metrics has also been investigated in the academic literature; a recent survey by the authors of this report presents a survey of SQM and other detection techniques [5]. Other methods within this category are [78]:

- Antenna-based (spatial filtering)
- Consistency checks of the code and phase rates
- Power based methods
  - AGC monitoring [82]
  - C/N_0 monitoring
  - Absolute power monitoring
  - Receiver power variation
  - L1 and L2 power comparison
- Machine learning [83, 84]
- Time of arrival discrimination
  - PRN code and data bit latency
  - L1/L2 signals relative delay

3.2.3 Multipronged Spoofing Detection

Since a single spoofing technique might not be able detect sophisticated spoofing attacks, multiple techniques can be combined to provide robust spoofing detection [69, 85]. For example, correlation-based methods can be combined with received power monitoring [69]. A multipronged approach is presented in [86], where the authors carry out signal power, measurement, navigation message and position tests to determine a spoofing attack. Another example can be found in [87] where auxiliary peak tracking and navigation message inspection are combined. With respect to fusing the outcome of multiple detection methods, [88] investigated the use of the Dempster-Shafer theory for evidence combination.

3.3 Conclusions

With current state-of-the-art, it is evident that a multifaceted approach is required for jointly detecting GNSS attacks such as jamming and spoofing. Whereas detecting a jamming attack can be fairly straightforward as the receiver loses lock and the attack can be inferred to be in progress or have occurred, spoofing detection on the other hand can be difficult if the threat actor has the required technical knowledge and is in proximity to the target receiver. It is thus essential that GNSS OEMs continue to invest in joint jamming and spoofing detection mechanisms for GNSS chipsets. With respect to CAM service providers, an overlay detection layer can also be included in the system design for increased robustness of autonomous vehicles.

4 Threat Mitigation

Jamming and spoofing attacks can be mitigated using diverse means as shown in this chapter. In the following section, mitigation techniques adopted in the academic literature are presented. It is worthwhile to note that some of these techniques have already been adopted by GNSS receiver OEMs [89, 90]. However, it is important to test the efficacy of the mitigations implemented by the OEMs, which first requires an understanding of the mitigation techniques and their limitations.

4.1 GNSS Jamming Mitigation

The jamming interference mitigation techniques presented in this section are classified using [66]. A combination of multiple techniques results in a more robust mitigation strategy; more details can be found in [27, 66, 67].

4.1.1 External Aiding — Inertial Systems

GNSS and INS are complementary, as they have different pros and cons [11]. INS is typically based on the dead-reckoning method, whereby an inertial measurement unit (IMU), such as an accelerometer [91] and gyroscope, are used to measure angular velocity and linear acceleration. With information on the orientation, position and velocity of the target device known, this method employs kinematic equations to estimate the position of a target device. Whereas this method is immune to jamming, as it does not involve RF signals, it accumulates the positioning error over time [92]. In Figure 4.1, a generic block diagram of GNSS/INS integration is presented [11]. Depending on how the corrections are integrated, the type of GNSS measurements used, the integration algorithm and how the GNSS receiver is aided by the INS, the following integration architectures can be found in the academic literature [11, 66]:

- Loosely coupled: The PVT solution from the GNSS receiver is fed into the integration algorithm. This approach is easy to implement as it is independent of the GNSS and INS navigation functions. This architecture requires the GNSS receiver to track at least four satellites concurrently [66].
- Tightly coupled: The pseudorange, pseudorange-rate, and delta pseudo-range from the GNSS receiver are fed into the integration algorithm. This approach conceptualises the GNSS receiver as a sensor device.
- Deeply coupled: This approach combines GNSS/INS integration and GNSS signal tracking and formulates this into an estimation problem with an optimal solution. In a deeply coupled system, the outputs of the correlator (I and Q) are used as direct inputs in the integration algorithm, which is usually based on a Bayes filter [11, 66].

4.1.2 Antenna-Based (Spatial Filtering)

These techniques are based on antenna array processing, which requires that the GNSS receiver is equipped with multiple receiving antennas, optimally spaced to minimise coupling. With antenna arrays, the target device can adopt filtering techniques that shape the reception antennas' beam pattern [66, 93]. This is achieved by weighting the output of the individual antennas and

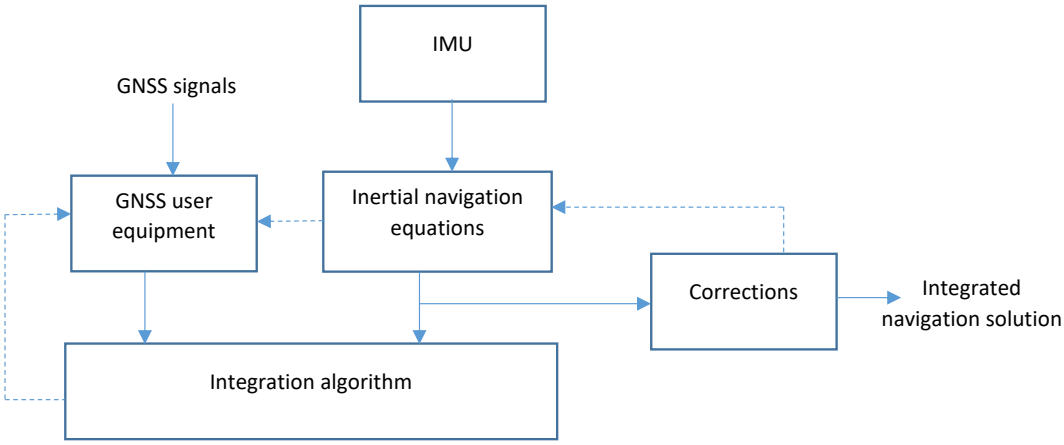


Figure 4.1: Generic architecture for GNSS/INS integration (adapted from [11])

optimally combining them using suitable array processing algorithms. In the event of a jamming attack, the receiver should be able to steer the antenna pattern/beam towards authentic signals and generate nulls towards the jamming signal. This technique has been adopted in the academic literature as shown in [94, 95]. Since the angle-of-arrival (AoA) of satellite signals is not known *a priori* [66], the power inversion method is usually adopted in GNSS receivers [96]. This adaptive array processing technique does not require information about the desired signal or its arrival angle [96].

4.1.3 Signal Conditioning (Time-Frequency)

Similar to DSP-related jamming detection techniques, frequency-domain, time-domain and joint time-frequency-domain algorithms can be used to mitigate jamming in GNSS receivers. A widely used time-domain technique is *pulse blanking*. This method zeros the signal as soon as the signal amplitude exceeds a predefined threshold. Frequency-domain algorithms, such as the adaptive notch filter, have also been adopted in mitigating narrowband interference [27, 97]. The notch filter is designed to attenuate signals within a specific frequency band. Whereas frequency- and time-domain techniques have gained wide usage, they both have limitations. Joint mitigation algorithms optimally combine time-domain pulse blanking and frequency-domain notch filtering. With respect to selecting the most suitable interference mitigation technique, readers can consult [66] for guidelines and operating domains.

4.1.4 Receiver-Based — Vector Tracking

Rather than individual tracking loops in conventional GNSS receivers, vector tracking processes the satellite channels together using a Bayes filter, such as the Kalman filter. This technique also uses the same filter to estimate the user position. This technique is known to enhance the performance of GNSS receivers operating in degraded conditions, such as during intentional jamming [66]. This method has also been used to mitigate non-cyber GNSS attacks, such as multipath radio propagation [98]. Other techniques in this domain are active signal cancellation and multi-constellation receivers [97].

4.2 GNSS Spoofing Mitigation

Various classifications for spoofing countermeasures exist in the literature [20, 27, 69, 78]. The structure adopted in this report is based on [78], with some input from other classifications. Note

that some techniques presented here provide hybrid mitigations for both jamming and spoofing simultaneously (as seen in [93, 99]). These techniques are usually based on antenna array signal processing, and typically introduce additional complexity to the target receiver.

4.2.1 Position Solution and Navigation Level

The receiver autonomous integrity monitoring (RAIM) method is based on fault detection exclusion whereby *faulty* GNSS signals are detected and excluded. In order for this process to occur, the receiver needs to be able to obtain a group of self-consistent measurements [100]. This technique is adopted in most commercially available GNSS receivers. Whereas this technique can be efficient when only one or two spoofed signals exist, its performance is severely impaired when there are more spoofed signals. This is due to RAIM decreasing the residuals by rejecting the authentic signals [78].

4.2.2 Signal Processing Level

Since it is almost impossible for the spoofer to completely suppress the authentic signal at the RF front-end of the target, vestigial signal defence mechanisms can be adopted at the expense of increased receiver complexity [10, 78]. In the event of a spoofing attack, the receiver can use additional tracking channels to track authentic and spoofed signals. Antenna-based (spatial filtering) can also be included in this domain [93, 101, 102, 103].

4.2.3 Data Bit Level Cryptographic Approaches

Cryptographic-based authentication schemes can be used to verify the authenticity of the source of the GNSS data stream. These techniques are in part used by existing GNSS service providers to supply data of a higher accuracy, typically for military purposes [8, § 7.3]. Such signals are encrypted in order to protect the confidentiality of the message, however, in combination with other primitives the authenticity of the message can be checked. Without the secret keys used to encrypt the data, an adversary will be unable to successfully spoof this signal.

For GNSS data that is intended to be used for unrestricted purposes, there is no need to provide confidentiality (and hence encyrpt the signal) as the data is intended for all recipients. Instead, authentication techniques should be used instead. A summary of the different primitives that can be used to provide different security properties is shown in Table 4.1. There are three main options (i) symmetric key message authentication code (MAC), (ii) asymmetric key digital signatures, and (iii) symmetric key techniques that achieve similar properties to asymmetric key signatures (e.g., TESLA [104]). These techniques allow spoofing to both be detected and mitigated, because a spoofed signal will be unable to provide a signature or MAC that will allow a signal to be successfully authenticated, allowing that spoofed data to be discarded.

A similar decision has recently been needed to be made for vehicle-to-vehicle communication, where digital signatures which require public key infrastructure (PKI) have been chosen to provide message authentication without confidentiality [105, 106].

In 2020, Galileo will enable its Open Service Navigation Message Authentication (OS-NMA) based on TESLA to authenticate messages [107]. Future plans for Galileo involve switching to a code-based authentication scheme [108, Slide 18]. Other backwards compatible authentication approaches have also been proposed for GPS [109], such as IS-AGT-100 [110] which uses an additional signal to supply a digital certificate which can be verified using the public key of the transmitting satellite. Considering which techniques to use to perform authentication is important, as different approaches have different computation costs [111], which impact the speed at which GNSS messages can be authenticated.

However, message authentication is not a panacea for all classes of spoofing attacks. For example, replay attacks such as those via a repeater, will include valid authentication information and will be successfully authenticated [112]. GNSS receivers will need to use additional techniques to detect and mitigate these classes of attacks.

Security Property	Cryptographic Primitive			
	Hash	(H)MAC	Digital Signature	Encryption
Integrity	✓	✓	✓	✗
Authenticity	✗	✓	✓	✗
Non-repudiation	✗	✗	✓	✗
Confidentiality	✗	✗	✗	✓

Table 4.1: Obtaining security properties via different techniques

4.3 Software Attack Mitigation

Software attack mitigations follow similar recommendations to Security Development Lifecycle (SDL) recommendations for software [113, 114]. In this case, certain aspects need to be altered due to the GNSS receivers being part of an automotive embedded system. For example, delivering firmware updates to mitigate vulnerabilities may be difficult for GNSS receivers in general. As vehicles have the capability to be connected to systems which they were previously isolated from, software updates [115] are becoming the norm hence potentially facilitate an improved SDL process.

There are many recommendations that can be made to improve software-level security. For example, three of Microsoft's recommended actions are to: (i) perform threat modelling to identify vulnerabilities, determine risk and identify mitigations, (ii) perform static analysis of the source code, and (iii) perform runtime dynamic testing of the deployed implementation.

A static analysis approach may be to verify the correctness of the implementation according to a specification. This would include ensuring validation of all received data and ensuring that state transitions within a program are correct and do not violate security properties.

Performing an analysis of the implementation typically requires access to internal details of a system which are not always available to security testers, so a black box approach to performing runtime testing under adversarial conditions additionally needs to be performed to assess resilience to attack [21]. Issues identified by these runtime tests can be mitigated by reporting to the supplier and deploying their developed mitigations, or implementing mitigations in the system that do not require modifying a GNSS receiver. For example, one mitigation would be to perform sensor fusion with vehicular sensors to mitigate the loss of GNSS information in the case of jamming, or incorrect GNSS information in the case of spoofing. An example was presented in [116], where spoofing and jamming detection was performed using a wide array of sensors available on an Android phone to detect anomalies. Sensors used included: the accelerometer, GNSS gain and Android's network location provider system which uses cell tower and Wi-Fi signals. The vehicle's IMU, odometry [117] and cellular [118] systems can also support a vehicle performing dead reckoning to mitigate jammed or spoofed GNSS signals.

4.3.1 Impracticality of Exhaustive Testing

Each GPS satellite sends 5 subframes, which are 300 bits long, providing 1500 bits of data in total to a GPS receiver over 12.5 min. Much of this data is redundant as each subframe contains ten 30 bit words of which 24 bits are data and 6 bits are parity. Each subframe also begins with two

words used to provide an initial preamble [8, § 7.4]. This data needs to be parsed and validated by a GPS receiver and if performed incorrectly may lead to security vulnerabilities.

One popular technique for detecting bugs in parsing and input validation is fuzzing, where potentially invalid random data is provided instead of valid data. In [21] the authors concluded that fuzzing GNSS was impractical because of (i) the long period of time it takes for data to be received and (ii) the black box nature of GNSS receivers. Fuzzing works for other systems due to the ability to test a large number of inputs in a short period of time to detect bugs. As it takes 12.5 min for all 1500 bits to be received, it would take $2^{1500} \times 12.5$ min to test all possible combinations.

An alternate approach is to not fuzz all of the message and to instead focus on the most important bits. An analysis of GPS receiver software was performed in [119] where the authors used the Spirent GSS7000 GNSS simulator to perform attacks on GPS receivers. Using a sensitivity analysis, three key values (shown in Figure 2.3) in the GPS data stream were identified: Ω_0 (longitude of ascending node of orbit plane at weekly epoch), $\dot{\Omega}$ (rate of right ascension) and $\sqrt{A}$ (square root of semi-major axis). The values these variables were set to in the experimental analysis were chosen by sampling between their minimum and maximum values.

By focusing on the most impactful values of the GPS data stream, exhaustive testing is still impractical. Even if only 24 bits were chosen to be tested, it would take 399 years to test all combinations. Therefore, important values (e.g., $\sqrt{A} = 0$ [21, § 5.1]) need to be identified to be tested instead.

4.4 Conclusions

There has been much theoretical and practical work on developing mitigations for these kinds of attacks against PNT systems, however, there is no individual panacea. Therefore, it is necessary to apply multiple techniques and ensure that their interaction ensures correct functioning. Irrespective of the system design, a robust CAM service would need to ensure attack countermeasures are in place at the RF front end and the receiver software. Moreover, it is also necessary to further understand the practical ability for these techniques to withstand attacks, necessitating testing in real-world environments which can replicate the capabilities of adversaries.

5 Community Experience

As evident in this report and the academic literature, civilian GNSS has become essential in a wide range of vertical and horizontal markets. With the development of CAVs and CAM services, it is evident that GNSS technology will be essential to CAV localisation and situation awareness as well as the realisation of intelligent road transport networks. In order to understand which of our identified threats are currently being performed, are believed to have a high impact and where future effort needs to be focused, we interviewed a range of experts with experience and knowledge of GNSS attacks and automotive cyber-security. This chapter will present the results from these interviews and highlights important issues and future areas for investigation that were raised by the experts interviewed. Also included in this chapter is a summary of the main points raised by the survey participants — these are presented in a non-attributable format — and finally some general conclusions that can be drawn from the comments/opinions that they provided in the course of the survey[1].

5.1 PNT Experts

The survey consisted of 14 core questions seeking opinions on the vulnerabilities, risks, potential attack vectors and possible mitigations from key industry and regulator stake holders with a view to helping optimise an evaluation of the usefulness of a Cyber-Security testbed. Stakeholders interviewed included senior personnel involved in and with a wide experience of PNT systems for CAV, along with a strong knowledge of threats and hazards to space-based PNT systems. Further information about how this set of interviews was performed can be found in Appendix A. The statements below were all made by participants in the interviews that were conducted over the telephone over a one-hour period.

Necessity of PNT and GNSS for CAVs

> “GPS is the only way to have independent time between vehicles . . . There are lessons to learn from the financial sector regarding timestamping of transactions.”

> “GNSS is critical for the *NT* of *PNT* not so much the *P*.”

> “GNSS provides extremely low cost, accurate time, and position and velocity data.”

These interviews highlighted that PNT (and GNSS) are vital for CAV operation. There were some differences in the opinions of the experts with which aspects of PNT are the most important, with some ranking attacks against the supply of position information higher and others ranking timing information higher. The key point is that GNSS provides PNT information to a high accuracy with ease, that GNSS receivers can be attacked, and that there is a need for supplemental sources of this information.

Jamming

> “Jamming becomes a cyber-crime as it is a Denial of Service type of attack.”

[1] We have protected the identity of the respondent in each case and it must be stressed that the statements here reflect the personal opinion of the respondent and are not necessarily the opinion of the organisations they represent.

> PNT needs to be protected with critical infrastructure. The governmental concern that jamming is serious, is apparent from the issue of the new presidential executive order from the US.

> ...also have spent time with a colleague using a jammer detector — we regularly saw alerts for GNSS interference. I am also aware of the STRIKE 3 project in which 1000s of occurrences have been captured.

> Risk depends on how CAV PNT systems are designed and set up. Lots can be done to design-in resilience — continued operation with integrity flag — so it is a difficult question. More jamming than spoofing is carried out today, but occurrences of both are rising. It is difficult to be predict whether one or the other will dominate.

Jamming attacks are practical to perform on GNSS receivers, with the current view being that this kind of attack is currently more commonly performed compared to spoofing. Jamming has been identified as a serious threat and there are initiatives from the USA [120] to identify threats, perform testing and develop mitigations for GNSS.

Spoofing

> Spoofing will become easier. I'd anticipate that integrity monitoring or inherent integrity / authentication techniques will need to improve.

> Many receivers we tested had anti-spoof technology, but could still be spoofed.

> Spoofing is more insidious, more technically interesting, harder to detect and counter, but in numerical terms probably not a greater threat.

> Spoofing is a sinister problem, which is being taken more and more seriously. It is a much more dangerous threat than jamming.

Spoofing attacks are currently believed to be harder to perform than jamming attacks, although there is an expectation that this difficulty will decrease in the future. These attacks are also more difficult to detect and mitigate compared to jamming attacks, due to the need for spoofed signals to share characteristics with GNSS signals in order to be successful. There was some disagreement whether spoofing or jamming could create greater impacts. Experience of the participants highlighted that even when GNSS receivers advertised spoofing resiliency, it was still possible to spoof them under certain circumstances. This highlights the need for more standardised testing of these devices.

Timing

> The time aspect is always important, location depends on where the vehicle ends up being — a fall back must exist — e.g., in an area where positioning signals are difficult to receive, they cannot just hand back control directly to the driver.

The importance of Precision Timing in CAVs is often understated, as is the reliance on GNSS as the source of Precision Time data. There will be a need to have independent timing between vehicles and also to have timestamped transactions. This is likely to pose additional cyber-security challenges.

Personal Experience

> I have witnessed collateral effects from a GPS spoofer/jammer — affected airport — even taxi's going to and from the airport. Location was jumping from airport to city and taxis were losing their place in line as a result.

> I personally experienced disruption to mobile phones at ION GNSS 2017 due to a leaky simulator, resulting in an incorrect phone time. SMS and email time-stamps were wrong, creating confusion due to wrongly sequenced messaging. Some phones completely died.

> The threat is very real — we have gathered over 100 records of incidents/attacks, which were a mix of deliberate and accidental incidents, covering all areas from accidental leakage, to malfunctioning devices and fraud.

> I haven't seen any real examples yet of spoofing or meaconing, but criminals are exploiting technology so that kind of manipulation is definitely going to happen in future.

> The current status of the resiliency of all PNT systems is not enough. Every receiver we tested could be penetrated easily with the tools we used. Many of the receivers we tested had anti-spoof technology, but could still be spoofed.

The threats to PNT are real. Examples had been seen by survey participants, at least one survey participant has been consulted on several real-world attacks, all others have seen or are aware of real-world examples of jamming and spoofing, with more examples of jamming than spoofing.

Adversaries

> Criminals favour very broad *hedgehog* RF jammers — and take out everything they can. Criminals don't target the signals, but the devices.

> The risk of anti-collision measures being used by hi-jackers is also high.

> There will be a growth in use of SDR technology to attack CAVs due to its high availability and low-cost SDRs are already being used for a variety of RF cyber-attacks e.g., in car thefts based on keyless systems.

> PNT Security is a high priority for cyber-security. Eventually all cars will be connected to the internet. This should be a high priority, especially now with the rapid growth in this sector.

> Spoofing will be increasingly used to obtain money, e.g., fraud from drivers spoofing to get money for journeys. The more autonomous we become, the bigger the threat to PNT security.

Criminals or malicious actors may target CAV PNT systems in unexpected ways. Experience shows that criminals target devices rather than signals (e.g., use of multi-band jammers to take out every device they can). Which means that as part of a testbed, a wide variety of OEM equipment will need to be testable.

The increasing use of SDR technology is a real concern. SDRs are low cost and are an excellent example of how evolving technology can dramatically lower the barriers to potential attackers. Code that can turn an SDR into a malicious tool is widely available to download from the internet, and the SDR can be configured to perform a wide variety of wireless attacks on CAVs. Examples include their use as a GPS spoofer and as a tool to implement attacks on wireless key fobs.

Fusion With Other PNT Sources

> I would like to see other signals/alternative technologies to aid and support navigation which would improve resilience over time.

> There may be different ways to enhance PNT with visual experience, for example, but PNT is the only absolute source of position and timing, and we believe this limitation will remain at least for the near future.

> Sensor fusion and PNT data need to be secured. Systems trying to be autonomous are reliant on GPS/GNSS. We believe there will always be PNT in the makeup of autonomous vehicles.

As GNSS receivers are vulnerable to jamming and spoofing attacks it is important for vehicular systems to fuse sensor input from sources that are not vulnerable to the attacks performed against GNSS signals. Some of these sensors are currently available within vehicles, however, there may also be a need for additional infrastructure to support supplying additional information.

Management and Methodology

> Measuring and understanding integrity is important.

> Responsible disclosure of incidents is essential.

> No individual element gives enough resilience in isolation . . . structured requirements, test, risk assessments using available data . . . innovation will happen with an intelligent structured approach. Honesty/ethics type design questions. Objectives: test drive or more?

> There are a few experts who understand resilience, but no quantitative or structured assessments exist today. There is a need for a methodology to define requirements/performance and to look at different attack vectors, which could quickly reach conclusion on system exposure and decide whether risks are significant. Smartphones have obviously carried this out — fantastic example of where this is done — they don't worry about the level of accuracy, but quick delivery/availability are the key factors. Human factors are also important, especially with high levels of automation.

> We have developed a list of cyber-attacks that can't be got rid of — characteristics of system, data driven, conflicting objectives for data. The space available for a cyber-attack is infinite, and can't be prioritised in terms of attack. We have to look at every layer throughout the system, and need to understand the full characteristics and model to understand what is outside the model. We have to do a better job in articulating the problem.

Improvements or standardisation of approaches to measuring resiliency to attacks and reporting those attacks are needed. This means testbeds need to have the connections to receive information from relevant attack detection organisations (such as in the STRIKE3 project) and also have the ability to report novel vulnerabilities to relevant bodies (such as government departments). The way that resilience is measured also needs to have standardised methodologies developed and used. This may need to be a continuous assessment (instead of a one-time activity performed at a testbed) over the combination of national infrastructure and active vehicles on roads.

Future

> The more autonomous we become the bigger the threat to PNT security.

> Aim for as much resilience as possible, but *resilience* can mean acceptance of incorrect results which is not a good thing. There is a sweet spot between usability and denial of service. We really need to arrive at a probability of failure for the safety case, but how do we do that for a cyber-attack?

> We believe there are ways to counteract, but we are not there yet, although there is good technology out there to protect GNSS. We need to take advantage of the technology.

A variety of future aspects of PNT cyber-security for CAVs were raised by the participants. There were three main themes: (i) the impact of autonomy, (ii) the need for resilience and (iii) the need to improve implemented mitigations. These points highlight the need for future work testing and developing mitigations of GNSS and PNT for CAVs.

5.2 Cyber-security Experts

These interviews were performed by staff from the University of Warwick, where participants were asked to respond to 11 prompting questions on PNT threats pertaining to CAV systems and recommendations to improve CAV cyber-security. Those interviewed had a diverse background including: transport, maritime, communications and infrastructure. Ethical approval was granted for these interviews to be performed with the reference BSREC 61/19-20. Further information on how this set of interviews was performed can be found in Appendix B.

Jamming

> For jamming, it is very easy to get access to this device. However, this depends on the scale and impact of the attack. It is different if you want to jam a small area compared to several miles of highway.

Spoofing

> Spoofing is becoming a big problem where nation states jam and spoof GNSS. Spoofing has now evolved from the military domain into civilian usage (general hacker domain) with the usage of SDR platforms.

Timing

> Spoofing involves both timing and position, as we cannot spoof position without timing and timing without positioning. So it is sophisticated.

> Timing attacks can be dangerous. But attacks that target position and navigation for CAVs are critical.

> There's a perceived lack of awareness of where time information comes from. For time-synchronization of CAVs to infrastructure, timing attacks become a big challenge.

> An attack on timing is the most severe, given that substantial devices rely on timing information.

> There is an over-reliance on GNSS for scheduling and sequencing, accurate timing is required. But to what accuracy? These are things that needs to be investigated.

The interviewees highlighted both the difficulty of spoofing time, but also the capability to deliver threats with a high impact by doing so. An impact on spoofing of position can be more obvious than an impact on spoofing of time.

Threats

> Attack severity depends on how much the CAV relies on the location. If absolute trust is placed on GNSS/PNT, then these kind of attacks are severe. With the current state of the automobiles, this isn't a severe problem yet.

> Likelihood has to come from the motivation of an adversary and their attack's desired effect. The context in which the vehicle is operating and attacked is important.

> The objective of the attacker needs to be determined before evaluating the severity. The mindset of the adversary is essential to determine the severity or effects. All could be low or high impact. Objectives can vary widely.

A common theme when discussing the potential severity of either jamming or spoofing attacks against GNSS, was that the severity is highly dependant on the context in which the attack takes place. This context includes, the CAV, the CAV's operational state, and the adversary's goals and motivations. As the scenarios in which a CAV operates will be highly dynamic, it will be important to consider this when assessing the likelihood and impact of these threats.

Facilities and Testing

> A test facility is key, both a real-world and synthetic capability (such as a digital twin) to create conditions that represent an attack that might be used on a system.

> Performance degradation can be characterised using a simulator. This also needs to factor in the environment in question.

> Access to a national database of testing facilities would be useful due to the difficulties of performing practical testing without a Faraday cage.

> Environment space required outside in order to avoid impacting users of GNSS/PNT services.

> A full risk hazard assessment needs to be performed, so a better understanding is obtained and used for testing CAV PNTs.

> Test in the wild, the reality of testing in the field is essential. A blended fleet needs to be investigated to ascertain the level of assurance required. Failure mode and effects analysis (FMEA) testing needs to take place. Cyber-resilience and security need to be studied and investigated in equal measures.

The need for either more testing facilities, or an increase in their discoverability was highlighted by the participants. There is a need for facilities with a wide range of testing capabilities for CAM systems (such as for shipping and drones) and not solely for CAV systems. These facilities need to support a spectrum of testing from simulation to real-world over-the-air (OTA) testing. The other aspect that was highlighted was the need to include environmental considerations both when performing testing with simulators, and when performing OTA testing in anechoic chambers. This is necessary to improve the real-world relevance of this testing.

> Consider architectures of different vehicle manufactures as well as different PNT implementations and architectures. Different architectures would be hacked in different ways. Testing needs to be manufacturer agnostic and should be able to apply to any manufacturer architecture.

> Consider interactions with PNT and road side infrastructure.

> There are many stand alone testing platforms. A cross platform needs to be investigated.

> Vehicles need to be tested as a system-of-systems

When performing testing it is important to not solely focus on the impact of the vehicle, but also consider indirect impacts from attacks on infrastructure and other interacting systems. This testing needs to be designed in a generic way to facilitate testing arbitrary combinations of equipment from different OEMs. Test facilities will also need to be able to undertake testing from a wide system-of-systems perspective, which will include testing additional equipment that is connected to or interacts with a vehicle.

Personnel

> It is not only about investing in the technology and the infrastructure, but also about the people and the process. Therefore, you need to have the technology in place and then you need to train people on how to use the technology and understand the differences in the technologies applied. You also want to train people in matters of raising awareness on what they are doing and what problems could appear, so they can report any abnormality that they identify.

While technology can be key in detecting and mitigating attacks on GNSS systems, it is important to consider the human element of securing a complex system. While mandating a human-in-the-loop for all autonomous activities may be undesirable, it may be suitable for highly trained staff to monitor events at a higher level. Such staff would need to apply suitable training and intuition to identify attacks that autonomous systems may not be looking for.

Equipment

> Equipment to perform GNSS attacks is available on the internet. Legislation across borders needs to be investigated. Detecting shipment of these devices needs to be in place.

> The equipment needed to perform an attack depends at which level the attack is carried out. Attacks at satellite level will be difficult. Localised effects are easy using technology that is available.

Equipment to perform jamming and spoofing attacks on GNSS receivers is easily available. Restricting access to these devices is difficult, as they can be easy to assemble, or make use of hardware (such as SDRs) with other valid and legal purposes.

Fusion with Alternate Sensors

> Improve robustness and resilience by having an alternative positioning system. Vehicles already have IMU and other sensors to cover the position when GNSS signal is lost, and then they use mapping software which results in a good quality level of the position. But for fully autonomous vehicles, accuracy is more important, so a higher level of robustness to spoofing is required.

> A fail-safe needs to be implemented. An alternative true PNT needs to be available, some version of truth that is firewalled to other sensor inputs.

> How the CAV is set up will impact the attack likelihood. There are many other sensors (CCTV, LIDAR, and others), which will assist with maintaining position.

> A single sensor input can't be used to detect an event. Multiple sensors needs to adopted.

One key point regarding the resilience of a PNT system is the need to fuse information with alternate sensors. As a vehicle will not only have access to GNSS to provide PNT information, other sensors such as IMUs, LIDAR, and local clocks need to be used to provide redundancy when GNSS is under attack and vice versa. However, this raises further considerations as the weight of trust between sensors needs to evaluated. Future testbeds need to be able to support verifying the ability of these sensors to provide redundancy and also be able to test concurrent attacks against multiple sensors.

Mitigations

When considering mitigations, the interviewees highlighted the need to consider a wide variety of aspects of the technology in use, its complexity and applications from other domains.

> Safety and security need to be investigated hand-in-hand.

> Some principles can be applied relating to cyber-resilience and integrity, whereby there is a redundancy and diversity of systems. The CAV is a high integrity system that needs to be fail-safe, fail-secure, fail-operational in equal measure. In addition, how quick the system recovers from an attack needs to be investigated. So a highly resilient system is required.

> A vehicle needs to be considered as a holistic entity, not just as individual functional systems. Data and context of data (information) need to be investigated (pattern of communication). The car is a rich information resource and it needs to be investigated as such.

> CAVs are part of an intelligent transport network (ITS). So security of the rest of the ITS needs to be studied. A CAV can also be an attack vector to an ITS and this also needs to be studied. The security of a CAV can not be addressed in isolation.

From expert opinions, it is evident that security in CAVs cannot be considered in isolation. It is vital that safety and operational aspects of a vehicle are also considered when providing security. This is difficult due to the complexity of the system in which a CAV operates. Testing facilities need to provide suitable space to ensure security mechanisms do not impact safety and also ways to test how quickly a CAV can recover from attack. As these attacks may be persistent, some permanent facilities are required to perform long-term testing. Testing facilities will also need to provide infrastructure on which attacks can be emulated, so the impact on a CAV can be examined.

> Process and procedure need to be investigated regarding how OEMs communicate notifications and alarms (warning systems).

Also of importance are how detected attacks are reported. Depending on the level of autonomy of the vehicle, the driver may be expected to take control if a cyber-attack sufficiently blinds a vehicle and prevents it from making safe decisions. How these alarms are reported to the diver (and/or passengers) of the vehicle are important to consider so that the appropriate action can be taken. This may require additional education of drivers so that they are aware of the correct procedures.

> “PNT mitigations from quantum technologies should also be considered. These technologies can be complementary.”

Finally, mitigations either inspired by or using other relevant technologies could be considered in the future. An example given was in terms of quantum technologies; outputs from the quantum-enabled maritime navigation workshop held at Loughborough University [121] may be relevant to CAV PNT systems.

5.3 Conclusions

The opinions provided by the experts interviewed highlighted that jamming, spoofing and timing attacks are practical for an attacker to perform and can lead to impacts on a vehicle. Perspectives from the participants on vulnerabilities of PNT in CAVs appear to depend on the variety of industry perspectives. Some differences were observed between the groups of participants, those with automotive and PNT expertise had observed the impact of attacks personally, and those with a cyber-security expertise highlighted the need for facilities to perform the testing. In terms of considering adversaries, automotive experts focused on a small number of specific attackers, whereas cyber-security experts raised the importance of the context (in which a CAV system operates) in determining an attacker's motivations and attack techniques. Such differences in focus are useful to identify and motivate the need for further collaboration between these communities.

We have made some general conclusions in areas where general (if not unanimous) agreement was observed by participants in the survey. However, the conclusions expressed below do not necessarily reflect the views of all of the individual participants or of the organisations they represent.

- The threats to CAV PNT cyber-security should be dealt with as a high priority matter.
- There is a need to develop a common and consistent methodology for assessing PNT cyber-security risks.
- There is a need to consider the impact of sensor fusion on testing attacks and developing mitigations.
- The responsible disclosure of incidents and discovered vulnerabilities is essential in the commercial sector, especially for safety and liability-critical applications such as CAVs.
- There is a risk that manufacturers expect a certain level of performance from the devices they procure, hence do not test them for resilience and robustness themselves.
- The newly announced National Timing Centre in the UK has the aim to improve “security and resilience, communication and implementation of new technologies, and pave the way for trusted time and frequency across the country” [122]. The UK CAV industry may find it advantageous to work with the National Timing Centre to develop new methods for delivering and securing the precise timing data needed by CAVs.

- There is room for greater co-ordination/co-operation between agencies and industry. The STRIKE 3 project [123] has shown that the collection, storage and characterisation of real world interference threats is possible, but the sharing and reporting mechanisms are currently fragmented and un-coordinated.
- The range of opinions given by all survey participants suggests that a future public round table involving CAV cyber-security stakeholders from industry, government, academia, regulators and institutes could prove to be very beneficial to all parties involved in CAV PNT system cyber-security.

Specifications for CAV PNT testbeds and further recommendations based on the outcomes of these interviews are made in Report 2 [2].

6 Lab2Live Attack Emulation and Testing

In this chapter, we describe the testing that was performed as well as their results. The attacks performed on the GNSS receivers investigated was guided by the academic literature and expert opinions from conducted interviews. Before we describe the tests, we address issues relating to the legal restrictions of performing these tests.

6.1 Legality

In the UK there are two main pieces of legislation that need to be considered when performing the type of tests (jamming and spoofing of GNSS signals) envisaged in this feasibility study. The first and most important is Section 68 of The Wireless Telegraphy Act 2006, which deems jamming and spoofing of signals illegal in the UK. For this study, therefore, we have either performed indoor OTA tests inside an anechoic chamber, or outdoor non-OTA tests during which the jamming or spoofing signal was added to the authentic signal through coaxial cables and a high-power RF combiner, with negligible spurious emissions. The second piece of legislation is The Electromagnetic Compatibility Regulations 2016, SI 2016/1091 which restricts the import and sale of jammers and requires that apparatuses must not cause excessive interference. The attack emulators used in this feasibility study are test signal generators and their transmissions are strictly contained either over coaxial cable or within an environment that do not allow for RF leakage, such as an anechoic chamber or a Faraday cage.

Currently, the regulator for the UK communications services (Ofcom) only allows GNSS jamming testing by the Ministry of Defence, and considers it a crime if carried out by anyone else [124, § 68]. To use any radio transmitting device in the UK, it will need to either be licensed, or have a specific licence exemption. Ofcom's most related licence products are the GNSS repeater licence and the Innovation and trial license[1]. The latter is a non-operational licence for testing, research or demonstration, and is also recommended for work carried out inside a Faraday-shielded chamber. The detailed information regarding these pieces of legislation should be fed into LR43 [126, p. 99] on the Zenzic Roadmap, and used to simplify the process of obtaining relevant licences to perform testing or to document under which circumstances licences are not required.

An alternate approach to mitigate the legal issues surrounding testing of licensed frequencies is to up or downconvert GNSS frequencies before transmission and after reception. In [71], GNSS frequencies were downconverted from 1575.42 MHz to 915 MHz (the US ISM band[2]). Other applications using these bands (such as for communication), must tolerate any interference generated from collocated technologies within the band. A downside to this technique is that the downconversion could change aspects of the signal. This may lead to attacks and defences not precisely matching those an attacker would use to attack the system and the techniques the system could use to defend against those attacks. Extensive research is required to determine the efficacy of this approach.

[1] `https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/non-operational-licences`

[2] The ISM bands are for industrial, scientific and medical applications

6.2 Test Methods and Devices

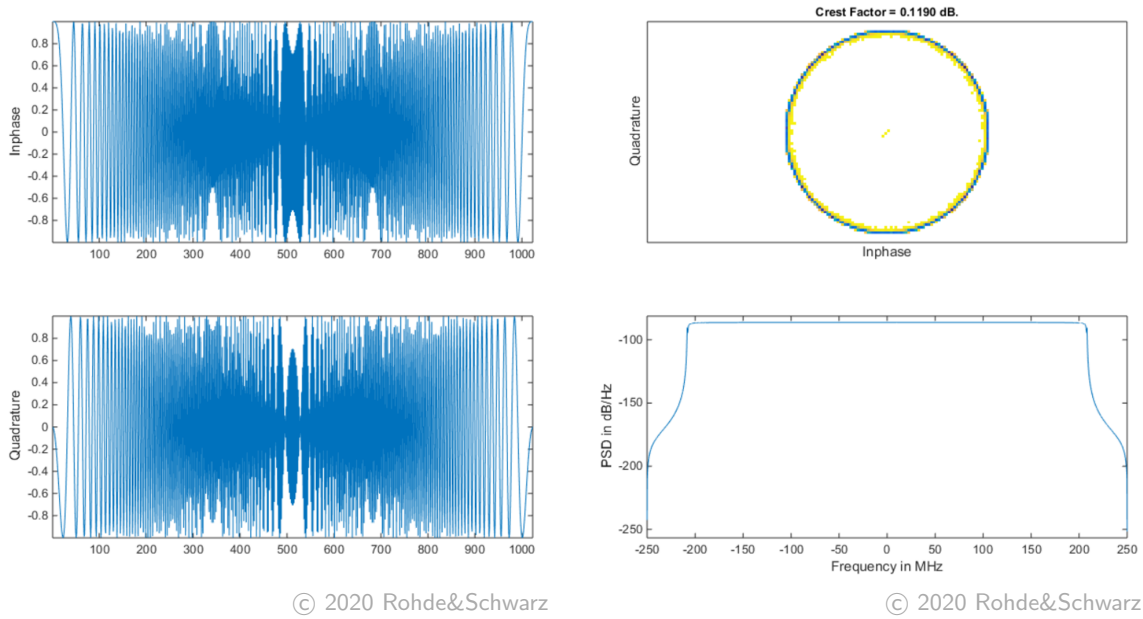
Due to the protocol required in officially obtaining a jammer (PPD) and the timeline of this feasibility study, a vector signal generator (VSG) was used to replicate intentional EM interference (also referred to as jamming) and a hardware-software platform from Spirent was used to emulate other attacks. These devices were used in both laboratory and field tests as discussed in this chapter for testing commercially available PNT devices.

6.2.1 PNT Attack Emulator (Spirent)

Figure 6.1: Positioning, Navigation and Timing Attack Emulator

The PNT Attack Emulator (PNTAE) comprises a hardware-software suite of multi-frequency, multi-GNSS RF constellation simulation and emulation, with true performance under all dynamic conditions, and can be placed into CAVs at any stage of conception in either laboratory or real world scenarios. The PNTAE's main functionality is replicating to the CAV under test, GNSS live sky as is, or under any possible cyber-attack situation, from accidental interference to sophisticated spoofing, offset timing etc. It uses correct and accurate techniques/models to derive satellite constellation and navigation data parameters commensurate with the applicable interface control documents. The software allows for fully automatic and propagated generation of precise satellite orbital data, ephemerides and almanac. Moreover, the PNTAE's stable clock, low latency remote control and extreme flexibility allowing reconfiguration during live, real-world deployment. The PNTAE is able to replicate any currently known PNT attack and those being developed and/or hypothesised in the cyber-security community through the generation of real signals that would be incident on the target CAVs' antennas. This optional OTA capability, which includes the emulation of attenuation, fading, delay, Doppler effects etc., allows the PNTAE to work with any CAV, and requires no knowledge of the VUT.

6.2.2 Vector Signal Generator and Signal and Spectrum Analyser (Rohde & Schwarz)



(a) I and Q characteristics for a sequence of 1023 samples

(b) Crest factor and PSD using a sequence of 120,000 samples and a bandwidth of 500 MHz

Figure 6.2: Representative FZC-waveform characteristics

The jamming tests require a VSG that is able to generate a signal that controllably overpowers the received live-sky GNSS signals. As highlighted in Table 1.1, current GNSS frequencies span the range from 1164 MHz (GPS L5 / Galileo E5a) to 1610 MHz (GLONASS L1OF). Individual bands associated with single constellations can be effectively jammed with a VSG in CW-mode, as will be detailed in Section 6.3. In our real-world tests, a constant amplitude, zero auto-correlation jamming signal was generated, based on a Frank–Zadoff–Chu (FZC) mathematical sequence. This signal is graphically depicted in Figure 6.2a. The signal bandwidth adopted in the test was 500 MHz as shown in Figure 6.2b. This bandwidth covers the entire GNSS frequency range. As will be described later, output power levels up to 25 dBm can be required to jam all SV's in view. A device that supports these technical requirements is displayed in Figure 6.3a.

(a) SMBV100B VSG capable of generating waveforms up to 6 GHz

(b) FSV3007 Signal and Spectrum Analyser operating up to 7.5 GHz

Figure 6.3: Signal generating and analysing devices used during jamming tests

In order to observe, record and investigate in detail the power spectrum that is seen by a GNSS receiver, or generated by a VSG, a signal and spectrum analyser is used. Ideally, its specifications match those of the VSG, having broadband capability over a wide frequency range, and a low displayed averaged noise level of $-164\,\mathrm{dBm/Hz}$. Thus, supporting very sensitive signal detection. A device that supports these technical requirements is displayed in Figure 6.3b.

6.2.3 Uninterruptible Power Supply

During real-world, mobile, field tests, testing equipment requires a safe and reliable power source. As commercial power inverters in-between a potential electric-powered CAV's battery and the equipment might not support the required power levels, an uninterruptible power supply with battery extension (SMX2200RMHV2U + SMX120RMBP2U) was used. With this approach, the testing equipment were deployed inside the VUT to run for a full working day.

6.2.4 Receivers under Test

In this project, three receivers were tested and evaluated for a range of GNSS attacks. These receivers are introduced in Table 6.1. With respect to performance and robustness, these devices cover a broad spectrum of receivers with diverse implementations of patented technologies. With respect to GNSS receiver OEM and CAV manufacturers, Receiver C is known to be used in Level-4 CAVs [3], hence evaluated in more detail in this project.

Receiver	OEM	Ref	Features
A	u-blox NEO-M8T	[128]	Multi-constellation, NMEA 0183
B	Septentrio AsteRx-UAS	[129]	Multi-band, Multi-constellation, NMEA 0183, RTK ready*
C	Swift NAV Piksi Multi	[130]	Multi-band, Multi-constellation, NMEA 0183, RTK enabled*

Table 6.1: Test receiver mapping

* This technology provides enhanced positioning accuracy by evaluating the carrier of the GNSS signals.

6.3 Lab-based Jamming Tests

The jamming-to-signal-power ratio (J/S) should be measured across the specified bandwidth [65, 131], where J is the jamming signal power and S is the GNSS signal power from the GNSS simulator/PNTAE. In this study, jamming tests were carried out in an Anacheoic chamber located at WMG. The tests were conducted by connecting the receivers under test via RF cables and a combiner. The RF combiner allows for a test procedure that facilitates overlaying of authentic and interference signals. This approach allows for reproducibility and repeatability of the work carried out. With respect to jamming tests, the following performance metrics were evaluated:

- Time to first fix (TTFF) — Nominal: This is the time taken by the receiver to determine its location under open sky condition and no interference.
- Time to first fix (TTFF) — After jamming: This is the time taken by the receiver to regain its position information after an interference (or jamming attack) has occurred.

[3] Readers can refer to the SAE standard document J3016 which details the levels of driving automation. A graphic can be found in [127]

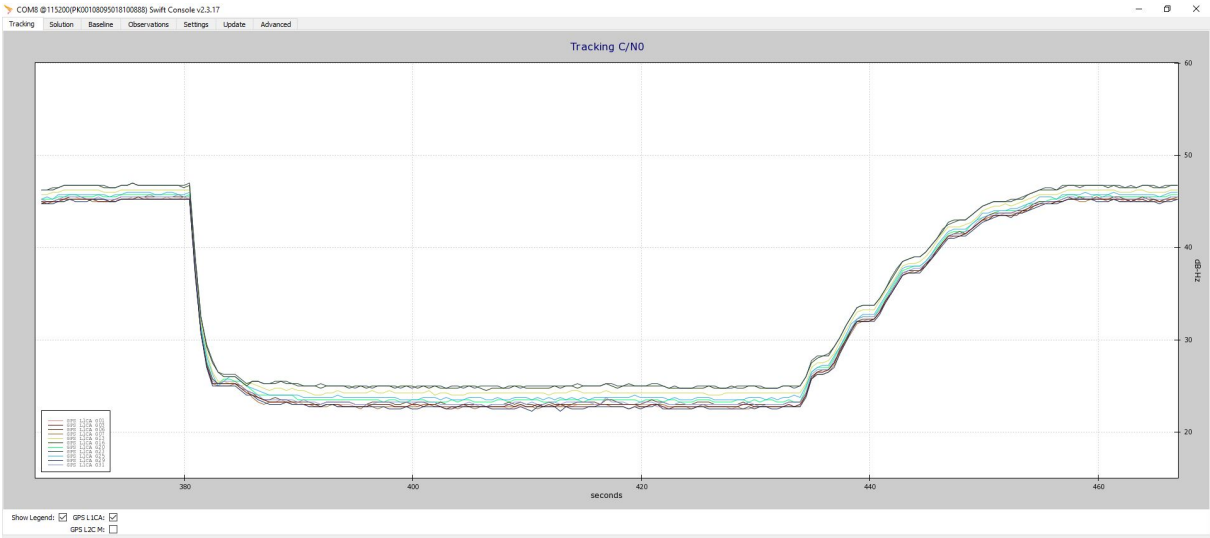


Figure 6.4: Receiver-C behaviour under low CW jamming power (J/S = 20 dB)

- Number of visible SVs: This is the number of satellites visible to the receiver front-end during an interference or jamming attack. It is expected that the receiver is able to *see* fewer satellites as the satellite signals become masked by the jamming signal.[4]

In order to emulate jamming in the laboratory, a VSG was used to generate CW jamming signals with the centre frequency set to GPS L1.

6.3.1 TTFF for Jamming with CW Jamming

In line with the literature, a maximum J/S of 90 dB was used to evaluate the TTFF. The nominal TTFF was obtained by connecting the receivers to a Spirent GNSS simulator running a live scenario and observing the time required by the receiver to obtain a fix. To simulate a jamming attack, the VSG was turned ON for 90 seconds. The TTFF with and after a CW jamming attack is summarised in Table 6.2.

Receiver	TTFF-Nominal (s)	TTFF-After (s)
A	33	3.2
B	30	3.5
C	34	3.5

Table 6.2: TTFF CW jamming test performance

6.3.2 Sensitivity & Satellite Visibility with CW Jamming

With respect to the individual devices tested in the laboratory, the tracking sensitivities are approximated below:

- Receiver A: J/S = 52 dB.
- Receiver B: J/S = 48 dB.

[4]This value rapidly reduces as interference increases. For a 3D fix, the receiver requires 4 visible SVs

- Receiver C: J/S < 20 dB. For the single constellation-single frequency CW jamming attack, this receiver lost its PVT solution at the minimum J/S specified in this test as shown in Figure 6.4. This is because the C/N_0 of the satellites in view at the receiver did not meet the minimum requirement for tracking or estimating a PVT solution.

Further increase in the jamming signal power (J) causes a DoS as the receiver can not produce a PVT solution. The base values of the C/N_0 and No. of SVs (without interference) are shown in Table 6.3.

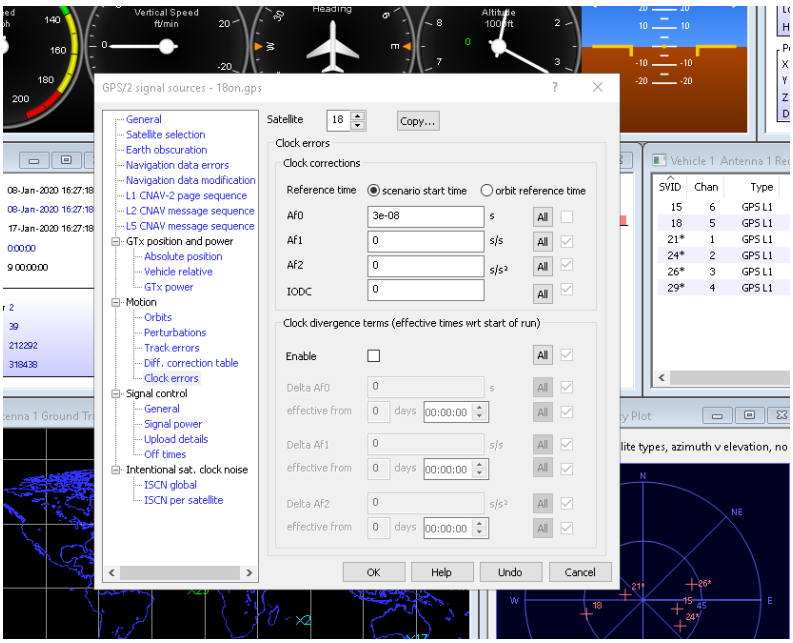
Receiver	C/N_0 (dB-Hz)	No. of SVs
A	43.42	11
B	42.46	11
C	44.22	11

Table 6.3: Base values for the different receivers tested

6.4 Lab-based Spoofing and Emulation Tests

In this subsection, laboratory spoofing tests carried out using Receiver-C and Spirent's PNTAE are described. This simulation technique uses two vehicles and a single RF output. By increasing the signal strength of the spoofer-vehicle 2 (v2), the receiver drifts from the true position (located at vehicle 1 (v1) to the spoofed position at v2.

6.4.1 Tests with Corrupt GNSS NAV Data



© 2020 Spirent Communications Plc

Figure 6.5: SimGEN GPS signal source showing Clock Error Parameters

- SV Clock Bias: Clock corrections for GNSSs are transmitted in the Navigation Data message of the satellites in a given constellation. These corrections characterise the drift experienced by the on board satellite clock over time [132]. In the clock bias test, a clock

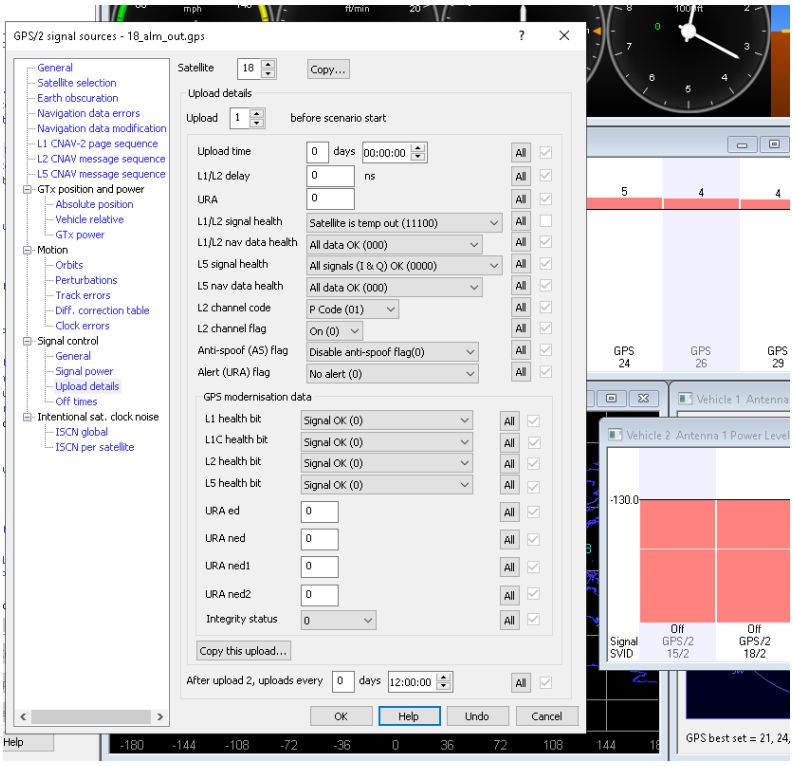
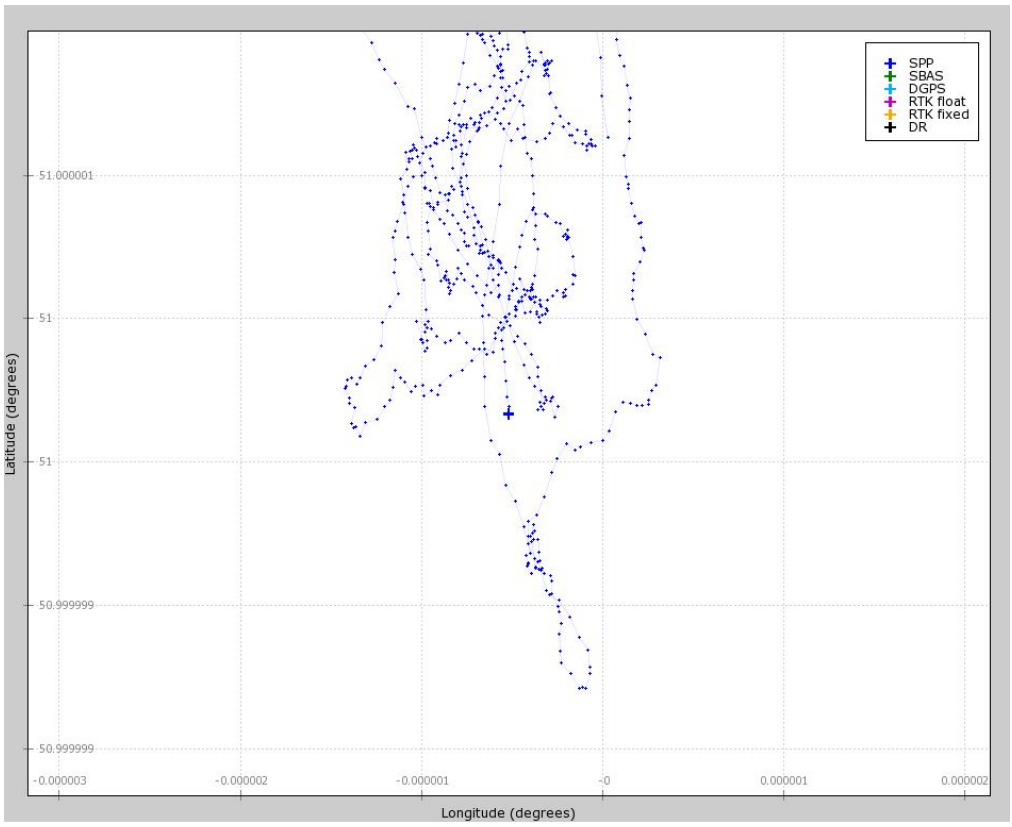


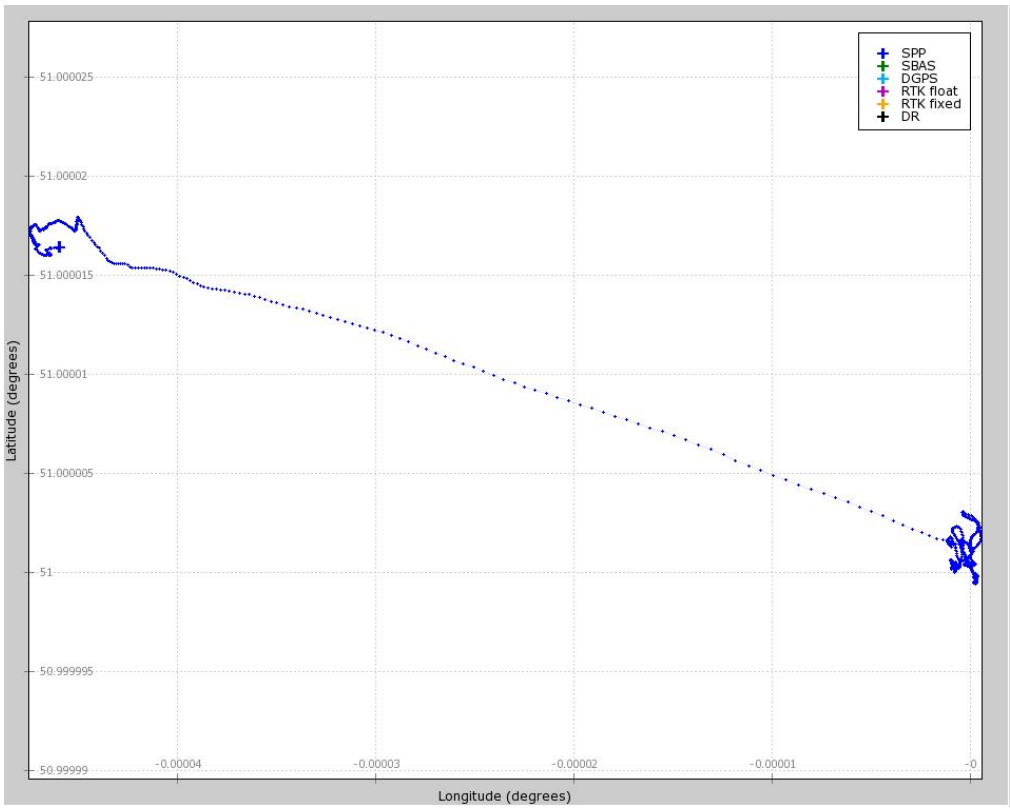
Figure 6.6: SimGEN GPS signal source showing satellite upload information

error parameter (*Af0*) for GPS SV 18 (as shown in Figure 6.5) was modified. *Af0* is a first order clock correction error parameter and it is analogous to introducing a pseudorange error on that SV [132]. With respect to other SVs in the constellation, the *Af0* parameter was set to 0. In Figure 6.7a, the true position (N 51° E 0°) of Receiver C is shown. From this figure, it can be seen that the receiver is precisely located at the required location specified in SimGEN (± 0.000 001°/15 cm). The test without the spoofed SV is run for approximately 2 minutes and the spoofed SV is turned ON for 20 seconds. In Figure 6.7b, the location of the receiver when the spoofed SV is turned ON is shown. This attack causes the receiver to drift approximately 2 m (longitude) and 1 m (latitude), thus introducing errors in the location estimated by the receiver. From this test, it can be shown that a spoofed SV can cause severe errors in the position estimation.

- SV Health Flag: This test investigates how spoofed NAV data can alter the performance of a receiver. In this test, SV 18 is spoofed such that the health flag of the SV is set to *temp out* as shown in Figure 6.6. This dialog box can be used to specify satellite upload from ground stations [132]. The expected outcome of this attack is that the SV is not tracked or used for estimating the PVT at the receiver. In situations where the receiver has 3–4 satellites in view, this attack can cause the receiver to lose 3D fix if 4 satellites were in view or results into a DoS as the receiver is unable to compute a position due to very few satellites in view. In Figure 6.8a, the observation table of Receiver C is shown. In normal operation, GPS SV 18 is present. After the receiver has obtained a position fix from the GNSS simulator, the spoofed signal is turned ON for 60 seconds. In Figure 6.8b, the observation table during the spoofing attack shows that the receiver is not tracking SV 18.

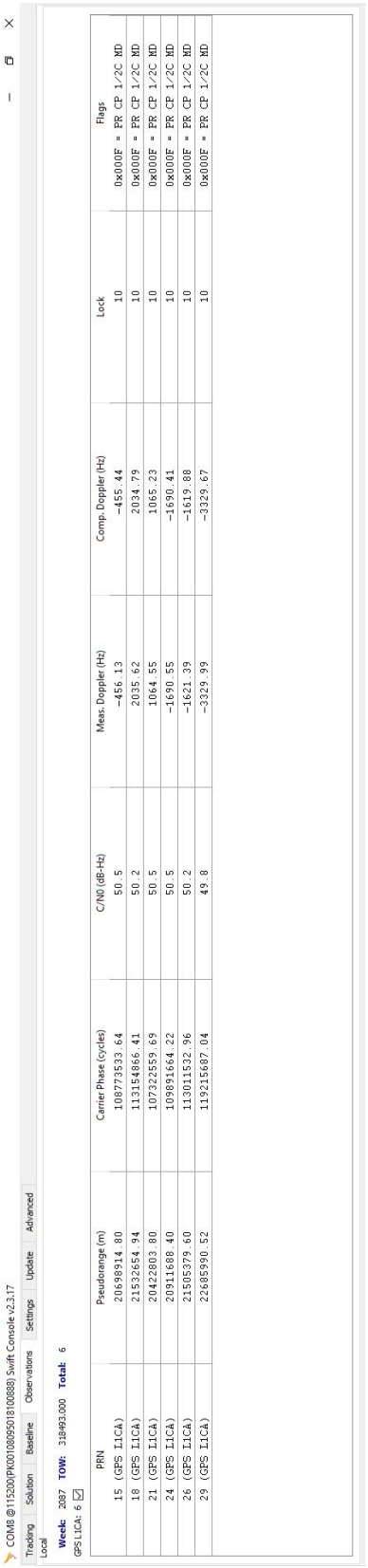


(a) True position of receiver



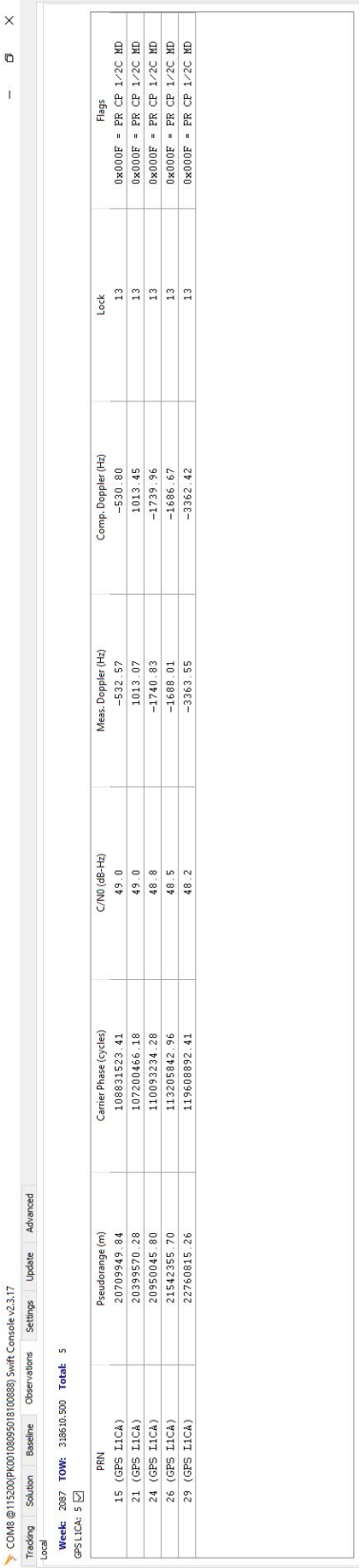
(b) Receiver position as a result of Spoofed SV clock bias

Figure 6.7: Effect of clock bias on position



PRN	Pseudorange (m)	Carrier Phase (cycles)	C/N0 (dB-Hz)	Meas. Doppler (Hz)	Comp. Doppler (Hz)	Lock	Flags
15 (GPS L1CA)	20698914.80	108773533.64	50.5	-456.13	-455.44	10	0x000F = PR CP 1/2C MD
18 (GPS L1CA)	21532654.94	113154866.41	50.2	2035.62	2034.79	10	0x000F = PR CP 1/2C MD
21 (GPS L1CA)	20422803.80	107322559.69	50.5	1064.55	1065.23	10	0x000F = PR CP 1/2C MD
24 (GPS L1CA)	20911688.40	109891664.22	50.5	-1690.55	-1690.41	10	0x000F = PR CP 1/2C MD
26 (GPS L1CA)	21505379.60	113011532.96	50.2	-1621.39	-1619.88	10	0x000F = PR CP 1/2C MD
29 (GPS L1CA)	22685990.52	119215687.04	49.8	-3329.99	-3329.67	10	0x000F = PR CP 1/2C MD

(a) Normal



PRN	Pseudorange (m)	Carrier Phase (cycles)	C/N0 (dB-Hz)	Meas. Doppler (Hz)	Comp. Doppler (Hz)	Lock	Flags
15 (GPS L1CA)	20709949.84	108831523.41	49.0	-532.57	-530.80	13	0x000F = PR CP 1/2C MD
21 (GPS L1CA)	20399570.28	107200466.18	49.0	1013.07	1013.45	13	0x000F = PR CP 1/2C MD
24 (GPS L1CA)	20950045.80	110093234.28	48.8	-1740.83	-1739.96	13	0x000F = PR CP 1/2C MD
26 (GPS L1CA)	21542355.70	113205842.96	48.5	-1688.01	-1686.67	13	0x000F = PR CP 1/2C MD
29 (GPS L1CA)	22760815.26	119608892.41	48.2	-3363.55	-3362.42	13	0x000F = PR CP 1/2C MD

(b) During Attack

Figure 6.8: Observation table of receiver under test

6.4.2 Tests with False Position

Static

In this test, the receiver's intended true position is specified in SimGEN. After the receiver has obtained a position fix, the spoofing attack is initiated. In this spoofing attack, the false position is obtained by slowly increasing the power of the spoofed signal. The nominal received power of the simulated true position is $-128.5\,\mathrm{dBm}$. After the receiver has obtained a position fix, the spoofing signal is initiated 3 minutes into the scenario. At regular intervals of 60 seconds, the power of the spoofed receiver location in the simulator is increased by $1\,\mathrm{dBm}$ from -138.5 to $-118.5\,\mathrm{dBm}$. The true position of the receiver as specified in the simulator is the same as Figure 6.7a. As the power of the spoofed signal increases, the position estimated by Receiver C varies and drifts away from the true position as shown in Figure 6.9a. At 75% maximum spoofing power, the receiver position drifts to about $30\,\mathrm{m}$ East and $2.5\,\mathrm{m}$ North, whereas at maximum spoofing power of $-118.5\,\mathrm{dBm}$, the receiver position is approximately $50\,\mathrm{m}$ East as shown in Figure 6.9b.

Dynamic trajectory

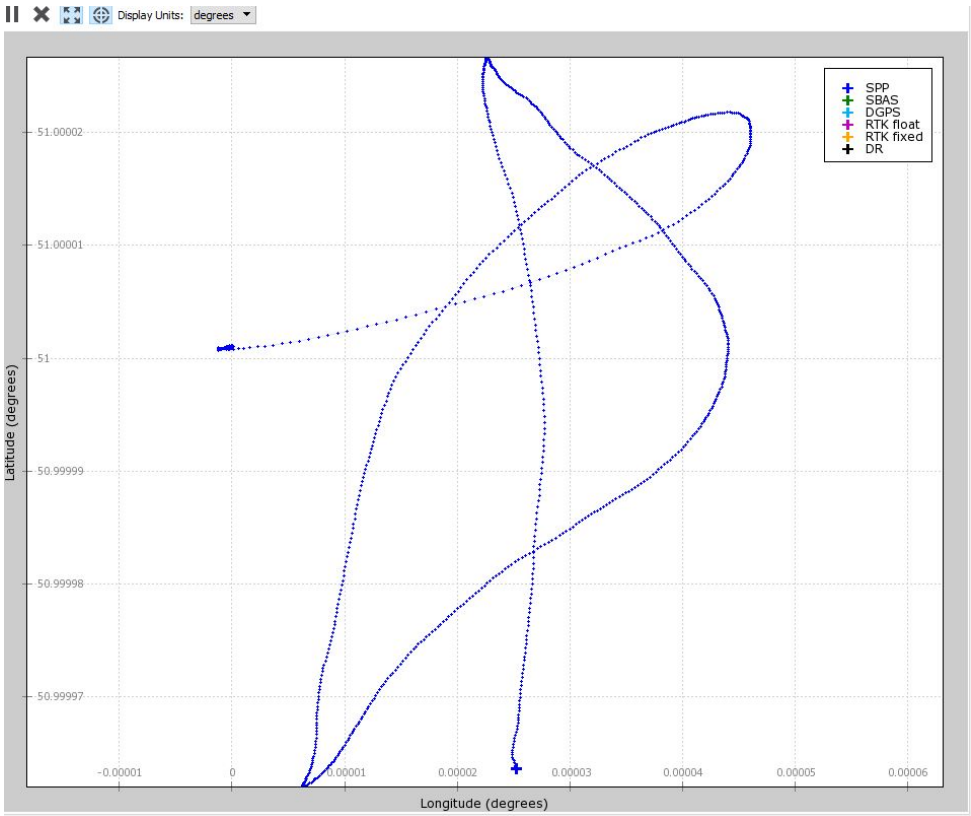
This scenario is similar to the Static test, however the receiver under test is specified as a moving land vehicle in the simulator. The spoofed signal emulates this attack by reusing the true trajectory but $100\,\mathrm{m}$ South of the path travelled by the vehicle/receiver under test (v1). After the receiver obtains a fix, the spoofing signal is introduced 90 seconds into the simulation. Both vehicles are set to travel at a constant speed of $10\,\mathrm{m\,s^{-1}}$. In Figure 6.10a the trajectory of the vehicle before an attack is shown. From Figure 6.10b, it can be seen that the receiver loses lock just after the attack commences as the trajectory now deduced from the composite signal (Authentic and Spoofed) slightly varies from the smooth straight path prior to attack. In advanced applications, as shown in Chapter 2, the temporary loss of lock can indicate that a spoofing (or jam and spoof) attack has occurred.

6.5 Real-World, Live-Sky Tests

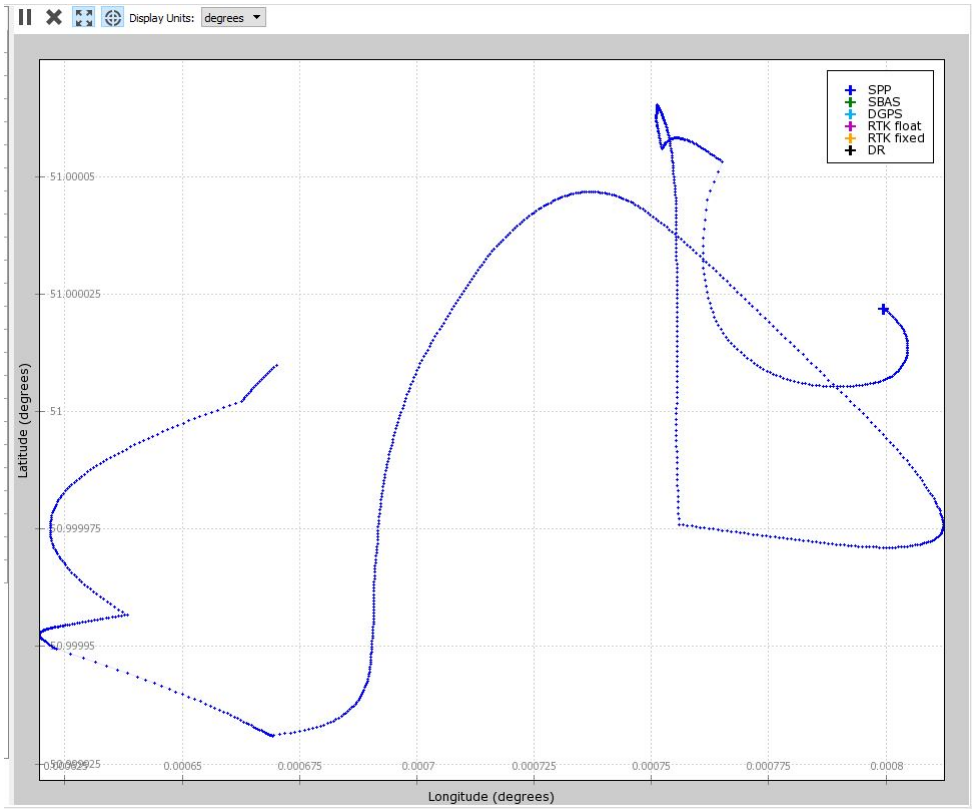
The live testing on the vehicle under test (VUT) was carried out at the Wellesbourne Campus of the University of Warwick. In Figure 6.11a, the VUT is shown at one of the way points of the pre-mapped trajectory. The test site resembles a car parking space with brick buildings on one side and Life Sciences research units on the other. In Figure 6.11b, the trajectory mapped for the VUT is shown. For the entire trajectory, the GNSS receiver in the VUT was able to access all the constellations presented in Chapter 1 from its live-sky view.

The lab-based tests presented in Section 6.3 were based on a single constellation and single frequency — GPS L1. As an unknown GNSS receiver inside a black box CAV might be able to work across a wide range of constellations and frequencies, the most effective method to cause a DoS attack for the VUT, is through jamming the entire GNSS bandwidth (1150 to 1650 MHz) for the constellations present using an FZC sequence, as previously described in Section 6.2.2. Commercially available PPDs (as shown in Section 2.1) typically broadcast a similar type of jamming signals and are thus credible threat actors to GNSS/PNT. Because of legality reasons presented in Section 6.1, a conducted approach was used, with shielded cables conveying the RF power from the VSG into an RF combiner, which fed the GNSS receiver in the VUT[5]. A summary of the observed C/N_0 and satellite visibility for increasing jamming power is presented in Table 6.4.

[5]During this test, RF leakage from the cables and combiner was negligible, as no spurious emissions were detected during testing

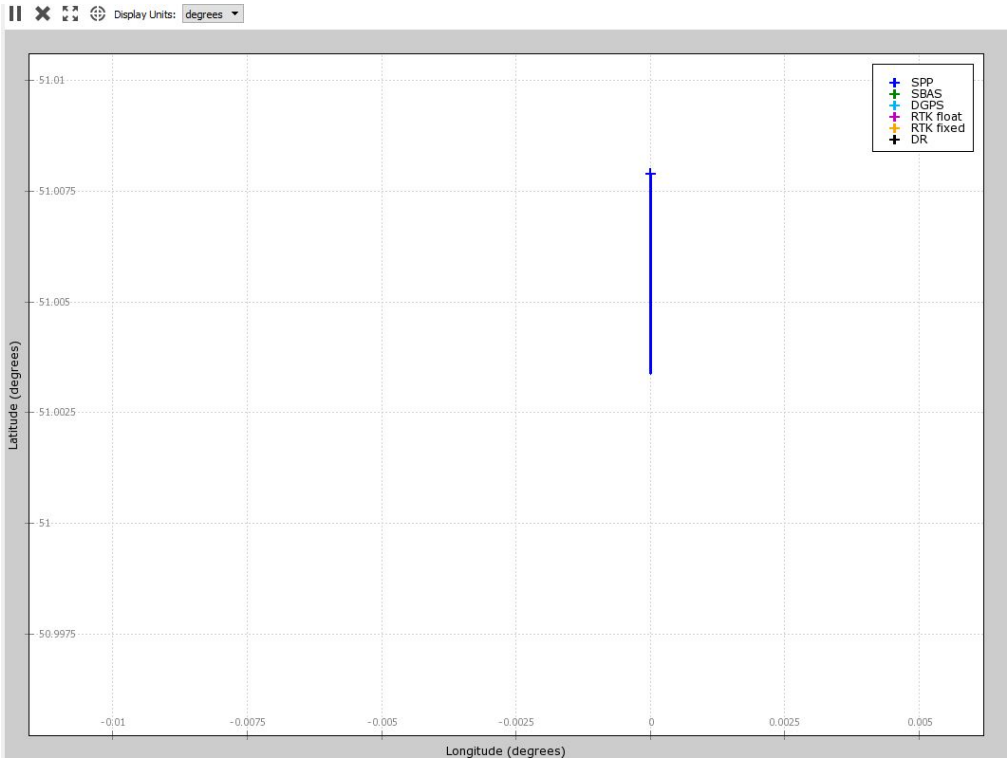


(a) Receiver position varying with spoofing signal

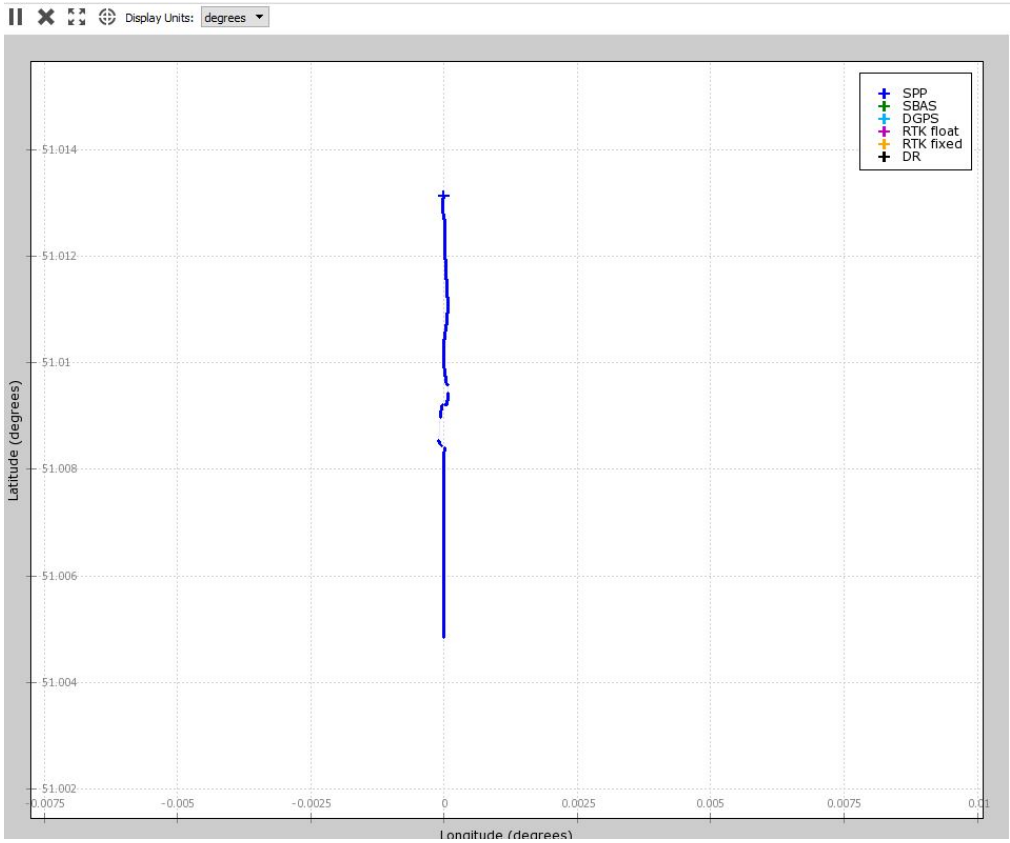


(b) Receiver position with spoofing signal at full power

Figure 6.9: Effect of spoofing signal power



(a) Receiver trajectory



(b) Receiver trajectory during attack

Figure 6.10: Effect of a spoofed location

PSD (dBnW/Hz)	C/N_0 (dB-Hz)	No. of used SVs	Test inference
No interference	46.65	10	Normal operation, similar to lab-based results.
-20 – -17	37.72 – 42.68	9 – 10	Acceptable noise level.
-16 – -7	< 37.72	7 – 8	Attack is detected and live results differ from lab results.
-6 – -2	—	No signal	Similar to signal blockage.

Table 6.4: Summary of FZC jamming and receiver sensitivity (Field)

The most important inference from these real-world jamming tests is that some observations were made that differ substantially from those previously obtained in a lab environment. As at this stage the VUT was tested as a black box CAV, with unrestricted movement, the potential implementation of sensor fusion algorithms in the decision-making process of the CAV's operating system could have played a distinct, but unknown role. The VUT's odometry, inertial sensing and detection sensing systems were all able to obtain live input. Thus, an in-depth system-of-systems testing approach is required if all details and underlying processes need to be understood. Similarly, the live spoofing attacks provided a large amount of observations that differed from the lab-based results, but a technically detailed description is commercially sensitive and beyond the scope of this project, as its focus is on the creation of testing methodologies to determine GNSS resilience and identify vulnerabilities.

© 2020 WMG

(a) VUT at Wellesbourne

Map data © 2020 Google

(b) VUT test trajectory

Figure 6.11: VUT testing performed at Wellesbourne

6.6 Practicality and Realism of Testing

Lab-based device and CAV PNT cyber testing allows for a controlled and partially programmable research methodology, with straightforward to reproduce results. Live testing, on the other hand, involves a number of uncontrollable and unknown parameters which increase the amount of required testing before a well-founded conclusion can be made about a VUT's PNT attack resilience. Moreover, real-world CAV and PNT testing is bounded by legal restrictions, amongst others on spurious RF emissions. Real OTA PNT attacks to a VUT, mimicking most realistically an adversary's capabilities, are thus difficult to achieve without a dedicated, limited-access, large

area, testing facility.

Confirming the results from surveyed academic work previously described in this report, CW and WB jamming attacks are straightforward to perform in practice with high chances on impacting the CAV under attack. Spoofing attacks require more detailed knowledge of the target CAV and sophisticated technical equipment, but allow for more subtle attacks to be performed, with similarly diverse impacts on CAVs. Depending on the goals, motivation and resources of an adversary, spoofing attacks are thus an equally realistic, but less immediate threat.

6.7 Conclusions

Lab-based and real-world, live-sky testing of a device's or CAV's PNT cyber resilience, can provide different, but complementary results that feed into the understanding. Whereas lab-based work is safe, and almost fully controllable and reproducible, live work is completely real, and thus most similar to the conditions the CAV or CAV-subsystem is designed to operate and function in. Because of the versatility of PNT attack scenarios, both lab-based and live testing require labour-intense work to be executed in order to investigate in detail all parameters of interest, and be able to provide a comprehensive and reliable conclusion on a system's PNT-attack resilience. The research methodologies for carrying out both aspects of this work, ideally involve single set-ups that enable their users to carry out comparative and sophisticated tests with minor tweaking of settings, for example, the PNT attack emulator described and used in this presented work.

7 Conclusions

In this chapter, the work carried out in this feasibility study is summarised. Within this chapter, the authors reiterate findings, lessons learnt as well as present recommendations. In addition, avenues for future work based on this study is also highlighted.

7.1 Findings and Discussion

From the academic literature surveyed in this project, as well as the practical Lab2Live work carried out in the course of it, it is evident that robust countermeasures for GNSS vulnerabilities are required for CAVs, CAM and an ITS. Because it is envisaged that the threat landscape will evolve, nation states must invest in addressing cyber-security as it relates to public infrastructure that relies, in full or in part, on GNSS for operation.

With respect to GNSS threats, a wide range of attacks can be carried out both at the physical layer (RF) and software layer. At the physical layer, jamming attacks are prevalent in today's transport networks. Because most of these occurrences are unintentional, threat actors can employ similar commercially available devices for the purpose of disrupting a CAV or CAM. In addition, spoofing attacks are also likely to occur, but in comparison to jamming attacks, require advanced knowledge and fine detailed information about the target. Thus, it can be viewed as a possible attack vector, but not an immediate threat due to technical requirements and know-how. Nonetheless, as described in this report and the surveyed academic literature, the ability of threat actors will evolve with the proliferation of SDR and networking capabilities. Finally, software attacks involve sending crafted packets in order to exploit software vulnerabilities in the GNSS receiver's implementation of calculating the position and time from the NAV data sent by GNSSs. Software attacks can lead to violations of availability or integrity depending on what implementation vulnerabilities are present.

Academia and industry are already developing detection and mitigation techniques to enhance the robustness of GNSS receivers. For detection techniques, these methods are generally based on classical detection theory whereby an observable from the GNSS receiver is characterised and decision-based algorithms are used to decide a null or alternate hypothesis. Nonetheless, as evident in this report and the reviewed literature, jamming and spoofing are usually detected using different techniques, which have different implementation architectures and varying complexity. After detecting a threat, the system can decide to de-weight or disregard data obtained from the affected sensor device (such as a GNSS receiver). The approach employed by the CAV or CAM designer can involve mitigation techniques with which the attack is not only detected, but also its effect is minimised. Similar to the detection techniques, mitigation of jamming and spoofing can be performed using different techniques too. In order to reduce the complexity and enhance the resilience testing, joint mitigation as well as joint detection techniques need to be adopted by OEMs. There has been much work on developing testing methodologies for software systems, however, due to the large input state-space exhaustive testing of all inputs is not possible. Important inputs can be identified with a sensitivity analysis and the crafted values to focus on testing can be chosen based on this analysis.

Whereas the academic literature generally focuses on research and innovations, this project also invited a wide range of experts from the automotive, PNT and cyber-security industries to provide their opinions on CAV GNSS resilience and vulnerabilities. This approach allowed the project team to obtain a different perspective from key industry players on how to address vulnerabilities associated with PNT for CAVs and CAM. In order to maximise the project's

resources with respect to time and logistics, independent surveys were carried out by Spirent and WMG, as WMG required prior approval from the university's scientific research ethics committee. From the interviews, it was evident that CAV PNT attacks such as jamming spoofing are credible, the PNT threat landscape needs to be studied as it evolves and the CAV needs to studied as a system-of-systems.

In regards to CAV PNT cyber resilience testing, a Lab2Live approach has been adopted in this project. The results from the lab-based and real-world, live-sky work provided different, but complementary results. A plethora of ways to execute PNT attack scenarios exists, hence both lab-based and live testing require labour-intense work before all interesting parameters are investigated, and a complete and reliable conclusion on a system's PNT-attack resilience can be provided. In order to carry out the full range of Lab2Live tests, the PNT attack emulator described and used in this presented feasibility study is an ideal component of a robust research methodology.

From the lessons learnt and findings of this project, it can be seen that threat actors, attack vectors, and required countermeasures will evolve. As a result, government and all associated stakeholders need to continue to work together to foster collaborative research and development that is capable of testing and certifying PNT for CAVs and CAM in the UK.

7.2 Future Work

7.2.1 Incentivise Non-GNSS Position and Timing Sources

> The [National Timing Centre] will provide additional resilience for the country's reliance on accurate timing which is currently provided by satellite technologies, and underpins many every day technologies including emergency response systems, 4G/5G mobile networks, communication and broadcast systems, transport, the stock exchange, and the energy grid.
>
> *Department for Business, Energy & Industrial Strategy et al., 2020 [122]*

To reduce a CAV's dependency on GNSS for position and timing, the provision of non-GNSS sources for this information should be incentivised. The Resilient Navigation and Timing Foundation makes this recommendation that other PNT sources should be provided to augment GNSS [133]. One possible source for this resilience may be from the recently announced UK National Timing Centre [122], which will see a network of atomic clocks being used to supplement GNSS-provided timing for aspects of the UK's CNI. Aspects of UK CNI for vehicles should consider using this timing source and potentially relaying it to connected vehicles in order to supplement GNSS.

7.2.2 Infrastructure

The Lab2Live approach described in this report, and the associated research methodology and testing equipment to investigate CAV PNT cyber resilience, allows for simple adaptation to investigate the resilience of CAV-related roadside infrastructure and supporting services, as has also been highlighted by the interviewed experts.

7.2.3 Potential Future Testing and Research Activities

In line with the intended aims and objectives of this short-term feasibility study, additional work is required in the following areas:

- Further understand and characterise likely attack locations and behaviours of threat actors.

- Monitor technology evolution and its effect on the capabilities of threat actors.
- Continue developing a national threat monitoring and reporting capability.
- Characterise attack coverage for different road transport network scenarios.
- Perform testing of system-of-systems with interactions between vehicles and roadside infrastructure.
- Understand the impact of moving vehicles versus the efficacy of stationary GNSS spoofing or jamming attacks.
- Perform testing of the impact of software-based attacks via maliciously crafted data messages on GNSS receivers.
- Grey box testing of CAVs with respect to jamming and spoofing attacks.
- Testing CAVs for the purpose of evaluating the time to recover after after a jamming attack.

With regards to future test facilities in the UK, detailed specifications and recommendations have been provided by the authors in Report 2 [2].

7.2.4 WMG and Spirent

Continuing their joint efforts, Spirent Communications Plc and WMG at the University of Warwick are looking into possibilities to further expand this presented, collaborative feasibility study into new areas of mutual interest.

A Spirent Interviews

Spirent would like to thank the organisations who participated in the survey.

A.1 Spirent PNT Cyber Security Round Table One Interview Guidelines

A.1.1 Guidance to the participants

The interview lead will be responsible for guiding the conversation and conducting most of the interaction with the interviewee. Other participants are asked to observe and take notes according to this guideline and actively contribute to the interview where their subject matter expertise or client relationship is of benefit to the process. While the guideline itself it quite firm, the interview itself may be conducted in a more conversational style to ensure interviewee comfort; therefore, a definite reply to all items of the guideline may be sacrificed to ensure a better flow of the interview.

A.1.2 Core Interview Guideline

- Interview lead to introduce him/herself as well as the participants.
  - Thank the interviewee for this time.
  - Give the interviewee the opportunity to introduce him/herself as well as the role currently occupied within the organisation.
- Introduce the objectives of the call (given that the interviewee is familiar with Spirent, otherwise please introduce Spirent PT).
- Introduce the process as follows: We will go through actors, vulnerabilities, attack vectors and potential mitigations. For each we'd like to discuss and capture your observations and concerns with a view to optimising the evaluation of a potential test bed's usefulness.
- Finally we'd also appreciate open discussion / feedback round at the end of the interview.

A.1.3 Background, Context and Prompting

1. Experience of you and/or company in field of PNT Security?
2. Are you familiar with GNSS specific vulnerabilities?
3. Have you any experience of applying PNT security to CAV or autonomous vehicles?
4. How important do you believe PNT to be for the operation of CAV or autonomous vehicles?
5. Do you believe that GNSS will be a vital component of PNT for CAV and/or autonomous vehicles? Please provide reasoning for your view.
6. Have you experienced any real examples of PNT Cyber attacks — intentional GNSS jamming, intentional GNSS spoofing or intentional cyber attack (man in middle etc) on PNT reporting systems?

7. If *yes* to question 2, can you describe what happened and the impacts caused by the event.
8. Have you experienced any real examples of collateral effects of GNSS jamming or spoofing?
9. If *yes* to question 5, please describe what happened and the impacts caused by the event.
10. If you answered *no* to questions 3 and 5 — i.e. you haven't had any direct experience of PNT cyber attacks — how real do you think the threat is?
    - Is GNSS spoofing more of a threat than GNSS jamming?
    - Does your view of the risk to CAVs through PNT cyber attack, change if you were asked to give an opinion for 5 years in the future? 10+ years?
11. Are cyber attacks on PNT systems through mechanisms other than RF (e.g., MITM) more likely than GNSS spoofing or jamming attacks?
12. Have you conducted any risk assessment of cyber threats to PNT systems?
13. In what ways do you think that the robustness and resilience of existing PNT systems needs to be improved?
14. Looking at CAV Cyber vulnerabilities in general, if you were asked to prioritise the greatest threats to CAV security, where would Cyber attacks against PNT Systems rank?

A.1.4 Follow-on Discussion on Actors

- Nation states
- Terrorists
- Criminals
- Vandals and miscreants
- Accidental
- Other

A.1.5 Follow-on Discussions

Questions asked were dependant on responses previously provided:

- Vulnerabilities of PNT solutions (reliant on GNSS?)
- Attack profiles
- Potential mitigations
- Capabilities and features of a test-bed

A.1.6 Follow-on Closing general discussion

1. Any comments on the value of a standardised approach to measuring and expressing robustness or vulnerability?
2. Any comments on the value of a making a test-bed available that could be used to assess risks?
3. Would you / your organisation be likely to make use of such a facility?
4. Are there any other comments that we've missed?
5. General feedback on Spirent as a service provider.

B Warwick Interviews

B.1 Prompting Questions

1. Do you or your organisation have any experience with cyber security and connected and automated vehicles (CAVs)? If so, please describe your experience.

2. Do you believe position, navigation, and timing (PNT) attacks are credible threats to CAVs and transport mobility?

   - Do you have any experience with PNT attacks?
   - Do you have any experience with PNT simulators or emulators?
     - What methods of attack do you believe can be replicated using them?

3. In terms of a CAV PNT system, do you believe spoofing attacks are likely to occur?

   - If so,
     - How would to expect these spoofing attacks to be performed?
     - What would the impact of these spoofing attacks be on the PNT system?
     - Are likely attacks such as spoofing the same attack methods that would deliver the highest impact?
     - Who are the threat actors you expect to carry out a spoofing attack? What is their motivation for doing so?
   - If not,
     - Why do you believe spoofing is unlikely to occur?

4. In terms of a CAV PNT system, do you believe jamming attacks are likely to occur?

   - If so,
     - How would to expect these jamming attacks to be performed?
     - What would the impact of these jamming attacks be on the PNT system?
     - Are the likely attacks such as jamming the same attack methods that would deliver the highest impact?
     - Who are the threat actors you expect to carry out a jamming attack? What is their motivation for doing so?
   - If not,
     - Why do you believe jamming is unlikely to occur?

5. What equipment would be needed to carry out these attacks? Do you believe it is feasible for relevant threat actors to gain access to it?

6. In your view, which attacks are more likely to target a CAV PNT system? Why?

7. In your view, which attacks are the most sophisticated? Why?

8. How would you rank these types of attack according to severity and possible effects?

   - Spoofing

- Jamming
- (others mentioned)

9. Do you have any recommendations to improve the cyber security of CAV PNT systems?
10. Do you have any recommendations to improve the cyber-security of CAVs in general?
11. What recommendations would you make to facilitate the testing of CAV PNT systems?

Bibliography

[1] E. Adegoke, M. Bradbury, E. Kampert, M. Higgins, T. Watson, P. Jennings, C. Ford, G. Buesnel, and S. Hickling. PNT Cyber Resilience: a Lab2Live Observer Based Approach, Report 1: GNSS Resilience and Identified Vulnerabilities. Technical Report 1, University of Warwick, Coventry, UK, April 2020. Version 1.0.

[2] M. Bradbury, E. Adegoke, E. Kampert, M. Higgins, T. Watson, P. Jennings, C. Ford, G. Buesnel, and S. Hickling. PNT Cyber Resilience: a Lab2Live Observer Based Approach, Report 2: Specifications for Cyber Testing Facilities. Technical Report 2, University of Warwick, Coventry, UK, April 2020. Version 1.0.

[3] E. Adegoke, J. Zidan, E. Kampert, C. R. Ford, S. A. Birrell, and M. D. Higgins. Infrastructure Wi-Fi for connected autonomous vehicle positioning: A review of the state-of-the-art. *Vehicular Communications*, 20: 100185, December 2019. ISSN 2214-2096. doi:10.1016/j.vehcom.2019.100185.

[4] C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello. A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis. *Applied Sciences*, 9(23):5101, November 2019. ISSN 2076-3417. doi:10.3390/app9235101.

[5] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins. GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. *IEEE Access*, pages 1–1, 2020. ISSN 2169-3536. doi:10.1109/ACCESS.2020.2973759.

[6] C. Whitty and M. Walport. *Satellite-derived Time and Position: A Study of Critical Dependencies*. London, UK, 30th January 2018. URL `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf`.

[7] M. Pattinson, S. Lee, Z. Bhuiyan, S. Thombre, V. Manikundalam, and S. Hill. Draft Standards for Receiver Testing Against Threats. Technical Report D4.2, STRIKE3, November 2017. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D42_Test_Standards_v2.0.pdf`. Issue 2.0.

[8] P. J. G. Teunissen and O. Montenbruck, editors. *Springer Handbook of Global Navigation Satellite Systems*. Springer International Publishing, Gewerbestrasse 11, 6330 Cham, Switzerland, first edition, 2017. ISBN 978-3-319-42926-7. doi:10.1007/978-3-319-42928-1.

[9] E. D. Kaplan and C. Hegarty. *Understanding GPS/GNSS: Principles and Applications*. Engineering professional collection. Artech House Publishers, Norwood, MA, USA, third edition, 2017. ISBN 9781630814427.

[10] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and J. Paul 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)*, pages 2314–2325, Savannah, GA, USA, 16–19 September 2008.

[11] P. D. Groves. *Principles of GNSS, inertial, and multi-sensor integrated navigation systems*. Artech House, Norwood, MA, USA, second edition, 2013. ISBN 978-1-60807-005-3.

[12] *GPS Standard Positioning Service (SPS) Performance Standard*. GPS.gov, September 2008. URL `https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf`.

[13] F. van Diggelen and P. Enge. The World's first GPS MOOC and Worldwide Laboratory using Smartphones. In *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation*, ION GNSS+, Tampa, Florida, USA, 14–18 September 2015.

[14] ETSI Technical Committee Intelligent Transport Systems. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Standard Final draft ETSI EN 302 637-2, European Telecommunications Standards Institute, Valbonne, France, January 2019. URL `https://www.etsi.org/deliver/etsi_EN/302600_302699/30263702/01.04.01_30/en_30263702v010401v.pdf`. V1.4.1 (2019-01).

[15] R. Zhang, L. Cao, S. Bao, and J. Tan. A method for connected vehicle trajectory prediction and collision warning algorithm based on V2V communication. *International Journal of Crashworthiness*, 22(1):15–25, 2017. doi:10.1080/13588265.2016.1215584.

[16] ETSI Technical Committee Mobile Standards Group. eCall communications equipment; Conformance to EU vehicle regulations, R&TTE, EMC & LV Directives, and EU regulations for eCall implementation. techreport ETSI TR 102 937, European Telecommunications Standards Institute, Valbonne, France, March 2011. URL `https://www.etsi.org/deliver/etsi_tr/102900_102999/102937/01.01.01_60/tr_102937v010101p.pdf`. V1.1.1 (2011-03).

[17] Z. Chen and B. B. Park. Preceding Vehicle Identification for Cooperative Adaptive Cruise Control Platoon Forming. *IEEE Transactions on Intelligent Transportation Systems*, 21(1):308–320, January 2020. ISSN 1558-0016. doi:10.1109/TITS.2019.2891353.

[18] K. F. Hasan, Y. Feng, and Y. Tian. GNSS Time Synchronization in Vehicular Ad-Hoc Networks: Benefits and Feasibility. *IEEE Transactions on Intelligent Transportation Systems*, 19(12):3915–3924, December 2018. ISSN 1558-0016. doi:10.1109/TITS.2017.2789291.

[19] J. T. Curran, M. Bavaro, P. Closas, and M. Navarro. On the Threat of Systematic Jamming of GNSS. In *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation*, ION GNSS+, pages 313–321, Portland, Oregon, USA, September 2016. ION. doi:10.33012/2016.14672.

[20] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Computing Surveys*, 48(4):64:1–64:31, May 2016. ISSN 0360-0300. doi:10.1145/2897166.

[21] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley. GPS Software Attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 450–461, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450316514. doi:10.1145/2382196.2382245.

[22] Global Navigation Space Systems: reliance and vulnerabilities. London, UK, March 2011. ISBN 1-903496-62-4. URL `https://www.raeng.org.uk/publications/reports/global-navigation-space-systems`.

[23] W. Lechner and S. Baumann. Global navigation satellite systems. *Computers and Electronics in Agriculture*, 2000. ISSN 0168-1699. doi:10.1016/S0168-1699(99)00056-3.

[24] J. W. Betz. Introduction. In *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers*, chapter 1, pages 1–15. Wiley-IEEE Press, November 2015. ISBN 978-1-118-61597-3. doi:10.1002/9781119141167.ch1.

[25] A. E. Süzer and H. Oktal. PRN code correlation in GPS receiver. In *Proceedings of 8th International Conference on Recent Advances in Space Technologies, RAST 2017*, pages 189–193, Istanbul, Turkey, 2017. IEEE. ISBN 9781538616031. doi:10.1109/RAST.2017.8002960.

[26] J. B.-Y. Tsui. *Fundamentals of Global Positioning System Receivers A Software Approach, Second Edition*. Engineering professional collection. John Wiley & Sons Publishers, 2005. ISBN 9780471706472.

[27] R. T. Ioannides, T. Pany, and G. Gibbons. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *Proceedings of the IEEE*, 104(6):1174–1194, June 2016. ISSN 1558-2256. doi:10.1109/JPROC.2016.2535898.

[28] L. Wang, P. D. Groves, and M. K. Ziebart. Multi-constellation GNSS performance evaluation for urban canyons using large virtual reality city models. *Journal of Navigation*, 65(3):459–476, 2012. ISSN 0373-4633. doi:10.1017/S0373463312000082.

[29] V. Sreeja. Impact and mitigation of space weather effects on GNSS receiver performance. *Geoscience Letters*, 3(1):24, August 2016. ISSN 2196-4092. doi:10.1186/s40562-016-0057-0.

[30] M. Pini, E. Falletti, and M. Fantino. Performance Evaluation of C/N0 Estimators Using a Real Time GNSS Software Receiver. In *10th IEEE International Symposium on Spread Spectrum Techniques and Applications*, pages 32–36, Bologna, Italy, 25–28 August 2008. doi:10.1109/ISSSTA.2008.12.

[31] The European Comission and The European GNSS Agency. GNSS Market Report. Technical Report 6, European Global Navigation Satellite Systems Agency (GSA), 2019. URL `https://www.gsa.europa.eu/system/files/reports/market_report_issue_6_v2.pdf`. TS-AB-19-001-EN-N.

[32] C. S. Carrano, C. T. Bridgwood, and K. M. Groves. Impacts of the December 2006 solar radio bursts on the performance of GPS. *Radio Science*, 44(1), 2009. doi:10.1029/2008RS004071.

[33] T. Harrison, K. Johnson, T. G. Roberts, M. Bergethon, and A. Coultrup. Space Threat Assessment 2019. Technical Report, Center for Strategic & International Studies, April 2019. URL https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf.

[34] B. Unal. Cybersecurity of NATO's Space-based Strategic Assets. Technical Report, Chatham House, London, UK, July 2019. URL https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets.

[35] C. Miller and C. Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. In *Black Hat USA*, Las Vegas, NV, USA, 2015. URL http://illmatics.com/Remote%20Car%20Hacking.pdf.

[36] J. Petit, B. Stottelaar, and M. Feiri. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. In *Black Hat Europe*, Amsterdam, Netherlands, 12–15 March 2015.

[37] G. Kar, H. Mustafa, Y. Wang, Y. Chen, W. Xu, M. Gruteser, and T. Vu. Detection of On-Road Vehicles Emanating GPS Interference. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 621–632, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450329576. doi:10.1145/2660267.2660336.

[38] R. Hamilton. GNSS Interference Detection and Mitigation. In *COPUOS Scientific and Technical Subcommittee Meeting*, Vienna, Austria, 7th February 2017. URL https://www.gps.gov/multimedia/presentations/2017/02/COPUOS/hamilton.pdf. Accessed: 2020-01-22.

[39] SENTINEL Project. Report on GNSS Vulnerabilities. Technical report, Chronos Technology Limited, Lydbrook, Gloucestershire, UK, 4th April 2014. URL https://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf.

[40] Out of sight, 27th July 2013. URL https://www.economist.com/international/2013/07/27/out-of-sight. Accessed: 2020-02-04.

[41] *Alert - GPS Tracker Jamming Devices*. Association for Public Service Excellence, Manchester, UK, February 2019. URL https://www.apse.org.uk/apse/index.cfm/members-area/briefings/2019/19-07-alert-gps-tracking-jamming-devices.

[42] L. Kugler. Why GPS Spoofing is a Threat to Companies, Countries. *Commun. ACM*, 60(9):18–19, August 2017. ISSN 0001-0782. doi:10.1145/3121436.

[43] S. Weckert. Google Maps Hacks, 2020. URL http://simonweckert.com/googlemapshacks.html. Accessed: 2020-02-17.

[44] Resilient Navigation and Timing Foundation. *Prioritizing Dangers to the United States from Threats to GPS: Ranking Risks and Proposed Mitigations*. Alexandria, VA, USA, 30th November 2016. URL https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf.

[45] Department for Business, Energy & Industrial Strategy. Satellites and space programmes from 1 January 2021, 9th August 2019. URL https://www.gov.uk/guidance/satellites-and-space-programmes-from-1-january-2021. Accessed: 2020-02-17.

[46] European Commission. Recommendation for a COUNCIL DECISION authorising the opening of negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland, February 2020. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0035. COM/2020/35 final.

[47] C4ADS. Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria. Technical report, C4ADS, Washington, DC, USA, March 2019. URL https://c4ads.org/s/Above-Us-Only-Stars.pdf.

[48] St. Petersburg Drivers Report Strange GPS Problems in City Center. The Moscow Times, 27th December 2016. URL https://themoscowtimes.com/news/drivers-in-st-petersburg-report-gps-problems-in-city-center-56653. Accessed: 2020-01-22.

[49] GPS World. Massive GPS Jamming Attack by North Korea. *GPS World*, 8th May 2012. URL https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/.

[50] North Korea 'jamming GPS signals' near South border. *BBC News*, 1st April 2016. URL https://www.bbc.co.uk/news/world-asia-35940542.

[51] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang. A Practical GPS Location Spoofing Attack in Road Navigation Scenario. In *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, HotMobile '17, pages 85–90, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349079. doi:10.1145/3032970.3032983.

[52] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang. All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1527–1544, Baltimore, MD, August 2018. USENIX Association. ISBN 978-1-939133-04-5. URL `https://www.usenix.org/conference/usenixsecurity18/presentation/zeng`.

[53] C. Maple, M. Bradbury, M. Elsden, H. Cruickshank, H. Yuan, C. Gu, and P. Asuquo. IoT Transport and Mobility Demonstrator: Cyber Security Testing on National Infrastructure. Technical Report, University of Warwick, May 2019. Version 1.0.

[54] E. Steindl, W. Dunkel, A. Hornbostel, C. Hättich, and P. Remi. The impact of interference caused by GPS Repeaters on GNSS receivers and services. In *European Navigation Conference*, ENC GNSS, Wien, Österreich, 22–25 April 2013. ISBN 978-3-200-03154-8.

[55] J. C. Grabowski. Personal Privacy Jammers: Locating Jersey PPDs Jamming GBAS Safety-of-Life Signals. *GPS World*, 1st April 2012. URL `https://www.gpsworld.com/personal-privacy-jammers-12837/`. Accessed: 2020-03-17.

[56] O. Towlson, D. Payne, P. Eliardsson, and V. Manikundalam. Threat Database Analysis Report. Technical Report D6.2, STRIKE3, January 2019. URL `http://www.aic-aachen.org/strike3/downloads/STRIKE3_D6.2_Threat_database_Analysis_Report_public_v1.0.pdf`. Issue 1.0.

[57] Inside GNSS. Spoofing Incident Report: An Illustration of Cascading Security Failure, 9th October 2017. URL `https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/`. Accessed: 2020-02-17.

[58] M. Harris. Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai. *MIT Technology Review*, 15th November 2019. URL `https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/`. Accessed: 2020-01-15.

[59] J. Torchinsky. There's Something Very Weird Going on With Cars' GPS Systems at the Geneva Motor Show. *Jalopnik*, 8th March 2019. URL `https://jalopnik.com/theres-something-very-weird-going-on-with-cars-gps-syst-1833138071`. Accessed: 2020-02-17.

[60] L. HUANG and Q. YANG. GPS Spoofing: Low-cost GPS simulator. In *DEFCON 23*, August, 2015. DEFCON. URL `https://media.defcon.org/DEFCON23/DEFCON23presentations/DEFCON23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf`.

[61] T. Ebinuma. Software-Defined GPS Signal Simulator. GitHub, 2020. URL `https://github.com/osqzss/gps-sdr-sim`. Accessed: 2020-02-18.

[62] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka. Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150, National Institute of Standards and Technology, Gaithersburg, MD, USA, October 2016.

[63] P. Papadimitratos and A. Jovanovic. GNSS-based Positioning: Attacks and countermeasures. In *IEEE Military Communications Conference (MILCOM)*, pages 1–7, Nov 2008. doi:10.1109/MILCOM.2008.4753512.

[64] *Committee on National Security Systems (CNSS) Glossary.* Committee on National Security Systems, Ft Meade, MD, USA, 2015. URL `https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf`.

[65] G. D. Rash. GPS Jamming in A Laboratory Environment. In *Proceedings of the 53rd Annual Meeting of The Institute of Navigation (1997)*, pages 389–398, Albuquerque, NM, USA, June 1997.

[66] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo. Protecting gnss receivers from jamming and interference. *Proceedings of the IEEE*, 104(6):1327–1338, June 2016. ISSN 1558-2256. doi:10.1109/JPROC.2016.2525938.

[67] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. *Proceedings of the IEEE*, 104(6):1233–1245, June 2016. ISSN 1558-2256. doi:10.1109/JPROC.2016.2543266.

[68] R. Mitch, R. Dougherty, M. Psiaki, S. Powell, B. O'Hanlon, J. Bhatti, and T. Humphreys. Signal characteristics of civil GPS jammers. In *24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011*, 24th International Technical Meeting of the Satellite Division of the Institute of Navigation 2011, ION GNSS 2011, pages 1907–1919, 12 2011. ISBN 9781618394750.

[69] M. L. Psiaki and T. E. Humphreys. GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6): 1258–1270, June 2016. ISSN 1558-2256. doi:10.1109/JPROC.2016.2526658.

[70] National Marine Electronics Association. NMEA 0183, November 2018. Version 4.11.

[71] V. Murray. Legal GNSS Spoofing and its Effects on Autonomous Vehicles. In *Black Hat USA*, Las Vegas, NV, USA, 7th August 2019. Black Hat.

[72] D. Mills, J. Martin, J. Burbank, and W. Kasch. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5905, RFC Editor, June 2010. URL `http://www.rfc-editor.org/rfc/rfc5905.txt`.

[73] *Networked Transport of RTCM via Internet Protocol (Ntrip)*, 2005. URL `https://igs.bkg.bund.de/root_ftp/NTRIP/documentation/NtripDocumentation.pdf`. Version 1.0.

[74] F. Bastide, D. Akos, C. Macabiau, and B. Roturier. Automatic Gain Control (AGC) as an Interference Assessment Tool . In *16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, pages 2042–2053, September 2003.

[75] E. Axell, F. M. Eklöf, P. Johansson, M. Alexandersson, and D. M. Akos. Jamming detection in gnss receivers: Performance evaluation of field trials. *Navigation*, 62(1):73–82, 2015. doi:10.1002/navi.74.

[76] J. Lindstrom, D. M. Akos, O. Isoz, and M. Junered. GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules. In *20th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2007)*, pages 2042–2053, September 2007.

[77] B. Motella and L. L. Presti. Methods of goodness of fit for GNSS interference detection. *IEEE Transactions on Aerospace and Electronic Systems*, 50(3):1690–1700, July 2014. ISSN 2371-9877. doi:10.1109/TAES.2014.120368.

[78] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*, 2012:16, 2012. doi:10.1155/2012/127072.

[79] A. Broumandan and G. Lachapelle. Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation. *Sensors*, 18(5), 2018. ISSN 1424-8220. doi:10.3390/s18051305.

[80] E. G. Manfredini, F. Dovis, and B. Motella. Validation of a signal quality monitoring technique over a set of spoofed scenarios. In *2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–7, December 2014. doi:10.1109/NAVITEC.2014.7045136.

[81] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, and W. Feng. GNSS Spoofing Detection by Means of Signal Quality Monitoring (SQM) Metric Combinations. *IEEE Access*, 6:66428–66441, 2018. doi:10.1109/ACCESS.2018.2875948.

[82] D. M. Akos. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Navigation*, 59(4):281–290, October 2012. doi:10.1002/navi.19.

[83] E. Shafiee, M. R. Mosavi, and M. Moazedi. Detection of Spoofing Attack Using Machine Learning Based on Multi-layer Neural Network in Single-frequency Gps Receivers. *Journal of Navigation*, 71(1):169–188, 2018. doi:10.1017/S0373463317000558.

[84] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke. A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles. *Array*, 5:100013, 2020. ISSN 2590-0056. doi:10.1016/j.array.2019.100013.

[85] A. Broumandan, R. Siddakatte, and G. Lachapelle. An approach to detect GNSS spoofing. *IEEE Aerospace and Electronic Systems Magazine*, 32(8):64–75, Aug 2017. ISSN 1557-959X. doi:10.1109/MAES.2017.160190.

[86] S. Jeong and J. Lee. Synthesis Algorithm for Effective Detection of GNSS Spoofing Attacks. *International Journal of Aeronautical and Space Sciences*, July 2019. ISSN 2093-2480. doi:10.1007/s42405-019-00197-y.

[87] A. Ranganathan, H. Ólafsdóttir, and S. Capkun. Spree: A spoofing resistant gps receiver. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, MobiCom '16, page 348–360, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450342261. doi:10.1145/2973750.2973753.

[88] H. Tao, H. Li, and M. Lu. A Method of Detections' Fusion for GNSS Anti-Spoofing. *Sensors*, 16(16):2187, December 2016. doi:10.3390/s16122187.

[89] Novatel. GAJT-710ML Anti-Jam Antenna, October 2016. URL `https://www.novatel.com/assets/Documents/Papers/GAJT-710ML-PS.pdf`. Version 0C, Accessed: 2020-03-24.

[90] Swift Navigation. Piksi Datasheet, 28th March 2016. URL `https://www.swiftnav.com/piksi-datasheet`. Version 2.3.1, Accessed: 2020-03-24.

[91] S. Lo, Y. H. Chen, T. Reid, A. Perkins, T. Walter, and P. Enge. The Benefits of Low Cost Accelerometers for GNSS Anti-Spoofing. In *ION 2017 Pacific PNT Meeting*, pages 775–796, Honolulu, Hawaii, USA, May 2017. doi:10.33012/2017.15109.

[92] D. Gingras. *An Overview of Positioning and Data Fusion Techniques Applied to Land Vehicle Navigation Systems*. Automotive Informatics and Communicative Systems: Principles in Vehicular Networks and Data Exchange. Information Science Reference, 2009. ISBN 9781605663388. URL `https://books.google.co.uk/books?id=ioVcDQEACAAJ`.

[93] Y. Hu, S. Bian, B. Li, and L. Zhou. A Novel Array-Based Spoofing and Jamming Suppression Method for GNSS Receiver. *IEEE Sensors Journal*, 18(7):2952–2958, April 2018. ISSN 2379-9153. doi:10.1109/JSEN.2018.2797309.

[94] M. V. T. Heckler, M. Cuntz, A. Konovaltsev, L. A. Greda, A. Dreher, and M. Meurer. Development of robust safety-of-life navigation receivers. *IEEE Transactions on Microwave Theory and Techniques*, 59(4): 998–1005, April 2011. ISSN 1557-9670. doi:10.1109/TMTT.2010.2103090.

[95] M. Cuntz, A. Konovaltsev, and M. Meurer. Concepts, Development, and Validation of Multiantenna GNSS Receivers for Resilient Navigation. *Proceedings of the IEEE*, 104(6):1288–1301, June 2016. ISSN 1558-2256. doi:10.1109/JPROC.2016.2525764.

[96] R. T. Compton. The Power-Inversion Adaptive Array: Concept and Performance. *IEEE Transactions on Aerospace and Electronic Systems*, AES-15(6):803–814, November 1979. doi:10.1109/TAES.1979.308765.

[97] T. Kraus, R. Bauernfeind, and B. Eissfeller. Survey of In-Car Jammers - Analysis and Modeling of the RF signals and IF samples (suitable for active signal cancellation). In *24th Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GNSS 2011)*, 2011.

[98] L.-T. Hsu, P. Groves, and S.-S. Jan. Assessment of the Multipath Mitigation Effect of Vector Tracking in an Urban Environment. In *Proceedings of the ION 2013 Pacific PNT Meeting*, pages 498–509, Honolulu, Hawaii, USA, April 2013.

[99] J. Zhang, X. Cui, H. Xu, and M. Lu. A Two-Stage Interference Suppression Scheme Based on Antenna Array for GNSS Jamming and Spoofing. *Sensors*, 19(18):3870, September 2019. ISSN 1424-8220. doi:10.3390/s19183870.

[100] L.-T. Hsu, H. Tokura, N. Kubo, Y. Gu, and S. Kamijo. Multiple Faulty GNSS Measurement Exclusion Based on Consistency Check in Urban Canyons. *IEEE Sensors Journal*, 17(6):1909–1917, 2017. ISSN 1530-437X. doi:10.1109/JSEN.2017.2654359.

[101] Q. Yang, Y. Zhang, C. Tang, and J. Lian3. A Combined Antijamming and Antispoofing Algorithm for GPS Arrays. *International Journal of Antennas and Propagation*, 2019:9, 2019. doi:10.1155/2019/8012569.

[102] J. Magiera and R. Katulski. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology*, 13(1):45–57, 2015. ISSN 1665-6423. doi:10.1016/S1665-6423(15)30004-3.

[103] J. Magiera. A Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing. *Sensors*, 19(10), 2019. ISSN 1424-8220. doi:10.3390/s19102411.

[104] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *CryptoBytes*, 5(2):2–13, 2002. URL `https://people.eecs.berkeley.edu/~tygar/papers/TESLA_broadcast_authentication_protocol.pdf`.

[105] J. Harding, G. R. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang. Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. Technical Report DOT HS 812 014, U.S. Department of Transportation, National Highway Traffic Safety Administration, Washington, DC, USA, August 2014.

[106] ETSI Technical Committee Intelligent Transport Systems. Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. Standard ETSI TS 102 940, European Telecommunications Standards Institute, Valbonne, France, April 2019. URL `https://www.etsi.org/deliver/etsi_EN/302600_302699/30263702/01.04.01_30/en_30263702v010401v.pdf`. V1.3.1 (2018-014.

[107] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle. A Navigation Message Authentication Proposal for the Galileo Open Service. *Navigation*, 63(1):85–102, 2016. doi:10.1002/navi.125.

[108] S. Binda. Galileo Open Service Navigation Message. In *GNSS Interference and Authentication Workshop*, Haarlem, Netherlands, 31st January 2018. Netherlands Institute for Navigation and Geo-Information. URL `http://www.navnin.nl/new/wp-content/uploads/2018/02/WSIA-4-ESA-NIN-Workshop-Galileo-NMA.pdf`.

[109] K. Wesson, M. Rothlisberger, and T. Humphreys. Practical Cryptographic Civil Gps Signal Authentication. *Navigation*, 59(3):177–193, 2012. doi:10.1002/navi.14.

[110] Space Vehicles Directorate, Advanced GPS Technology. Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface. Interface Specification IS-AGT-100, Air Force Research Laboratory, 17th April 2019. URL `http://www.gpsexpert.net/chimera-specification/IS-AGT-100.pdf`.

[111] S. Cancela, J. D. Calle, and I. Fernández-Hernández. CPU Consumption Analysis of TESLA-based Navigation Message Authentication. In *2019 European Navigation Conference (ENC)*, pages 1–6, April 2019. doi:10.1109/EURONAV.2019.8714171.

[112] M. Petovello. What is navigation message authentication? *Inside GNSS*, January/February:26–31, 2018. URL `https://insidegnss.com/wp-content/uploads/2018/04/janfeb18-SOLUTIONS.pdf`. Accessed: 2020=02-11.

[113] M. Howard. *The Security Development Lifecycle*. Microsoft Press, Redmond, Washington, USA, May 2006. ISBN 9780735622142.

[114] H. Assal and S. Chiasson. Security in the Software Development Lifecycle. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 281–296, Baltimore, MD, August 2018. USENIX Association. ISBN 978-1-939133-10-6. URL `https://www.usenix.org/conference/soups2018/presentation/assal`.

[115] M. Steger, C. A. Boano, T. Niedermayr, M. Karner, J. Hillebrand, K. Roemer, and W. Rom. An Efficient and Secure Automotive Wireless Software Update Framework. *IEEE Transactions on Industrial Informatics*, 14(5):2181–2193, May 2018. ISSN 1941-0050. doi:10.1109/TII.2017.2776250.

[116] D. Miralles, N. Levigne, D. M. Akos, J. Blanch, and S. Lo. Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pages 334–344, Miami, Florida, USA, September 2018. doi:10.33012/2018.15883.

[117] M. Ramezani and K. Khoshelham. Vehicle Positioning in GNSS-Deprived Urban Areas by Stereo Visual-Inertial Odometry. *IEEE Transactions on Intelligent Vehicles*, 3(2):208–217, June 2018. ISSN 2379-8858. doi:10.1109/TIV.2018.2804168.

[118] Z. Z. M. Kassas, J. Khalife, K. Shamaei, and J. Morales. I Hear, Therefore I Know Where I Am: Compensating for GNSS Limitations with Cellular Signals. *IEEE Signal Processing Magazine*, 34(5):111–124, September 2017. ISSN 1558-0792. doi:10.1109/MSP.2017.2715363.

[119] G. Mori Gonzalez, I. Petrunin, R. Zbikowski, K. Voutsis, and R. Verdeguer Moreno. Vulnerability Analysis of GPS Receiver Software. In *2019 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6, June 2019. doi:10.1109/ICL-GNSS.2019.8752862.

[120] D. J. Trump. Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services. Executive Order 13905, The White House, Washington DC, USA, 2020. URL `https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/`.

[121] K. N. Bjergstrom, V. M. Dwyer, M. J. Everitt, M. J. de C. Henshaw, A. J. Daw, and J. Lemon. Quantum-Enabled Maritime Navigation. Workshop Notes, Loughborough University, Epinal Way, Loughborough, LE11 3TU, UK, 15th April 2019. URL https://admin.ktn-uk.co.uk/app/uploads/2019/04/QNWorkshop_Notes_Final.pdf.

[122] Department for Business, Energy & Industrial Strategy, UK Research and Innovation, and Amanda Solloway MP. World's first timing centre to protect UK from risk of satellite failure , 19th February 2020. URL https://www.gov.uk/government/news/worlds-first-timing-centre-to-protect-uk-from-risk-of-satellite-failure. Accessed: 2020-02-26.

[123] M. Pattinson, D. Fryganiotis, and P. Eliardsson. Draft Standards for Threat Monitoring and Reporting. Technical Report D4.1, STRIKE3, November 2017. URL http://www.aic-aachen.org/strike3/downloads/STRIKE3_D41_Reporting_Standards_v2.1.pdf. Issue 2.1.

[124] Wireless Telegraphy Act 2006, 8th November 2006. URL www.legislation.gov.uk/ukpga/2006/36. Accessed: 2020-02-30.

[125] The Electromagnetic Compatibility Regulations 2016, 15th November 2016. URL http://www.legislation.gov.uk/uksi/2016/1091. Accessed: 2020-02-24.

[126] *UK Connected and Automated Mobility Roadmap to 2030*. Zenzic-UK Ltd., London, UK, 2019. URL https://zenzic.io/content/uploads/2019/09/Zenzic_Roadmap_Report_2019.pdf.

[127] SAE International. SAE Standards News: J3016 automated-driving graphic update, 2019. URL https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic. Accessed: 2020-03-25.

[128] *NEO/LEA-M8T: u-blox M8 concurrent GNSS timing modules*. ublox, Thalwil, Switzerland, 21st June 2016. URL https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_(UBX-15025193).pdf. R03.

[129] *AsteRx-i S UAS*. Septentrio, Leuven, Belgium, March 2020. URL https://septentrio.sharepoint.com/:b:/g/Marketing4Sales/Ebo5DP4dRT1Mn8Kxm0PdiTcBAS6Lha75QOBiHbfWm5XyAg?e=a1SsqO. Accessed: 2020-03-31.

[130] *Piksi Multi - GNSS Module - Hardware Specification*. Swift Navigation, San Francisco, California, USA, 6th February 2019. URL https://www.swiftnav.com/latest/piksi-multi-hw-specification. Version 2.2.

[131] D. Borio, C. O'Driscoll, and J. Fortuny. GNSS Jammers: Effects and countermeasures. In *6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) European Workshop on GNSS Signals and Signal Processing*, pages 1–7, Dec 2012. doi:10.1109/NAVITEC.2012.6423048.

[132] *SimGEN® Software Suite for Spirent GNSS Constellation Simulation Systems*. Spirent Communications Plc., July 2019. URL https://www.spirent.com/-/media/datasheets/positioning/simgen.pdf.

[133] Resilient Navigation and Timing Foundation. Policy Recommendations for GPS/GNSS. URL https://rntfnd.org/what-we-do/our-recommendations-gps-gnss/. Accessed: 2020-02-25.