



Dedicated to innovation in aerospace

COMPANY CONFIDENTIAL

NLR-CR-2019-001-PT-1-RevEd-1 | June 2019

GNSS spoofing

Revised Edition

CUSTOMER: Agentschap Telecom

NLR – Netherlands Aerospace Centre



Netherlands Aerospace Centre

NLR is a leading international research centre for aerospace. Bolstered by its multidisciplinary expertise and unrivalled research facilities, NLR provides innovative and integral solutions for the complex challenges in the aerospace sector.

NLR's activities span the full spectrum of Research Development Test & Evaluation (RDT & E). Given NLR's specialist knowledge and facilities, companies turn to NLR for validation, verification, qualification, simulation and evaluation. NLR thereby bridges the gap between research and practical applications, while working for both government and industry at home and abroad.

NLR stands for practical and innovative solutions, technical expertise and a long-term design vision. This allows NLR's cutting edge technology to find its way into successful aerospace programs of OEMs, including Airbus, Embraer and Pilatus. NLR contributes to (military) programs, such as ESA's IXV re-entry vehicle, the F-35, the Apache helicopter, and European programs, including SESAR and Clean Sky 2.

Founded in 1919, and employing some 600 people, NLR achieved a turnover of 76 million euros in 2017, of which 81% derived from contract research, and the remaining from government funds.

For more information visit: www.nlr.nl



Dedicated to innovation in aerospace

COMPANY CONFIDENTIAL

NLR-CR-2019-001-PT-1-RevEd-1 | June 2019

GNSS spoofing

Revised Edition



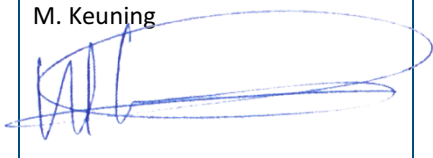
CUSTOMER: Agentschap Telecom

AUTHOR(S):

J.J.P. van Es	NLR
J.D. van Bruggen-van Putten	NLR
H.D. Zelle	NLR

No part of this report may be reproduced and/or disclosed, in any form or by any means without the prior written permission of the owner.

CUSTOMER	Agentschap Telecom
CONTRACT NUMBER	30000795
OWNER	Agentschap Telecom
DIVISION NLR	Aerospace Systems
DISTRIBUTION	Limited
CLASSIFICATION OF TITLE	COMPANY CONFIDENTIAL

APPROVED BY :		
AUTHOR	REVIEWER	MANAGING DEPARTMENT
J.J.P. van Es 	L. Timmermans 	M. Keuning 
DATE 240619	DATE 240619	DATE 240619

Executive summary

Global Navigation Satellite Systems

Global Navigation Satellite Systems (GNSS) like the American GPS and the European Galileo system are used more and more to provide accurate position, velocity and time for critical infrastructure and an overwhelming number of other applications. GNSS positioning is used for surveying, navigation, precision farming, road tolling, etc. Without accurate position, transport systems and supply chains would come to a halt. GNSS time is vitally important for synchronizing networks for communication and power distribution and for timestamping financial transactions. In the meantime these satellite signals are very vulnerable to disruption due to the low power with which they are received on earth. The awareness of this vulnerability is growing.

GNSS spoofing and meaconing

This report deals with a specific type of disruption: GNSS spoofing in which the legitimate satellite signals are overpowered by fake GNSS signals generated by an attacker, resulting in GNSS receivers calculating incorrect position and time. Meaconing is a related technique that consists of the replay of genuine satellite signals. GNSS spoofing and meaconing are sensitive subjects, because they are associated with governmental or military operations and/or criminal activities and vulnerabilities in, for example, critical infrastructure.

This report

The main goal of this report is to guide Agentschap Telecom (the Radiocommunications Agency in the Netherlands) in policy and decision making regarding GNSS spoofing, scoped to incidental spoofing, small criminals and terrorist activities. Military and Governmental spoofing activities are out of scope.

The research approach consisted of a literature study, supplemented with interviews with stakeholders and experts. The literature study gave first answers to the research questions from a technical point of view. This view was given to the interview candidates in advance of the interview. Objective of the following interviews was to improve this view - both technological and organizational - and to learn from experience in the field.

Types of spoofing attacks

Spoofing attacks are usually classified based on the basis of sophistication, the way in which the signal is presented to the GNSS receiver, the necessary equipment, etc.

- non-signal technique (cyberattack);
- cable inject;
- non-coherent technique, single spoofer;
- coherent technique, single spoofer;
- coherent technique, multiple spoofers.

Non-signal (cyber) attacks, cable injection and non-coherent RF spoofing attacks are most simple to implement, making these attacks more likely. More complicated techniques with a single or multiple coherent spoofing transmitters are much more difficult to realize, because they require more expensive RF equipment and knowledge.

Meaconing can be seen as a separate attack category that is simpler to perform than spoofing because there is no need for software to generate the GNSS signals. In its most simple form only a repeater is necessary. The advantage of meaconing is the fact that all the complete GNSS signals are obtained with high quality. The drawback is reduced freedom to tailor the signals for a specific purpose.

Note that non-signal and cable injection attacks do not abuse the RF spectrum and are not illegal in that respect. One could argue if they should be qualified as spoofing, especially the non-signal attack. They are included however, because if successful the result of these attacks is the same as for the other GNSS spoofing techniques.

Spoofing equipment

Non-signal (cyber) attacks need no RF equipment at all. Cable injection and non-coherent single spoofer techniques can be performed with consumer grade software-defined radio equipment. SDR platforms with adequate specifications are available in the price range between 100 and 1000 euro. Basic GPS spoofing software is freely available on the internet. It has also been shown that cheap electronic devices can be used to emit GNSS signals outside their intended band of operation.

For the more sophisticated coherent spoofing attacks, generally higher grade equipment is needed. Several research institutes have created spoofing hard- and software for research purposes, but these are usually not made available outside the institute.

To perform meaconing, only a hardware repeater system is necessary. Such GNSS repeater systems are available commercially for applications where GNSS reception is needed in-doors, e.g. in aircraft hangars or in buildings of emergency services. It is also possible to store the received GNSS signal and re-play the signal from memory. In that case there is still no need for the attacker to generate the GNSS signals himself.

Actors and motivations

There are different actors that can have various motivations for performing GNSS spoofing:

- drivers that want to spoof vehicle-based tracking systems to avoid paying road tolls and to evade regulations on driving hours;
- fishermen that want to spoof tracking equipment to remain undetected while entering illegal fishing grounds;
- traders that want to manipulate the timing of financial transactions to gain financial benefit;
- terrorists that want to create damage and fear by forcing vehicles off-course or disrupt time synchronization in distributed networks;
- offenders that want to spoof tracking equipment to evade house arrest;
- amateur hackers that want to perform spoofing out of curiosity, simply trying to see what they can achieve.

All these scenarios appear applicable to The Netherlands. Each possible motivation has a different target and requires different amplitude of the induced error.

Impact

Exact financial impact is hard to predict, but the largest impact is expected when spoofing attacks are aimed at critical national infrastructure such as Rotterdam Harbor, Schiphol airport or the national power network.

Likelihood of spoofing

Initially GNSS spoofing was merely a theoretical possibility. Over the years it has become technically feasible. Experts do not agree if spoofing currently is a real threat, or not. The likelihood of spoofing – both higher and lower – is influenced by several factors.

Higher likelihood factors are:

- the widespread use of GNSS receivers in critical infrastructure and other systems makes that there are many potential targets;
- there are many potential actors with a motivation to perform spoofing;
- spoofing equipment and software are available. Equipment is still improving and becoming cheaper. A motivated spoofer will be able and willing to purchase even the current advanced hardware;
- the chances of a low-power spoofing attack being detected are relatively small.

Lower likelihood factors are:

- spoofing has been demonstrated in the lab, but is difficult to achieve in the field;
- it requires detailed planning, knowledge of the target receiver such as receiving antenna location etc.;

- it is not obvious how a specific target will respond to spoofing, because it is not clear if and what mitigation measures are in place;
- besides spoofing, potential spoofers usually have other options for reaching their goals, such as GNSS jamming.

Occurrence of spoofing and meaconing

Spoofing has been demonstrated in the lab, but is still difficult to achieve in the field. All evidence indicates that spoofing is rare in real-life. There have been no authenticated reports of criminal or terrorist spoofing. Several cases of military, unintentional and scientific spoofing and meaconing have been registered in the past. The reports of unintentional GNSS meaconing were due to GNSS repeaters in hangars at airports.

It is possible that there have been isolated spoofing incidents that have not been reported, because

1. the spoofing signals were not detected due to their low RF power;
2. the real cause of the incident was not recognized;
3. stakeholders are unwilling to share information.

Future developments

The current SDR equipment is aimed at in-door use and not particularly portable. Experts fear that the emergence of small, light-weight, battery-operated spoofing devices will make spoofing more accessible. There are no technical reasons why spoofing devices could not be made smaller and battery-operated.

Detection of spoofing

Spoofing (except for non-signal and cable injection attacks) can be detected by interference monitoring in the RF spectrum. However, targeted spoofing attacks are assumed to use low RF power. To be able to detect such low-power signals with certainty, detection networks need to be sufficiently dense. Typical spacing of the nodes could be 100 – 1000 m. A dedicated monitoring network with such a density is difficult and rather expensive to install and to maintain.

Crowd-sourced interference monitoring is a concept in which smartphone owners voluntarily upload the raw measurement data of their phone's GNSS chip to a central server for analysis. Google and Apple have recently made this approach possible by granting apps access to the raw measurement data. The crowd-sourcing concept promises a dense GNSS interference monitoring network at limited cost.

Mitigation of spoofing

Mitigation usually consists of the detection of spoofing, followed by fallback to an alternate source of position or time. The two can therefore not be seen separately. Mitigation measures include:

- GNSS receiver-based measures
 - antenna-centered techniques, such as anti-jamming antennas;
 - signal quality monitoring techniques;
 - consistency checks on Position, Velocity and Time (PVT);
 - navigation message checks;
 - use of augmentation data;
 - fallback to other GNSS signals or non-GNSS sources of position and time;
- use of non-GNSS systems;
- non-technical anti-spoofing measures.

Organizational solutions to detect spoofing include assigning the GNSS frequency bands primary status and to create more awareness among the operators of GNSS equipment of the possibility of spoofing. Agentschap Telecom already

operates a hotline for radio interference in general. The added value of an additional hotline for GNSS spoofing, like the Federal Communications Commission (FCC) did for reporting GNSS jamming, appears to be small.

Usually a single spoofing countermeasure does not provide complete protection and a combination of mitigation measures is needed for optimal protection. The best (technically and economically) mitigation strategy depends on the specific application. It should be noted that the value of spoofing mitigation remains limited: an attacker can always refer to jamming if spoofing fails.

Recommendations

The occurrence of spoofing is low currently and it is hard to predict if spoofing will become a more serious threat in the coming years. At least several ingredients (potential targets, potential actors, equipment) are present to make it a more severe threat. It is thus recommended that Agentschap Telecom increases national resilience with a combination of measures.

- Increase the chances of interference and spoofing detection by expanding the monitoring of GNSS frequency bands, especially near critical infrastructure.
- Increase the chances of interference detection, by encouraging the monitoring of GNSS bands through crowd-sourcing networks.
- In case a GNSS spoofing incident occurs, make sure it receives a reaction not to be misunderstood, i.e. a proper fine or legal action. The agency could consider giving visibility to the fact that GNSS frequency bands are being actively protected by law enforcement, as a deterrent.
- Create awareness: inform GNSS users on the risk of GNSS spoofing and interference.
- Recommend best practices to professional users, e.g.
 - antenna installed in a high location without view of the street surface;
 - use a choke-ring antenna;
 - use a multi-constellation, multi-frequency receiver if possible;
 - apply best practices for cyber-security for internet-connected devices.
- Enforce the use of mitigation measures for critical infrastructure¹, specifically for GNSS timing:
 - all critical infrastructure using GNSS timing:
 - power plants;
 - financial institutions;
 - communication network providers;
 - timing receivers should include a hold-over clock with a detection and fallback mechanism for spoofing and interference.

¹ Enforcing measures for critical infrastructure is most likely outside of the scope of Agentschap Telecom responsibility; however it is seen as an important measure to increase resilience.

Managementsamenvatting

Global Navigation Satellite Systems

Satelliet navigatiesystemen (Global Navigation Satellite Systems - GNSS) zoals het Amerikaanse GPS en het Europese Galileo systeem worden steeds meer gebruikt om nauwkeurige positie, snelheid en tijd te leveren ten behoeve van kritieke infrastructuur en een enorm aantal andere toepassingen. GNSS-positionering wordt gebruikt voor landmeting, navigatie, precisielandbouw, tolsystemen, etc. Zonder nauwkeurige positie-informatie zouden transport- en logistieke systemen stilvallen. GNSS tijd is van vitaal belang voor het synchroniseren van communicatie- en elektriciteitsnetwerken en voor het dateren van financiële transacties. De signalen van de GNSS satellieten zijn echter gemakkelijk te verstoren door de lage signaalsterkte waarmee ze op het aardoppervlak worden ontvangen. Het bewustzijn van deze kwetsbaarheid is groeiende.

GNSS spoofing en meaconing

Onderwerp van dit rapport zijn spoofing en meaconing, twee specifieke verstoringen van de GNSS satelliet signalen. Bij spoofing vervangt een aanval de originele GNSS signalen door nepsignalen waardoor GNSS ontvangers een onjuiste positie en tijd berekenen. Meaconing is een verwante techniek die bestaat uit het heruitzenden van originele GNSS signalen door een aanval. GNSS spoofing en meaconing zijn gevoelige onderwerpen, omdat ze verband kunnen houden met overheids- of militaire operaties en/of criminele activiteiten en kwetsbaarheden in bijvoorbeeld kritieke infrastructuur.

Dit rapport

Het doel van dit rapport is het ondersteunen van Agentschap Telecom bij het beleid en de besluitvorming ten aanzien van GNSS spoofing. Dit rapport is beperkt tot onopzettelijke spoofing en spoofing met een crimineel of terroristisch oogmerk. Interstatelijke en militaire spoofing vallen buiten beschouwing.

De onderzoeks aanpak bestond uit een literatuuronderzoek, aangevuld met interviews met stakeholders en deskundigen. Het literatuuronderzoek gaf voornamelijk technische antwoorden op de onderzoeksvragen. De resultaten van het literatuuronderzoek werden gecommuniceerd aan de interviewkandidaten. Het doel van de interviews was vervolgens om het literatuuronderzoek informatie aan te vullen met zowel technische als organisatorisch aspecten en om te leren van de praktijk.

Soorten spoofing aanvallen

Spoofing aanvallen kunnen op verschillende manieren worden ingedeeld, bijvoorbeeld op basis van hun complexiteit, de wijze waarop de signalen worden gepresenteerd aan de GNSS ontvanger, de apparatuur benodigd voor de aanval, etc.

- cyberaanval;
- kabelinjectie;
- incoherente aanval, enkele spoofer;
- coherente aanval, enkele spoofer;
- coherente aanval, meerdere spoofers.

Cyberaanval, kabelinjectie en niet-coherente RF spoofing aanvallen zijn gemakkelijker uit te voeren en daardoor meer waarschijnlijk. De coherente technieken met een enkele of meerdere zenders zijn veel moeilijker uit te voeren omdat er duurdere RF apparatuur voor nodig is en meer specialistisch kennis.

Meaconing kan als een separate aanvalstechniek worden beschouwd die eenvoudiger is uit te voeren dan spoofing, omdat er geen software nodig is voor het genereren van valse GNSS signalen. In de meest eenvoudige vorm is er alleen een repeater nodig. Het voordeel van meaconing is gelegen in het feit dat alle GNSS signalen in originele kwaliteit worden aangeboden aan het doelwit. Het nadeel is dat het voor de aanvalleur moeilijker is de signalen op maat te maken voor een specifieke aanval.

De cyberaanval en kabelinjectie technieken maken geen misbruik van het RF spectrum om signalen van de spoofer naar het doelwit over te brengen en zijn om die reden niet illegaal. Het resultaat van deze aanvalstechnieken lijkt echter wel erg op de andere spoofing technieken. Daarom zijn ze wel in dit rapport opgenomen.

Spoofing apparatuur

In het algemeen is voor een cyberaanval is geen RF apparatuur nodig. Kabelinjectie en incoherente aanvallen met een enkele spoofer kunnen worden uitgevoerd met gemakkelijk verkrijgbare software-defined radio (SDR) apparatuur. Bruikbare SDR systemen zijn beschikbaar met prijzen tussen 100 en 1000 euro. Eenvoudige GPS spoofing software is gratis beschikbaar op het internet. Het is ook mogelijk om goedkope consumentenelektronica te misbruiken om GNSS signalen uit te zenden, ook buiten de banden waarin deze apparatuur werkt.

Voor de meer geavanceerde coherente spoofing aanvallen is in het algemeen meer specialistische apparatuur nodig. Diverse onderzoeksinstituten hebben spoofing hard- en software gemaakt voor onderzoeksdoeleinden. Deze hard- en software zijn normaliter alleen voor eigen gebruik en niet beschikbaar voor buitenstaanders.

Om een meaconing aanval uit te voeren is alleen een repeater systeem noodzakelijk. Dergelijke GNSS repeater systemen zijn commercieel beschikbaar voor toepassingen waarbij GNSS binnen in gebouwen nodig zijn, zoals bijvoorbeeld in hangaars en in de gebouwen van brandweer en andere hulpdiensten. Het is ook mogelijk om de ontvangen GNSS signalen eerst op te slaan in een geheugen alvorens ze weer uit te zenden. Maar ook in dat geval hoeft de aanvaller de GNSS signalen niet zelf te genereren.

Aanvallers en motivaties

Potentiele aanvallers kunnen verschillende motivaties hebben om een spoofing aanval op te zetten:

- bestuurders van voertuigen willen hun voertuigvolgsystemen spoofen om te voorkomen dat ze toll moeten betalen of om regelgeving op het gebied van rijtijden te omzeilen;
- vissers willen volgsystemen spoofen om ongedetecteerd te kunnen vissen buiten hun visgronden;
- handelaren willen het tijdstempel van hun transacties manipuleren om daar financieel voordeel uit te halen;
- terroristen willen schade veroorzaken en angst zaaien door voertuigen van koers te laten veranderen of door de tijdsynchronisatie in energie- en communicatienetwerken te verstoren;
- veroordeelde criminelen willen hun enkelband spoofen om aan hun huisarrest te ontkomen;
- amateur hackers spoofen uit nieuwsgierigheid, eenvoudigweg om te zien wat ze voor elkaar kunnen krijgen.

Al deze scenario's lijken van toepassing op Nederland. Iedere motivatie is gericht op een ander doelwit en beoogd een fout met specifieke grootte in de GNSS positie en tijd..

Impact

De exacte financiële gevolgen van spoofing aanvallen zijn moeilijk te voorspellen, maar de grootste impact ontstaat naar verwachting wanneer spoofing aanvallen zijn gericht op de kritieke infrastructuur zoals de haven van Rotterdam, Schiphol of het elektriciteitsnetwerk.

Waarschijnlijkheid van spoofing

Over de jaren is GNSS spoofing veranderd van een theoretische mogelijkheid in iets dan technisch haalbaar is. Experts zijn het er niet over eens of spoofing tegenwoordig een echte bedreiging is of niet. De waarschijnlijkheid van spoofing – zowel hoger als lager – wordt beïnvloed door verschillende factoren:

Hogere waarschijnlijkheid:

- er zijn vele potentiële doelwitten doordat het wijdverspreide gebruik van GNSS ontvangers in de kritieke infrastructuur en in allerlei andere systemen;
- er zijn veel verschillende potentiële spoofers met verschillende motivaties om een spoofing aanval op te zetten;
- spoofing hard- en software zijn beschikbaar. De apparatuur wordt steeds beter en goedkoper. Een gemotiveerde spoofer kan en wil de huidige hardware aanschaffen;

- de kans dat een laagvermogen spoofing aanval wordt gedetecteerd is relatief klein.

Lagere waarschijnlijkheid:

- spoofing is gedemonstreerd door wetenschappers in het laboratorium, maar is moeilijk uit te voeren in het veld;
- het vereist een gedegen voorbereiding en kennis van het doelwit zoals de locatie van de ontvangstantenne etc.;
- het is op voorhand niet duidelijk hoe een doelwit zal reageren op spoofing, omdat niet duidelijk waarneembaar is of er tegenmaatregelen getroffen zijn;
- naast spoofing, hebben potentiële spoofers meestal ook nog andere middelen om hun doelen te bereiken, bijvoorbeeld GNSS jamming.

Spoofen en meaconing voorvallen

Spoofing is gedemonstreerd in het laboratorium, maar moeilijk uit te voeren in het veld. Alles wijst er op dat spoofing zeer zeldzaam is in het dagelijkse leven. Er zijn geen verifieerbare verslagen van spoofing aanvallen met een crimineel of terroristisch oogmerk. Er zijn wel verschillende gevallen van militaire, onopzettelijke en wetenschappelijke spoofing en meaconing gevonden. De gevallen van onopzettelijke meaconing betroffen GNSS repeaters in hangaars op vliegvelden.

Toch is het mogelijk dat er geïsoleerde incidenten hebben plaatsgevonden die niet zijn gemeld, omdat

1. de spoofing signalen niet zijn opgemerkt vanwege hun lage signaalsterkte;
2. de echte oorzaak van het incident niet onderkend is;
3. de betrokkenen het niet in de openbaarheid hebben gebracht.

Toekomstige ontwikkelingen

De huidige SDR apparatuur is gemaakt voor gebruik binnenshuis en niet erg draagbaar. Experts zijn bang voor de komst van kleine, lichtgewicht spoofing apparaatjes gevoed door batterijen die het spoofen nog veel toegankelijker zouden maken. Er zijn geen technische belemmeringen voor het maken van dergelijke kleine, batterij-gevoede spoofing apparaten.

Detectie van spoofing

Spoofing (behalve cyberaanvallen en de kabelinjectietechniek) kan worden gedetecteerd door middel van monitoring van het RF spectrum. Gericht spoofing aanvallen gebruiken naar verwachting een laag RF signaalniveau. Om dergelijke zwakke RF signalen met zekerheid te kunnen detecteren, is het nodig dat detectienetwerken een voldoende hoge dichtheid hebben. De typische afstand tussen de sensoren in het netwerk bedraagt 100 – 1000 m. Een spoofingdetectienetwerk met zo'n hoge dichtheid is moeilijk en vrij duur om te installeren en te onderhouden.

Crowd-sourced interferentiemonitoring is een concept waarin gebruikers van smartphones vrijwillig de meetgegevens van de GNSS chip in hun telefoon delen voor analyse op een centrale server. Google en Apple hebben dit concept recentelijk mogelijk gemaakt door apps van derden toegang te geven tot deze ruwe GNSS meetgegevens. Crowd-sourcing is een veelbelovend concept om tegen beperkte kosten een dicht GNSS interferentiemonitoring netwerk te realiseren.

Mitigerende maatregelen

Mitigatie bestaat meestal uit de detectie van spoofing, gevolgd door een terugvallen op andere bronnen van positie- en tijdinformatie. Mitigatie en detectie kunnen daardoor niet los van elkaar gezien worden. Mitigerende maatregelen zijn:

- GNSS ontvanger-gebaseerde maatregelen
 - antennetechnieken, bijvoorbeeld anti-jamming antennes;
 - controleren van de RF signaal kwaliteit;
 - controleren van de consistentie van de tijd- en positieoplossing van de ontvanger;
 - controleren van het navigatiebericht;

- terugvallen op andere satellietnavigatiesignalen of naar bronnen van plaats en tijd informatie die niet afhankelijk zijn van satellietssystemen;
- technische maatregelen buiten GNSS ontvangers;
- niet-technische (organisatorisch) maatregelen.

Organisatorische maatregelen voor het detecteren van spoofing zijn o.a. het toekennen van een primaire status aan de GNSS frequentiebanden en het waarschuwen van de gebruikers van GNSS apparatuur voor de mogelijkheid van spoofing. Agentschap Telecom heeft al een meldpunt voor radio-interferentie. De toegevoegde waarde van een meldpunt specifiek voor GNSS spoofing, vergelijkbaar met het meldpunt van de Federal Communication Commission (FCC) voor GNSS jamming, lijkt klein.

Geen van de beschikbare mitigerende maatregelen geeft een volledige bescherming tegen spoofen. Een combinatie van maatregelen is nodig voor een optimale bescherming. De beste mitigatie strategie (technisch en economisch) verschilt per toepassing. Opgemerkt moet worden dat de waarde van spoofingmitigatie beperkt blijft: een aanvaller kan altijd terugvallen op jamming als spoofing mislukt.

Aanbevelingen

Spoofing komt nu nog niet (of nauwelijks) voor en het is moeilijk te voorspellen of spoofing een grotere bedreiging wordt in de komende jaren. Een aantal van de ingrediënten daarvoor (potentiële doelwitten, potentiële daders, apparatuur) is echter wel aanwezig. Agentschap Telecom wordt daarom aangeraden de nationale weerbaarheid tegen spoofing te vergroten met een combinatie van maatregelen.

- Vergroot de kansen dat GNSS interferentie en spoofing worden gedetecteerd door het uitbreiden van de bestaande detectiemiddelen, vooral bij kritieke infrastructuur.
- Vergroot de kansen dat GNSS interferentie wordt gedetecteerd door het stimuleren van crowd-sourcing interferentiemonitoring.
- Zorg voor een niet mis te verstane reactie (boete of vervolging) in geval van het GNSS spoofing incident. Agentschap Telecom kan overwegen meer zichtbaarheid te geven aan de bescherming van de GNSS frequentiebanden als afschrikkend voorbeeld.
- Verhoog het bewustzijn: informeer gebruikers van GNSS over de risico's van GNSS spoofing en interferentie.
- Adviseer best practices aan professionele gebruikers, bijvoorbeeld:
 - installeer antennes op een hoog punt waar ze niet zichtbaar zijn vanaf de straat;
 - gebruik choke-ring antennes;
 - gebruik een multi-constellation, multi-frequentie ontvanger;
 - pas best practices toe voor het vergroten van de cyber-veiligheid in geval van ontvanger die verbonden zijn met internet.
- Dwing het gebruik van mitigerende maatregelen ten behoeve van de kritieke infrastructuur af², vooral voor het gebruik van GNSS tijd:
 - alle kritieke infrastructuur die gebruik maakt van GNSS tijd:
 - energiecentrales;
 - financiële instellingen;
 - communicatienetwerken;
 - timing ontvangers zouden gebruik moeten maken van een stabiele referentieklok samen met een adequaat detectie en terugvalmechanisme bij het optreden van spoofing en interferentie.

² Het afdwingen van maatregelen voor de kritieke infrastructuur ligt waarschijnlijk buiten de verantwoordelijkheid van Agentschap Telecom. Het is desalniettemin van belang voor het vergroten van de weerbaarheid.

Contents

Abbreviations	13
1 Introduction	15
1.1 Objective	15
1.2 Research questions	15
1.3 Research approach	16
1.3.1 Literature study	16
1.3.2 Interviews	17
1.4 Document structure	17
2 Spoofing	18
2.1 Introduction	18
2.2 Spoofing scenarios	19
3 GNSS background	23
3.1 GNSS systems	23
3.2 Augmentation	23
3.3 Signal characteristics	24
3.4 Interference	25
3.5 Historic development of GNSS spoofing	25
4 GNSS spoofing techniques	27
4.1 GNSS spoofing attack types	27
4.1.1 Non-signal (cyberattack)	27
4.1.2 Cable inject	28
4.1.3 Non-coherent, single spoofer	28
4.1.4 Coherent, single spoofer	28
4.1.5 Coherent signal, multiple spoofers	29
4.1.6 Meaconing	29
4.2 Spoofing hardware and software	29
4.3 GNSS receiver susceptibility to spoofing	32
4.3.1 Receiver categories	32
4.3.2 Receiver susceptibility	32
5 Detection and mitigation of GNSS spoofing	33
5.1 GNSS receiver-based spoofing mitigation	34
5.1.1 Antenna-centered techniques	34
5.1.2 Signal quality monitoring techniques	34
5.1.3 Consistency checks on PVT	35
5.1.4 Navigation message checks	35
5.1.5 Use of augmentation data	36
5.1.6 Fallback options	36

5.2	Dedicated interference detection systems	37
5.3	Non-technical anti-spoofing measures	38
5.4	Conclusions	38
6	Spoofing in the real world	40
6.1	Information obscurity	40
6.2	List of GNSS spoofing and meaconing events	40
6.3	Risk and Impact	42
7	Vision and recommendations	43
7.1	Specific spoofing scenarios for NL	43
7.1.1	Rotterdam harbor	43
7.1.2	Schiphol airport	44
7.1.3	Road tolling	44
7.1.4	Amsterdam stock exchange	45
7.2	Recommendations to Agentschap Telecom	45
8	Summary and conclusions	47
9	References	51
Appendix A	Summary of papers	54
Appendix A.1	GNSS Interference threats and countermeasures	54
Appendix A.1.1	Chapter 3, The Spoofing Menace	54
Appendix A.1.2	Chapter 8, Antispoofing Techniques for GNSS	59
Appendix A.2	A Survey of Spoofing and Counter-Measures	63
Appendix A.2.1	Introduction	63
Appendix A.2.2	Spoofing	63
Appendix A.2.3	Countermeasures	64
Appendix A.3	Improving the Operation and Development of Global Position (GPS) Equipment Used by Critical Infrastructure	67
Appendix A.3.1	Installation and Operation Strategies for Owners, Operators, and Installers	67
Appendix A.3.2	Development Strategies for Manufacturers	67
Appendix A.3.3	Research Opportunities	68
Appendix A.4	The economic impact on the UK of a disruption to GNSS	69
Appendix B	Interviews	70

Abbreviations

ACRONYM	DESCRIPTION
AGC	Automatic Gain Control
BPSK	Binary Phase Shift Keying
CRPA	Controlled Radiation/Reception Pattern Antenna
DGNSS	Differential GNSS
DME	Distance Measuring Equipment, an aeronautical radio navigation technology
EC	European Commission
EIRP	Equivalent Isotropically Radiated Power
EGNOS	European Geostationary Navigation Overlay Service
FCC	Federal Communications Commission
FRPA	Fixed Radiation/Reception Pattern Antenna
GAGAN	GPS Aided Geo Augmented Navigation
GLONASS	GLOBAL'naya NAVigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
IC	Integrated Circuit
ILS	Instrument Landing System
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
JRC	Joint Research Centre
MBOC	Multiplexed Binary Offset Carrier
MSAS	Multi-functional Satellite Augmentation System
MSPS	Mega-Samples Per Second
NLR	Netherlands Aerospace Centre
NMA	Navigation Message Authentication
NSL	Nottingham Scientific Limited
OS	Open Service
PNT	Position, Navigation, Time
PPD	Personal Privacy Device
PPP	Precise Point Positioning
PRN	Pseudo Random Number
PVT	Position, Velocity, Time
QPSK	Quad Phase Shift Keying
RF	Radio Frequency
RTK	Real Time Kinematics

ACRONYM	DESCRIPTION
SBAS	Satellite Based Augmentation System
SCER	Security Code Estimation and Replay
SDR	Software-Defined Radio
UHF	Ultra High Frequency, the radiospectrum between 300 and 3000 MHz
UTC	Coordinated Universal Time
WAAS	Wide Area Augmentation System

1 Introduction

This report describes the findings of an exploratory study into GNSS spoofing and meaconing performed by the Netherlands Aerospace Center (NLR) for Agentschap Telecom. Agentschap Telecom is the Radiocommunications Agency in the Netherlands responsible for obtaining and allocating frequency space and monitoring its use. The work of the agency also covers the entire field of wireless and wired communication.

1.1 Objective

The main goal of this report is to guide the Dutch Radiocommunication Agency in policy and decision making regarding GNSS spoofing, scoped to incidental spoofing, small criminals and terrorist activities. Military and Governmental spoofing activities are out of scope, but are reported where appropriate.

1.2 Research questions

The investigation is based on the research questions defined in the request for quotation [1], including the traceability to answers in this report:

1. Provide an up-to-date inventory (including trends and expectations) of the possibilities and developments that can lead to the deception of equipment that uses GNSS signals, where:
 - a. a subdivision is made of equipment for place, navigation or time which is insensitive or sensitive to deception of GNSS signals;
Answered in chapter 4.2;
 - b. a detailed overview is provided of all actors who influence the occurrence of spoofing or meaconing;
Answered in chapter 2 and more specifically for the Netherlands in chapter 7.1;
 - c. a detailed overview is provided of all occurrences that have already taken place with an indication of the likelihood of spoofing or meaconing (nationally as well as internationally).
Answered in chapter 6.2;
2. Paint a detailed picture of future spoofing and meaconing threats and their manageability in relation to the further increasing use of GNSS.
This question is not easily answered in a single, detailed picture as it deals with future, unknown developments. Chapter 2 lists the currently foreseen threats. The manageability is addressed with countermeasures in chapter 5, and recommendations for manageability are provided in chapter 7.2.
3. Provide the substantiated vision of the researcher about the feasibility (economic/technical) to detect meaconing and spoofing (at an early stage). In addition to detection techniques evaluate organizational solutions such as a reporting hotline.
Answered in chapter 5; The researcher vision is provided in the conclusions of this chapter (chapter 5.4).

4. Given the ever increasing use of GNSS and the inherent vulnerability of the technology, what measures can be taken to reduce the risk of spoofing
 - a. from the point of view of protecting the frequency spectrum?
 - b. regarding certification and approval of electronic equipment and radio equipment?
 - c. from the point of view of cybersecurity and electronic radio equipment?

Answered in chapter 5; Specific recommendations for the Netherlands are provided in chapter 7.2.

5. According to the observation and judgment of the researcher, what are the possibilities and trends that (can) increase national resilience, regarding both measures taken by the end user as well as governmental measures?

Answered with recommendations to Agentschap Telecom in chapter 7.2.

1.3 Research approach

The research approach consisted of a literature study, supplemented with interviews with stakeholders and experts. The literature study gave first answers to the research questions from a technical point of view. This view was given to the interviewees in advance of the interview. Objective of the interviews was to improve this view - both technological and organizational - and to learn from experience in the field.

1.3.1 Literature study

The keywords GNSS, GPS, spoofing, meaconing, interference were used to identify useful sources of information. Of the resulting sources especially the more recent publications were selected. Because of the (assumed) increasing risk of GNSS spoofing over the last decade, older publications were perceived as less valuable.

Conference papers on GNSS spoofing and meaconing were generally rather easy to find, because GNSS conference nowadays have separate sessions dedications to GNSS spoofing and interference.

Some important sources of information are:

- GNSS Interference threats and countermeasures (chapters 3 and 8), Fabio Dovic (Editor), Artech House, London, 2015, ISBN 978-1-60807-810-3;
- A Survey of Spoofing and Counter-Measures, Christoph Günther, Navigation: Journal of the Institute of Navigation, vol. 61, no. 3, pp. 159-177, 2014;
- The economic impact on the UK of a disruption to GNSS, London Economics, 2017;
- GNSS user technology report – issue 2, European Global Navigation Satellite Systems Agency GSA, 2018;
- Improving the Operation and Development of Global Position System (GPS) Equipment Used by Critical Infrastructure, National Cybersecurity & and Communications Integration Center, and National Coordinating Center for Communication, 2017;
- Conference proceedings of the most recent GNSS conferences (ENC, ION, Navitec).

A full list of references is found in chapter 9.

1.3.2 Interviews

Each interview addressed the following topics from the point of view of the stakeholder:

- Importance of GNSS;
- Most seen spoofing techniques;
- Most promising detection and mitigation measures;
- Known spoofing incidents;
- Recommendations for governmental support.

The stakeholders were selected based on their knowledge of GNSS applications, GNSS technology, the use of GNSS in critical infrastructure and/or GNSS interference and spoofing. The following stakeholders were interviewed.

1. Lennard Huisman, geodesic at Kadaster;
2. Mark Dumville, general manager and Enrique Aguado, principle project manager at Nottingham Scientific Limited (NSL);
3. Jean-Paul Henry, operational manager O6-GPS;
4. Daniele Borio, researcher at the EC Joint Research Centre;
5. Peter Zwamborn, scientist at TNO;
6. Allard Dijk, lecturer ICT at Netherlands Defense Academy.

The interviews were mostly conducted via telephone. A summary of each interview is found in Appendix B.

1.4 Document structure

This report is structured as follows:

Chapter 2 introduces the importance and use of GNSS, introduces GNSS vulnerabilities and sketches different GNSS spoofing scenarios.

Chapter 3 provides background information about GNSS in general and the different types of interference that can impact GNSS applications. Furthermore it is described how the perceived threat of spoofing has grown over time. This chapter is mainly of interest to readers that are less familiar with GNSS.

Chapter 4 introduces the classification of spoofing attack types and explains the susceptibility of GNSS receivers to spoofing. Spoofing attacks are classified according to their complexity.

Chapter 5 contains an overview of all the different mitigation measures against spoofing that have been proposed and in some cases are already implemented. This chapter also describes methods to detect spoofing.

Chapter 6 describes the actual impact of spoofing. This chapter contains a list of spoofing incidents that have been reported in the past.

Chapter 7 further details two high-impact spoofing scenarios that are very relevant to the Netherlands and contains the recommendations to Agentschap Telecom that will increase resilience against spoofing.

Chapter 8 contains the summary and conclusions.

2 Spoofing

2.1 Introduction

Nowadays, using smartphones and other electronic devices, we have access to accurate time and our position almost continuously and it takes no effort to work out a convenient route to go from A to B. This is made possible by GNSS satellites that continuously transmit highly accurate timing signals towards earth. Tiny receivers, embedded in phones, cars, and in all sorts of devices, pick up these signals and within seconds works out the actual time and position.

Each GNSS satellite is equipped with a highly accurate atomic clock. With four or more satellites in view a receiver can work out the signal delay from each satellite and determine its own position with meter-accuracy and time accurate to better than a microsecond. The Global Navigation Satellite Systems (GNSS) are so effective at delivering position and time accurately and reliably that our societies have become dependent upon them. GNSS is available worldwide, it is highly accurate and it is essentially free of charge. Alternative means for deriving time and position exist, but these cannot compete with GNSS on price and convenience. As a result, GNSS receivers are now deeply embedded in countless systems and applications. GNSS has become the dominant engineering solution when building systems requiring position and timing.

GNSS time and position is indispensable in numerous applications. Position services are used in surveying, navigation, precision farming, road tolling, etc. Without accurate position, transport systems and supply chains would come to a halt. GNSS time is vitally important in computer networks, electricity transmission, and broadcasting and telecommunications networks. The systems all require accurate and synchronized time across a geographically distributed network. Additionally GNSS is used for the distribution of UTC time, the international time scale, such that events can be timestamped no matter where they take place. A service that is vital for financial trading and in the analysis of market anomalies. Many applications derive GNSS time to a far greater accuracy than they actually require, taking advantage of the availability and affordability of GNSS signals.

Despite all the advantages of GNSS, there are drawbacks. The GNSS signals are inherently weak such that GNSS receivers struggle in built-up areas and reception is virtually impossible in-doors. Additionally, the weak GNSS signals are easily corrupted due to unintentional or intentional interference and the receivers are increasingly vulnerable to cyber-attacks. Given the interdependency of modern networks, a system of systems has developed in which GNSS is the dominant source of position and time. Our awareness of the fact that GNSS is becoming the single point of failure is growing.

A specific GNSS vulnerability is spoofing: the interference of the genuine satellite signals with artificial GNSS signals from a different source. Spoofing can be very deceptive. If done properly, a GNSS receiver will lock on to these artificial signals and generate false position and time without signaling that something is wrong. Potentially this is more damaging than ordinary interference that causes an outage of GNSS when the receiver loses track of the signals. In that case no misinformation is generated. Spoofing can be both unintentional and intentional.

2.2 Spoofing scenarios

Spoofing effects can happen due to malfunctioning GNSS equipment or the erroneous use of equipment such as GNSS repeaters. As an example realistic scenario, a GNSS repeater in an aircraft hangar is left on while the hangar doors are open. The signal of the repeater propagates outside the hangar, affecting the navigation systems of nearby aircraft landing, taxing and taking off. Their on-board GNSS receiver may lose reception, or worse, it can be misled to think it is positioned in the hangar. The risk of an accident is increased accordingly [32].

More often, spoofing is associated with intentional attacks to mislead GNSS receivers. The potential motivations for spoofing attacks are rather diverse, reaching from terrorism, through fraud, to avoiding traceability by the employer. Each possible motivation has a different target and requires a different amplitude of the induced error. The following scenarios/motivations are found in literature. In the cases where the attacker has a clear alternative to achieve his goals, the alternative is indicated.

Scenario #1:	Road vehicle
Description	A terrorist who wants to send a road vehicle onto a collision path. The necessary position error is only a few tens of meters, corresponding to a fraction of a microsecond in propagation time [9].
Actor	terrorist
Goal	strike chaos and fear
Potential impact	vehicle damage; danger to driver or passengers; danger to surrounding people.
Equipment	advanced
Alternative	-

Scenario #2:	Curious hacker
Description	A curious amateur hacker has read an article about modern software-defined radio hardware and is interested to try it himself. He buys a SDR platform for a few hundred euros and starts experimenting. After first experimenting with RF reception, he then tries the generation and transmission of RF signals. Generally it is difficult to judge the quality of the generated RF signals without more advanced RF equipment such as a spectrum analyzer. He then discovers GPS simulator software [10]. Generating GPS signals is fun, because with any GPS receiver, he can immediately see what is happening. While enthusiastically experimenting with the SDR hardware and the navigation system in his car, he forgets that he is also spoofing other GPS systems in his surroundings as well.
Actor	amateur hacker
Goal	satisfy curiosity
Potential impact	unintentional disruption of nearby GNSS receivers
Equipment	simple
Alternative	-

Scenario #3:	Toll evasion
Description	Drivers who want to evade toll need to displace their position by a few kilometers, i.e., delays in the order of tens of microseconds [9].
Actor	drivers / vehicle owners
Goal	tax evasion
Potential impact	financial damage
Equipment	simple to medium
Alternative	GNSS jamming depending on implementation

Scenario #4:	Digital tachograph
Description	Drivers who want to manipulate their digital tachograph to be able to drive more hours than allowed by regulations [50].
Actor	professional drivers / vehicle owners / company
Goal	illegal economic gain
Potential impact	tax evasion; unsafe driving / increased accident risk.
Equipment	simple to medium
Alternative	-

Scenario #5:	Avoid traceability
Description	Drivers who want to avoid traceability for privacy reasons or to hide criminal activities.
Actor	thieves of cars or cargo / drivers of company cars
Goal	avoid tracking
Potential impact	economic damage / theft
Equipment	simple to medium
Alternative	GNSS jamming

Scenario #6:	Fishing
Description	Fishermen who want to catch fish outside of the permitted areas need displacements in the order of tens of kilometers, i.e., delays up to a fraction of a millisecond [9].
Actor	professional fishermen
Goal	illegal economic gain
Potential impact	environmental damage
Equipment	simple to medium
Alternative	GNSS jamming

Scenario #7:	Financial transactions
Description	Organizations who want to make money by manipulating financial transactions need timing errors at the millisecond-level [9] [21]. The motivation is financial benefit, but it remains unclear how this benefit arises exactly.
Actor	financial professionals
Goal	illegal financial gain
Potential impact	impact: large financial damage
Equipment	advanced
Alternative	cyberattack?

Scenario #8:	Synchronization power network
Description	Spoofing attacks that impact the GPS timing signals for network synchronization in the energy sector [21] [2]. Because of the large amounts of (electrical) power involved small synchronization errors can potentially result in permanent damage to the electrical power generating and transport infrastructure.
Actor	terrorist
Goal	large-scale power outage, strike chaos and fear
Potential impact	large scale economic and societal damage due to prolonged power outage
Equipment	advanced
Alternative	-

Scenario #9:	Synchronization communication network
Description	Spoofing attacks that impact the GPS timing signals for network synchronization in the telecom sector making communication impossible [2].
Actor	terrorist or criminal
Goal	strike chaos or hide criminal activities
Potential impact	local or large-scale communication disruption
Equipment	advanced
Alternative	-

Scenario #10:	Offender tracking
Description	Offender tracking is particularly vulnerable to jamming and spoofing because this would liberate the offenders, and allow them to leave the fenced area that they may legally occupy [21] [2].
Actor	criminal
Goal	restrictions to freedom of movement
Potential impact	escape of criminal; undetected criminal activity; reduced trust in legal system.
Equipment	medium
Alternative	GNSS jamming depending on implementation

Scenario #11:	Ship
Description	A terrorist who wants to change the course of a ship to make it collide or run ashore [2]. This scenario is similar to scenario #1, but a large ship is a higher value target.
Actor	terrorist
Goal	strike chaos and threaten government
Potential impact	large economic/financial impact; loss of life; environmental damage.
Equipment	advanced
Alternative	(coordinated) GNSS jamming

Scenario #12:	Augmented reality
Description	Playing an augmented reality game on their smartphone, some players decide to cheat and use GPS spoofing apps to fake their position to collect more points [19]. The spoofing is purely done in software, no RF signals are generated, but the effect is the same as an RF-signal GNSS spoofing attack.
Actor	civilian
Goal	virtual gain
Potential impact	(minor) reputation damage to game owner
Equipment	simple / software
Alternative	-

3 GNSS background

3.1 GNSS systems

GNSS is the term for any “Global Navigation Satellite System”. Currently there are four main systems in different stages of completion:

- GPS (U.S.);
- GLONASS (Russia);
- GALILEO (Europe);
- Beidou-2 (China).

Each system of satellites maintained by one organization is termed a “constellation”. The overall designs of different constellations are remarkably similar. All transmit three basic messages:

1. a ranging signal for position, velocity and timing (PVT);
2. precise ephemeris data, which specifies the exact location of the individual satellite;
3. an almanac, which specifies the locations and orbits of all satellites in the constellation, along with status information, used to select satellites for tracking.

This basic degree of interoperability allows GNSS receivers to read signals from the four satellite constellations and so avoid blackouts or poor reception by taking into consideration satellites from other constellations that may be visible. It has been estimated that by 2020 around 100 GNSS satellites will be available, with 30-40 visible at any one time [2].

3.2 Augmentation

In addition to the main GNSS signals there are also local corrective signals which use a variety of techniques. Differential GPS uses ground-based receivers in precisely-determined locations that measure the local signal errors for each GNSS satellite in view. These errors are then re-broadcast either using ground-based (GSM) networks, or using geostationary satellites. The correction signals are picked up by GNSS receivers and used to refine the navigational and timing solution. When combined with the main GNSS signals, these methods can provide positional accuracy up to 10-15 cm. The drawback with all augmentation systems is that they only provide useful information for the area in which the augmentation system is located. Typical augmentation technologies used for commercial applications are Precise Point Positioning (PPP, regional) and Real Time Kinematics (RTK, local).

In aviation, the focus of augmentation is not on accuracy but on integrity. A landing aircraft must have a very high degree of confidence in its navigation systems to perform a landing with partial or zero visibility. This means that the chance of a false position being reported *without* the pilot being warned, must be extremely low. To this end, specific augmentation systems have been designed and built called Satellite Based Augmentation Systems (SBAS). SBAS systems typically cover a continental region and use geo-stationary satellites for transmission of correction data. The most well-known SBAS systems are WAAS (continental U.S. and Hawaii), EGNOS (Europe), MSAS (Japan), and GAGAN (India) [2].

3.3 Signal characteristics

At the lowest level a GNSS navigation signal can be seen as a sinusoidal wave in frequency bands between 1164 MHz (GALILEO E5a) to 1610 MHz (GLONASS L1) (Figure 1). In all cases what is encoded onto the analog carrier wave is a PRN (pseudo random number) sequence using digital modulation methods like BPSK (binary phase shift keying, GPS and GLONASS), QPSK (quad phase shift keying, Beidou-2) and MBOC (multiplexed binary offset carrier, GALILEO). These PRN codes are what the satellite receiver locks onto.

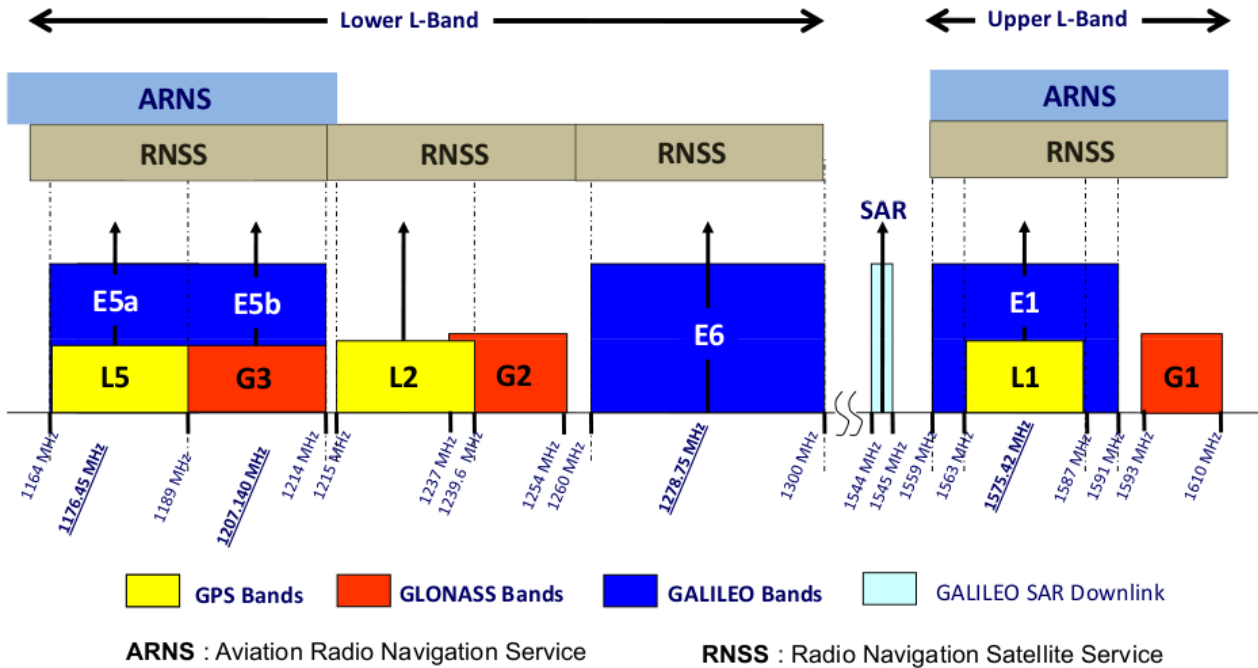


Figure 1: GPS, GLONASS and GALILEO frequency bands [3]

The GNSS satellites circle the earth at an altitude of between 19100 (GLONASS) to 35786 km (Beidou-2) and transmit the navigation signals with an RF power on the order of 100 Watt [5]. At the earth’s surface the GNSS signal power is received with a power between -163 dBW and -152 dBW. This is considered weak to most standards. It is below the noise floor of the GNSS receiver which is determined by the thermal noise level (-174 dBm/Hz) and the noise figure of the receiver [4]. This means that a local noise signal, transmitted at an appropriate frequency can easily overpower the legitimate satellite signals. In other words, all GNSS signals are susceptible to interference.

3.4 Interference

Due to the low received signal power, GNSS receivers are susceptible to interference. Interference can be subdivided by origin as follows:

- **Internal:** interference from the electronic circuits making up the GNSS receiver or larger system of which the GNSS receiver is a part.
- **External:** interference from external radio transmitters.
 - **Allowed:** interference from legal radio systems in or near the GNSS frequency bands (e.g. DME transmitters and other GNSS signals from other constellations).
 - **Unintentional:** interference originating from, sometimes, defective equipment or due to erroneous use of radio equipment.
 - **Intentional:**
 - **Jamming:** transmitting a noise signal at the appropriate frequency to overpower the legitimate satellite signals and make a GNSS receiver lose track of its PVT.
 - **Meaconing:** capturing and retransmitting of legitimate GNSS signals after a delay such that the GNSS receiver locks on to the retransmitted signals
 - **Spoofing:** involves the generation of counterfeit GNSS signals with the right strength to lift the GNSS receiver from the legitimate GNSS signals and trick the receiver into computing false positions, velocities and/or times.

3.5 Historic development of GNSS spoofing

In the early days of satellite navigation systems knowledge of the signals was not widespread and the equipment necessary to make spoofing devices was expensive. GNSS spoofing was unlikely and received little attention. Also the dependence on GNSS and thus the possible impact were relatively low.

The situation changed with time and the Volpe report [6] raised the issue in 2001. In the same year, Scott published his paper [7] on anti-spoofing and authentication, which triggered awareness in the scientific community and became the root paper for later research [9].

Nowadays the situation is very different compared to those earlier days. Information about the structure of GNSS signals is widely available on the internet [3] and a GPS signal generator is available for download [10]. Furthermore, software-defined radio (SDR) devices have become ever more powerful and are available at low prices. They provide generic platforms for the transmission and reception of radio signals in the GNSS and other frequency bands. This became very clear at the hacker's conference DEFCON 23 in 2015 where Chinese researchers in Huang and Qing Yang demonstrated GPS spoofing with relatively cheap, consumer-grade electronics and open-source software [11]. From that moment on, GPS spoofing was considered something within reach of the average hacker. Since that demonstration even cheaper hardware has become available. Currently a simple €5 USB to VGA adapter can spoof L1 GPS signals using open source software available on the Internet [14, p.22].

The interest in GNSS spoofing increased strongly with the introduction of Pokémon Go. Pokémon Go is a game developed for smartphones developed by Niantic and published by the Pokémon Company in the Pokémon Series. It was introduced in July 2016 in several parts of the world. The game uses augmented reality and GPS positioning to

project animations on pictures taken by the camera of the smartphone. The players of the game need to find, catch, and train the virtual Pokémon creatures. The creatures are found in different places in the real world [19].

To be able to find and catch Pokémon without having to leave their homes, many players were tempted to apply GPS spoofing. Figure 2 shows the relative popularity of the search terms 'Pokemon Go' and 'GPS spoof' in Google. Clearly the introduction of the popular game induced a large interest in the GPS spoofing. In reaction Niantic took some measures to make it more difficult to cheat. Nevertheless, the interest in GPS spoofing has not yet decreased to the level before the introduction of the game.

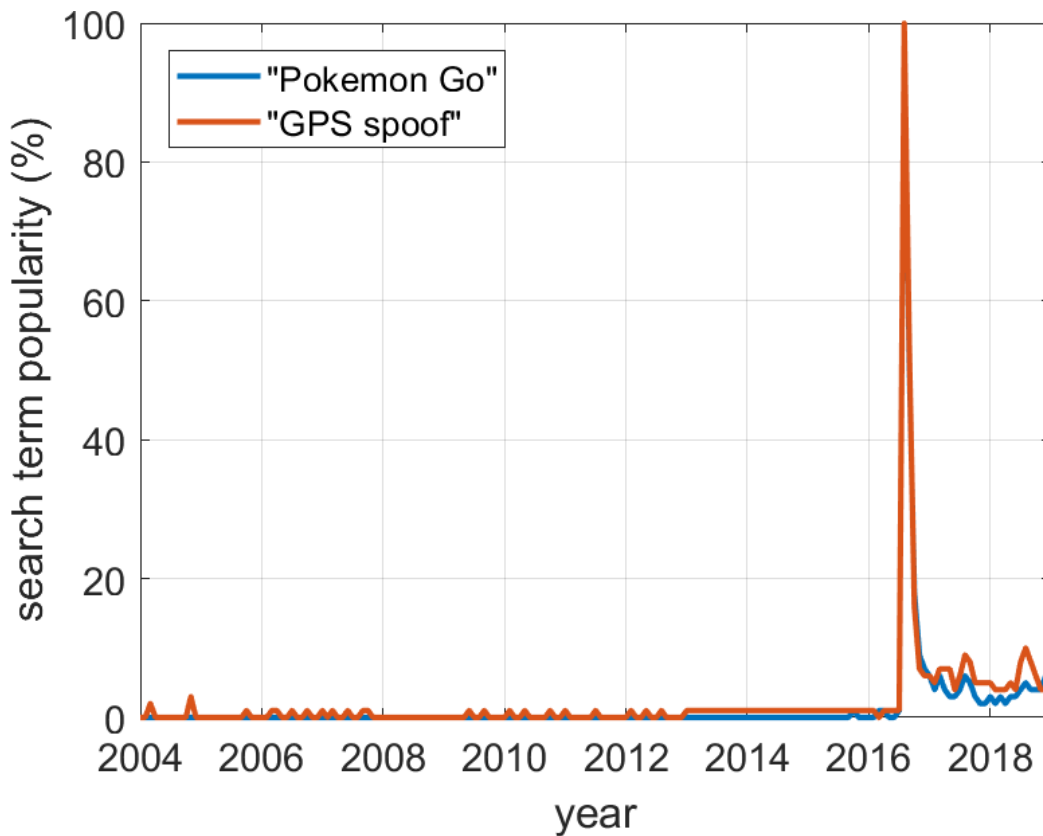


Figure 2: World-wide popularity of the search terms 'Pokemon Go' and 'GPS spoof' in Google [20]

4 GNSS spoofing techniques

Spoofed GNSS signals typically contain either a modified navigation message or a modified ranging code, or a combination of both. In case the GNSS receiver also uses augmentation, also the augmentation information can be manipulated. It might even be necessary to manipulate the ranging code, navigation messages and augmentation information to make sure they are consistent and let the receiver converge to the desired PVT.

4.1 GNSS spoofing attack types

There are different kinds of GNSS spoofing attacks or techniques. These techniques can be classified in different ways. Various formats have been described in the literature on the basis of sophistication, the way in which the signal is presented to the GNSS receiver, the necessary equipment, etc. [8,9].

The most important spoofing categories are

- non-signal technique (cyberattack);
- cable inject;
- non-coherent technique, single spoofer;
- coherent technique, single spoofer;
- coherent technique, multiple spoofers;
- meaconing.

The different spoofing techniques are compared below. It is noted that the first three techniques and meaconing appear the most relevant to small criminals and terrorists as limited hardware and control of the signals are needed. The coherent techniques give greater control over the victim receiver, but are harder to implement and require more hardware.

4.1.1 Non-signal (cyberattack)

In many cases, the easiest way to mislead a device into producing false PVT information is not to tamper with the GNSS signals. Instead, the PVT solution of a receiver can be altered after it has been calculated. This attack applies to integrated systems that contain a GNSS module. The interface between the GNSS chip and the system is taken over, replacing the observed PVT solution with the desired falsified data. Such an attack has the property of only affecting the targeted system, and does not require spoofing RF signals to be transmitted. To achieve this, the communication between the GNSS module and the application could be intercepted, falsified and attacked. This could be carried out on hardware level or on software level where the data-interface is hacked. In most cases this type of attack will apply to networked devices such as smart phones, by breaking into the device using the available internet connection. Non-signal spoofing can even happen accidentally when the interface between the GNSS chip and the system is disrupted due to legitimate software upgrades.

Strictly speaking a non-signal attack is not a GNSS spoofing attack, since no actual GNSS signals are spoofed. Nevertheless the method is presented here as it has the same result as a GNSS spoofing attack. It has a few advantages above the real spoofing attacks:

- No RF equipment is needed;

- The non-signal attack cannot be detected by monitoring the RF spectrum;
- Only the intended device is affected, instead of all devices in a particular area as with spoofing over the air.

4.1.2 Cable inject

In this case, the spoofer directly injects his signal into the receiver front-end either by unplugging the antenna cable and by connecting it to the spoofing source or by significantly attenuating the GNSS signals and injecting the spoofing signal at the same time. This option gives the spoofer the maximum control possible. It can be implemented whenever the receiver is under the spoofer's control, e.g. in the case of drivers that are trying to manipulate the tracking systems of their own vehicles (road monitoring). This is also known as a collaborative spoofing attack as there is a certain cooperation from the receiver.

The spoofing signals do not travel through the air and, in principle, cannot be detected by monitoring the spectrum. The spoofer has full control of all RF signals that enter the receiver and only the intended device is affected.

4.1.3 Non-coherent, single spoofer

In this case a single spoofer device transmits its signals through the air to the victim receiver. The spoofer and the authentic GNSS signals are not coherent, such that there is no fixed relation between the phase of the two signals at the antenna of the victim receiver. The spoofer cannot coherently cancel the authentic GNSS signals. It has to jam and/or overpower them with the spoofed signals.

The spoofing signals travel through the air making that in principle all GNSS devices in a certain area are affected and that the attack in principle can be detected by monitoring the RF spectrum. The spoofer can also be detected based on the fact that all (false) satellite signals originate from the same direction.

The hardware requirements for a non-coherent, single spoofer attack are very low. In general a suitable antenna, computer and consumer-grade radio front-end are sufficient. The necessary software can be found on the internet.

4.1.4 Coherent, single spoofer

In this case the spoofer knows the precise location of the receiver's antenna, as well as the phasing of the signal. In the coherent case, the spoofer suppresses the main component of the authentic satellite signal by subtracting a synthesized copy of that component for a time long enough to capture the receiver to his signal.

The greater control of the RF signal makes this attack more difficult to detect by the receiver, but at the same time it is more difficult to implement. It only works when the spoofer and victim antennas are known with sub-cm accuracy such that the signal propagation delays can be determined sufficiently accurately. While already challenging for a stationary victim, this is even more difficult for a moving victim. It only works perfectly for one victim receiver at a time. For other receivers with antennas placed elsewhere the signal propagation delays are different and the spoofer does not reach the desired effect.

The attack can be detected by monitoring the RF spectrum. The spoofer can also be detected based on the fact that all satellite signals originate from the same direction.

4.1.5 Coherent signal, multiple spoofers

In this case the attacker uses multiple spatially-distributed, coherent spoofing transmitters such that it can mimic the direction of arrival of the genuine GNSS signals. As in the previous case the antenna positions of the transmitters and receiver(s) need to be known with sub-cm accuracy. Due to the high level of control this attack can be very effective and is also difficult to defend against, but at the same time it is very difficult to implement. For this reason it is also seen as very sophisticated spoofing.

4.1.6 Meaconing

Meaconing can be seen as a separate attack category that is simpler to perform than spoofing because there is no need for software to generate the GNSS signals. In its most simple form, only a hardware repeater system is necessary. Such GNSS repeater systems are available commercially for applications where GNSS reception is needed indoors, e.g. in aircraft hangars or in buildings of emergency services. It is also possible to store the received GNSS signal and re-play the signal from memory. Digital processing is not required for a simple meaconing attack, but may be used in more complex attacks.

As live signals are recorded and replayed, a meaconing attack always consists of exactly the same satellites as the real signals. Also, all GNSS constellations will be included by definition. The meaconing signal is usually (much) stronger than the live satellite signals. However, the signal shape is identical to the original signals. In a successful meaconing attack the victim GNSS receiver will obtain the PVT of the meaconing antenna at the moment it received the signals. A meaconing attack can be recognized by the resulting jump in position and/or time in the PVT.

4.2 Spoofing hardware and software

Various types of hardware and software can be used for GNSS spoofing, ranging from very simple to extremely complex. This section provides an overview of the hardware and software currently available to a would-be spoofer.

The required hardware and software varies with the spoofing attack type. Typical spoofing equipment requires the following components:

- software capable of generating GNSS signals;
- software capable of generating GNSS navigation messages;
- a software-defined radio transmitter that transforms a digital data stream into an analog UHF signal;
- an amplifier to boost the UHF spoofing signal to the desired strength;
- an antenna to transmit the UHF analog signal.

Obviously a non-signal attack requires no specific RF hardware and software, only generic computer tools. A cable injection attack does not require a transmit antenna.

More advanced types of spoofing may require additional software or hardware:

- an antenna to receive incoming GNSS signals;
- a software-defined radio to record incoming signals (analog to digital);
- algorithms to synchronize incoming and outgoing signals;
- algorithms to slowly ramp up spoofing signals;
- algorithms to slowly vary time / position of spoofed signals.

Table 1: Overview of spoofing hardware

Device	Reference	RF properties	Remarks	Price
bladeRF	https://www.nuand.com	61.44 MSPS Tx: 47 – 6000 MHz +8 dBm RF power		\$ 480, \$ 720
HackRF One	https://greatscottgadgets.com/hackrf/ https://www.elektor.com	20 MSPS Tx: 1 – 6000 MHz	Also cheaper clones with uncertain quality available online.	€ 300
USRP	https://www.ettus.com/ http://www.ni.com/nl-nl/shop/select/usrp-software-defined-radio-device		Available from Ettus and NI. Broad product range. Practically all devices can be used for spoofing.	€ 600 - € 12000
Avnet Zynq®-7000 SoC / AD9361 SDR kit	https://www.xilinx.com/products/boards-and-kits/1-45sl7b.html	0.20 – 56 MSPS Tx: 70 – 6000 MHz		\$ 1295
LimeSDR	https://limemicro.com/products/boards/limesdr	100 kHz – 3.8 GHz 61.44 MHz bandwidth +10 dBm		\$300 - \$800
ADALM-PLUTO	https://wiki.analog.com/university/tools/pluto	0.065 – 61.44 MSPS Tx: 325 – 3800 MHz +7 dBm RF power	Aimed at education.	€ 120

Table 1 contains a list of SDR devices that are commercially available and have the technical specifications necessary to spoof GNSS signals. The SDR hardware requirements to perform GNSS spoofing are:

1. The hardware platform needs to be able to transmit RF signals. Especially many low-cost SDR devices (e.g. RTL-SDR dongles) are receive-only and do not pose a threat.
2. The hardware platform needs to be able to transmit RF signals in the GNSS frequency band(s) (1200-1600 MHz). Popular transceiver chips, such as the Analog Devices AD9364, support the entire frequency range between 70 – 6000 MHz, giving easy access to the GNSS bands. However, even if the device is not (officially) capable of transmitting in the GNSS bands, it has been shown that out-of-band emissions (harmonics) can be abused to generate GNSS signals [42].
3. Sufficient bandwidth: The instantaneous bandwidth of the device needs to be sufficient. It needs to be as large as the bandwidth of the GNSS signal (at least few MHz). This is not normally a limitation as modern computer interfaces and DAC's easily provide the needed data rate.
4. Sufficient RF power. The platform needs to be able to generate sufficient RF power. This is normally no limitation. The typical SDR output is around 0 dBm, which is already orders of magnitude stronger than the level with which the GNSS signals are received. If needed the spoofing signal can easily be amplified further with an external amplifier.

5. The genuine GNSS signals are derived from very high quality clocks on-board the satellites. In order to generate credible spoofing signals the clock on the spoofing platform needs to be of a sufficient quality. The quality of the local oscillator can be a limitation on especially the cheaper SDR platforms.

If needed, additional equipment (GNSS antennas, cables, amplifiers) is available from companies like Mini-Circuits (www.minicircuits.com), Tallysman (www.tallysman.com) and Farnell (www.farnell.com). Prices typically range between € 10 and € 100.

Several software codes can be used for GNSS spoofing. Some of the more well-known codes are

- `gps-sdr-sim` : a simple, open source GPS spoofer [10];
- GNSSim : open source GNSS simulator [41];
- National Instruments Global Navigation Satellite System Toolkits, € 4670 (<http://sine.ni.com/nips/cds/view/p/lang/nl/nid/204980>).

Various research institutes and GNSS receiver manufacturers have implemented their own GNSS simulator to perform spoofing for test purposes. These software codes are typically closed, and only available upon request (if at all). On the other end of the spectrum, several commercial solutions exist which are aimed at developing and testing GNSS receiver hardware. Such fully-fledged GNSS simulators can simulate complete constellations, including effects such as interference, multipath and ionospheric disturbances. A GNSS-simulator connected to a transmitter becomes a GNSS spoofer. Some of the more common brands are listed below. Prices range from approximately € 10.000 to € 200.000 with a range of options.

Some well-known manufacturers are:

- Spirent;
- Ifen;
- Syntony;
- Orolia / Spectracom.

For more information also see the GPS World's annual Simulator Buyers Guide [43]. The more expensive GNSS simulators usually simulate all GNSSs. The open source `gps-sdr-sim` currently only generates GPS signals, but it appears reasonable to expect that it will be expended to also include other GNSSs such as GALILEO and GLONASS.

This assessment describes spoofing hardware and software available at the beginning of 2019. This overview will change as new RF hardware enters the market and new software becomes available. Over the years there has been a trend towards cheaper and more powerful hardware. This trend is driven by the development of ever cheaper and more potent computers and the wireless exchange of more and more data. There is no indication that this development will discontinue in the coming years.

4.3 GNSS receiver susceptibility to spoofing

4.3.1 Receiver categories

GNSS receivers can be categorized into snap-shot and tracking receivers [9].

- **Snap-shot receivers** sample the signal and subsequently process these samples from memory. The time span between two measurements varies widely. It is chosen in a trade-off of functional requirements and power consumption. This type of receivers is used in most consumer products.
- **Tracking receivers** continuously estimate the frequency, delay, and phase of the signal, i.e., they extensively use prior knowledge about the signal.

4.3.2 Receiver susceptibility

GNSS receivers go through a process of signal acquisition before going into the tracking phase. The susceptibility to spoofing attacks is rather different for the different phases [9]:

- **Cold Start** - Spoofing starts before acquisition and the receiver has no a priori knowledge. This situation occurs after a receiver is switched on (cold start). The receiver cannot distinguish the spoofer's signal from an authentic GNSS signal unless the signal is somehow authenticated [45].
- **Reacquisition** - Spoofing starts before acquisition but the receiver has a priori knowledge. This situation occurs if the receiver has lost one or all satellites for a short while, or acquires satellites that have newly raised above the horizon. Snap-shot receivers are in this situation for every estimate that they perform once they have prior knowledge.
- **Tracking** - Spoofing during tracking. This is the most demanding situation for the spoofer, since the signals now have to change in a manner compatible with the detailed physical movement of the receiver, as well as with the changes in its environment.

In addition to spoofing, GNSS receivers may have other vulnerabilities. There is a possibility that there are backdoors in GNSS chips similar to backdoors in other ICs. Backdoors can be used to bypass certain security measures. The chips could be made to respond in a certain way whenever a specific (RF) signal is received. The backdoor could be placed in the design of the IC by malicious employees of GNSS chip manufacturers. This vulnerability does not qualify as spoofing, but is seen as a possible threat. The RF signal necessary for activation of the backdoor could be seen as abuse of the RF spectrum.

5 Detection and mitigation of GNSS spoofing

It is safe to say that most available anti-spoofing techniques primarily perform detection. Given that spoofing signals can easily override true signals in strength, it is either difficult or impossible to filter out the original GNSS signals. This means that detection is most often followed by a fallback to an alternate navigation signal. This can be another satellite, another frequency band, another GNSS system or a completely different, non-GNSS system such as INS. In case no fallback is available, the minimum mitigation action is to warn the user with a spoofing alert.

The remainder of this chapter discusses the different options in more detail. Figure 3 shows the different mitigation options and their place in the system.

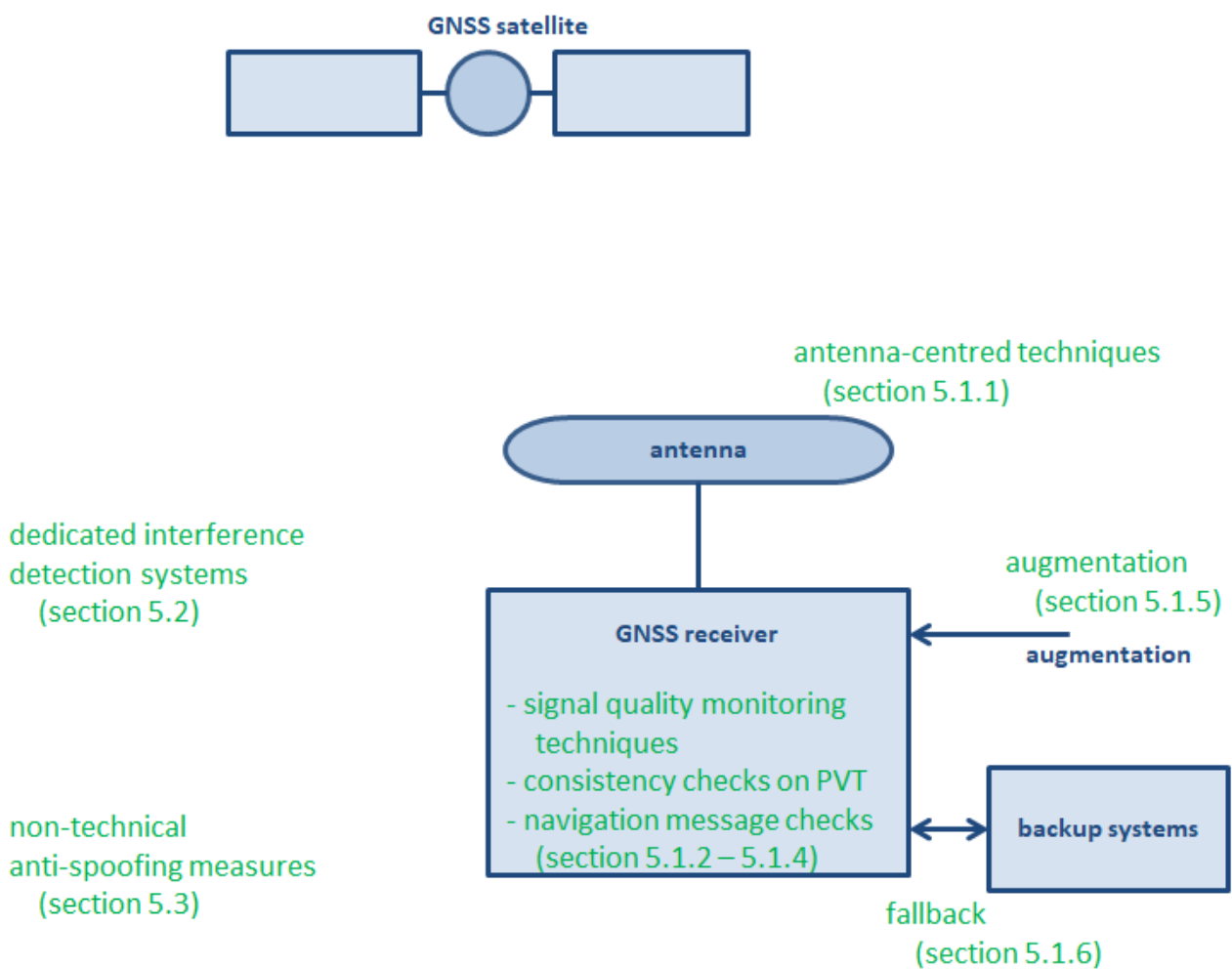


Figure 3: GNSS spoofing detection and mitigation options

5.1 GNSS receiver-based spoofing mitigation

5.1.1 Antenna-centered techniques

In most cases (simplistic and intermediate attacks), a spoofer uses a single antenna. Thus the spoofed signals all arrive from one single direction. The authentic satellite signals, on the other side, arrive from different directions. The genuine signals always arrive from the sky above whereas a spoofed signal will often arrive from the horizon or below. This may be used to detect and even localize the spoofer. This requires a directionally-sensitive antenna, typically implemented as an antenna array. A controlled radiation pattern antenna (CRPA) is such an antenna array. This antenna not only detects where the signal is coming from, but it can dynamically place a reception-null in the direction of the spoofer. This can effectively suppress an interference source or a spoofer, acting as a true mitigation, without the need for changes to the receiver itself. But CRPA antennas come at a price. They are larger, heavier and more expensive than the usual fixed radiation pattern antennas (FRPA). Traditionally CRPAs have been used in military applications, but there is a trend towards smaller, lighter and cheaper CRPA antennas for civil applications [8,9].

Instead of the direction of arrival of the GNSS signals, also the polarization of the signals can be used to distinguish between the genuine satellite signals and spoofed signals [12]. This method is not as wide-spread as the use of CRPA antennas.

A different method to detect spoofing uses two separate GNSS antennas placed at a fixed small distance from each other. In normal operation the positions obtained from these antennas have a fixed difference. However, in case of a successful attack with a single spoofer, both antennas will lock on to the same spoofed position. The absence of a position difference is a clear indication of spoofing. By careful analysis of the carrier phase and/or clock bias obtained from the two antennas, it is possible to extract more information such as the angle-of-arrival at both antennas [50].

5.1.2 Signal quality monitoring techniques

These techniques are applied in the RF front-end and at baseband processing in the GNSS receiver and utilize the differences between the genuine GNSS signals and the spoofed signals to detect spoofing.

5.1.2.1 Signal strength

A typical jamming or spoofing signal will enter the receiver with a higher power than the genuine GNSS signals. In poorly performed attacks the signal power might even be much higher. An attack can thus be detected by monitoring the signal power in the RF front-end. The automatic gain control (AGC) dynamically adjusts to the received RF signal power. The instantaneous AGC setting can thus be used as indication for jamming and spoofing. This requires the receiver manufacturer to monitor the AGC setting and apply an algorithm that signals suspected changes in the AGC [8,9].

5.1.2.2 Correlation properties

Spoofing can be detected by carefully monitoring the correlation function between the GNSS signal and a local replica. A regular GNSS signal will have a symmetrical correlation function with a given peak height. A spoofed signal will have an asymmetric peak or a peak which is atypically sharp or flat. This technique can be used to detect even sophisticated spoofing attacks at the moment that the spoofed signal is ramped up to override the original signal.

The superposition of signals is difficult to distinguish *a priori* from multipath (risking false alarms), but previous tests show that multipath and spoofing have different properties. In general situations it is recommended to estimate the multipath components associated with the signals transmitted by the visible satellites on all carrier frequencies and to use these to discriminate the spoofer from multipath [8,9].

5.1.3 Consistency checks on PVT

A simple way of detecting spoofing is by performing consistency checks on the PVT. These checks are applied on application level in the GNSS receiver and are based on the fact that spoofing can induce unphysical changes in the PVT:

- check for position discontinuities (sudden jumps in position);
- check for time discontinuities (sudden jumps in time);
- check for position changes (velocity, acceleration) that are impossible for the specific application;
- cross-compare single-constellation PVT solutions (use difference GNSSs);
- perform consistency check of code and phase range rate measurements. For authentic signals the Doppler frequency and code delay rate are consistent;
- check time consistency (check consistency of GNSS system times from different satellites).

Depending on the application the GNSS receiver might be integrated with an INS or an atomic clock. In these cases spoofing can be detected from regular comparisons between the PVT and the INS or atomic clock.

These consistency checks have relatively low complexity and receiver cost. They can only provide spoofing detection not mitigation so they are best combined with a fallback option. Consistency checks do not completely rule out GNSS spoofing, but they make life hard for the spoofer as he has to provide multiple constellations and multi frequencies and is limited in the size of the PVT changes that he can impose [8,9].

5.1.4 Navigation message checks

Currently all open civil GNSS signals are transmitted in the clear, conforming to interface specifications that are available fully in the public domain. Receivers will accept any input that conforms to the specifications and treat it as if it came from a GNSS satellite. Given the low power of the GNSS signals, this makes it very easy to spoof a GNSS receiver. This is true not only for the ranging signals, but also for the navigation messages which contain information about the GNSS satellite orbits. To mitigate GNSS spoofing these navigation messages should be checked by the GNSS receiver.

Synthetic or manipulated navigation messages can be detected by analyzing

- the scheduling of changes in the navigation message;
- the conformances of changes in the parameters with models of satellite orbits;
- the signature (authentication) of the navigation message.

Navigation message authentication (NMA) has long been considered as an important anti-spoofing measure. This cryptographic technique leaves the navigation message readable in open form, but adds an encrypted digital signature of the navigation message using a secret key only known to the GNSS system provider. The digital signature is transmitted as part of a data block alongside the navigation message. After reception the end user can verify the signature is true giving confidence that the navigation message is authentic.

The length of the public key and the cryptographic signature should be long enough to guarantee acceptable security. However, long signatures can take considerable time to transmit on a typical channel of 50 bps. Furthermore a receiver needs to receive the entire navigation message before it can be verified. This means that there is a delay between the moment a navigation message is introduced and the moment it can be checked in the receiver. This delay might be abused by an attacker [48]. Due to the possibility of transmission errors, signatures need to be protected by error correcting codes. In order to reduce the authentication delay, the navigation messages may additionally be signed using a different asymmetric cryptosystem in the Internet. This requires that the receiver has access to the Internet, which most receivers do [8,9,13].

Navigation message authentication will be introduced to GPS and Galileo in the coming years. After introduction in the space segment and the GNSS signals, receiver manufacturers still need to implement NMA in receivers. But navigation message checks and authentication are no panacea. They are robust against simplistic spoofing, but they are of no use against GNSS meaconing, because meaconing re-broadcasts the authentic navigation messages including the signatures. It is thus recommended to combine NMA with other anti-spoofing measures. More thorough encryption techniques, such as navigation message encryption and encryption of the full GNSS signal are technically feasible, but out of scope in view of the current research questions.

5.1.5 Use of augmentation data

For many applications the availability and accuracy of a PVT based on the bare GNSS signals is insufficient. Such applications typically use augmentation techniques for improved performance (e.g. RTK in precision farming). In general, the use of augmentation data opens up a new vulnerability as also these signals can be manipulated. But at the same time the augmentation will increase robustness against spoofing. If the local RF signals from the satellites are spoofed, but the augmentation signal is genuine, the receiver will generally be unable to match the two signals and converge to a solution. Without additional information the receiver will not be able to determine that GNSS spoofing is the cause of the problems, but it can detect something is wrong [49].

5.1.6 Fallback options

Two forms of fallback are distinguished:

- fallback to other GNSS signals;
- fallback to non-GNSS systems.

If a specific GNSS signal is spoofed, the first option is to fallback to different GNSS signals. These signals can be at different frequencies and/or part of a different constellation. Prerequisites are that the antenna is multi-band and that the receiver is capable of multi-band and/or multi-constellation. Obviously, the other GNSS signals can also be spoofed, but complexity is raised significantly if signals belonging to different constellations and at different

frequencies need to be generated in a consistent manner. Possible discrepancies between the different GNSS signals can also be used as an indicator for spoofing. There is already a trend in GNSS receivers towards multi-frequency and multi-constellation driven by a need for higher PVT accuracy and availability. To counter the use of multiple frequencies and multiple constellations, a spoofer might decide to jam a number of signals/frequencies and spoof only one (or a limited number of signals) to reduce the spoofing complexity [8].

Fallback to non-GNSS systems is essential to completely remove the vulnerability to RF interference. Typical fallback systems are:

- communication systems (such as WiFi, GPRS, Iridium);
- Inertial Navigation Systems;
- stable clocks (such as atomic clocks).

The best (technical and economical) mitigation measure depends on the type of application. For example, in a vehicle the best solution might be to check the consistency of the PVT against a wheel sensor, in a smartphone the GPS time might be checked with the time received from the network, while for a military application a CRPA might be a suitable option [50]. For critical timing applications, a robust (atomic) clock is the best fallback in most cases.

5.2 Dedicated interference detection systems

Dedicated GNSS interference detection, for instance using an interference monitoring network, can be performed. These networks detect interference by measuring the amount of RF power in a given frequency band. Initially no analysis of the signal type or content is performed. Since they do not make use of the content of the RF signals, they function equally well against GNSS jamming and GNSS spoofing.

Agentschap Telecom operates an interference detection network in the Netherlands consisting of 15 nodes [46]. This national network also covers the GNSS frequency bands, but distance between the nodes is too large to reliably detect weak GNSS interference. A network with complete coverage that can also detect weak GNSS jamming and spoofing requires a much higher density. Typical spacing of the nodes would need to be 100-1000 m. It is difficult and especially very expensive to realize a nation-wide network with such density.

The EU H2020 STRIKE3 project performed dedicated GNSS interference monitoring in the GPS L1 band. The sensors used in STRIKE3 monitor the RF signal power to detect the interference. Interference signal characterization was performed only after detection. The STRIKE3 project also proposed GNSS interference reporting standards [24].

Crowd-sourced interference monitoring is an interesting concept that actually promises to realize very high network densities. The concept of crowd-sourced interference monitoring has been around since at least since 2011 [15]. In this concept a dense network of smartphones is used to monitor interference in the GNSS bands. The concept did not catch on immediately, also due to the quality of the smartphone GNSS chips and the inaccessibility of the GNSS measurement data. Only in recent versions of their operating systems have Google (Android 8.0) and Apple made available raw measurement data and AGC setting available to app developers. This enables the realization of actual smartphone-based interference monitoring apps. But for crowd-sourced networks to become a reality, several remaining issues need to be addressed:

- How to handle differences in the performance and quality of the different smartphones?
- How to persuade sufficient people to participate to crowd sourced interference monitoring?

- How to handle privacy of the participants and take care of possible legal constraints?
- What is an appropriate format in which the interference can be reported to the server?
- How should the server be organized? What should the algorithm look like that combines the reports from the individual smartphones?
- How and to whom should the interference monitoring results be presented?

Meanwhile, initial tests have confirmed the basic principle of crowd-sourced GNSS interference monitoring [16,17].

Large, dense interference monitoring networks (e.g. based on the crowd-sourcing concept) will generate large amounts of data. Specific techniques are needed to process this data and extract useful information from it, such as determining nominal GNSS performance, degraded performance, presence of interference. Big data and/or artificial intelligence techniques are expected to be necessary for the processing of the data from large interference monitoring networks. Similar technology is already being used for traffic information systems that utilize smartphone position information to estimating traffic delays.

5.3 Non-technical anti-spoofing measures

All the anti-spoofing measures described above have a technical nature. This reflects the focus of scientific literature on technical solutions. Below is a list of non-technical GNSS anti-jamming and anti-spoofing, partially inspired by the recommendations published at the website of the Resilient Navigation and Timing Foundation [18]:

- recognize GNSS as part of critical infrastructure and recognize the GNSS frequency bands as being of primary importance [46];
- protect the adjacent frequency bands to GNSS as “quiet” neighborhoods;
- raise awareness of the vulnerabilities of GNSS systems under users of these systems;
- encourage and support the development of complementary terrestrial PVT services as backup;
- ensure GNSS jamming and spoofing are recognized as a crime;
- ensure sufficient enforcement personnel to detect, prevent, respond to and prosecute jamming;
- support the creation of dense interference monitoring networks based on crowd-sourcing.

The effectiveness of a hotline specifically to report GNSS spoofing is questionable. Agentschap Telecom already operates a general hotline for radio interference that also covers GNSS jamming and spoofing. Users that are educated enough to recognize GNSS spoofing can be expected to contact this hotline. Furthermore, it is uncertain if actors or victims are willing to report GNSS spoofing as these incidents are usually associated with crime and/or the vulnerabilities of the victims. Taking that into account, a duty to report GNSS spoofing incidents to the existing hotline is probably more effective than a separate spoofing hotline. The duty to report could be similar to cyber security incidents reporting obligations.

5.4 Conclusions

The GNSS receiver plays an important role in the mitigation of GNSS spoofing as many mitigation options are receiver based. However, in many cases it is unclear if receiver manufacturers have implemented any anti-spoofing measures at all. And if so, it often remains unclear which measures have been implemented. Generally anti-jamming and spoofing measures make the receiver more complicated, more expensive, more power-hungry, etc. without

immediately contributing to the performance. The most important incentive for manufacturers to implement anti-spoofing measures is a clear demand for it from GNSS receiver users and authorities. This only happens when users and authorities are aware of GNSS spoofing and perceive it as a realistic threat. To the knowledge of the researchers thus far little anti-spoofing measures have been applied in receivers. One of the reasons the uptake of anti-spoofing measures is slow is that the optimal mitigation measure depends on the type of application.

In the meantime there are a growing number of GNSS receivers in use in various applications, including business and mission critical infrastructure. Often the detailed information on these receivers (make, type, age) is lacking [48]. Most likely they are not equipped with any anti-spoofing measures. So even if new GNSS receivers are protected with appropriate anti-spoofing measures, most of the receivers installed are expected not to have any anti-spoofing measures installed.

This holds especially for the timing receiver market. It is known that most timing receivers currently used, only make use of the GPS L1 C/A signal. Most of these receivers do not implement advanced features such as interference or spoofing detection. This is unfortunate because each timing receiver includes at least a reasonable clock which can be used as a fallback mechanism. This does require a proper detection mechanism to be implemented.

At this point it feels appropriate to refer to the publication “Improving the Operation and Development of Global Position System (GPS) Equipment Used by Critical Infrastructure” of the Department of Home Security [25]. This publication - released in 2017 - is intended as a Best Practices Guide to be used for improving the operations and development of GPS equipment used by Critical Infrastructure. It is mainly focused on GNSS jamming, but many of the recommendations are also beneficial against spoofing. They range from very practical (obscure antennas, provide decoy antennas) to rather general (enhance anti-jam capabilities). The paper is summarized in Appendix A.3.

Parallel to the above report, a study by the UK Government Office for Science was published in 2018 titled “Satellite-derived Time and Position: A Study of Critical Dependencies” [44]. In this report a broad analysis is presented of GNSS, its vulnerabilities and the dependence of the UK society on GNSS. Recommendations are made to increase resilience, particularly for critical infrastructure. The report provides a good overview of the challenges related to GNSS use. It is clear that in agencies in the UK have similar awareness of the issues as Agentschap Telecom. It is not known if the recommendations in the report are being implemented.

Apart from the recommendations by US Homeland Security and the UK Government Office for Science, the research has not revealed specific measures against spoofing in foreign countries. It is known that most receiver builders are including interference and spoofing measures in their latest receivers, especially the high-end models. At system level, both GPS and Galileo are introducing new signals and features in their latest satellites (GPS III and Galileo v2). These features include dual frequency use for open signals, and authentication for the Galileo OS. Especially signal authentication can increase the resilience to spoofing significantly. Generally, GNSS system-level modifications take a long time to implement: after introduction of a new signal it may take years for the full constellation to support it.

Finally the weakest link determines the security of the entire system. If a receiver implements automatic fall back from an encrypted/authenticated signal to an open signal, the protection may be negated. An attacker can jam all signals and then provide only the spoofed, unprotected open signal. If the receiver can be persuaded to use this signal it is effectively spoofed, despite the presence of the encrypted/authenticated signal.

6 Spoofing in the real world

6.1 Information obscurity

Information about actual events of GNSS jamming, spoofing and meaconing is scarce. The parties involved usually have little reason to make these events known, because they are illegal and usually associated with governmental or military operations or criminal activities. They also point towards vulnerabilities of legitimate applications of GNSS and critical infrastructure. Most of the time there is little reason to expose such vulnerabilities. Furthermore, GNSS jamming, spoofing and meaconing can be performed with low RF power such that only a limited number of receivers is affected and the effects are contained in a small area. In such cases events might remain unnoticed. In the cases where GNSS spoofing or meaconing are detected often the actors, equipment and motives remain unknown or undisclosed [23].

Interference monitoring by the STRIKE3 network appears to indicate that actual GNSS spoofing and meaconing events are very rare. STRIKE3 was an EU H2020 project, led by Nottingham Scientific Limited (NSL), aimed at GNSS interference monitoring [22]. As part of the project actual interference monitoring was performed worldwide, mainly using NSL's Detector probes. The monitoring was aimed at non-military GNSS interference. No monitoring was performed in warzones and areas of political sensitivity. Countries like Syria, Ukraine, Korea (North and South), Russia and China were excluded. In 3 years' time (January 2016 – December 2018) some 500.000 interference events in the GPS L1 band were detected with a few tens of sensors in about 100 locations worldwide. The majority of the interference events were interpreted as unintentional interference. Some 75.000 events were interpreted, based on the signal shape, as being intentional GNSS jamming. Some tens of events were detected where the interference signal had GNSS-like properties. The signals are believed to be non-malicious, although in general GNSS-like signal properties may indicate spoofing [23, 48].

Although much remains undisclosed, some (mostly high-power) GNSS interference events make it to the news. The Resilient Navigation and Timing Foundation [26] and its president Dana Goward are sources of up-to-date information on GNSS developments, including such interference, spoofing and meaconing incidents [48].

6.2 List of GNSS spoofing and meaconing events

This list contains the GNSS spoofing and meaconing incidents known to the researchers. Most of them appear to be of governmental/military, scientific or unintentional nature. Up until 2017 there have been no authenticated reports of criminal spoofing [27].

1. A prominent but contested spoofing incident is Iran's claim to have forced the landing of an American drone "RQ-170 Sentinel" in December 2011 by spoofing its GPS receiver [28, 29].
2. Humphreys demonstrated the feasibility of the capture of a UAV with unencrypted signals in 2012 [30].
3. In 2013 Humphreys controlled the course of a yacht at sea [31].

4. In 2010 a case of interference was experienced in Germany by a GPS repeater operated in a hangar in Hannover. The interference resulted in an alert of the Enhanced Ground Proximity Warning System providing the messages "pull-up" and "FMS/GPS Position disagree" during taxing and departure. With an EIRP of the GPS repeater in the order of -60 dBm (to be confirmed) the interference range was several hundred meters. The operation of the GPS-repeater has been suspended until the end of the investigation. It was noted that it remains to be seen whether the EIRP limit of -77 dBm as stipulated in the draft ECC recommendation ECC/REC/(10)02 would have ensured sufficient protection [32]. Apparently similar things have happened at Manila airport [33].
5. In late 2016, reports flooded in from Moscow about a strange disturbance near the Kremlin. When passing by the fortified complex at the cold heart of the Russian government, drivers found the GPS systems in their cars had been suddenly spoofed. In December, CNN confirmed that instead of showing the cars where they really were — cruising along the Moskva River — the GPS suddenly insisted the cars were 20 miles away, at the Domodedovo or the Vnukovo International Airport [34]. Similar reports have been received from St Petersburg where the apparent location is that of the Pulkovo airport [36].
6. Between 22 and 24 June 2017 a number of ships in the Black Sea reported anomalies with their GPS-derived position. They found themselves located at a nearby airport, some 25 nautical miles away. The anomaly has all the characteristics of a spoofing or meaconing attack: some 20 different vessels (GPS receivers) were affected, all reporting the same in-correct position. The position would periodically jump between the true location and the incorrect location. Who caused the anomaly, and why, is unknown [35, 36].
7. Also referred to as the Portland Spoofing Event, this incident occurred in the Portland Convention Center, Exhibition Hall on 28 September 2017 during the ION GNSS+ 2017 Conference. A GNSS simulator with 6 output ports was used for a demonstration. Only 1 of the outputs was actually connected to a device; the other 5 outputs were sealed with plastic caps. Even without an antenna the GNSS signal radiated tens of meters from the 5 unused outputs. Numerous smartphones were affected, but different phones reacted differently. Some maintained correct date and time, but gave wrong position. Other phones displayed both incorrect time (January 2014) and position. Especially the time shift resulted in the reappearance of old text messages, inability to fetch e-mail and problems with installing software updates. In one case it was necessary to wipe the phone and reinstall the firmware to get to a factory fresh state [37].

GPS spoofing related to Pokémon Go is not included in the list of GNSS spoofing events. There are two reasons for this:

1. It appears that most of the spoofing attacks for Pokémon Go were non-signal attacks (cyberattacks) involving manipulation of the smartphone software without actually broadcasting manipulated GNSS signals.
2. No authenticated reports were found that RF spoofing of the GPS signals was performed for the benefit of Pokémon players.

There has been speculation about the motif for the large-scale spoofing incidents in Russia. They could be a defensive measure to prevent drones from flying in certain areas [40]. Large manufacturers of commercial drones like DJI equip their devices with geofencing technology that prevents them from flying at places such as airports, prisons and nuclear power plants [38, 39]. In these geofenced areas drones cannot take off or fly. By spoofing the GPS receivers in drones and projecting them at an airport, the geofence is activated and the drones will not fly at certain high-profile locations.

6.3 Risk and Impact

The potential financial impact of GNSS spoofing and meaconing is unknown. London Economics determined the financial impact of a 5-day outage of GNSS in the UK as 5.2 billion Pounds [21]. Spoofing and meaconing were not considered in this report. Financial implications of spoofing and meaconing strongly depend on the precise spoofing scenario. Due to the deliberate nature, potentially small spoofing incidents can have a large financial impact. For spoofing incidents with a terrorist motivation, financial impact might not be the biggest concern.

Spoofing incidents are currently extremely rare. In section 6.2 above, only a limited number of incidents are reported; none of which with a criminal or terrorist nature. Due to the nature of (criminal) spoofing attacks it is logical that little public information is available. This makes it impossible to give a reliable estimate of the current and future impact of spoofing.

It is likely that GNSS spoofing will happen in the future, because several conditions for the occurrence of GNSS spoofing are being met:

- with terrorism and personal financial benefit there are clear motivations for GNSS spoofing;
- with GNSS-based communication, road tolling, offender tracking, and other systems available there are many potential targets;
- the technical means for performing spoofing are already available and are still becoming more and more accessible. The technical specifications are continuously improving while prices are going down. It appears a matter of time before a small, mobile, battery-operated spoofing device becomes available.

The reason that we are currently not seeing a large number of spoofing events lies in the fact that it is complicated to perform a good spoofing attack. Just the availability of spoofing hardware is insufficient. A successful attack also requires a detailed planning, knowledge of the target receiver, such as the position of the receiving antenna, and matching GNSS spoofing signals. Given these practical hurdles, many potential spoofers will probably choose different, simpler, means to achieve their objectives, such as GNSS jamming or a software hack.

While the planning required for a successful spoofing attack may be an obstacle for small criminals, it is less of a problem for organized criminals and state actors. These actors will probably have a larger financial budget available, allowing for a better preparation. This results in a small but real chance of sophisticated spoofing attacks by such actors. State actors are outside the scope of the current investigation.

Terrorism is a completely different motivation. GNSS spoofing offers interesting attack vectors to a terrorist, but for a large-scale attack advanced hardware and extensive planning are required. Such a large scale attack could have a large impact, but the chance of success is limited by the scale and complexity level. If the intention is just to create chaos, terrorists are likely to revert to less advanced methods, such as (distributed) GNSS jamming or the use of an explosive.

7 Vision and recommendations

The use of GNSS equipment and radio equipment in general is well-regulated in the Netherlands. Agentschap Telecom is responsible for granting permits for use of radio equipment as well as enforcement of the regulations. This means that jammers are forbidden, whereas GNSS repeaters are subject to licensing. At present no occurrences of spoofing are known in the Netherlands. However, the existing spectrum monitoring network of Agentschap Telecom is not nearly dense enough to detect all GNSS spoofing or meaconing incidents. In addition, short-lasting events may remain unnoticed as the response-time of the agency is limited. Concluding, it is possible that the number of spoofing and interference events is underestimated.

In chapter 3 it was identified that the risk of spoofing attacks has evolved from academic possibility to a real threat. Combined with several realistic incentives and targets, this means that Agentschap Telecom should be prepared for spoofing incidents in the future.

In section 7.1 below, a number of specific scenarios from chapter 2 is projected on the situation in the Netherlands. The risk and impact is provided for each of the scenarios.

Following the detailed scenarios, a number of concrete recommendations to Agentschap Telecom are formulated in section 7.2. These recommendations are intended to help AT to increasing the resilience of GNSS use in the Netherlands.

7.1 Specific spoofing scenarios for NL

The GNSS spoofing scenarios described in chapter 2 are all valid for the Netherlands. We can however identify a couple of specific critical infrastructures that could run an increased risk of spoofing:

- Rotterdam harbor;
- Schiphol airport;
- Dutch highway system and road tolling (“rekeningrijden”);
- Amsterdam stock exchange.

7.1.1 Rotterdam harbor

Target: Rotterdam harbor is one of the biggest ports in the world. It is accessed by a single fairway (Nieuwe Waterweg) only just big enough for the biggest category of ships. Due to its size and economic importance, Rotterdam is a potential target for terrorists and criminals (blackmail). If a large ship were to run aground in the fairway, it could cause a long-term blockage of the harbor.

Attack vector: a prepared container. A terrorist organization takes a cargo container and equips it with GNSS spoofing equipment. The spoofer is autonomous or can be controlled remotely. When the ship approaches the narrow fairway, the spoofer is activated and uses its true position to generate a slight course deviation. The captain or the auto-pilot notices the false course deviation, corrects for it, and subsequently steers the ship out of the channel, leading to a grounding. This technique was demonstrated by Humphries with an ocean-going yacht [31].

Risk: The risk of GNSS spoofing is limited due to the fact that large ships approaching Rotterdam are obliged to use a pilot service. Pilots carry their own differential GNSS system, which is of above-average quality. The use of DGNSS makes a spoofing attack more difficult. A distributed interference attack (jamming) may pose a larger risk.

Impact: Long-term access to the harbor blocked, leading to significant economic damage. Oil spillage may cause severe environmental damage to the Dutch coastline.

7.1.2 Schiphol airport

Target: Amsterdam airport Schiphol is a primary hub in the international air traffic system. As such it is a potential target for criminals (blackmail) and terrorists. The crash of an approaching airplane would be a high-value goal for a terrorist. On the other hand Schiphol is a poor target for spoofing as GNSS-assisted approach procedures are not yet in common use. Nevertheless such procedures are being introduced and in the future air traffic might become vulnerable to spoofing attacks.

Attack vector: During a low-visibility approach an aircraft could be fooled into flying a false approach, lower than intended. The aircraft could be directed to fly into the ground or a building, provided that visibility is low enough. The attacker is most likely to hide outside the airport area under the flight path and may use a directional antenna to target a specific aircraft.

Risk: the risk is currently low due to the fact that GNSS is not commonly used for landing aircraft at Schiphol airport. The risk is low, because EGNOS procedures do not allow approaches down to ground level and other systems (ILS, visual, ...) will provide indications that something is wrong.

Impact: Crash of an airplane, significant loss of life of passengers, crew and possibly ground personnel. Significant publicity damage leading to fear, increased security measures and follow-up economic damage.

7.1.3 Road tolling

Target: In various European countries different forms of road tolling (for trucks) have been introduced. If road tolling ("rekeningrijden") is introduced in the Netherlands, it can become a target for GNSS spoofing. An important goal of the introduction of road tolling in the Netherlands is to reduce traffic during rush hours by increasing the price of driving during these hours.

Attack vector: The spoofing attack will depend strongly on the tolling implementation. A spoofer could falsify the vehicle position in order to place the car on a road with no/lower toll. Alternatively the spoofer may leave the position of the car unchanged, but modify the recorded time to be outside the toll period.

The same result could be achieved with jamming, where an onboard receiver is not able to report any time and position. Given the fact that the GNSS receiver is under control (within physical reach) of the driver, a line injection attack is also feasible.

Risk: The risk is high as a large number of people is affected by road tolling. At the same time, a properly designed road tolling system will use cross-checks, both inside the road tolling device in the car and outside at toll-gates (license plate recognition by camera). Proper cross-checks can reduce or eliminate the risk of effective spoofing. The change of being caught will determine the final risk of GNSS spoofing attacks aimed at road tolling.

Impact: mainly small-scale financial impact through toll evasion. Secondary impact may be caused by spoofing or jamming which can affect nearby autonomous vehicles.

7.1.4 Amsterdam stock exchange

Other scenarios such as attacks to financial institutions (the Amsterdam stock exchange and the main banks) are valid for the Netherlands, but are difficult to specify as the exact attack vector is unpredictable. The most likely attack appears to be spoofing of GNSS time to manipulate the order of transactions, although it is unclear how the financial benefit arises exactly. The incentive for this type of attack is strong, as the potential financial gains are large. However, financial institutions can protect themselves relatively easily by using redundant time sources.

7.2 Recommendations to Agentschap Telecom

Currently interference in the GNSS frequency bands in the Netherlands mostly consists of unintentional interference and (intentional) jamming. There have been no registered events of GNSS spoofing. It is hard to predict if spoofing will become a more serious threat in the coming years. At least several ingredients (potential targets, potential actors, equipment) are present to make it a severe threat. It is thus recommended that Agentschap Telecom increases national resilience with a combination of measures. The proposed measures are both technical and organizational. Most of these measures are not limited to spoofing, but also increase resilience against unintentional interference and jamming.

1. Increase the chances of interference and spoofing detection by expanding the monitoring of GNSS frequency bands, especially near critical infrastructure.
 - Rotterdam harbor
 - Schiphol airport
2. Increase the chances of interference detection, by encouraging the monitoring of GNSS bands through crowd-sourcing networks.
 - Development of a smartphone app to detect jamming/spoofing.
 - Coordinate/regulate the standards to which such a smartphone app and the connecting database must adhere
 - Monitor the resulting interference map and act where necessary.
3. In case a GNSS spoofing incident occurs, make sure it receives a reaction not to be misunderstood, i.e. a proper fine or legal action. The agency could consider giving visibility to the fact that GNSS frequency bands are being actively protected by law enforcement, as a deterrent.
4. Create awareness: inform GNSS users on the risk of GNSS spoofing and interference
5. Recommend best practices to professional users
 - Antenna installation with a clear sky view
 - Antenna installed in a high location without view of the street surface
 - Use a choke-ring antenna
 - Use a multi-constellation, multi-frequency receiver if possible
 - Apply best practices for cyber-security for internet-connected devices
 - Other recommendations from [25]

6. Enforce the use of mitigation measures for critical infrastructure³, specifically for GNSS timing:
 - All critical infrastructure using GNSS timing:
 - power plants
 - financial institutions
 - communication network providers
 - Timing receivers should include a hold-over clock with a detection and fallback mechanism for spoofing and interference.

³ Enforcing measures for critical infrastructure is most likely outside of the scope of AT responsibility, however it is seen as an important measure to increase resilience.

8 Summary and conclusions

Importance and vulnerability of GNSS

GNSS is an efficient technology for providing accurate time and position worldwide. Critical infrastructure and many other systems depend on GNSS for time and position information. All GNSS's are similarly susceptible to jamming, spoofing and meaconing because of the low signal power of the satellite signals and the openly available signal characteristics. The possible disruption of GNSS signals makes these systems vulnerable. The awareness of this vulnerability is lacking.

GNSS spoofing and meaconing

GNSS spoofing and meaconing concern the deception of GNSS receivers by providing fake GNSS signals. Meaconing is about the replay of genuine satellite signals and spoofing about the synthesis of artificial signals. GNSS spoofing and meaconing are sensitive subjects, because they are associated with governmental or military operations and/or criminal activities and vulnerabilities in business and mission critical infrastructure. As a result stakeholders and experts are generally hesitant to share information about the subject.

Types of spoofing attacks

Spoofing attacks are usually classified based on the basis of sophistication, the way in which the signal is presented to the GNSS receiver, the necessary equipment, etc.

- non-signal technique (cyberattack);
- cable inject;
- non-coherent technique, single spoofer;
- coherent technique, single spoofer;
- coherent technique, multiple spoofers.

Non-signal (cyber) attacks, cable injection and non-coherent RF spoofing attacks are most simple to implement, making these attacks more likely. More complicated techniques with a single or multiple coherent spoofing transmitters are much more difficult to realize, because they require more expensive RF equipment and knowledge.

Meaconing can be seen as a separate attack category that is simpler to perform than spoofing because there is no need for software to generate the GNSS signals. In its most simple form only a repeater is necessary. The advantage of meaconing is the fact that all the complete GNSS signals are obtained with high quality. The drawback is reduced freedom to tailor the signals for a specific purpose.

Note that non-signal and cable injection attacks do not abuse the RF spectrum and are not illegal in that respect. One could argue if they should be qualified as spoofing, especially the non-signal attack. They are included however, because if successful the result of these attacks is the same as for the other GNSS spoofing techniques

Spoofing equipment

Non-signal (cyber) attacks need no RF equipment at all. Cable injection and non-coherent single spoofer techniques can be performed with consumer grade software-defined radio equipment. SDR platforms with adequate specifications are available in the price range between 100 and 1000 euro. Basic GPS spoofing software is freely available on the internet. It has also been shown that cheap electronic devices can be used to emit GNSS signals outside their intended band of operation.

For the more sophisticated coherent spoofing attacks, generally higher grade equipment is needed. Several research institutes have created spoofing hard- and software for research purposes, but these are usually not made available outside the institute.

To perform meaconing, only a hardware repeater system is necessary. Such GNSS repeater systems are available commercially for applications where GNSS reception is needed in-doors, e.g. in aircraft hangars or in buildings of emergency services. It is also possible to store the received GNSS signal and re-play the signal from memory. In that case there is still no need for the attacker to generate the GNSS signals himself.

Actors and motivations

There are different actors that can have various motivations for performing GNSS spoofing:

- drivers want to spoof vehicle-based tracking systems to avoid paying road tolls and to evade regulations on driving hours;
- fishermen want to spoof tracking equipment to remain undetected while entering illegal fishing grounds;
- traders want to manipulate the timing of financial transactions to gain financial benefit;
- terrorists want to create damage and fear by forcing vehicles off-course or disrupt time synchronization in distributed networks;
- offenders want to spoof tracking equipment to evade house arrest;
- amateur hackers want to perform spoofing out of curiosity, simply trying to see what they can achieve.

All these scenarios appear applicable to The Netherlands.

Impact

Exact financial impact is hard to predict, but the largest impact is expected when spoofing attacks are aimed at critical national infrastructure such as Rotterdam Harbor, Schiphol airport or the national power network.

Likelihood of spoofing

Initially GNSS spoofing was merely a theoretical possibility, over the years it has become technically feasible. Experts do not agree if spoofing currently is a real threat, or not. The likelihood of spoofing – both higher and lower – is influenced by several factors.

Higher likelihood factors are:

- the widespread use of GNSS receivers in critical infrastructure and other systems makes that there are many potential targets;
- there are many potential actors with a motivation to perform spoofing;
- spoofing equipment and software are available. Equipment is still improving and becoming cheaper. A motivated spoofer will be able and willing to purchase even the current advanced hardware;
- the chances of a low-power spoofing attack being detected are relatively small.

Lower likelihood factors are:

- spoofing has been demonstrated in the lab, but is difficult to achieve in the field;
- it requires detailed planning, knowledge of the target receiver such as receiving antenna location etc.;
- it is not obvious how a specific target will respond to spoofing, because it is not clear if and what mitigation measures are in place;
- besides spoofing, potential spoofers usually have other options for reaching their goals, such as GNSS jamming.

Occurrence of spoofing and meaconing

Spoofing has been demonstrated in the lab, but is still difficult to achieve in the field. All evidence indicates that spoofing is rare in real-life. There have been no authenticated reports of criminal or terrorist spoofing. Several cases of military, unintentional and scientific spoofing and meaconing have been registered in the past. The reports of unintentional GNSS meaconing were due to GNSS repeaters in hangars at airports.

It is possible that there have been isolated spoofing incidents that have not been reported, because

1. stakeholders are unwilling to share information, or
2. the spoofing signals were not detected due to their low RF power.

Future developments

The current SDR equipment is not particularly portable. Experts fear that the emergence of small, light-weight, battery-operated spoofing devices will make spoofing more accessible. There are no technical reasons why spoofing devices could not be made as small as PPDs (GNSS jammers).

Detection of spoofing

Spoofing (except for non-signal and cable injection attacks) can be detected by interference monitoring in the RF spectrum. Targeted spoofing attacks are assumed to use low RF power. To be able to detect such low-power signals with certainty, detection networks need to be sufficiently dense. Typical spacing of the nodes could be 100 – 1000 m. A dedicated monitoring network with such a density is difficult and expensive to install and maintain. Crowd-sourced interference monitoring is a promising concept for achieving a dense GNSS interference monitoring network at limited cost.

Mitigation of spoofing

Mitigation usually consists of the detection of spoofing, followed by fallback to an alternate source of position or time. The two can therefore not be seen separately. Mitigation measures include:

- GNSS receiver-based measures
 - antenna-centered techniques, such as anti-jamming antennas;
 - signal quality monitoring techniques;
 - consistency checks on PVT;
 - navigation message checks;
 - use of augmentation data;
 - fallback to other GNSS signals or non-GNSS sources of position and time;
- use of non-GNSS systems;
- non-technical anti-spoofing measures.

Organizational solutions to detect spoofing include assigning the GNSS frequency bands primary status and to create more awareness among the operators of GNSS equipment of the possibility of spoofing. Agentschap Telecom already operates a hotline for radio interference in general. The added value of an additional hotline for GNSS spoofing appears small.

Usually a single spoofing countermeasure does not provide complete protection and a combination of mitigation measures is needed for optimal protection. The best (technically and economically) mitigation strategy depends on the specific application. It should be noted that the value of spoofing mitigation remains limited: an attacker can always refer to jamming if spoofing fails.

Vision and recommendations

Occurrence of spoofing is low currently. It is hard to predict if spoofing will become a more serious threat in the coming years, or if it will remain in the background. In the view of the researchers, spoofing cannot be ignored. The combination of ever cheaper and more affordable hardware combined with several real incentives for spoofing, leads to a significant chance that an incident occurs. On the other hand, a successful spoofing attack requires detailed planning, knowledge of the target receiver and its location, and a fairly advanced spoofing algorithm to fool more than the simplest receivers. These complexities mean that real-world spoofing is not simple and therefore does not occur often.

Agentschap Telecom can play an important role increasing national resilience. By providing objective information and advice to end users, awareness and use of best practices can be increased. By market enforcement, the agency can limit the availability of spoofing equipment. And, finally, by strictly monitoring the GNSS spectrum and enforcing the regulations, the agency can avoid a future increase of spoofing and interference incidents.

9 References

1. "Meervoudige Offerteaanvraag 'Onderzoek Spoofing'," Agentschap Telecom, 20 augustus 2018.
2. "A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures," D. Schmidt, K. Radke, S. Camtepe, E. Foo, M. Ren, ACM Computing Surveys, Vol. 48(4), pp. 1-31, May 2016, https://www.researchgate.net/publication/301798786_A_Survey_and_Analysis_of_the_GNSS_Spoofing_Threat_and_Countermeasures, accessed 22-01-2019.
3. "GNSS signal", navipedia, https://gssc.esa.int/navipedia/index.php/GNSS_signal, accessed 22-01-2019.
4. "Measuring the GNSS Signal Strength," A. Joseph, InsideGNSS November/December 2010, <http://insidegnss.com/wp-content/uploads/2018/01/novdec10-Solutions.pdf>, accessed 29-01-2019.
5. "GNSS Satellite Transmit Power and its Impact on Orbit Determination," P. Steigenberger, S. Thöler, O. Montenbruck, Journal of Geodesy 92(3), November 2017.
6. "Vulnerability Assessment for the Transportation Infrastructure Relying on the Global Positioning System", J. A. Volpe, National Transportation System Center, 2001.
7. "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, September 2003, pp. 1543-1552.
8. "GNSS Interference Threats and Countermeasures," Fabio Dovis (ed.), Artech House, Boston, 2015.
9. "A Survey of Spoofing and Counter-Measures," C. Günther, Navigation: Journal of the Institute of Navigation, vol. 61(3), pp. 159-177, 2014.
10. "Software-Defined GPS Signal Simulator," <https://github.com/osqzss/gps-sdr-sim>, accessed 29-01-2019.
11. "DEF CON 23 – Lin Huang and Qing Yang – Low cost GPS simulator: GPS spoofing by SDR," https://www.youtube.com/watch?v=iwJKMti_aw0, <https://github.com/op7ic/defcon-23-slides-only/blob/master/DEF%20CON%2023%20presentations/Speaker%20%26%20Workshop%20Materials/Lin%20Huang%20%26%20Qing%20Yang/DEFCON-23-Lin-Huang-Qing-Yang-GPS-Spoofing.pdf>, accessed 24-01-2019.
12. "Authentication by Polarization: A Powerful Anti-Spoofing Method," W. De Wilde et al., Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 2018, pp. 3643-3658.
13. "What is navigation message authentication," InsideGNSS, 1 January 2018.
14. "GNSS user technology report – issue 2", European Global Navigation Satellite Systems Agency GSA, https://www.gsa.europa.eu/system/files/reports/gnss_user_tech_report_2018.pdf, accessed 13-11-2018.
15. "J911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches," L. Scott, Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, September 2011, pp. 1931-1940.
16. "Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution," D. Miralles, N. Levigne, D.M. Akos, J. Blanch, S. Lo, Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 2018, pp. 334-344.

17. "GNSS Jamming – Crowd Sourcing Detection and Geolocation," webinar sponsored by InsideGNSS, 22 January 2019, <https://register.gotowebinar.com/register/9129823782682449923>.
18. Resilient Navigation and Timing Foundation recommendations, <https://rntfnd.org/what-we-do/our-recommendations-gps-gnss/>, accessed 24-01-2019.
19. "Pokémon Go", Wikipedia, https://en.wikipedia.org/wiki/Pok%C3%A9mon_Go, accessed 22-01-2019.
20. Google Trends, <https://trends.google.nl/trends/?geo=NL>, accessed 29-11-2018.
21. "The economic impact on the UK of a disruption to GNSS," London Economics, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf, accessed 27-08-2018.
22. STRIKE3 project, <http://www.gnss-strike3.eu>, accessed 13-12-2018.
23. STRIKE3 project workshop, 11-12 December 2018, Linköping Sweden.
24. "Draft Standards for Threat Monitoring and Reporting," STRIKE3 consortium, 2017, http://www.aic-aachen.org/strike3/downloads/STRIKE3_D41_Reporting_Standards_v2.1.pdf, accessed 28-01-2019.
25. "Improving the Operation and Development of Global Position System (GPS) Equipment Used by Critical Infrastructure," National Cybersecurity & and Communications Integration Center, and National Coordinating Center for Communication, 2017, <https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf>, accessed 14-12-2018.
26. Resilient Navigation and Timing Foundation, <https://rntfnd.org>.
27. "Ships fooled in GPS spoofing attack suggest Russian cyberweapon," New Scientist, August 2017, <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/>, accessed 24-01-2019.
28. "Iran–U.S. RQ-170 incident," Wikipedia, https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident, accessed 24-01-2019.
29. "Why Iran's capture of US drone will shake CIA," BBC News, December 2011, <https://www.bbc.com/news/world-us-canada-16095823>, accessed 24-01-2019.
30. "Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV," 2012, <https://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing>, accessed 12-11-2018.
31. "Spoofing a Superyacht at Sea," 2013, <https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea/>, accessed 12-11-2018.
32. ICAO Information Paper ACP-WGF23/IP-21, 2010.
33. "GPS unter Beschuss: Jamming und Spoofing nehmen bei Ortungssystemen zu," Daniel AJ Sokolov, 2018, <https://www.heise.de/newsticker/meldung/GPS-unter-Beschuss-Jamming-und-Spoofing-nehmen-zu-4038137.html?seite=all>, accessed 16-11-2018.
34. "Getting lost near the Kremlin? Russia could be 'GPS spoofing'," CNN, December 2016, <https://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/index.html>, accessed 24-01-2019.

35. "Mass GPS Spoofing Attack in the Black Sea? – Maritime Executive," Resilient Navigation and Timing Foundation, July 2017, <https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/>, accessed 24-01-2019.
36. "PRESS RELEASE - GPS Spoofing Patterns Discovered," Resilient Navigation and Timing Foundation, September 2017, <https://rntfnd.org/wp-content/uploads/GPS-Spoofing-Patterns-Press-Release.1-26-Sep-17-RNT-Foundation.pdf>, accessed 24-01-2019.
37. "Spoofing Incident Report: An Illustration of Cascading Security Failure," L. Scot, InsideGNSS, 9 Oct. 2017, <https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/>
38. Drone geofencing, <https://www.dronewatch.nl/tag/geofencing/>, accessed 24-01-2019.
39. "DJI Improves Drone Geofencing for Airport Safety Zones," October 2018, <https://www.unmannedsystemstechnology.com/2018/10/dji-improves-drone-geofencing-for-airport-safety-zones/>, accessed 24-01-2019.
40. "Russia Undermining World's Confidence in GPS," Resilient Navigation and Timing Foundation, April 2018, <https://rntfnd.org/2018/04/30/russia-undermining-worlds-confidence-in-gps/>, accessed 24-01-2019.
41. "GNSSim: An Open Source GNSS/GPS Framework for Unmanned Aerial Vehicular Network Simulation," F. Jahan, A. Y. Javid, W. Sun, M. Alam, EAI Endorsed Transactions on Mobile Communications and Applications 12 2014 – 0.8 2015, Vol. 2(6), e2, https://www.researchgate.net/profile/Ahmad_Javid/publication/280921883_GNSSim_An_Open_Source_GNSSGPS_Framework_for_Unmanned_Aerial_Vehicular_Network_Simulation/links/55cb4a5408aea2d9bdcd9ca/GNSSim-An-Open-Source-GNSS-GPS-Framework-for-Unmanned-Aerial-Vehicular-Network-Simulation.pdf?origin=publication_detail, accessed 18-02-2019.
42. "(In)Feasibility of Multi-Frequency Spoofing," J.T. Curran, Inside GNSS, 14 June 2018, <https://insidegnss.com/infeasibility-of-multi-frequency-spoofing/>, accessed 18-02-2019.
43. "GPS World's 7th annual Simulators Buyers Guide," GPS World, 10 March 2018, <https://www.gpsworld.com/2018-simulator-buyers-guide/>, accessed 18-02-2019.
44. "Satellite-derived Time and Position: A Study of Critical Dependencies", Government Office for Science, 2018, <https://www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review>, accessed 09-01-2019.
45. "From Data Schemes to Supersonic Codes; GNSS Authentication for Modernized Signals," O. Pozzobon, G. Gamba, M. Canale, S. Fantinato, Inside GNSS, January 2015, <https://insidegnss.com/wp-content/uploads/2018/01/janfeb15-WP.pdf>, accessed 08-04-2019.
46. Discussion with Loek Colussi (Agentschap Telecom), 7 January 2019.
47. Interview with Lennard Huisman (Kadaster), 8 January 2019.
48. Interview with Mark Dumville and Enrique Aguado (NSL), 8 January 2019.
49. Interview with Jean-Paul Henry (06-GPS), 14 January 2019.
50. Interview with Daniele Borio (JRC), 9 January 2019.
51. Interview with Peter Zwamborn (TNO), 4 March 2019.
52. Interview with Allard Dijk (Netherlands Defense Academy), 7 March 2019.

Appendix A Summary of papers

This appendix contains the summaries of the most relevant publications that were part of the literature study.

Appendix A.1 GNSS Interference threats and countermeasures

This book edited by Fabio Dovis and published in 2015 [8] contains two chapters very relevant to GNSS spoofing:

Chapter 3: The Spoofing Menace;

Chapter 8: Antispoofing Techniques for GNSS.

Appendix A.1.1 Chapter 3, The Spoofing Menace

All present GNSS systems (GPS, Galileo, Glonass and Beidou) are vulnerable to spoofing. Some of the reasons all systems are vulnerable are the following:

- The signal levels are so weak that it is easy to override the real signals with a simple transmitter.
- GNSS systems publish their signal structure so that a receiver can track and interpret the signals. This information can also be used to generate counterfeit signals.
- Computer systems have become so powerful that generating a real-time GNSS signal is not limited to supercomputers or dedicated hardware.

Appendix A.1.1.1 Classification

Two main types of attacks are identified:

1. Non-signal attacks
These include all attacks that do not try to reproduce a GNSS signal, but instead find another way to attack a receiver and fool it into thinking it is somewhere else (or at another moment in time). Examples are breaking into an internet-enabled device, and corrupting the device to report a false position.
2. Signal attacks
These include all attacks where a receiver is attacked through false signals. These signals can be random, they can be a copy of the true signals or they can be artificially generated to look like real GNSS signals.

When speaking of spoofing, in general the second type (signal attacks) is meant. This type of attack can be further divided in three subcategories:

- a) Jamming
Purposeful emission of noisy signals with the purpose of preventing a receiver from locking on to the very weak GNSS signals.
- b) Meaconing
A delayed rebroadcast of true GNSS signals, with the purpose of confusing a receiver into thinking it is at a false location or time.

c) Spoofing

Synthesis and broadcast of artificially generated GNSS signals. Using such signals a receiver can be fooled into thinking it is at any arbitrary place or time.

Jamming (2a) is classified as unstructured interference, whereas attacks meaconing (2b) and spoofing (2c) are classified as structured interference. Here we focus only on types 2b and 2c.

Spoofing (attack type c) can be further classified in three categories. The classification is based on the implementation complexity. Other classifications are also used in literature. The classification used here is further detailed under Spoofing below.

- I. simplistic
- II. intermediate or shadowed
- III. sophisticated

Appendix A.1.1.2 Meaconing

Meaconing is a relatively simple attack. It consists of the reception, delay and rebroadcast of real GNSS signals. A meaconing can be performed using readily available commercial hardware (for example a GPS repeater). It can also be performed with simple RF hardware. Digital processing is not required for a simple meaconing attack, but may be used in more complex attacks.

As live signals are recorded and replayed, a meaconing attack always consists of exactly the same satellites as the real signals. Also, all GNSS constellations will be included by definition. The meaconing signal is usually (much) stronger than the true signals. The signal shape is identical to the original signals.

Hardware requirements

- RF antenna
- Low-noise amplifier
- RF Transmitting front-end

Impact on receiver

The target receiver is fooled into thinking it is at the position and (time) of the meaconing antenna. As the signals were delayed before rebroadcast, the receiver displays a time that is running behind.

During acquisition of the meaconing signal, the receiver may temporarily lose lock of the original signals. A jump in position is likely to occur. A jump in time may occur, depending on the level of sophistication of the attack.

Context requirements

For an effective attack, the broadcast has to be close to the target receiver. Alternatively the LNA gain must be adjusted to ensure a believable power level to fool the target receiver.

Limitations for implementation

None or very limited. Only simple RF components required, possibly complemented with software for a much more advanced attack.

Detection

Simple meaconing may be detected if the target receiver monitors position and time, detecting jumps. A more advanced (gradual) meaconing attack makes detection very difficult.

Appendix A.1.1.3 Spoofing

Spoofing attacks can range from fairly straightforward to very complex. The detectability of a spoofing attack can be strongly reduced when moving to more complex attack. At the same time the level of coordination and the hardware required for proper execution go up very fast with the complexity of the attack. The implementation effort required for a spoofing attack is the basis for the subdivision used here in categories “simplistic”, “intermediate” and “sophisticated”.

Appendix A.1.1.3.1 Simplistic attack

A simplistic spoofing attack is performed with a GNSS simulator that generates artificial signals that mimic the true GNSS signals. The signals are produced in such a way that the apparent receiver position and time can be controlled. The GNSS simulator can be an advanced hardware device, but it can also be as simple as a piece of software generating signals in advance, which can then be replayed with a radio frontend. The artificial signals are transmitted with high power to overrule the true GNSS signals.

Hardware requirements

- GNSS signal simulator
- Power amplifier
- RF Transmitting front-end

Impact on receiver

Although this attack is called “simplistic”, the impact on a receiver can be very big. Many commercial off-the-shelf receivers are known to be fooled by this attack. Once the receiver starts to track the non-authentic signals, the PVT solution is almost completely under control by the attacker.

To a receiver tracking true signals, the spoofed signals will appear as noise (the attack signal is not time-synchronised to the true signals). The receiver may lose lock of the true signals and be forced into a partial reacquisition.

Context requirements

The attacker will typically place the broadcasting antenna close to the receiver antenna. Alternatively the signals can be directly injected into the receiver antenna cable (complicit spoofing).

Limitations for implementation

The implementation of this attack is easy. Only commercial components are required. No specific software development is needed for a simplistic attack (open source GNSS spoofers exist). More advanced GNSS simulators are big and very expensive, though.

Detection

A simplistic spoofing attack is relatively easy to detect. The signals are not synchronised to the true signals. This means that almost by definition a jump in the PVT solution will occur when the spoofing begins. There may also be inconsistencies in the Navigation message that can be detected.

Appendix A.1.1.3.2 Intermediate attack

This form of attack is already quite advanced to the simplistic spoofing attack above. The spoofer receives true GNSS signals while generating the artificial signals. The artificial signals are code-phase aligned with the true signals (possibly also carrier-phase aligned). The relative position of the receiver and spoofer must be known, and are used to start the spoofer “at the receiver position” to prevent PVT jumps. Artificial signals are first phase-aligned, then increased in strength (signal lift-off) to gradually suppress the true signals.

Hardware requirements

- Custom spoofing device
- Alternatively a modified GNSS receiver
- Power amplifier
- RF Transmitting front-end

Impact on receiver

As the signals are first phase-synchronised with the true signals and then raised in power, the receiver will not notice that the correlation peak it is seeing is not the true signal. Provided the peak is then moved gradually, a receiver will be transparently fooled into tracking new signals.

Context requirements

Accurate knowledge of both the receiver antenna location (and speed) and the transmitting antenna (and speed) is required for this attack. A way around this limitation is self-spoofing, where a small spoofing device is placed right next to the receiver antenna.

Limitations for implementation

This type of attack requires fairly sophisticated spoofing software. The software must be able to perform code-phase synchronisation, on-the-fly signal generation for multiple channels and signal lift-off.

Detection

A properly executed “intermediate” attack is very hard to detect. Detection cannot take place in the receiver signal processing, as the signals are synchronised and gradually increased in power. This means that C/N0 monitoring and PVT consistency monitoring will have no effect.

More complex detection measures such as antennas which can detect the angle-of-arrival of a signal can still be used to detect this attack.

Appendix A.1.1.3.3 Sophisticated attack

This form of attack addresses the one remaining vulnerability of the intermediate attack: although the signals may appear perfectly genuine, they are coming from a single transmitter nearby, allowing the detection of the signal source.

To address this weakness, multiple coordinated antennas are used to transmit the spoofing attack. By using the constructive properties of RF signals, the receivers can combine to create artificial signals that appear to arise from the satellite. Note that each spoofing antenna has the same synchronisation capabilities as for the intermediate attack.

Hardware requirements

- Multiple phase-locked intermediate spoofing devices (portable).

Impact on receiver

The impact on the target receiver is similar to that of the intermediate attack.

Context requirements

The location and velocity of the target receiver's antenna phase centre must be known with sub-cm accuracy for this attack.

Limitations for implementation

This attack is very complex, requires detailed knowledge of the target receiver's location as well as multiple spoofing devices that must be placed precisely around the target receiver. This means the attack will be difficult and expensive to implement.

Detection

As this attack is able to fool even directionally-sensitive antennas, it is likely impossible to detect it with GNSS-only based spoofing defenses.

Appendix A.1.1.4 Hybrid attacks

The techniques described above can be readily combined into hybrid attack forms. These are not discussed in the same level of detail, but they are mentioned here.

A **relaying attack** is a modified meaconing attack where the recorded signal is not at the same location as the transmitted signal. This can have advantages when the recording antenna is moving in a location and pattern which the target antenna is to believe as true. A remote antenna is moved while recording signals. The signals are broadcast via a modem and a radio link to the remote spoofing device (transmitter) which has a decoding modem. Finally, the spoofer transmits the recorded GNSS signals through its transmitting antenna toward the target receiver.

A **meaconing** attack with **variable delay** attempts to overcome detection by preventing jumps in time. The meaconing attack begins by immediately re-transmitting the original signals. Especially if combined with signal lift-off, the target receiver can be seamlessly fooled into tracking the meaconed signals. Once a tracking lock is obtained, a variable delay is introduced, gradually slowing down the re-transmitted signals. The tracking loop of the target receiver will lock onto to the delaying signals, gradually introducing a time delay in the PVT solution. If executed properly, this attack is not detected as a jump in time.

This attack type is useful to implement a security code estimation and replay (SCER) attack.

A **SCER** attack aims to defeat signals which have authentication bits embedded in the navigation or data message. Such signals include, as part of their navigation message, some unpredictable bits or chips that can be used to validate that the signal came from the true GNSS system and is not spoofed. An example is the Galileo Open Service Navigation Message Authentication (OS-NMA). Such signals are difficult to spoof as the authentication bits cannot be reliably predicted. This means that spoofed signals can be detected as false by verifying a cryptographic checksum. To defeat such signals, a meaconing attack with variable delay is introduced. First, the receiver is fooled into tracking the meaconed signals with 0 delay. Then, a small delay is gradually introduced. Once the delay is sufficiently long, the

security authentication bits can be read by the spoofer *before* generating the counterfeit signals. It can now produce spoofed signals with the *correct* security authentication, and broadcast those instead of the original signals. Using a **high gain antenna** aimed directly at a GNSS satellite, the code and navigation bits of a GNSS signal can be directly observed without using correlation. This allows for a much more advanced spoofing / meaconing attack. Using 4 (or more) high gain antenna's, the signals of at least 4 GNSS signals are read and recorded. The signals can then be mixed again with a varying relative delay to create a spoofed signal at an arbitrary location. Alternatively, a high gain antenna can be used to read the security authentication bits in a GNSS signal directly, allowing a spoofer to use them in generating signals. Thankfully, attacks with multiple high-gain antennas are complex and costly to realise.

Appendix A.1.2 Chapter 8, Antispoofing Techniques for GNSS

Appendix A.1.2.1 Classification of anti-spoofing techniques

Anti-spoofing techniques for GNSS can be classified in different categories. The classification is useful to separate techniques by their effectiveness and by the complexity of implementation, both at system level and at receiver level.

The first distinction to be made is

1. Detection techniques
Techniques that detect that spoofing is occurring. This means that the receiver knows the GNSS signals used are no longer reliable, and can make a choice what to do next. For instance, an alarm can be sounded alerting the user to the situation.
2. Mitigation techniques
These techniques try to address the issue of spoofing, either by filtering true signals from false signals, or by using alternative positioning methods in the presence of spoofing.

It is safe to say that most available techniques primarily perform detection of spoofing. Given that spoofing signals can easily override true signals in strength, it is either difficult or impossible to filter out the original GNSS signals. This means that detection is most often followed by a fallback to an alternate navigation signal. This can be another satellite, another frequency band, another GNSS system or a completely different, non-GNSS system such as INS.

The second distinction made in Dosis 2015 is between

1. Cryptographic defenses
2. Non-cryptographic defenses

The distinction is quite straightforward; cryptographic defenses typically make use of a secret key to either encrypt or sign a part of the GNSS signal. Given that a spoofer doesn't have the secret key, they cannot artificially generate correct signals. It is noteworthy that cryptographic defenses blur the line between detection and mitigation. In principle, encryption results in detection of spoofing: a receiver can recognize a fake signal as non-original to discard it. In practice, this reduces a spoofed signal (without proper encryption) to a form of interference, which can still prevent proper tracking of the original signal.

It is important to note that current (2015) commercial receivers typically do NOT include any anti-spoofing measures. Some receivers have navigation filters that act as a kind of protection against simplistic spoofing attacks, however.

The following types of defenses are described in more detail:

Stand-alone

- Consistency checks
- Signal quality monitoring (SQM)

Hybrid

- Integration with Inertial Navigation System (INS)
- Integration with communication system

Encryption

- Navigation message authentication (NMA)
- Navigation message encryption (NME)
- Spreading code authentication (SCA)
- Spreading code encryption (SCE)

Appendix A.1.2.2 Consistency checks

The simplest way of detecting spoofing is by performing consistency checks. A receiver can by check for inconsistencies introduced by the spoofer:

- Position discontinuity (sudden jumps in position)
- Time discontinuity (sudden jumps in time)
- Monitoring of signal power (C/No)
Signals with a C/No higher than theoretically possible can be discarded.
- Unusual power variations correlated with the receiver movement are a sign of a nearby source
- Monitor relative delay between L1/L2 correlation peak for a specific satellite
- Cross-compare single-constellation PVT solutions
- Consistency check of code and phase range rate measurements. For authentic signals the doppler frequency and code delay rate are consistent.
- Time consistency (check consistency of GNSS system times from different satellites)

The above defenses work as they make life hard for the spoofer: the spoofer has to build and support an advanced signal generator which supports multiple constellations as well as multiple frequencies.

Appendix A.1.2.3 Signal Quality Monitoring

Spoofing can be detected by carefully monitoring correlation function between GNSS signal and local replica. A regular GNSS signal will have a symmetrical correlation function with a given peak height. A spoofed signal will have an asymmetric peak or a peak which is atypically sharp or flat. This technique can be used to detect intermediate or even sophisticated spoofing attacks at the moment that the spoofed signal is ramped up to override the original signal.

Appendix A.1.2.4 Integration with Inertial Navigation System (INS)

In this case the additional sensors of an INS are leveraged to detect and/or mitigate spoofing. An INS system is

- immune to interference
- drifts significantly
- has unbounded errors due to drift
- has very low noise

In contrast, a GNSS receiver has

- relatively high noise
- no drift
- bounded, well-known errors
- a low measurement rate

The two systems combined complement each other nicely, compensating for the weaknesses of each system. The GNSS receiver can detect spoofing by comparing the GNSS velocity estimate with INS acceleration measurements. The difference in measurements can be monitored over time or compared to a threshold, raise an alarm. Once detected, the system can fall back to INS only in a transparent manner until the spoofing condition goes away.

Appendix A.1.2.5 Integration with communication system

A communication system can be used in a similar manner as an INS, in this case however the position solution of each system is cross-checked with the other. Here too, the communication system can be used as a fallback for GNSS once spoofing is detected. Both WIFI and GPRS can provide a form of positioning. A significant problem is the accuracy of current communication systems for positioning: cell towers are spaced too far apart for useful positioning compared to GNSS. Future systems (5G) or trilateration may enable communications to be used effectively as anti-spoofing technique.

Appendix A.1.2.6 Navigation message authentication (NMA)

This first form of encryption computes a digital signature of the Navigation Message using a secret key only known to the GNSS system provider. The digital signature is transmitted as part of a data block alongside the navigation message. The end user can verify the signature is true using a public key, available for example over the internet.

- + Low complexity : software routine only, signature / checksum routine on NM
- + Robust against simplistic spoofing
- - Suffers from delay (whole portion of message with valid signature must be received)
- - Fails against meaconing, SCER, intermediate and sophisticated attacks

It is recommended to combine NMA with another form of (non-encryption) anti-spoofing.

Appendix A.1.2.7 Navigation message encryption (NME)

The next step up is to encrypt the complete navigation message. This requires a symmetric key pair, where the user must have a secret key as well and *must be trusted* to keep this key secret.

- - requires secret key for both encryption AND decryption
- - key distribution issues
- - medium receiver complexity
- - tamper-resistant hardware required
- + decryption module may be external to receiver chip (smart card)
- + no need to track an encrypted spreading code
- - moderate increase in receiver cost
- + robust against simplistic attack
- - fails meaconing and intermediate + sophisticated spoofers (SCER)

Appendix A.1.2.8 Spreading code authentication (SCA)

Instead of just signing or encrypting the navigation message, it is also possible to sign or encrypt the spreading code used for ranging itself. In the case of SCA the digital signature can be embedded between ranging codes at fixed time intervals (spread spectrum security codes, SSSC). The receiver collects the signals (raw IF data) for these intervals. After receiving the signature as part of the NM, the receiver can correlate the SSSC data with the signature to detect a match.

- - Medium system complexity: spreading codes interleaved with security codes
- + Best applied to GNSS signals with separate data and pilot channels
- - receiver must store and process raw IF samples
- - receiver must process both data and pilot channel at once
- - authentication delay applies like NMA
- - medium increase in receiver cost (HZ: don't really believe this medium)
- + robust against simplistic and intermediate attacks
- - Fails against high gain antenna's directly reading (and replaying) the SSSC bits
- - fails against meaconing

Appendix A.1.2.9 Spreading code encryption (SCE)

The final step is full encryption of the spreading codes, as applied for the GPS P(Y) code and the Galileo PRS signal. This requires tamper-proof hardware in the user receiver not only to store a secret key, but also to generate the spreading codes based on this key.

- - Increased system complexity
- - Key distribution and management issues
- - Increased receiver complexity
- - tamper-resistant hardware for secret key and code generation
- - tamper-resistant hardware embedded in receiver
- - significant receiver cost increase
- - must acquire and track encrypted spreading code
- ++ robust against simplistic, intermediate and sophisticated spoofing
- - fails against meaconing
- - high gain antennas might break encryption or replay codes

Appendix A.2 A Survey of Spoofing and Counter-Measures

Article of Christoph Günther in Navigation: Journal of the Institute of Navigation in 2014 [9].

Appendix A.2.1 Introduction

The growing economic importance of Global Navigation Satellite Systems (GNSS) makes it rewarding for malevolent people to aim at misleading receivers in their position and time estimation. This can be achieved by replacing or superposing signals to the authentic GNSS satellite signals. Most current receivers are not designed to detect spoofing. The present article aims at a systematic exposition of threats. In many cases, they can be addressed by comparing the received signals, the estimated states, and their respective dynamics against models. A cryptographic signature of the navigation message would furthermore improve the detectability of fake synthetic signals, and should be implemented in the definition of new GNSS signals. In general, the analysis of spoofing should receive the same attention as the analysis of natural impairments.

Appendix A.2.2 Spoofing

The potential motivations for spoofing attacks are rather diverse, reaching from terrorism, through fraud, to avoiding traceability by the employer. Each possible exemplary motivation has different target and requires different amplitude of the induced error:

- A terrorist who wants to send a vehicle onto a collision path must induce an error of a few tens of meters – this corresponds to a fraction of a microsecond in propagation time.
- Drivers who want to evade toll need to displace their position by a few kilometers, i.e., delays in the order of tens of microseconds.
- Fishermen who want to catch fish outside of the permitted areas need displacements in the order of tens of kilometers, i.e., delays up to a fraction of a millisecond, and
- Criminal organizations who want to manipulate the timing of financial transactions need errors at the millisecond-level.

The limited spread of know-how in the early phase of satellite navigation made spoofing unlikely. The understanding of GPS as well as the skills needed to mount an intentional spoofing attack is becoming more widely available.

Satellite navigation receivers can be categorized into snap-shot and tracking receivers.

- Snap-shot receivers sample the signal and subsequently process these samples from memory. The time span between two measurements varies widely. It is chosen in a trade-off of functional requirements and power consumption. This type of receivers is used in most consumer products.
- Tracking receivers continuously estimate the frequency, delay, and phase of the signal, i.e., they extensively use prior knowledge about the signal.

Satellite navigation receivers are susceptible to spoofing attacks rather differently during the acquisition and the tracking phase:

- *CS (Cold Start)* Spoofing starts before acquisition and the receiver has no a priori knowledge. This situation occurs after a receiver is switched on (cold start). The receiver cannot distinguish the spoofer's signal from an authentic GNSS signal unless the signal is somehow authenticated.

- *Ra (Reacquisition)* Spoofing starts before acquisition but the receiver has a priori knowledge. This situation occurs if the receiver has lost one or all satellites for a short while, or acquires satellites that have newly raised above the horizon. Snap-shot receivers are in this situation for every estimate that they perform once they have prior knowledge.
- *Tr (Tracking)* Spoofing during tracking. This is the most demanding situation for the spoofer, since the signals now have to change in a manner compatible with the detailed physical movement of the receiver, as well as with the changes in its environment.

There are two fundamentally different types of spoofing signals. The first one is a (local) replay of authentic GNSS satellite-generated signals – this form is called meaconing. For the spoofer it is attractive since any form of signal authentication is maintained, including the encryption used in military and Public Regulated Signals (PRS), such as GPS P(Y) and GPS M-code as well as Galileo PRS. The spoofer is, however, limited to delay signals. The second form of spoofing used fully synthetic signals. Since the current open services do not include any cryptographic protection, these open GNSS signals can be synthesized by everyone.

The spoofer has different options for injecting the signal:

- **Cab (Cable inject)** In this case, the spoofer directly injects his signal into the receiver front-end either by unplugging the antenna cable and by connecting it to the spoofing source or by significantly attenuating the GNSS signals and injecting the spoofing signal at the same time. This option gives the spoofer the maximum control possible. It can be implemented whenever the receiver is under the spoofer's control.
- **Coh (Spoofing by coherent superposition)** In this case, the spoofer knows the precise location of the receiver's antenna, as well as the phasing of the signal. In the coherent case, the spoofer suppresses the main component of the authentic satellite signal by subtracting a synthesized copy of that component for a time long enough to capture the receiver to his signal.
- **NCo (Spoofing by non-coherent superposition)** In this case the spoofer has lesser control. He must hide the authentic signal in noise. This option is more widely applicable but is easier to defend.

Table 2: Difficulty for a spoofer to succeed in different scenarios. The target receiver is assumed to be maximally smart in all cases.

	Cab	Coh	Nco
CS	very easy	-	less difficult
Ra	easy	-	very difficult
Tr	very difficult	very difficult	very difficult

A spoofer can misrepresent the state of the receiver by acting on the GNSS signals and the navigation messages. If the target receiver uses assistance or augmentation data, a spoofer can also influence the receiver by manipulating this data.

Appendix A.2.3 Countermeasures

Synthetic or manipulated navigation messages can be detected by analyzing

- The scheduling of changes in the navigation message,
- The conformances of changes in the parameters with models,
- The consistency of measurements with the navigation solution, and
- The signature (authentication) of the navigation message.

The navigation messages shall in particular remain readable in open form. This excludes the use of message encryption. An asymmetric cryptographic signature appears a good solution. The length of the public key and the

cryptographic signature should be long enough to guarantee acceptable security. However, long signatures can take considerable time to transmit on a typical channel of 50 bps. Due to the possibility of transmission errors, signatures need to be protected by error correcting codes. In order to reduce the authentication delay, the navigation messages may additionally be signed using a different asymmetric cryptosystem in the Internet. This requires that the receiver has access to the Internet, which most receivers do.

In case the delay caused by a cryptographic signature scheme is too large, a promising approach is to use inertial measurements for propagating the GNSS measurements from the past instant at which they can be authenticated to the present. On aircraft, the propagation can be implemented using a navigation grade INS.

With coherent and non-coherent signal injection, the receiver's antenna captures a superposition of the authentic and spoofed signal. This provides an opportunity for the receiver to detect the spoofer. The superposition of signals is difficult to distinguish *a priori* from multipath, but previous tests show the multipath and spoofing to have different properties. In general situations it is recommended to estimate the multipath components associated with the signals transmitted by the visible satellites on all carrier frequencies and to use these to discriminate the spoofer from multipath.

Finally the receiver must also analyze the consistency of its solution. In the presence of *a priori* information, the options of the spoofer become rather limited both with respect to the timing and the size of the state changes that can be induced if the receiver performs these types of verifications.

Authentication schemes will not help to discover a meaconing attack. Meaconing can be detected by through the jump in position at the time at which the receiver locks on the spoofer's signal and/or the clock jump, which is positive whenever the target receiver is not collocated with the spoofer at the time of lock.

Typical spoofers transmit their signals using a single antenna. Thus the spoofed signals all arrive from one single direction. The authentic satellite signals, on the other side, arrive from different directions. This may be used to detect and even localize the spoofer. It requires a receiver capable of estimating directions of arrival, e.g., by evaluating the phases of the signals received by a set of antennas.

The article shows a spoofing monitor that can be included in GNSS receivers to judge the consistency of the measurements (Figure 4).

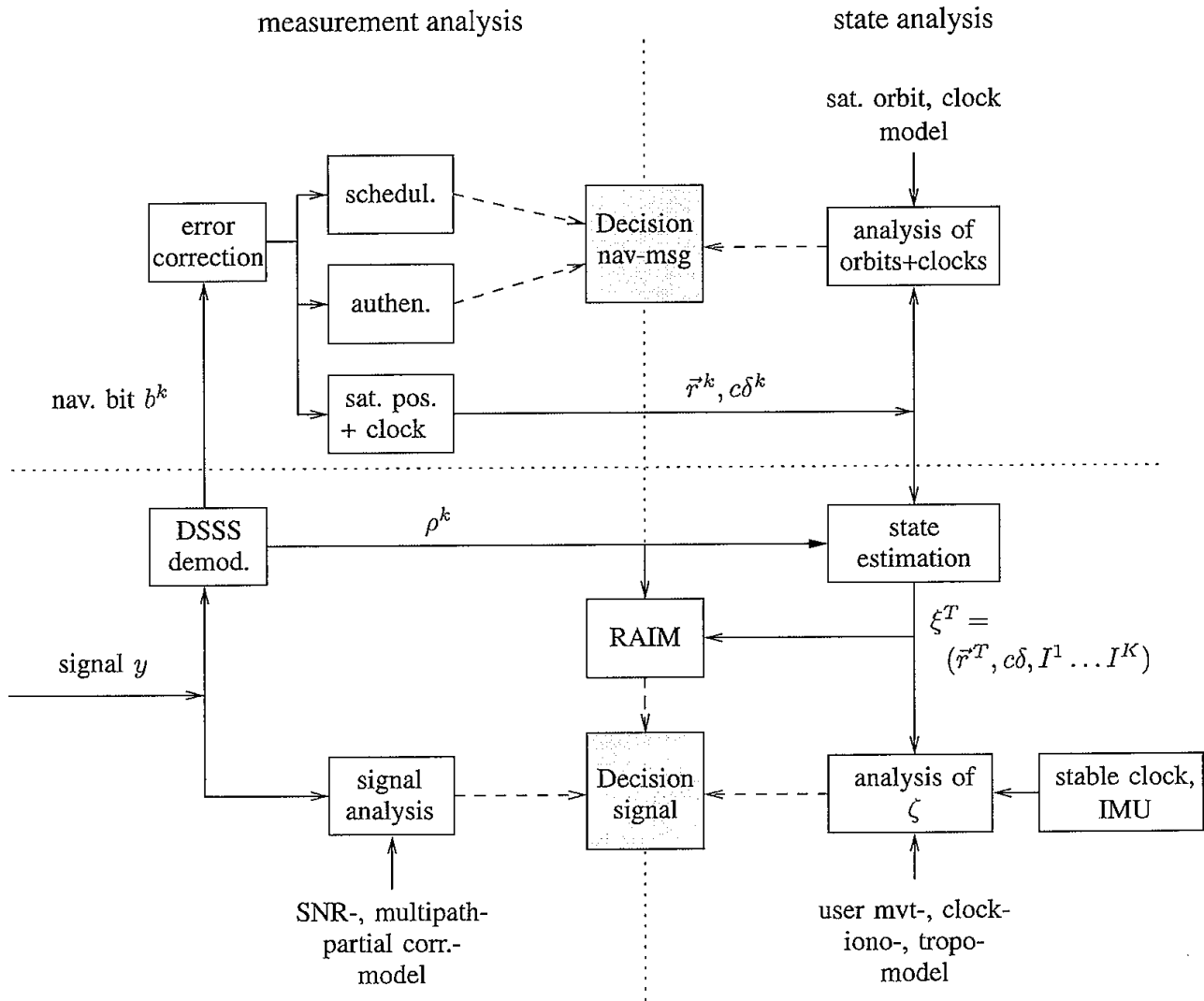


Figure 4: Spoofing monitor consisting of a number of estimation and evaluation units. The sampled signal is analyzed with respect to its conformance to models describing the signal and the multipath. "RAIM" finally establishes the consistency of the measurements amongst themselves

Appendix A.3 Improving the Operation and Development of Global Position (GPS) Equipment Used by Critical Infrastructure

Publication by the National Cybersecurity & and Communications Integration Center, and National Coordinating Center for Communication [25].

This paper is intended as a Best Practices Guide to be used for Improving the operations and development of GPS equipment used by Critical Infrastructure.

Appendix A.3.1 Installation and Operation Strategies for Owners, Operators, and Installers

1. Obscure antennas such that they are not visible from publicly accessible locations
2. Provide decoy antennas
3. Carefully select antenna locations for a clear sky view, but low multipath and little RF propagation from the ground
4. Employ blocking antennas (or CRPAs)
5. Introduce redundancy
6. Calibrate (time delay of the antenna and the antenna electronics)
7. Avoid using low elevation signals
8. Use position hold for stationary timing receivers
9. Employ high-quality holdover devices
10. Add a sensor/blocker
11. Practice good cyber hygiene

Appendix A.3.2 Development Strategies for Manufacturers

1. Extend data spoofing whitelists to sensors
2. Plan for growth
3. Implement software assurance
4. Return to known good state
5. Address all components
6. Enable secure remote access and management
7. Enhance anti-jam capabilities
8. Enhance anti-measurement spoof processing
9. Implement anti-data spoofing
10. Use more GPS signal types
11. Instrument receivers capture data

Appendix A.3.3 Research Opportunities

1. Extended whitelists and associated government reference software
2. Generalize blocking antenna polarization
3. Exploit other sources of data messages
4. Reduce latency in recognition and reporting of interference, jamming, and spoofing

Appendix A.4 The economic impact on the UK of a disruption to GNSS

In this report by London Economics in 2017 the economic impact on the United Kingdom of a disruption to GNSS is quantified [21]. GNSS is assumed completely unavailable for 5 days. The cause does not really matter. It can be a failing of the GNSS system(s) or large scale interference or a different cause. Per sector the financial losses due to the outage are investigated and quantified. Spoofing is mentioned briefly, but is out of scope for most part in this report.

Some spoofing scenarios that are mentioned:

- Spoofing attacks that impact the GPS timing signals for network synchronisation in the energy sector.
- Offender tracking is particularly vulnerable to jamming and spoofing because this would liberate the offender, and allow them to leave the fenced area that they may legally occupy.
- A successful spoofing attack of a financial institution could result in significant losses.

Appendix B Interviews

The interviews are contained in a separate document (NLR-CR-2019-001-PT-2).

NLR

Anthony Fokkerweg 2
1059 CM Amsterdam, The Netherlands
p) +31 88 511 3113
e) info@nlr.nl i) www.nlr.nl