TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 12
Number 4
December 2018
DOI: 10.12716/1001.12.04.01

Foundations of GNSS Spoofing Detection and Mitigation with Distributed GNSS SDR Receiver

M. Filić
University of Ljubljana, Ljubljana, Slovenia

ABSTRACT: GNSS spoofing is an intentional and malicious action aimed at degrading and suppressing GNSS Positioning, Navigation, and Timing (PNT) services. Since it affects data and information segment of GNSS, it is considered a GNSS information (cyber-) security attack. Considering a significant and powerful threat, GNSS spoofing should be treated seriously to avoid damage and liabilities resulting from disruptions of GNSS PNT services. Here the GNSS position estimation procedure is examined for potential vulnerabilities, and the nature of and motivation for GNSS spoofing attacks exloiting the vulnerabilities assessed. A novel GNSS Spoofing Detection and Mitigation (GNSS SDM) method is proposed within the established computational and communication infrastructure, that allows for successful overcoming and classification of GNSS spoofing attacks. Proposed method is applicable without requirements for core GNSS modification, and leaves majority of user equipment easily transferable to the GNSS spoofing-free environment. Potential GNSS spoofing effects and GNSS anti-spoofing opportunities in maritime sector were given a particular attention.

1 INTRODUCTION

In times when satellite navigation literary lies in foundations of modern society (UK Government Office of Science, 2018), every threat to GNSS Positoning, Navigation, and Timing (PNT) services should be considered with due attention. GNSS spoofing is a malicious actions aimed at degradation of GNSS PNT services, with potential huge consequences on life, safety, security, health, property and economy. Identified as an information security-related issue, GNSS spoofing is the target of growing number of research studies across the world.

Here a novel concept of GNSS spoofing counter-measure is proposed, established on identification of GNSS position estimation process and GNSS receiver design shortcomings and vulnerabilities, characterisation of the nature of GNSS spoofing, and survey of recent research in GNSS anti-spoofing methods development. The GNSS Spoofing Detection and Mitigation (GNSS SDM) method is founded on a dedicated architecture and capabilities of modern computational and communication technologies. It does not require core GNSS system modification, and allows for seamless transition of majority of GNSS-enabled devices towards safety from GNSS spoofing .

The manuscript reads as follows. This Section outlines the motivation for research, and introduces the content of the manuscript. Section 2 details the GNSS position estimation mathematical method and procedure, while identifying potential vulnerabilities. Section 3 addresses recent trends in GNSS receiver design, especially a more direct implementation of mathematical methods using software solutions, rather with model approximation using electronic circuitry. Section 4 outlines the results of the previous

research survey, and summarises potential approach in GNSS spoofing counter-measures development. Section 5 presents the details of the proposed GNSS SDM method, the architecture in support of GNSS SDM method implementation, results of practical validation and concluding comments. Section 6 addresses potential benefits of the GNSS SDM implementation in maritime sector. Manuscript concludes with summaries of findings and proposals for further research in Section 7, and with an exhaustive list of references.

2 GNSS POSITION ESTIMATION MODEL

The satellite-based position estimation relies upon the accurate measurement of satellite signal propagation time between satellite and receiver aerials, and on provision of accurate position of every satellite involved in estimation process (Petrovski and Tsujii, 2012), and (Filić and Filjar, 2018a) for discussion. A GNSS receiver measures the satellite signal propagation time (and, therefore, the distance, pseudorange, between the satellite and receiver aerials, providing the satellite signal propagates at the constant velocity equal to the velocity of light in vacuum) using a cross-correlation-based statistical signal processing procedure (Petrovski and Tsujii, 2012) applied on the Pseudo-Random Noise (PRN) codes broadcast by GNSS satellites as components of the composite GNSS signals. PRN codes uniquely identifies aGNSS satellite and allows for accurate and precise propagation time measurement. (Petrovski and Tsujii, 2012) reports research initiatives to modernise GNSS systems and service through replacement of currently used PRN codes with chaotic signals. The transition may allow for more accurate measurements through improved synchronisation (Pecora et al, 1997), and enhanced resilience against natural and artificial (Alvarez and Li, 2006) sources of interference, as it has been demonstrated in theory and in the other telecommunication systems (Sun, 2015), (Babu and Singh, 2013). (Vaudenay, 2005), (Alvarez and Li, 2006) and (Sun, 2015) discussed opprtunities of chaos-based cryptography in securing communication systems and advancing the quality of their services.

Broadcast satellite signal may be formally described as in (1), given is the description of the US-operated GPS composite signal structure for commercial-grade single-frequency GPS receivers (Petrovski and Tsujii, 2012).

$$s_{GPSL1} = a_p P_i(t) D_i(t) \sin(2\pi f_{L1} t + \phi_{L1}) + a_c C_i(t) D_i(t) \cos(2\pi f_{L1} t + \phi_{L1}) \quad (1)$$

where:
s_{GPSL1}… denotes broadcast composite GPS satellite signal transmitted on L1 = 1575.420 MHz carrier (commonly used by commercial-grade single-frequency GPS receivers)
i … index of the satellite in consideration (i-th)
t … time instant
a_p … denotes amplitude of authorised component of broadcast composite GPS satellite signal
$P_i(t)$… denotes the Precision GPS PRN binary code for pseudorange measurement provided to authorised (dual-frequency) GPS users
$D_i(t)$ … denotes binary coded navigation message, with satellite ephemeris data for satellite position determination, parameters for error correction models, satellite and system health status information, and the other related datasets
f_{L1} = 1575.420 MHz
φ_{L1}… phase of L1 carrier
a_c … denotes amplitude of the Coarse Acquisition (C/A) component of broadcast composite GPS satellite signal
$C_i(t)$… denotes the Coarse Acquisition (C/A) GPS PRN binary code for pseudorange measurement provided to all (both authorised, dual-frequency, and civil, single-frequency) GPS users

A dedicated GNSS statistical signal processing procedure within a GNSS receiver returns a pseudorange estimate comprising the actual (true) distance between a satellite and a receiver aerials, denoted with R, and a number of error components that compromise measurements process, and cause the GNSS position estimation error. The pseudorange observation structure is given with (2) (Filić and Filjar, 2018a).

$$\rho = R + c\delta t_{rec} + \epsilon_{ionospheric} + \epsilon_{tropospheric} + \epsilon_{multipath} + \epsilon_{sat-eph} + \epsilon_{sat-clock} + \epsilon_{random} \quad (2)$$

where:
ρ … denotes a pseudorange, measured using statistical signal processing procedure in GNSS receiver, between the satellite in observation and the user GNSS receiver aerial in [m]
c … denotes velocity of electromagnetic wave propagation in vacuum
δt_{rec} … denotes user GNSS receiver clock error (large, unknown, but statistically independent from the choice of satellite)
$\varepsilon_{ionospheric}$ … denotes pseudorange measurement error due to ionospheric effects (Filić and Filjar, 2018a)
$\varepsilon_{tropospheric}$ … denotes pseudorange measurement error due to tropospheric effects (Petrovski and Tsujii, 2012)
$\varepsilon_{multipath}$ … denotes pseudorange measurement error due to multipath effects (Petrovski and Tsujii, 2012)
$\varepsilon_{sat-eph}$ … denotes pseudorange measurement error due to satellite ephemeris errors (Petrovski and Tsujii, 2012)
$\varepsilon_{sat-clock}$ … denotes pseudorange measurement error due to variations in satellite clock accuracy (Petrovski and Tsujii, 2012)
ε_{random} … denotes the other pseudorange measurement errors, uncorrelated to previous groups and of random nature (Filić, Filjar, 2018) (Petrovski and Tsujii, 2012)

The aim of the GNSS position estimation process is to yield the measurement-based unambiguous estimate of user GNSS aerial position in three-dimensional WGS-84 coordinate system, time in Universal Time Co-ordinated (UTC) system, and GNSS positioning error vector. The GNSS-based description of user state comprises four spatio-temporal state variables, as presented with (3), where x, y, and z denotes the three components of a position

estimate vector in respective WGS-84 datum frame (Petrovski and Tsujii, 2012).

$$\hat{\vec{x}} = \left(x, y, z, \delta t_{rec}\right) \tag{3}$$

The GNSS problem (3) solution is commonly obtained using the iterative procedure given in (4) and (5) (Petrovski and Tsujii, 2012), (Filić, 2017), (Filić, Grubišić and Filjar, 2018), (Filić and Filjar, 2018a), where *k* denotes the iteration step.

$$\begin{aligned} x_{k+1} &= x_k + \Delta x \\ y_{k+1} &= y_k + \Delta y \\ z_{k+1} &= z_k + \Delta z \end{aligned} \tag{4}$$

$$\begin{bmatrix} \Delta x \\ \Delta y \\ \Delta z \\ c\delta t_{rec} \end{bmatrix} = \begin{bmatrix} \frac{x_k - x_{S1}}{R_{1,k}} & \frac{y_k - y_{S1}}{R_{1,k}} & \frac{z_k - z_{S1}}{R_{1,k}} & c \\ \frac{x_k - x_{S2}}{R_{2,k}} & \frac{y_k - y_{S2}}{R_{2,k}} & \frac{z_k - z_{S3}}{R_{3,k}} & c \\ \frac{x_k - x_{S3}}{R_{3,k}} & \frac{y_k - y_{S3}}{R_{3,k}} & \frac{z_k - z_{S3}}{R_{3,k}} & c \\ \frac{x_k - x_{S4}}{R_{4,k}} & \frac{y_k - y_{S4}}{R_{4,k}} & \frac{z_k - z_{S4}}{R_{4,k}} & c \end{bmatrix} \cdot \begin{bmatrix} \rho_1 - R_{1,k} \\ \rho_2 - R_{2,k} \\ \rho_3 - R_{3,k} \\ \rho_4 - R_{4,k} \end{bmatrix} \tag{5}$$

where:
(x_k, y_k, z_k) … denotes user GNSS position estimate in k-th iteration step
(x_{Si}, y_{Si}, z_{Si}) … denotes i-th satellite position at the time of satellite signal broadcast
{ρi, i = 1, …, 4} … a set of GNSS pseudorange measurements taken with four different satellites independently and at the same time

$$R_{i,k} = \sqrt{\left(x_k - x_{Si}\right)^2 + \left(y_k - y_{Si}\right)^2 + \left(z_k - z_{Si}\right)^2} \tag{6}$$

The 4 x 4 matrix in (7) is commonly known as geometric (***G***) matrix.

$$G = \begin{bmatrix} \frac{x_k - x_{S1}}{R_{1,k}} & \frac{y_k - y_{S1}}{R_{1,k}} & \frac{z_k - z_{S1}}{R_{1,k}} & c \\ \frac{x_k - x_{S2}}{R_{2,k}} & \frac{y_k - y_{S2}}{R_{2,k}} & \frac{z_k - z_{S3}}{R_{3,k}} & c \\ \frac{x_k - x_{S3}}{R_{3,k}} & \frac{y_k - y_{S3}}{R_{3,k}} & \frac{z_k - z_{S3}}{R_{3,k}} & c \\ \frac{x_k - x_{S4}}{R_{4,k}} & \frac{y_k - y_{S4}}{R_{4,k}} & \frac{z_k - z_{S4}}{R_{4,k}} & c \end{bmatrix} \tag{7}$$

System (4) and (5) may be deployed for direct user state (position and time) estimation under condition of successful suppression of all the error effects (Filić, 2017), (Filić, Grubišić, and Filjar, 2018), (Filić and Filjar, 2018a). However, if the residual errors cannot be neglected, an advanced optimisation approach should be taken to assure the solution stability and quality of position estimates (Filić, 2017), (Filić and Filjar, 2018a).

Weighted Least-Square position estimation method may be considered the solution of the above-stated optimisation problem (Filić, 2017), (Gustafsson, 2010), (Gallier and Quaintance, 2018). In general, the Weighted Least-Square method aims at solving the problem (8), minimising the square error between observed and estimated value of a variable y.

$$miny_i - \hat{y}_W^2 \tag{8}$$

Considering unequal contribution (importance) of particular predictors (input variables), the minimisation problem solution may be expressed using weights $\vec{w}$, as expressed in (9) (Gustafsson, 2010).

$$miny_i - \hat{y}_W^2 = \sum_{i=1}^{n} w_i \cdot \left(y_i - \hat{y}\right)^2 \tag{9}$$

Weighted Least-Square method yields the GNSS navigation problem solution in the form of (10), where x_w denotes weighted user state estimate, ***G*** denotes geometric matrix, ***W*** denotes matrix of weights, and $\vec{y}$ denotes vector of GNSS pseudorange measurements (Filić, 2017), (Filić and Filjar, 2018a). Weights may be defined in a manner to address the particular effect of known statistical description, as discussed and demonstrated in (Filić, 2017) for the problem of uncorrected random component of GNSS ionospheric delay.

$$\hat{\vec{x}}_w = \left(G^T W G\right)^{-1} G^T W \vec{y} \tag{10}$$

Eq (10) yields a single point solution of GNSS navigation problem, which may be corrupted still with residual errors, mostly of stochastic nature. Further clearing of GNSS-based position estimates is commonly performed through implementation of Kalman filter for removal of Gaussian position estimation errors (Filić and Filjar, 2018a), (Petrovski and Tsujii, 2012).

3 GNSS SOFTWARE-DEFINED RADIO (SDR) RECEIVER CONCEPT

Position estimation process based on GNSS observations takes place in a user GNSS receiver. This service arrangement allows for privacy protection and the GNSS position estimates to remain in user equipment only, since no communication response is ever sent from a GNSS receiver to a GNSS satellite in a core positioning service scenario, under condition of the user's consent. Information on the user's whereabouts may be exchanged for operation of GNSS-based applications, but this extends the scope of the core GNSS positioning service.

The GNSS position estimation procedure comprises signal and data processing at the three essential domains, as depicted in Figure 1.: (i) Radio Frequency (RF) domain, (ii) Base-Band (BB) domain, and (iii) Navigation domain. Figure 1 outlines the signals and data considered in related domains, as well as results of the domain-related processing. Detailed description may be found elsewhere (Petrovsky and Tsujii, 2012), (Filić and Filjar, 2018a).

A traditional GNSS receiver deploys an electronics-based approach in processing GNSS signals and data, where dedicated and tailored electronics circuitry is utilised to perform processing tasks governed by mathematical methods and models. In recent years, the Software-Defined Radio (SDR) approach has gained popularity. Aimed at replacement of every possible electronics-based solution with a software-based solution operated on a general purpose hardware (such as a personal computer, or a smartphone), SDR allows for more accurate, efficient, flexible and re-configurable receiver architecture. Those are accomplished with the direct implementation of mathematical methods and models in software, instead of approximating them with electronics circuits (Stewart et al, 2015), (Filić and Filjar, 2018a).

Origins of the Software-Defined Radio may be traced to research conducted by Joseph Mitola III (Mitola, 1995). A comprehensible and problem-oriented coverage of the subject may be found in (Stewart et al, 2015). (Petrovski and Tsujii, 2012) and (Filić and Filjar, 2018a) gave a systematic view on SDR utilisation in satellite navigation, including a brief outline given in this Section.

GNSS is a telecommunication system, and a GNSS receiver is its component. With a GNSS receiver complying to common procedures of a telecommunication system, it has been a straightforward action to render a transition from the traditional to SDR-based GNSS SDR receiver design. GNSS SDR receiver has advanced in the means that the Base-Band (BB) and Navigation domain signal and data processing moved from (mostly) hardware-based to (entirely) software-based. Such a transition has opened a wide perspective for advanced and independent development of error correction and position estimation methods and models, tailored to satisfy targeted requirements of GNSS-based applications (systems and services) (Filić and Filjar, 2018a).

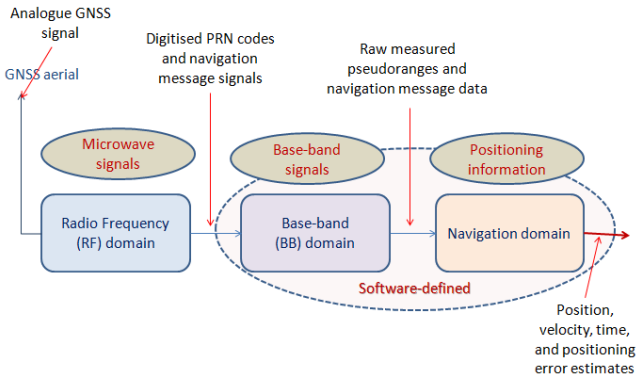

Figure 1. GNSS signal and information processing in GNSS Software-Defined Radio (SDR) receiver

A vast room for opportunities has been opened in both the BB and Navigation domains for improvements and enhancements. Additionally, recent developments in gaining access to raw GNSS observations (GNSS pseudoranges and navigation message data) in smartphones through transparent interface between BB and Navigation domains (Filić and Filjar, 2018b) attracts research interests in exploiting new source of massive data sets bearing marks of positioning environment effects, both natural (ionospheric and multipath effects) and artificial (spoofing and jamming).

The advancement prospects have arisen from the methodology of data processing in Navigation domain, as depicted in Figure 2. The implementation of a selected GNSS position estimation method is preceded by raw GNSS observations, commonly pseudoranges, assessments and corrections for known sources of systematic errors. Ionospheric delay effects that corrupt pseudorange measurements are commonly corrected using NeQuick (for Galileo pseudoranges) or Klobuchar (for GPS and Bediou pseudoranges) error correction models, which parameters are sent as a part of navigation message (Filić and Filjar, 2018) (Petrovski and Tsujii, 2012). Tropospheric effects on GNSS pseudoranges are corrected using Saastamoinen or Neill mapping function error correction models (Petrovski and Tsujii, 2012). Satellite clock errors are corrected using stochastic models with parameters broadcast in navigation message, again.

GNSS pseudoranges corrected for foreseeable and known systematic errors are used for GNSS-based position and positioning error estimation, as outlined in Section 2 of this mansucript.

Considering recent developments in computer science, telecommunications, and signal processing disciplines, the GNSS SDR concept may be enhanced further with the proposal of distributed GNSS SDR receiver concept. With the reference to Figure 3, a novel GNSS SDR receievr design is proposed herewith, that leaves the RF component only in a mobile part of a GNSS SDR receiver, together with provision of reliable and uninterrupted communication with the rest of the receiver (BB and Navigation domain processors), hosted by an external facility, in the computing environment with a suitable computational capacity and the access to position estimation assistance data (for instance, tailored local/regional error correction model, bespoke position estimation method that complies to requirements of targeted GNSS application etc.).

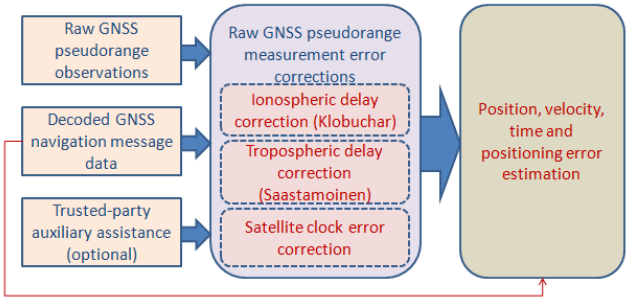

Figure 2. GNSS information processing in Navigation domain

In implementation of a distributed GNSS SDR receiver, mobile unit would send a series of snapshots of digitised waveforms of demodulated composite GNSS signal components (C/A PRN codes, navigation message data/signals) to the BB and Navigation domain processing facility (running in cloud, as an example) for the complete observations-based position estimation, thus allowing for personalised,

assisted and more accurate position estimation, that will spare mobile unit from power-consuming extensive computation with insufficient assistance.

4 GNSS SPOOFING

GNSS spoofing is an intentional malicious and pernicious information security attack on GNSS, conducted through broadcast of counterfeit (manipulated) GNSS signals with malicious intention of deception of GNSS receiver to estimate incorrect position using allegedly original GNSS signals.

With GNSS becoming an essential component of national infrastructure, resilience against any GNSS Positioning, Navigation, and Timing (PNT) service distortion has become the prioritised task to resolve to allow for seamless and uninterrupted operation of GNSS-based applications. Numerous often multi-disciplinary research groups affiliated to respected research organisation addressed the problem in their research studies.(Schenewerk et al, 2016) outlined a procedure for navigation message examination for quality assurance in the matters of archiving the material with the International GNSS Service (IGS) repository (Jafarnija-Jahromi et al, 2012) presented a detailed study of the problem, its nature, technology background, and possible approaches for counter-measures development. (Tippenhauer et al, 2011) presented a thorough study of requirements to be fulfilled for a successful GNSS spoofing cyber-attack. T E Humphreys and his team defined the problem first, and then examined a number of different scenarios of GNSS spoofing attacks, proposing several approaches to GNSS anti-spoofing methods development in (Humphreys et al, 2008), (Nighswander et al, 2012), (Wesson, Rothlisberger, and Humphreys, 2012), (Kerns et al, 2014a), (Kerns et al, 2014b), and (Psiaki and Humphreys, 2016). The group even demonstrated successful GNSS spoofing attacks that resulted with remote overtaking control of a vessel (Bhatti and Humphreys, 2017) and an aircraft (Kerns et al, 2014a).

Survey of research accomplishments so far, conducted during the study presented here, reveals the Base-Band (BB) domain as the target of GNSS spoofing methods. Attacks focus generally on both PRN signals and navigation message data forgery, thus persuading a GNSS receiver to determine a pre-engineered incorrect position. Still, majority of GNSS spoofing attacks address modification of GNSS navigation message as a more efficient and pragmatic means for GNSS PNT services distortion.

The GNSS spoofing counter-measures (GNSS anti-spoofing) concentrate on patching the inherited GNSS vulnerabilities in all three domains of GNSS signal and data processing (Figure 1). GNSS anti-spoofing methods rely almost entirely on modification of the core GNSS system, with the only exception of multi-aerial user equipment utilisation. (Humphreys et al, 2008) identified the following candidate GNSS anti-spoofing measures: (i) amplitude discrimination, (ii) time-of-arrival discrimination, (iii) assessment of consistency of navigation inertial measurement unit (IMU), (iv) discrimination of polarisation, (v) angle-of-arrival discrimination, and (vi) cryptographic authentication. All the proposed approaches assures user equipment independence from any kind of communication network. Assurance that the received signal and navigation message are genuine (original) is the aim of the GNSS anti-spoofing methods. The matter has recently become known as the GNSS signal authentication requirement (O'Driscoll, 2018), (Capparra et al, 2016). Its development and implementation is increasingly regarded to utilisation of tailored encryption (Wesson, Rothlisberger, and Humphreys, 2012), (Kerns et al, 2014b) that will provide authenticity assurance, and even enhance the GNSS pseudorange measurement accuracy, unrelated to its the initial purpose. A prospect of utilisation of a 'trusted' receiver for GNSS spoofing detection was examined in (Kuhn, 2010). The concept may be extended with consideration of scenarios such as EGNOS assistance data streaming service, or A-GNSS service provided by mobile telecommunications networks as the means of provision of GNSS data from 'trusted' receiver. The EU global satellite navigation system Galileo offers such a service in its portfolio. However, the implementation and operation of the encrypted services will call for different user equipment.

5 GNSS SPOOFING DETECTION AND MITIGATION USING DISTRIBUTED GNSS SDR.

Resulting from understanding of GNSS position estimation process in modern GNSS receivers (Sections 2 and 3) and the nature of the GNSS spoofing problem (Section 4), the GNSS spoofing detection and mitigation (GNSS SDM) method that utilises distributed GNSS SDR (introduced in Section 3) is proposed in this Section, and depicted in Figure 3.

The introduction of the GNSS SDM counter-measure relies on the presumptions, as follows: (i) implementation of distributed GNSS DR concept, with the required computational and communication capacity fully operational (Section 3), (ii) seamless and continuous access to GNSS assistance data (including streams of broadcast navigation message) from sources such as EGNOS data streaming, or A-GNSS service provided with mobile telecommunication networks(Petrovski and Tsujii, 2012).

The GNSS SDM counter-measure method is implemented within the architecture depicted in Figure 3 using a spoofing detection algorithm (**Algorithm** 1, below) based on comparison between the broadcast ('trusted') and received (by user GNSS receiver) navigation message. The GNSS SDM algorithm is developed in order to identify potential mis-matches in the two sets of data, and to attempt to classify the cause of such a mis-match (loss of data in communication, or a pattern that suggest possible intentional manipulation with data).

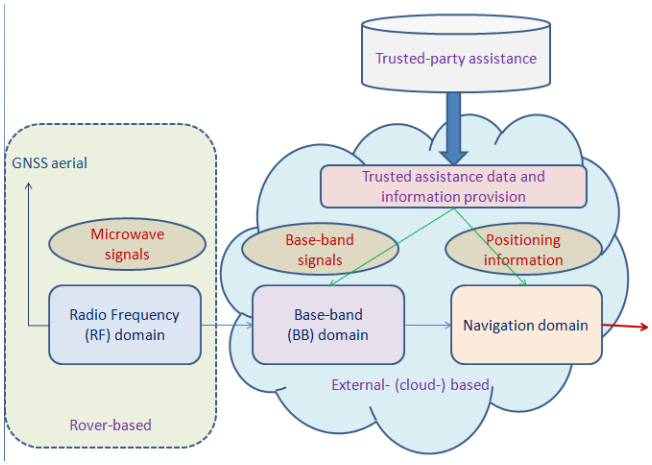

Figure 3. GNSS anti-spoofing operational method, based on distributed GNSS SDR receiver and auxiliary assistance

Algorithm 1: Spoofing detection by comparison of broadcast and received navigation messages

Data: Two equally dimensioned data frames *b[n, m]* and *r[n, m]* containing binary content of broadcast, and received GPS navigation message, respectively.
Result: Data frame *flags[n, m]* of flags indicating equality of related bits of binary content

```
1  read two data frames b and r;
2  create empty result data frame flags[n,m];
3  for i := 1 to n do
4      for j := 1 to m do
5          if (b[i,j] == r[i,j]) {
6              flags[i,j] == 1}else{
7              flags[i,j]==0}
8          end;
9      end;
10 end;
```

Proposed concept, including the GNSS SDM architecture and algorithm, was validated under this study through simulation developed in the open source R framework for statistical computing. (R-project, 2018). Different approaches in data frame comparison were used that allows for identification of mis-matches and generation of flag matrix indicating them. The R-based algorithms were based on the early works in string comparison (Levenshtein, 1966), (Landau and Vishkin, 1988), and (Navarro, 2001) and their implementations either in core R, or in supported R software libraries, such as: *compareDF* and *arsenal*. The initial successful results of the GNSS SDM method deployment have been accomplished, encouraging further research in advanced GNSS spoofing detection through statistical learning-based mis-match pattern detection and classification. With simple statistical learning models already providing unexpected good performance, the GNSS SDM method is a potential candidate for successful detection and classification of various forms of GNSS spoofing attacks.

Data transfer of RF domain signal snapshots and original (broadcast) navigation message may be performed using the advanced cryptographic methods to assure communication security. Quantum computing and cryptography methods may considerably rise the security level. At the same time, the analytics of communications may reveal hidden details of the attacks declined and of their perpetrators (Wittek, 2014).

Once discovered, cases of GNSS spoofing attacks may be examined further to identify the region(s) of GNSS spoofing operation, and even to identify the perpetrator using spatial statistical learning and location intelligence techniques and methods. GNSS SDM method is deployed at the cloud level, thus capable of aggregation and analytics of massive data sets with potential sources of GNSS spoofing data. At the same time, access to 'trusted' navigation message allows for correct implementation and GNSS spoofing elimination in distributed GNSS SDR position estimation process. Statistical learning-based characterisation, classification and location intelligence may mature in a powerful tool to combat GNSS spoofing attacks on the grounds of artificial intelligence.

Proposed GNSS SDM deployment does not require any modification of the core GNSS systems, but the provision of original (broadcast) navigation message content using the alternative means (internet streaming, A-GNSS etc.). Moreover, modern mobile platforms with embedded GNSS receivers (smartphones, Internet-of-Things GNSS-equipped devices, vehicles, aeroplanes, vessels etc.) may render transition to distributed GNSS SDR fairly easily. In sum, the establishment of the environment for the GNSS SDM method implementation may be performed seamlessly and efficiently.

6 GNSS SPOOFING IN MARITIME SECTOR

The problem of GNSS spoofing attacks should be thoroughly considered as serious threat for GNSS-based applications in maritime sector. Research groups have already demonstrated successful GPS spoofing attacks in air (Kerns et al, 2014), maritime (Bhatti, and Humphreys, 2017), and land (Zeng et al, 2017) navigation applications. Maritime sector relies increasingly on information and communication technologies, with numerous operational procedures under development and data management not always considered a critical element of sustainable development and operations. Despite the allegations, there has not been confirmations of any real GNSS spoofing attack in practice yet. However, this may be taken as an advantage only, providing the breathing time to develop and validate GNSS anti-spoofing measures before the actual GNSS spoofing attack occurs.

Proposed GNSS SDM is applicable in maritime sector through various means of implementation. Improved communication capacity even at the open sea assures access to GNSS assistance data. Compared with personal mobile platforms, vessels may host more capable computational facilities to serve as mobile hubs for GNSS spoofing detection and classification in a mobile environment, providing the GNSS spoofing-related knowledge on the global basis.

7 CONCLUSION

GNSS spoofing has been recognised a particularly harmful and serious form of threat to GNSS performance and operation. Numerous research groups have worked extensively on the problem. GNSS spoofing operation has been demonstrated in a number of research projects, justifying a significant effort in counter-measures development.

Curiously enough, only the unconfirmed allegations of GNSS spoofing in operation have been recorded so far. However, the threat must not be treated lightly, but just as an opportunity to counter-measure the cyber-attack of potential serious effects on the economy, safety and security, and society in general.

Here the foundations of a novel approach in combating GNSS spoofing threats are presented. After a brief outline of GNSS position estimation process and its shortcomings and vulnerabilities, a thorough examination of the GNSS spoofing problem is given. Potentials of various GNSS spoofing counter-measures development were assessed. The GNSS Spoofing Detection and Mitigation (GNSS SDM) method was developed and outlined, within the established framework architecture and requirements for GNSS anti-spoofing. The proposed method does not require modification of either the existing GNSS core systems, or the prevailing majority of the existing user equipments (smartphones, in particular). The proposed concept is validated in simulation-based scenario developed within the R framework for statistical computing, demonstrating GNSS spoofing detection and statistical learning-based classification. GNSS spoofing mitigation was conducted using the very nature of the proposed concept.

GNSS spoofing is a serious information security threat that should be mitigated efficiently and completely. Potential damage and liabilities resulting from GNSS spoofing are enormous. It is believed that the proposed method, based on statistical learning, and potentially enhanced further with cryptography methods, may provide a successful tool in combating GNSS spoofing.

REFERENCE

Alvarez, G, and Li, S.(2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *Int J of Bifurc and Chaos*, 16(8), 2129-2151.

Babu, A M, and Singh, K J. (2013). Performance Evaluation of Chaotic Encryption Technique. *Amer J of Appl Sci*, 10(1), 35-41.

Bhatti, J, and Humphreys, T E. (2017). Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *NAVIGATION: Journal of the Institute of Navigation*, 64(1), 51-66. doi: 10.1002/navi.183

Capparra, G et al. (2016). Navigation Message Authentication Schemes. *Inside GNSS*, Sep-Oct 2016, 64-73.

Filić, M, and Filjar, R. (2018a). Forecasting model of space weather-driven GNSS positioning performance. Lambert Academic Publishing. Riga, Latvia.

Filić, M, Filjar, R. (2018b). Smartphone GNSS positioning performance improvements through utilisation of Google Location API. Proc of 41 st International Convention MIPRO/CTI, 507- 510. Opatija, Croatia. doi: 10.23919/MIPRO.2018.8400087

Filić, M, Grubišić, L, and Filjar, R. (2018). Improvement of standard GPS position estimation algorithm through utilization of Weighted Least-Square approach. *Proc of 11th Annual Baška GNSS Conference*, 7-19. Baška, Krk Island, Croatia. Available at: https://www.pfri.uniri.hr/web/hr/dokumenti/zbornici-gnss/2018-GNSS-11.pdf

Filić, M.(2017).Analysis of the position estimation procedure based on the given GNSS pseudoranges in the Software-Defined Radio satellite navigation receiver (Msc thesis, in Croatian). University of Zagreb, Faculty of Science, Dept for Mathematics. Zagreb, Croatia. Available at: https://bit.ly/2DlX9O6

Gallier, J, and Quaintance, J. (2018). Fundamentals of Linear Algebra and Optimization. Dept of Computer and Information Science, University of Pennsylvania. Philadelphia, PA. Avaialble at: https://www.seas.upenn.edu/~cis515/linalg.pdf

Gustafsson, F. (2010). Statistical Sensor Fusion. Studentlitteratur. Linkoepping, Sweden.

Humphreys, T et al. (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. *Proc of ION GNSS 2008*, 3584-3590. Savannah, GA.

Jafarnija-Jahromi, A et al. (2012). GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Int J of Nav and Obs*, 2012, Article ID 127072, 16 pages. doi:10.1155/2012/127072

Kerns, A J, Shepard, D P, Bhatti, J A, and Humphreys, T E. (2014a). Unmanned Aircraft Capture and Control via GPS Spoofing. *J of Field Robotics*, July/Augist 2014, 617-636. doi: 10.1002/rob.21513

Kerns, A J, Wesson, K D, and Humphreys, T E. (2014b). A Blueprint for Civil GPS Navigation Message Authentication. *Proc of IEEE/ION PLANS 2014* (8 pages). Monterey, CA.

Kuhn, M G. (2010). Signal Authentication in Trusted Satellite Navigation Receivers. Chapter in: Sadegi, A-R, and Naccache, D (eds). (2010). Towards Hardware-Intrinsic Security: Foundations and Practice. Springer Verlag. New York, NY.

Landau, G M, and Vishkin, U. (1988). Fast String Matching with k Differences. J Comp and Syst Sci, 37, 63-78.

Levenshtein, V I. (1966). Binary Codes Capable of Correcting Deletions, Insertions, and Reversals (translated from Russian version). Cybernetics and Control Theory, 10(8), 707-710.

Mitola, J. (1995). The Software Radio Architecture. *IEEE Comm Mag*, May 1995, 26-38.

Navarro, G. (2001). A Guided Tour To Approximate String Matching. *ACM Comp Surveys*, 33(1), 31-88.

Nighswander, T et al. (2012). GPS Software Attacks. *Proc of CCS 2012 Conference*. Raleigh, NC.

O'Driscoll, C. (2018). What is navigation message authentication? *Inside GNSS*, Jan/Feb 2018, 26-31. Available at: https://bit.ly/2SEM6UC

Pecora, M et al. (1997). Fundamentals of synchronisation in chaotic systems, concepts, and applications. *Chaos*, 7, 520-543.

Petrovski, I G, and Tsujii, T. (2012). Digital Satellite Navigation and Geophysics: A Practical Guide with GNSS Signal Simulator and Receiver Laboratory. Cambridge University Press. Cambridge, UK.

Psiaki, M L, and Humphreys, T E. (2016). GNSS Spoofing and Detection. *Proc of IEEE*, 104(6), 1258-1270.

Schenewerk, M et al. (2016). Quality Controlling RINEX Navigation Message Files. *Proc IGS Workshop: GNSS Futures*. Sydney, NSW. Available at: https://bit.ly/2RwUvIu

Stewart R W et al. (2015). Software Defined Radio using MatLab & Simulink and the RTL-SDR. Strathclyde Academia Media. Glasgow, UK.

Sun, K. (2015). Chaotic Secure Communication: Principles and Technology. Walter De Gruyter GmbH. Berlin, Germany.

Tippenhauer, N O, Poepper, C, Rasmussen, K B, and Čapkun, S. (2011). On the Requirements for Successful GPS Spoofing Attacks. *Proc of the 18th ACM conference on Computer and communications security*, 75-86. Chicago, IL.

UK Government Office for Science. (2018). Satellite-Derived Time and Position: A Study of Critical Dependencies. HM Government of the UK and NI. Available at: https://bit.ly/2E2STnd

Vaudenay, S. (2005). A Classical Introduction to Cryptography: Applications for Communications Security. Springer Verlag. New York, NY.

Wesson, K, Rothlisberger, M, and Humphreys, T. (2012). Practical Cryptographic Civil GPS Signal Authentication. *NAVIGATION: Journal of the Institute of Navigation* , 59(3), 177-193.

Wittek, P. (2014). Quantum Machine Learning: What Quantum Computing Means to Data Mining. Academic Press/Elsevier. London, UK.

Zeng, K et al. (2017). A Practical GPS Location Spoofing Attack in Road Navigation Scenario. *Proc of HotMobile 2017 Conference* (6 pages). Sonoma, CA