Receiver Independent Implementation Of The Galileo Open Service Navigation Message Authentication

Xabier Zubizarreta, Johannes Rossouw van der Merwe, Ivana Lukčin, Alexander Rügamer, Wolfgang Felber

Receiver Independent Implementation of the Galileo Open Service Navigation Message Authentication (OS-NMA)

Xabier Zubizarreta, J. Rossouw van der Merwe, Ivana Lukčin, Alexander Rügamer, Wolfgang Felber
Fraunhofer IIS, Germany
Email: xabier.zubizarreta@iis.fraunhofer.de

BIOGRAPHIES

Xabier Zubizarreta is currently a researcher at the Fraunhofer IIS in Nuremberg, Germany. He earned his Master of Science on Communication Engineering at the University of Erlangen-Nuremberg with a work on the assessment of the Open Service Navigation Message Authentication (OS-NMA). His research interests include the design of robust GNSS receivers and the analysis, characterization and mitigation of GNSS interference and spoofing.

J. Rossouw van der Merwe received his M.Eng. Masters degree in Engineering at the University of Pretoria, South Africa, in 2016. He joined the Fraunhofer IIS in 2016, where his main research is in signal processing methods for interference mitigation and array processing applications.

Ivana Lukčin received her MSc. degree in Mathematics from the University of Zagreb, Croatia, in 2012. Since then, she has been working at the Fraunhofer Institute for Integrated Circuits IIS in the field of compressed sensing and snapshot positioning.

Alexander Rügamer received his Dipl.-Ing. (FH) degree in Electrical Engineering from the University of Applied Sciences Würzburg-Schweinfurt, Germany, in 2007. Since then he has been working at the Fraunhofer Institute for Integrated Circuits IIS in the Field of GNSS receiver development. He was promoted to Senior Engineer in February 2012. Since April 2013, he is head of a research group dealing with secure GNSS receivers and receivers for special applications. His main research interests focus on GNSS multi-band reception, integrated circuits and immunity to interference.

Wolfgang Felber received his Dipl.-Ing. degree in electrical engineering in 2002 and his doctoral degree Dr.-Ing. in 2006 from Helmut-Schmidt-University of Federal Armed Forces Hamburg, Germany. Since 2014 he is head of the Satellite-based Localization Systems department of Fraunhofer IIS in Nuremberg. The main topics in his department are energy harvesting and low power technologies, hardware development of satellite navigation receivers and sensor fusion in positioning applications.

ABSTRACT

In this paper, we present a practical implementation and evaluation of the open service navigation message authentication (OS-NMA) scheme proposed for Galileo. A file-system based solution is used to parse the results, making this implementation receiver independent. Therefore, extending to current commercial receivers to support OS-NMA, without additional receiver redesign and by using openly available and independently developed crypto libraries, is facile. With this implementation we provide some experimental results of nominal OS-NMA usage. Its advantages and disadvantages are evaluated for challenging use-cases as well as for spoofing, jamming, and signal shortage scenarios. It was concluded that the biggest constrains of OS-NMA reside on the delayed authentication. The time to first authenticated fix (TTFAF) from a cold-start of the decoder as well as the time to first alert in case of a spoofing attack will limit the application cases for OS-NMA. However, OS-NMA provides a good practical protection against most common signal forgery at low implementation cost.

1 INTRODUCTION

With the rise on location based applications, such as autonomous driving or eCall, a broader audience requires not only accurate and precise positioning solutions, but also secure and reliable ones. Recent studies [1] [2] [3] and incidents [4] [5] have shown that spoofing and jamming attacks have become commonplace and pose a considerable threat to satellite based positioning solutions. Well protected signals using spreading code encryption such as GPS P(Y), M-Code or Galileo PRS are currently deployed and in use; however, they are mostly under the control of governmental agencies and hardly available to the general public. Therefore, there is a need in the mass market for secure and spoofing-proof receivers. The European Commission (EC) proposes the use of an authentication scheme for the open service (OS) of the Galileo system [6]. This new scheme should grant means to authenticate meaningful sections of the Galileo

International Technical Symposium on Navigation and Timing (ITSNT) 2018
13-16 Nov 2018
ENAC, Toulouse, France

navigation message as well as potential proxy authentication to other satellite navigation systems. Open service navigation message authentication (OS-NMA) is planned to be in full operational capabilities by 2020 [7].

The European satellite based navigation system, Galileo, started offering Early Operational Capability (EOC) on December 2016 and it is planned to reach full operational capabilities (FOC) by 2020. The Galileo system broadcasts four navigation messages: the Freely-accessible Navigation Message (F/NAV), the Integrity Navigation Message (I/NAV), the Commercial Navigation Message (C/NAV), and the Governmental Navigation Message (G/NAV). I/NAV contains 120 reserved bits, as shown in Figure 1: where 72 are on the E5b-I signal and 48 on the E1B. Due to a redefinition of Galileo's original intended Safety-of-Life (SoL) service towards Galileo integrity via EGNOS / SBAS, a proposal was made to use 40 of the now reserved bits from E1B to implement navigation message authentication (NMA) for the open service (OS) [8]:

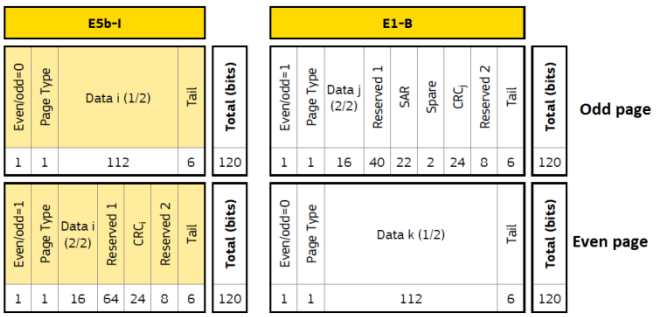

Figure 1 – Galileo I/NAV message bit structure, from [8]

Objectives of the intended authentication scheme are to retain backwards compatibility and to require minimum change to the existing infrastructure. The scheme should also support the low data-rate (125 bps) of the I/NAV and be robust enough to support occasional data-loss, as is the case for GNSS receivers in environments with reduced visibility [6].

The paper is structured as follows: In Section 2, the authentication scheme is described with the underlying cryptographic primitives. Section 3 shows the architecture of the developed demonstrator system, focusing on each of the stages. The designed system is put under test by performing several measurements of its speed, operational timing limits, and practical use-cases. These tests are carried out for nominal, limited, and spoofing test cases. The results are sketched and discussed in Section 4. Finally, in Section 5 a summary of the obtained results is shown and hints for future development are suggested.

2 OPEN-SERVICE NAVIGATION MESSAGE AUTHENTICATION (OS-NMA)

The main complexity of GNSS authentication lies on the broadcast nature of the signals. While the signal transmitted by the satellites can reach a large number of users, there is no feedback channel from the users to the satellites. Authentication can also be provided on a signal level or a navigation message level. NMA provides means to verify that the origin of the navigation message lies on a licit sender by means of signature. One of the means to authenticate messages is symmetric cryptography, i.e. cryptographic algorithms that rely on keeping a common secret key accessible only to the transmitter and receiver intended to partake in the communication exchange. This approach requires a careful custody of the key used. Asymmetric cryptography provides an alternative in which a pair of keys is used. A key is kept secret by one of the parties while the other one is made public. The receiver possessing the public key can decode any message that was encrypted using the secret key, and this way authenticate that the messages originates on the correct party.

2.1 Timed Efficient Stream Loss-tolerant Authentication (TESLA)

The Timed Efficient Stream Loss-tolerant Authentication (TESLA) was originally designed to provide authentication for multimedia broadcast applications [9]. This environment is analogous to the multicast (one-to-many) nature of GNSS. It is based on a hybrid symmetric/asymmetric cryptography solution to sign the data to authenticate.

TESLA has a low computational complexity and can authenticate a high downstream data throughput with minimum up-stream transmission by means of delayed disclosure of keys. First, a Message Authentication Code (MAC) is generated to authenticate the plaintext message (M_i). The MACs are generated using a key (K_i). MACs are transmitted first, followed by the key (K_i). This key is extracted from a key-chain, which is generated by applying a one-way hashing function (H) subsequently starting from a seed key (K_N). This transmission and generation sequence is shown in Figure 2.

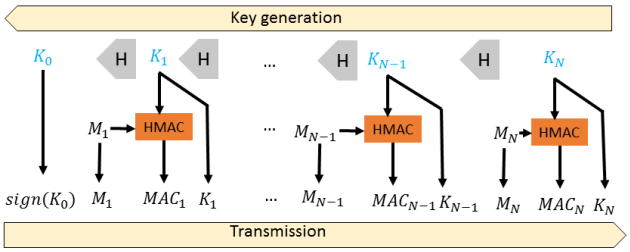

Figure 2 – Key-chain and message coding used in TESLA

The keys are disclosed only after the plaintext message they encrypt and the produced MAC are transmitted. Further, the keys are disclosed in the reverse order of the generation. This way, messages can neither be verified before their corresponding key is received, nor rogue MACs generated. Future keys can also not be derived from previous ones [10].

The first disclosed key is called the root-key (K_0) and through its signature ($sign(K_0)$) it allows to authenticate all subsequent keys. This signature, as it needs to be verified only once, can be performed by means of

computationally more expensive asymmetric cryptography. Asymmetric cryptography relies on the usage of a pair of keys from which one of the keys is used to produce the signature (private-key) and the other one is used to authenticate it (public-key). This way, any user knowing the public-key will be able to trust a given message, as only a licit sender possessing the private-key will be able to produce an authenticable signature. Elliptic Curve Digital Signature Algorithm (ECDSA) is a suggested asymmetric method for OS-NMA. The signature produced by this algorithm is roughly twice the size of the public-key required to authenticate it.

2.2 OS-NMA Field

Together with the MACs, several other parameters and values need to be transmitted in order to use TESLA for Galileo navigation message authentication. The overview of an OS-NMA subframe is shown in Figure 3.

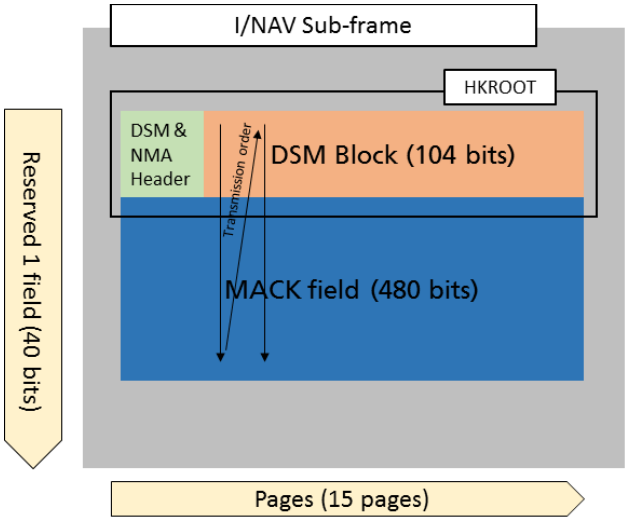

Figure 3 – OS-NMA subframe structure

Each subframe has 600 available bits (40 bits from the reserved field times 15 odd pages per subframe) which are split in two main sections: The Header and Root-key (HKROOT) section and the MAC and key (MACK) section.

The HKROOT section contains all system parameters (current operational status, length of the keys, length of the MACs, the hashing algorithms used to produce them, and root-key identification parameters), the root-key, and the signature of the root-key, known as Digital Signature Message (DSM). The first 8 bits of the 40 bits are allocated to OS-NMA.

The HKROOT section is split over several I/NAV subframes, as one DSM Block is insufficient to accommodate the root-key together with the signature.

The MACK section contains the most meaningful bits to perform the authentication: the MAC tags and the keys. The amount of MACs per section depends on the length of the MACs themselves and the length of the keys. This section occupies the remaining 32 bits of the field [11].

3 SYSTEM DESCRIPTION

In order to evaluate the operation of OS-NMA under controlled laboratory conditions, experimental and commercial receivers were selected. As OS-NMA processing takes place on the latest stages of message decoding, a receiver independent solution was chosen. Additionally, since no OS-NMA signal is currently broadcast by the Galileo satellites, a message generator was developed based on the openly available latest version of the OS-NMA ICD.

The OS-NMA demonstrator consists of three main parts: a software module responsible for key generation, message generation, and message parsing; a signal generator; and a receiver.

3.1 Software module

The OS-NMA based authentication is performed during the last stages of navigation message decoding. Therefore, it can be completely detached from the receiver itself. To achieve this purpose a file-system based approach was selected. This way, only a basic interface needs to be developed to read the raw navigation message bits from the receiver and write them with the correct format in a file. Additionally, by using a network based interface, remote authentication can be performed. Finally, the parser scans continuously for changes on the file-system and reacts accordingly in case that a meaningful amount of information is received. Figure 4 shows said folder structure, as well as the content of each subframe data.

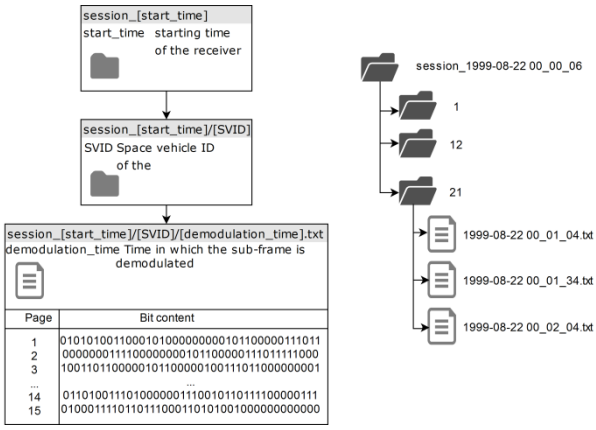

Figure 4 – Folder structure of the producer-consumer file-system

In addition to allowing receiver independent operation this architecture provides seamless logging and storage capabilities. Moreover, as there are currently no testing signals available to replicate an OS-NMA containing Galileo system, a message generator is developed together with the parser. The generated OS-NMA message is then preloaded in the signal generator.

3.2 Signal generator

A Spirent GSS9000 GNSS simulator is used to produce the signal broadcast from the Galileo satellites. The settings of the simulator, as well as the triggering of its start and stop, can be controlled remotely through a

TCP/IP link in real time or by uploading pre-generated user command files. This control link allows setting up each individual bit of the navigation message for all the systems. Therefore, the required bits for OS-NMA can be set accordingly to contain the pre-computed values.

3.3 Receiver

As all the processing of OS-NMA takes place on a navigation message level, the authentication scheme can be implemented in virtually any current Galileo E1B compatible GNSS receiver which provides access to the raw I/NAV navigation message bits. Table 1 shows some of the receivers that are used to check the implementation:

Manufacturer	Receiver	Raw bits
Septentrio	PolaRx5	Accessible as GalRawINAV
u-blox	M8T	Accessible in UBX-RXM-SFRBX
Fraunhofer IIS	GOOSE [12]	Custom direct write to file

Table 1 – Table summarizing receivers compatible with the suggested approach

Not only high-end or specialized receivers offer access to the raw navigation message bits; but, since the application programming interface (API) version 24 from Android, GNSS raw measurements are also provided by this mobile-phone operating system. Raw navigation message bits are among the values returned by the API. As a matter of fact, there are already some phone manufacturers supporting the Galileo signal and raw measurement output, opening the door to a plethora of new applications profiting from NMA [13].

4 MEASUREMENTS

First of all, the correct operation of the receiver was evaluated by using the end-to-end demonstrator under a nominal scenario, that is, a scenario under commonly found conditions. A general overview of the system's operation time was obtained at this stage. The Time to the First Authenticated Fix (TTFAF) was measured and evaluated for several parameter combinations. The authentication data throughput, i.e. the amount of navigation bits that could be authenticated through the scheme, was also evaluated. Next, analysis was performed to check the resilience of the authentication scheme in case of data-loss.

Finally, the main functionality of OS-NMA was put under test, namely the possibility to avoid data forgery based spoofing attacks. For that purpose the licit self-generated OS-NMA signal was spoofed using a forged licit-looking Galileo E1B signal. The mismatch of the public-key, resulted in the authentication scheme to serve its purpose to identify the rogue signal. The receiver alerted with a minimum delay about the ongoing attack.

4.1 Nominal use-cases

A nominal scenario lasting 3 minutes and with clear sky view was used. The OS-NMA signal was transmitted only by a single satellite (SVID = 3) authenticating its own navigation message. The OS-NMA bits were pre-calculated and pre-loaded into the signal generator. The receiver was directly connected to the RF output of the signal generator.

The TTFAF limits the end-user applications of the authentication scheme. While for the case of freight tracking it could be permissible to obtain an authenticated position fix after a long delay, and at a reduced rate, in the case of the automotive industry, more precisely for autonomous driving applications, authentication delay may play a vital role.

In the OS-NMA scheme the receiver must undergo three steps until the navigation data bits are authenticated. Figure 5 summarizes these steps as a time-sequence.

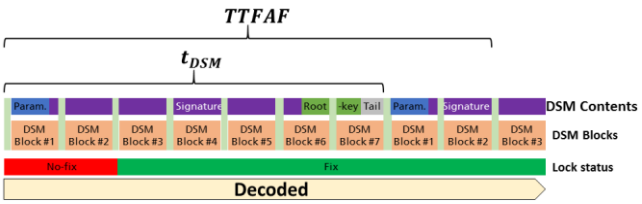

Figure 5 – TTFAF time-sequence. KS = 80 bits; Signature size = 512 bits

First, the receiver must obtain the public key corresponding to the root-key which is currently in use. Although the Interface Control Document (ICD) of the OS-NMA considers Over-the-air (OTA) transmissions of the public-key, it is not yet defined on the current issue of the ICD. Another option would be pre-programming the receivers with the required public keys or providing said keys through third-party channels such as internet, cellular network, or broadcast radio. Next, the receiver must fully receive the DSM message, which extends through several 30 second subframes depending on the signature and key lengths chosen. Finally, the receiver can start processing the MACs.

In order to analyze the lower and upper boundaries of the TTFAF, and the authenticated data-volume, it was iterated through several system parameters. The TTFAF mostly depends on the key-size and the signature size.

The fastest TTFAF occurs for the combination of the shortest possible key-size (80 bits) and the shortest possible signature size (448 bits, rendered by using the P-224 curve for the ECDSA signature). It takes 6 subframes for the complete reception of the parameters, root-key, and its signature for this combination. Therefore, the first navigation data bits can be first authenticated after 180 seconds. Figure 6 shows the evolution of the authentication process versus time.

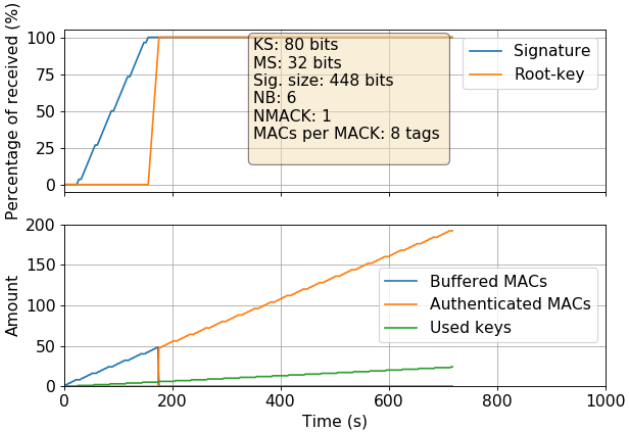

Figure 6 – Time-sequence of signature, root-key, and MAC reception for the fastest possible TTFAF.

The slowest possible authentication occurs for the selection of the longest possible key (256 bits, un-truncated SHA-256 hash) together with the longest possible signature (1042 bits, produced from using the P-521 curve with the ECDSA). In this case, 14 sub-frames are necessary to fully receive the necessary fields which correspond to 420 seconds. Figure 7 shows the time-sequence of the slowest TTFAF.

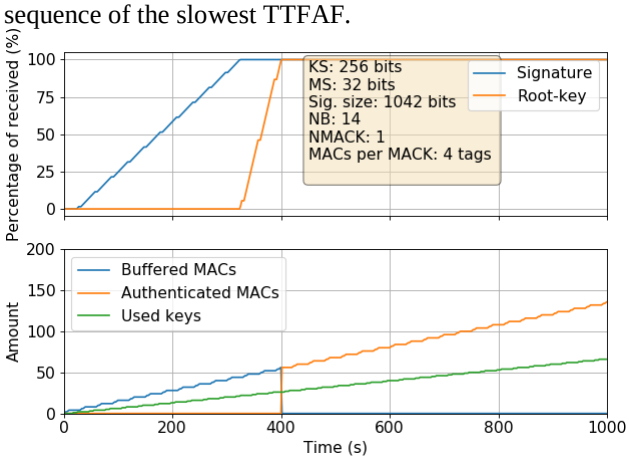

Figure 7 – Time-sequence of signature, root-key, and MAC reception for the slowest possible TTFAF.

The authentication data size is an important factor. There is a trade-off between the key-lengths and MAC lengths and the security level they provide. While short lengths permit to fit more MAC tags in each subframe, and consequently can authenticate more data, they reduce the cryptographic robustness of the system.

4.2 Data-loss resilience

One of the requirements for a GNSS authentication scheme is the ability to still function properly in challenging environments. Bits of the navigation message can be lost due to signal shadowing or interference. Although the low bit-rate of the navigation message transmission together with the used Forward Error Correction (FEC) may compensate any short-time signal-loss events, longer signal-loss time may impair the correct operation of OS-NMA.

As far as data-loss is concerned, two main stages can be distinguished on the functioning of OS-NMA. On a first stage in which the receiver is unaware of any of the system parameters and values of the authentication scheme, every single bit carries meaningful and required information. However, once the root-key, system parameters, and the verifying signature are received the whole HKROOT section is dispensable, at least until a new key-chain with a different root-key is introduced. This makes only 80% of the OS-NMA field susceptible to disruption.

Not only is data-loss more critical on different operational stages, but also on different parts of the messages. While MACs missing a few arbitrary bits can still be authenticated, provided that the key is received and the loss on security due to incomplete MACs is permissible, missing parts of the root-key signature voids the signature fully and requires to receive the missing bits again. ECDSA requires the complete error-less signature, and it is not compatible with any type of truncation. Moreover, ECDSA produces unique, non-deterministic, signatures which do not permit to amend lost chunks of a signature with bits received on the future.

4.3 Spoofing resilience

The main purpose of the OS-NMA is to provide protection against data spoofing attacks. Spoofing attacks comprise a wide range depending on the complexity of implementation as well as the damage they may cause. By being able to authenticate the contents of the navigation message, protection against signal forgery is provided by OS-NMA. The key-chain has the benefit that the contents of the OS-NMA field cannot be pre-computed in advance by an attacker [14]

A spoofing attack was carried out by jamming the receiver and forcing reacquisition on a forged signal as shown in Figure 8 [15]. An attacker would be unable to re-generate future values of the OS-NMA field, therefore the transmitted data is invalid but licit looking. The receiver still did not fully receive the authentic HKROOT field when the jamming occurred. Therefore, it needed to re-start the HKROOT decoding process from the beginning, reading the forged root-key, and signature. Provided that the receiver contains a valid and licit public-key, the alert first comes up at the verification of the root-key's signature. The length of the root-key and the signature ultimately determine this maximum time to first alert. This time coincides with the lower and upper time boundaries of the TTFAF.

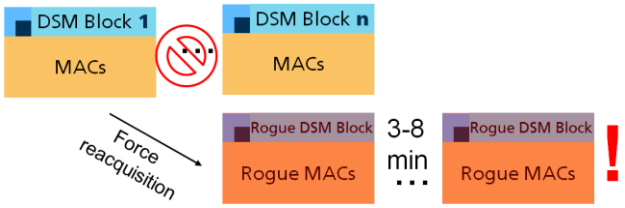

Figure 8 – Schematic representation of a jam and spoof attack.

OS-NMA does not provide protection against attacks based on signal recording and rebroadcasting. These

replay attacks usually have some time delay caused be the rebroadcasting of the signal and the travel time between the attacker and the receiver. If a licit signal is re-transmitted at a later time, its contents, including the OS-NMA field will appear to be valid. Therefore, for the OS-NMA scheme to function properly a reliable external time reference is required. The receiver must know the time within an accuracy of at least 2 seconds, which corresponds to knowing which page is currently being received, and thus, also regenerate the key-chain adequately. Receivers that rely solely on the time provided by GNSS are susceptible to signal replay attacks.

5 CONCLUSIONS AND FUTURE WORK

With the growth of new GNSS based applications the need of increased security proved to be necessary. By introducing OS-NMA on the navigation message, Galileo will be the first GNSS containing an in-built cryptographic authentication mechanism intended for the use of the general public. The scheme has a minimum development overhead and could be implemented in most receivers by only updating their firmware.

Additionally, spoofing attacks relying on signal forgery could be successfully detected. With a minimal technical overhead, the least complex way to carry out attacks could be rendered ineffective. As far as more complex threats are concerned, more reliable and instant authentication mechanisms, such as the spreading code encryption e.g. provided by the Public Regulated Service (PRS) or also intended for the Commercial Service authentication have to be utilized but with further introduced complexity.

Issues such as public-key dissemination and storage, time-synchronization, and inter-system compatibility, still need to be addressed and further defined on new issues of the OS-NMA ICD. When the OS-NMA test transmission commences, the assumptions and conclusions of this exemplary implementation can be tested and validated by future research.

ACKNOWLEDGMENTS

The work for this paper has been conducted under the PRoPART project, which has received funding from the European GNSS Agency under the European Union's Horizon 2020 research and innovation program under grant agreement No 776307.

REFERENCES

[1] E. P. Marcos, S. Caizzone, A. Konovaltsev, M. Cuntz, W. Elmarissi, K. Yinusa and M. Meurer, Interference Awareness and Characterization for GNSS Maritime Applications, Proceedings of IEEE/ION PLANS 2018, 2018.

[2] A. Rügamer, D. Meister, J. R. van der Merwe, C. Otto, M. Stahl and W. Felber, A Versatile and Configurable GNSS Interference Detection and Characterization Station, Proceedings of the ION Pacific PNT Meeting, 2017.

[3] C. Günther, A Survey of Spoofing and Counter-Measures, Journal of the Institute of Navigation 61, 2014.

[4] USA Today, "Mysterious GPS glitch telling ships they're parked at airport may be anti-drone measure," 2017. [Online]. Available: https://eu.usatoday.com/story/tech/news/2017/09/26/gps-spoofing-makes-ships-russian-waters-think-theyre-land/703476001/.

[5] Reuters, "Cyber threats prompt return of radio for ship navigation," 2017. [Online]. Available: https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT.

[6] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez and J. D. Calle, A Navigation Message Authentication Proposal for the Galileo Open Service, Journal of the Institute of Navigation, 2016.

[7] Global Navigation Satellite Systems Agency (GSA), "A new generation of OS-NMA user terminals," 9 04 2018. [Online]. Available: https://www.gsa.europa.eu/newsroom/news/new-generation-os-nma-user-terminals.

[8] European Union, European GNSS (Galileo) open Service Signal-in-Space interface control document issue 1.3., 2016.

[9] A. Perrig, D. Song, R. Canetti, J. D. Tygar and B. Briscoe, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction," The Internet Society, 2005.

[10] G. Caparra, Evaluating the Security of One-way Key Chains in TESLA based GNSS Navigation Message Authentication Schemes, Barcelona (ICL-GNSS), 2016.

[11] European Union Satellite Navigation Programmes, OS-NMA Interface Control Document v1.0, 2016.

[12] M. Overbeck, F. Garzia, A. Popugaev, O. Kurz, F. Förster, W. Felber, A. Sicramaz Ayaz, S. Ko and B. Eissfeller, "GOOSE – GNSS Receiver with an Open Software Interface," Proceedings ION GNSS, 2015.

[13] Android, "Raw GNSS Measurements," 2018. [Online]. Available: https://developer.android.com/guide/topics/sensors/gnss.

[14] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, Assesing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, Proceedings of ION GNSS 2008, 2008.

[15] N. O. Tippenhauer and C. Pöpper, On the Requirements for Successful GPS Spoofing Attacks., Proceedings of the 18th ACM conference on Computer and communications security, 2000.

[16] G. Caparra, Navigation Message Authentication Schemes, Inside GNSS, 2016.