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

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

I. Extended abstract

With the increased 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 and incidents have shown that spoofing and jamming have become more commonplace and start to pose a considerable threat for satellite based positioning solutions. Although protected signals are currently deployed and in use, they are mostly under the control of governmental agencies. Recently, the European Commission (EC) has suggested to provide authentication for the open service (OS) of the Galileo system.

In this paper, we present a practical implementation and evaluation of this open service navigation message authentication (OS-NMA) currently planned to be realized within the Galileo OS E1B signal [1]. 40 bits of the odd pages from the integrity navigation message (I/NAV) message are repurposed to provide a signature based authentication for the Galileo satellite navigation system as well as potential proxy authentication to other satellite navigation system [2]. A hybrid symmetric/asymmetric cryptography based solution named Time-Efficient Stream Loss Tolerant Authentication (TESLA) will provide delayed signatures for meaningful chunks of the navigation message [3]. OS-NMA is planned to reach the testing stage in late 2018 and be in full operation capability starting from 2020 [4]. As part of the implementation, a Spirent GSS9000 simulator is extended to stream pre-calculated OS-NMA message contents. The simulator broadcasts the Galileo E1 signal into a variety of Galileo E1 OS receivers that are able to provide the raw I/NAV bits. Septentrio's PolaRx5 receiver and Fraunhofer IIS's own GNSS Receiver with Open Software Interface (GOOSE) [5] were chosen as exemplary off-the-shelf available receivers. Afterwards, the received OS-NMA contents are stored and parsed externally in real-time on a first-in-first-out basis. This approach keeps the OS-NMA implementation receiver independent and could virtually be implemented in any receiver which provides the raw bits of the navigation message. For both the pre-calculation as well as for the authentication of the OS-NMA, readily available Python crypto-libraries are used.

To the authors knowledge, this is one of the first multi-receiver, independent (meaning outside an EC or European Space Agency (ESA) contract), open-source, real-time, OS-NMA testbed implementations relying purely on the information provided by the first revision of the OS-NMA interface control document (ICD). It proves the feasibility of the underlying idea and proves the maturity of this specification. It also shows the ease of extending current commercial receivers to support OS-NMA without additional receiver redesign and by using openly available and independently developed crypto libraries.

Having presented the testbed with its functionality, the paper provides some first experimental results about using OS-NMA to assess its benefits for nominal use cases as well as under spoofing, jamming, and signal shortage scenarios. Potential weaknesses and constraints of OS-NMA are put under scope, emphasizing the time to first authenticated fix (TTFAF) and the time to first alert i.e. the time an OS-NMA enabled receiver takes to notice an on-going navigation message counterfeiting. These two time measurements will mostly limit the potential use-cases for OS-NMA. The paper also discusses implementation related concerns such as processing overhead, design complexity, and memory limitations. It was found that due to the delayed nature of the authentication provided by OS-NMA real-time use-cases cannot be contemplated and must still rely on a signal level security scheme. Furthermore, OS-NMA does not offer additional protection to more advanced spoofing techniques such as meaconing or security code estimation and replay (SCER) as shown in [6]. Therefore, users of safety critical services should still require more robust, secure, and reliable signals e.g. using spreading code encryption like the public regulated or the commercial authentication service of Galileo. Additional extended schemes have already been suggested to fix the potential weaknesses of OS-NMA [7]. Nevertheless, OS-NMA offers an elegant and easy to implement cross-system security solution. With an acceptable

complexity and reasonable overhead, it succeeds to provide basic anti-spoofing protection to a large user segment and reduces vastly the current spoofing threat.

REFERENCES

[1] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle, "A navigation message authentication proposal for the galileo open service," *Navigation: Journal of the Institute of Navigation*, vol. 63, no. 1, pp. 85–102, 2016.

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

[3] A. Perrig, D. Song, R. Canetti, J. Tygar, and B. Briscoe, "Timed efficient stream loss-tolerant authentication (tesla): Multicast source authentication transform introduction," Tech. Rep., 2005.

[4] S. Binda, "Galileo open service navigation message," in *Netherland Insistute of Navigation: GNSS Interference and Authentication Presentation*, 2018.

[5] M. Overbeck, F. Garzia, A. Popugaev, O. Kurz, F. Forster, W. Felber, A. S. Ayaz, S. Ko, and B. Eissfeller, "Goose - gnss receiver with an open software interface," in *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2015)*, 2015.

[6] D. Maier, K. Frankl, R. Blum, B. Eissfeller, and T. Pany, "Preliminary assessment on the vulnerability of nma-based galileo signals for a special class of record & replay spoofing attacks," in *IEEE/ION PLANS 2018*, 2018.

[7] B. Motella, D. Margaria, and M. Paonni, "Snap: An authentication concept for the galileo open service," in *IEEE/ION PLANS*, 2018.