Authentication of Galileo GNSS Signal by Superimposed Signature with Artificial Noise

Francesco Formaggio, Stefano Tomasin, Gianluca Caparra, Silvia Ceccato, Nicola Laurenti

Department of Information Engineering
University of Padova
Padova, Italy
E-mail: {formaggiof, tomasin, caparrag, ceccatos, nil}@dei.unipd.it

***Abstract*—Global navigation satellite systems (GNSS) are widely used in many civil applications to get information on position, velocity and timing (PVT). However, current systems (such as global positioning system (GPS) and Galileo) do not include any feature to authenticate the received signal, therefore leaving open the possibility from an attacker to spoof the GNSS signal and induce a wrong PVT computation at the receiver. In this paper we propose a solution based on the superposition of an authentication message (signature) and artificial noise (AN) on top of the existing navigation signal. Both the authentication message and AN are unpredictable and therefore can not be arbitrarily generated by an attacker. After transmission, through an external public authenticated but asynchronous (thus not useful for PVT) channel, both the authentication message and the AN are revealed, allowing the receiver to check if they were present along the previously received navigation signal. We consider the hypothesis testing problem at the legitimate receiver to decide the authenticity of the message, and we analyze its performance under two attacks: a generation attack in which the attacker does not generate the authentication signal and a replay attack in which a legitimate (including authentication message) signal is replayed by the attacker with a suitable delay in order to induce the desired PVT at the victim. The receiver operating characteristic (ROC) curve is obtained for the hypothesis testing problem under the two attacks.**

***Index Terms*—Global Navigation Satellite Systems (GNSS), Anti-Spoofing, Artificial Noise**

I. Introduction

Global Navigation Satellite Systems (GNSS) provide affordable and ubiquitous position, velocity and timing (PVT) service. The adoption of GNSS continuously grown over the years, entering in many sectors, form transportation to finance, from the synchronization of the mobile networks, to navigation in space. With the increase of the dependency on GNSS, the interest on security and authentication has increased too.

While GNSS signals reserved to military applications have built-in features such as access control that make them more resilient to spoofing attacks, signals dedicated to civilian use do not currently offer any security feature. Usually, the access control is implemented by the means of spreading code encryption, and the secure distribution of the secret key only to the authorized users. Several proposals of protecting the civilian signals using a similar approach are available in the literature [1]–[3].

In [4] instead, the introduction of an additional signal component devoted to security that exploits artificial noise was proposed. The authentication of the navigation signal is achieved at the cost of spending power to transmit the additional signal component. In this paper we further investigate the robustness to spoofing attacks taking into account also the channel gain and the channel estimation noise. In particular we consider two attacks: a generation attack in which the attacker does not generate the authentication signal and a replay attack in which a legitimate (including authentication message) signal is replayed by the attacker with a suitable delay in order to induce the desired PVT at the victim. We consider the hypothesis testing problem at the legitimate receiver to decide the authenticity of the message. The receiver operating characteristic (ROC) is then obtained. As an example, the additional component is described in the context of Galileo E1 Open Service [5], but can trivially be applied to any other GNSS signal.

The paper is organized as follows: in Section II we present the system model while the attack model is described in Section III. In Section IV we derive the analysis for the hypothesis testing of which numerical results are presented in Section V before drawing conclusions in Section VI.

II. System Model

Fig. 1 shows our reference scenario. A satellite (Alice) offers positioning services via a broadcast transmission to both the legitimate receiver (Bob) and the spoofer (Eve). The ground segment communicates with Bob through an *authenticated* channel, i.e., messages received by Bob over this channel come for sure from the ground segment (rather than from Eve). This channel can be either a terrestrial communication link or a signal component broadcast by the satellite. The information carried by the authenticated channel is available to all users including Eve.

Our model comprises three channels: the authentic navigation channel from the satellite, the authenticated data channel and the attack channel from Eve.

A. Navigation and Attack Channel

The navigation channel connects the satellite to users and is the means through which the legitimate signal $s_L(t)$ transmitted

ISBN 978-90-827970-1-5 © EURASIP 2018

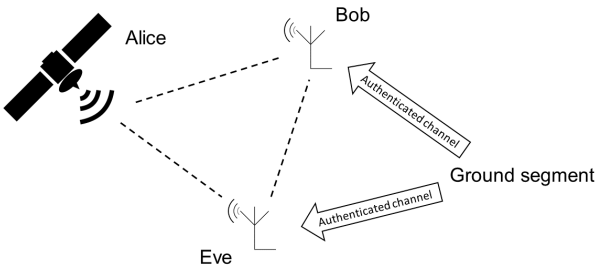

Figure 1. Reference scenario.

by Alice propagates. As from Fig. 1, we have two navigation channels: one from Alice to Eve, and the other from Alice to Bob. The attack channel connects Eve to Bob and carries the spoofing signal $s_E(t)$.

The Galileo Open Service (OS) signal is composed of two signal components: one modulated by the navigation message (the data component $\mathrm{E1}_B$), and one dataless (the pilot component $\mathrm{E1}_C$). The two components are transmitted in code division multiple access (CDMA) using different pseudo-random spread-spectrum sequences called *ranging codes*. Since the structure of the two components is identical, here we consider only $\mathrm{E1}_B$. The signal carries the unitary power binary data stream d_i that represents the navigation data for $\mathrm{E1}_B$ with symbol period T_s. The navigation signal can be written as:

$$s_N(t) = \sum_i d_i s_p(t - iT_s), \tag{1}$$

where

$$s_p(t) \triangleq \sum_{i=0}^{N_c-1} c_i u(t - iT_c) \tag{2}$$

is the spreading pulse with chip period $T_c = T_s/N_c$, spreading sequence $c_i = \pm\left(1/\sqrt{N_c}\right)$ $i = 0, \ldots, N_c - 1$ and unitary-energy chip pulse $u(t)$. Therefore, $S_N(t)$ has unitary power. In Galileo OS the chip pulse is a sequence of signed rectangular functions with finite support T_c [5].

B. Authenticated Channel

We assume that the ground segment can communicate with all the users through an authenticated data channel. The authenticated channel is assumed to be of large (infinite) bandwidth and can be for example an Internet connection. We suppose the authentication to be ensured by higher layer authentication protocols. We assume Eve has no control over the information travelling on the authenticated channel and, thus, she can not modify it. This channel is envisioned as a data channel and it is not used directly for ranging purposes.

C. Authentication Process

The considered authentication procedure works as follows. We superimpose a synchronous authentication signal $s_A(t)$ to the ranging signal $s_N(t)$ at the transmitter so that the transmitted signal is

$$\begin{aligned} s_L(t) &= s_N(t) + s_A(t) \\ s_A(t) &= x(t) + w^*(t), \end{aligned} \tag{3}$$

where $w^*(t)$ is the artificial noise (AN) component and $x(t)$ is a the authentication signal that has the same structure of (1) although with a different spreading sequence $s_{p_A}(t)$. $x(t)$ modulates a binary authentication message of length L that in vector notation we denote as $\mathbf{x}$. Both $x(t)$ and $w^*(t)$ are designed to be orthogonal to $s_N(t)$ so that the receiver can process navigation signal and authentication component separately. $x(t)$ and $w^*(t)$ are also unpredictable, i.e., random generated, however they are revealed to Bob through the authentication channel *after* the transmission of $s_L(t)$. Specifically they are revealed at the symbol level, i.e., $\mathbf{x}$ and $\mathbf{w}^*$, where the entries of $\mathbf{w}^*$ are the projections of $w^*(t)$ into $s_{p_A}(t)$. Bob then subtracts the AN samples and checks the correspondence of the received message with the revealed vector $\mathbf{x}$.

The theoretical analysis carried out in [4] uses concepts of confidential message transmission in physical layer security [6] to design the signaling and analyze its performance. Here instead we follow the hypothesis testing approach, as explained in Section IV.

D. Channel Model

In this work we consider a flat one-tap channel with additive white Gaussian noise (AWGN). Under these assumptions the legitimate signal received by Bob is

$$r_B(t) = g_{AB}(t) s_L(t) + w_B(t), \tag{4}$$

where $w_B(t)$ is a Gaussian process with zero mean and spectral density $N_0^{(B)}$; $g_{AB}(t)$ is the Alice-Bob channel gain. Similarly, Eve receives

$$r_E(t) = g_{AE}(t) s_L(t) + w_E(t), \tag{5}$$

where $w_E(t)$ is a Gaussian process with zero mean and spectral density $N_0^{(E)}$ and $g_{AE}(t)$ is the Alice-Eve channel gain.

III. Attack Model

In the navigation systems, the relevant information extracted by the receiver is the propagation delays estimated by the ranging process. The aim of Eve is to transmit a spoofing signal $s_E(t)$ that leads Bob to estimate the wrong distance from the satellite.

In absence of the authentication signal component this attack is trivially successful when Eve transmits a replica of $s_N(t)$, i.e., $s_E(t) = s_N(t - \tau)$. This is feasible because all the information, such as the spreading code and the navigation message structure needed for generating an arbitrary signal $s_N(t)$ are publicly available. The introduction of the authentication component $s_A(t)$ instead would require that Eve generates a spoofing signal that contains also unpredictable information. This has a twofold benefit: *a*) it forces Eve to observe (at least partially [7], [8]) the transmitted signal in

ISBN 978-90-827970-1-5 © EURASIP 2018

order to reproduce the unpredictable signal component $s_A(t)$, and *b*) because Eve shall observe the signal before reproducing, she can not generate an arbitrary non-causal spoofing signal.

In the following two kinds of attacks are considered:

1) **generation attack**: Eve neglects the authentication component and broadcasts a spoofing signal containing only the navigation component. The signal transmitted by Eve is:
$$s_E(t) = s_N(t-\tau). \tag{6}$$

2) **replay attack**: Eve generates a noiseless navigation signal according to the desired range, and a delayed replica of the authentication signal obtained from $r_E(t)$ given a perfect estimate of g_{AE}. In other words, Eve receives the authenticated message and transmits a suitably delayed replica of it to induce the desired location. The attack signal in this case becomes:
$$s_E(t) = s_N(t-\tau) + s_A(t-\tau) + w_E(t). \tag{7}$$
Differently from (6) we note that the replay attack signal is affected by thermal noise $w_E(t)$. Indeed, as Eve replays a received signal it also contains noise. If this was not the case, the authentication protocol would not work as $s_E(t)$ would be exactly equal to $s_L(t)$. Given that, we test the (more realistic) scenario in which Eve's front end is not ideal.

Several other attacks against navigation signals have been presented in the literature, such as security code estimation and replica (SCER) [9] or forward estimation attacks (FEA) [10]. Given the fact that no information bit of the secret message V is known a priori, estimation attacks operating at message level, are effective only in obtaining the redundancy of introduced by the channel coding. In this work we consider that the secret message $\mathbf{x}$ is uncoded, therefore FEA attack does not apply. Indeed, coding would be useful also to Eve so we do not see this as a restrictive assumption. The SCER attack does not apply to the authentication signal proposed because, even though the attacker can leverage a matched filter for performing an estimation of $x(t)$, he cannot do the same on the AN.

Due to the property of auto-correlation of the ranging signal, if the spoofing signal is not aligned within a chip of the spreading code and close in Doppler frequency with the legitimate signal, the two signals will not interfere each other. In this work we assume that the spoofing attack aims at changing significantly the PVT computed by the victim, so we neglect the presence of the legitimate signal when an attack is being performed.

IV. Detection Statistics

Bob tests the authenticity of the received signal from the demodulated data, i.e., after the tracking loop that performs despreading. In particular, Bob tracks the navigation signal $s_N(t)$ and buffers the down-converted RF samples and the channel gain estimation $\hat{g}_B$. When the system reveals the AN samples at a later time, Bob removes them from the stored signal and performs a hypothesis testing on the resulting signal. In the following analysis bold notation denotes the column vector counterpart of all signals. Moreover, we assume perfect synchronization with the navigation signal (both when it is legitimate and fake). We assume the channel to be constant over L transmitted symbols. Bob then performs channel estimation every L samples and his estimate is affected by a zero-mean Gaussian error ε with variance σ_ε^2 so that

$$\hat{g}_B = g + \varepsilon. \tag{8}$$

A. Generation Attack

The aim of Bob is to distinguish through the authentication procedure between the two hypotheses:

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{r} = g\mathbf{x} + \mathbf{w_B} + (g - \hat{g}_B)\mathbf{w}^* \\ \mathcal{H}_1 &: \mathbf{r} = \mathbf{w_B} - \hat{g}_B\mathbf{w}^*, \end{aligned} \tag{9}$$

where $\mathbf{r}$ is the vector containing the L received symbols after the removal of the AN $\mathbf{w}^*$ and $\mathbf{w_B}$ are the i.i.d. noise samples with zero mean and variance $\sigma_{w_B}^2$. Hypothesis $\mathcal{H}_0$ corresponds to an authentic transmission, while hypothesis $\mathcal{H}_1$ corresponds to a transmission without the authentication signal. The authenticity test is performed using binary hypothesis testing by computing the log-likelihood ratio Λ between the probability distribution of $\mathbf{r}$ under both hypotheses:

$$\Lambda = \frac{p(\mathbf{r};\mathcal{H}_1)}{p(\mathbf{r};\mathcal{H}_0)}, \tag{10}$$

where $p(\cdot)$ denotes the probability density function. The decision is taken by comparing Λ with threshold γ:

$$\begin{cases} \text{decide } \mathcal{H}_1 \text{ if } \Lambda > \gamma \\ \text{decide } \mathcal{H}_0 \text{ if } \Lambda < \gamma. \end{cases} \tag{11}$$

We can now define the probability of false alarm and miss detection as

$$\begin{aligned} P_{FA} &= P[\Lambda > \gamma; \mathcal{H}_0] \\ P_{MD} &= P[\Lambda < \gamma; \mathcal{H}_1], \end{aligned} \tag{12}$$

where $P[\cdot]$ is the probability function.

In general, the distribution of Λ is not known in closed form. However, Λ is the ratio between two Gaussian pdfs. This is because $\mathbf{x}$ and $\mathbf{w}^*$ are revealed to Bob and therefore are to be considered constant values. Then, under $\mathcal{H}_0$ $\mathbf{r}$ is a Gaussian vector with pdf:

$$p(\mathbf{r};\mathcal{H}_0) \sim \mathcal{N}\left(\hat{g}_B\mathbf{x}, \mathbf{X}\sigma_\varepsilon^2 + \sigma_{w_B}^2 I\right), \tag{13}$$

where

$$\mathbf{X} = (\mathbf{x} + \mathbf{w}^*)(\mathbf{x} + \mathbf{w}^*)^T. \tag{14}$$

Similarly, under $\mathcal{H}_1$

$$p(\mathbf{r};\mathcal{H}_1) \sim \mathcal{N}\left(-\hat{g}_B\mathbf{w}^*, \sigma_{w_B}^2 I\right). \tag{15}$$

If there is no estimation error, i.e., $\varepsilon = \sigma_\varepsilon^2 = 0$, it is possible to derive a closed-form expression for the distribution of the log-likelihood ratio. Taking the logarithm of Λ and doing simple algebraic calculations, the two $||\mathbf{r}||^2$ terms cancel out leaving with a linear combination of the scalar entries in $\mathbf{r}$. Since in both $\mathcal{H}_0$ and $\mathcal{H}_1$, $\mathbf{r}$ is an uncorrelated Gaussian vector, also

ISBN 978-90-827970-1-5

$\log\Lambda$ is normally distributed, and for the two hypotheses we have:

$$\begin{aligned}\mathcal{H}_0 &: \log\Lambda \sim \mathcal{N}\left(-\mu_\Lambda, \sigma_\Lambda^2\right)\\ \mathcal{H}_1 &: \log\Lambda \sim \mathcal{N}\left(\mu_\Lambda, \sigma_\Lambda^2\right),\end{aligned} \tag{16}$$

where

$$\mu_\Lambda = \frac{\hat{g}_B^2}{2\sigma_{w_B}^2}||\mathbf{x}+\mathbf{w}^*||^2, \quad \sigma_\Lambda^2 = \frac{\hat{g}_B^2}{\sigma_{w_B}^2}||\mathbf{x}+\mathbf{w}^*||^2. \tag{17}$$

We can compute P_{MD} given a fixed P_{FA}:

$$\gamma' = Q^{-1}(P_{FA}), \quad P_{MD} = 1 - Q(\gamma''), \tag{18}$$

where γ' and γ'' are the results of the normalizations needed to use the standard Gaussian tail distribution function $Q(\cdot)$.

Note that from (17) the balancing between the power of $\mathbf{x}$ and $\mathbf{w}^*$ is not relevant, as only the norm square of the sum matters. However, the unpredictability of the AN is still needed to avoid Security Code Estimation and Replay (SCER) attacks, while the binary message $\mathbf{x}$ does not suffer from the quantization issues discussed in [4].

B. Replay Attack

In case of replay attack the two hypotheses are:

$$\begin{aligned}\mathcal{H}_0 &: \mathbf{r} = g\mathbf{x} + \mathbf{w_B} + (g-\hat{g}_B)\mathbf{w}^*\\ \mathcal{H}_1 &: \mathbf{r} = g(\mathbf{x}+\mathbf{w_E}) + \mathbf{w_B} + (g-\hat{g}_B)\mathbf{w}^*,\end{aligned} \tag{19}$$

where $\mathbf{w_E}$ is the zero-mean Gaussian noise introduced by Eve's front end.

The distribution of $\mathbf{r}$ is known in closed form only under $\mathcal{H}_0$ and it is given by (13), while $\mathcal{H}_1$ requires numerical integration by conditioning over g and applying the total probability theorem:

$$p(\mathbf{r};\mathcal{H}_1) = \int_{-\infty}^{+\infty} p(\mathbf{r}|g;\mathcal{H}_1)p(g)dg, \tag{20}$$

where from (8)

$$g \sim \mathcal{N}\left(\hat{g}_B, \sigma_\varepsilon^2\right). \tag{21}$$

Therefore in this case p_{FA} and p_{MD} can not be obtained in closed form.

For the special case $\varepsilon = \sigma_\varepsilon^2 = 0$, the distribution of $\log\Lambda$ is available in closed form also in this case. Since $g = \hat{g}_B$, $\mathbf{r}$ becomes again a Gaussian vector, the two hypotheses become

$$\begin{aligned}\mathcal{H}_0 &: \mathbf{r} \sim \mathcal{N}\left(\hat{g}_B\mathbf{x}, \sigma_{w_B}^2 I\right)\\ \mathcal{H}_1 &: \mathbf{r} \sim \mathcal{N}\left(\hat{g}_B\mathbf{x}, (\hat{g}_B^2\sigma_{w_E}^2 + \sigma_{w_B}^2)I\right).\end{aligned} \tag{22}$$

If we define $\mathbf{r}' = \mathbf{r} - \hat{g}_B\mathbf{x}$ we can apply the results in [11] and write the test statistic

$$\Lambda' = \frac{\sigma_{w_B}^2 + \hat{g}_B^2\sigma_\varepsilon^2}{2(2\sigma_{w_B}^2 + \hat{g}_B^2\sigma_\varepsilon^2)}||\mathbf{r}'||^2, \tag{23}$$

which can be derived by taking the log of (10), scaling and ignoring the non $\mathbf{r}$-dependent terms. The entries of $\mathbf{r}'$ are independent Gaussian random variables and therefore

$$\Lambda' \sim \mathcal{X}_L^2 \tag{24}$$

The same procedure of (18) can be carried out using the cumulative distribution function of the Chi-square random variable instead of $Q(\cdot)$.

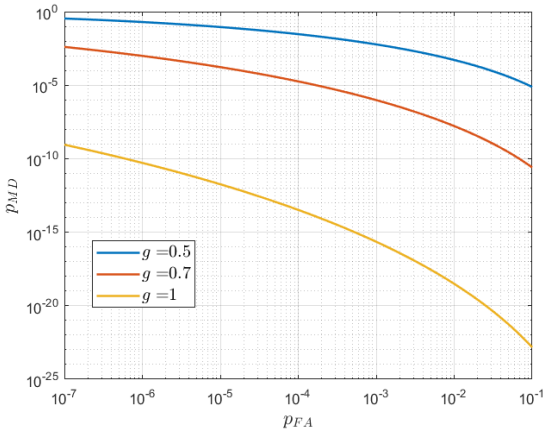

Figure 2. Generation attack with $\varepsilon = 0$. ROC for different values of the channel gain g. $\sigma_{w_B}^2 = -11$ dB, $L = 5$.

V. Numerical Results

A. Generation Attack

In Fig. 2 we show the ROC of the hypothesis testing problem under generation attack for the case $\varepsilon = 0$ following the procedure in (18). We set $\sigma_{w_B}^2 = -11$ dB, as it corresponds to 35 dB of carrier-to-noise ratio (C/N_0), a typical value for navigation systems. Moreover we set $L = 5$, which for the Galileo system corresponds to 20 ms of signal observation. Note that the defence against this type of attack is easy as Eve does not transmit any authentication component. Indeed, even with $L = 5$ we can obtain a miss detection probability of 10^{-10} for a false alarm probability of 4×10^{-7}.

Eve can still induce a lower channel estimate to Bob and as a result he will not be able to distinguish between $\mathcal{H}_0$ and $\mathcal{H}_1$, since the distributions of the two received signals become closer as g decreases. This results in worse p_{FA} and p_{MD} curves, as shown in Fig. 2. However, g can not be too low, otherwise Bob would not be able to track the signal, leaving Eve with an unsuccessful attack.

The same considerations hold for Fig. 3 showing the ROC for a scenario taking into account also the estimation noise variance σ_ε^2. In this case the noisy estimate $\hat{g}_B$ impacts on both the false alarm and miss detection performance.

B. Replay Attack

The replay attack is a powerful attack since Eve sends an exact copy (plus the noise $w_E(t)$) of the received signal, together with the authentication component. The two hypotheses are then more difficult to distinguish because, we recall, they differ only in the thermal noise $\mathbf{w_E}$.

In Fig. 4 we show the ROC using the procedure described in Section IV-B. For this scenario what matters is not the absolute value of $\sigma_{w_B}^2$, but it's ratio with $\sigma_{w_E}^2$. p_{FA} and p_{MD} are then shown as a function of the C/N_0 gap between Bob and Eve, where for a gap larger than 0 dB Eve has a physical advantage over Bob, i.e., $\sigma_{w_E}^2 < \sigma_{w_B}^2$. We see that in order to obtain an

ISBN 978-90-827970-1-5

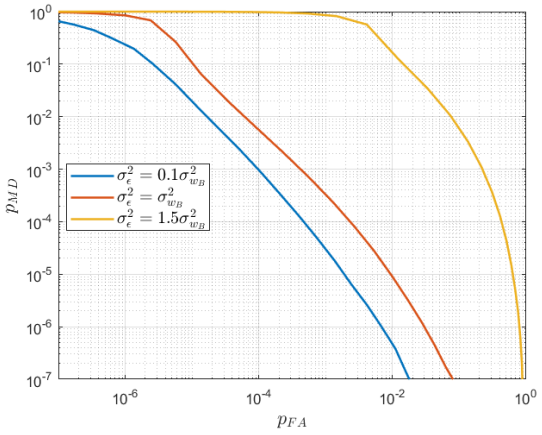

Figure 3. Generation attack with $\varepsilon \neq 0$. ROC for different values of the estimation noise variance σ_ε^2 expressed as a function of $\sigma_{w_B}^2$. $\sigma_{w_B}^2 = -6$ dB, $L = 10$.

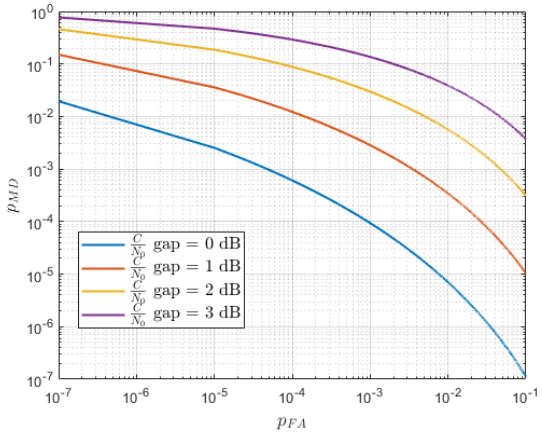

Figure 4. Replay attack for $\varepsilon = 0$. ROC for different values of C/N_0 gap between Eve and Bob. $L = 200$.

acceptable performance, either Eve has the same channel as Bob, or we need a larger L, as we show next.

Fig. 5 shows the ROC curve obtained evaluating numerically the integral in (20) to take into account also in this case the estimation noise power, which has been set to $\sigma_\varepsilon^2 = \frac{1}{10}\sigma_{w_B}^2$. We see how it is always possible to improve performance by increasing L which, however, is now at least 150 symbol long, corresponding to 600 ms. Note that defending against the generation attack is *easier* as it requires a shorter observation time.

VI. Conclusions

In this paper we provided an additional analytical analysis of the authentication protocol proposed in [4]. The analysis has been carried out using binary hypothesis testing and considering two types of spoofing attacks: a simple generation attack and a replay attack.

With respect of the original formulation of the protocol we introduced the presence of the channel gain and took into account the channel estimation error. We showed how using the authentication protocol against the generation attack requires a small amount of authentication symbols, while the replay attack is more powerful and requires the transmission of a longer authentication message.

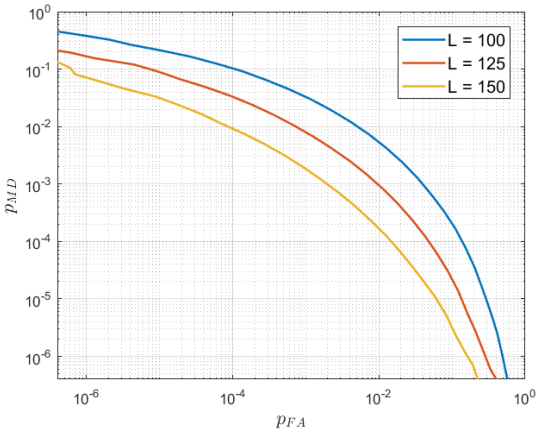

Figure 5. Replay attack for $\varepsilon \neq 0$. ROC for different values of L. $\sigma_{w_B}^2 = \sigma_{w_E}^2 = -11$ dB and $\sigma_\varepsilon^2 = \frac{1}{10}\sigma_{w_B}^2$.

References

[1] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," *Proceedings of the Institute of Navigation GPS/GNSS 2003 conference*, pp. 1543–1552, 2003.

[2] J. M. Anderson, K. L. Carroll, N. P. Devilbiss, J. T. Gillis, J. C. Hinks, B. W. O. Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, (Portland, Oregon), pp. 2388–2416, 2017.

[3] E. Gkougkas, D. Dötterböck, T. Pany, and B. Eissfeller, "A Low Power Authentication Signal for Open Service Signals," in *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, (Portland, Oregon), pp. 3865–3878, 2017.

[4] F. Formaggio and S. Tomasin, "Authentication of Satellite Navigation Signals by Wiretap Coding and Artificial Noise," *ArXiv e-prints*, Feb. 2018.

[5] European Union, "Galileo Open Service SIS ICD." 2016.

[6] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge: Cambridge University Press, 2011.

[7] G. Caparra, S. Ceccato, N. Laurenti, and J. Cramer, "Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication," in *Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*, (Portland, Oregon), pp. 3968 – 3984, 2017.

[8] G. Caparra, "On the Achievable Equivalent Security of GNSS Ranging Code Encryption," in *IEEE/ION Position, Location and Navigation Symposium (PLANS) 2018*, (Monterey, California), 2018.

[9] G. Caparra, N. Laurenti, R. T. Ioannides, and M. Crisci, "Improving Secure Code Estimation and Replay Attack and Detection on GNSS Signals," in *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, NAVITEC*, 2014.

[10] J. T. Curran and C. O'Driscoll, "Message Authentication and Channel Coding," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, (Portland, Oregon), pp. 2948 – 2959, 2016.

[11] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory*. New Jersey: Prentice-Hall Inc, 1993.

ISBN 978-90-827970-1-5 © EURASIP 2018