Preliminary Assessment on the Vulnerability of NMA-based Galileo Signals for a special class of Record & Replay Spoofing Attacks

Daniel Maier, Kathrin Frankl, Ronny Blum, Bernd Eissfeller, Thomas Pany
Institute of Space Technology and Space Applications
Universität der Bundeswehr München
Neubiberg, Deutschland

***Abstract*—The authentication of GNSS signals becomes more and more important in recent years. The Navigation Message Authentication (NMA) is one approach to provide authentication of the GNSS data level. In this work, the capability and vulnerability of NMA-authenticated Galileo E1B INAV signals are evaluated. To this end, different case studies emulating spoofing attacks are investigated. The results of these tests provide a first assessment on the capability and vulnerability of NMA-authenticated Galileo signals.**

Keywords—Navigation message authentication; Galileo signal transceiver; spoofing attacks

I. Introduction

In the last few years, the authentication of GNSS signals has increased in importance. The Navigation Message Authentication (NMA) is one promising approach discussed for the authentication of GNSS signals [1],[2],[3]. For the Galileo Open Service, several performance studies of the NMA have been carried out, see, e.g., [4],[5].

One main spoofing attack for NMA-based GNSS signals is the recording of the GNSS signals and their (time-delayed) replay. Also, the pre-estimation of signal symbols by the spoofer, before the (modified) signal is emitted, is conceivable. The objective of this work is to evaluate the vulnerability of NMA-based GNSS signals with respect to such spoofing attacks. On this way, the spoofing attacks are emulated by a wide applicable demonstrator. It consists of GNSS signal generators, GNSS signal receivers and NMA authentication tools Sisitau (SIgnal SImulation Tool for AUthentication). All these components can be plugged together in flexible manner that allows to emulate spoofing scenarios. This way, assessments on the vulnerability of NMA-authenticated GNSS signals against spoofing attacks can be provided.

In this work, case studies related to the capability and vulnerability of NMA-authenticated Galileo E1B INAV signals are investigated. To this end, the case studies are emulated using the demonstration platform. Applying the authentication tools of Sisitau, the capability and vulnerability of the NMA-authenticated Galileo signals can be assessed for the investigated case studies. The results may serve the decision on the deployment of NMA within Galileo satellite navigation system.

In the following section, the components and the interfaces within the demonstration platform are described. This includes the detailed setup of the demonstration platform to emulate the related test scenarios. Afterwards, the case studies are defined. Thereafter, the results of these tests are presented. An assessment on the applicability of NMA-authenticated Galileo signals concludes the work.

II. Demonstration Platform

A. GNSS Software Transceiver

The **Mu**lti **S**ensor **N**avigation **A**nalysis **T**ool (MuSNAT) is a real-time multi-frequency GNSS software receiver implemented in C++ and developed at the Institute of Space Technology and Space Applications (former called ipexSR) [6]. In the scope of this work the MuSNAT software package was extended to a software transceiver, to not only process GNSS sample stream files provided by a GNSS receiver front end, but also to generate GNSS sample stream files. This way, GNSS signals can be recorded, processed and (re-)generated. In the processing mode, the symbols and the ephemeris data of the tracked satellite signals can be extract and saved. For the signal generation, the satellite ephemeris, the corresponding symbols and the user position or user trajectory, respectively, need to be provided. All this files are text based and modifiable. A schematic sketch of the software transceiver with the corresponding input and output files is given in Fig. 1.

B. Authentication Tools of Sisitau

There are two authentication tools within Sisitau. Both are framed by blue boxes in Fig. 1.

The first tool adds authentication data to the data stream of the Galileo signal. Up to now, the Galileo satellites broadcast zero bits within the data fields designated for NMA. Thus, this tool reads in the symbols of the navigation data from the text-based nav-file created with the MuSNAT and transforms them

Diese Arbeit wird durch das Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages gefördert und vom Projektträger des Deutschen Zentrums für Luft- und Raumfahrt (DLR) in Bonn verwaltet.

978-1-5386-1647-5/18/$31.00 ©2018 IEEE

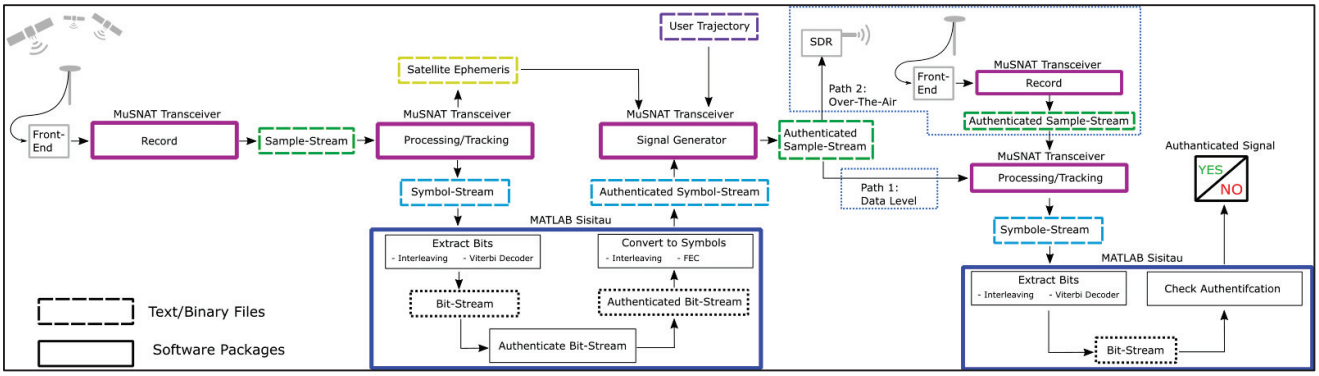

Fig. 1. Schematic workflow diagram for generating and testing GNSS signals with authentication.

into bits. Afterwards, the NMA keys, the MACs, and all other authentication data are generated for each Galileo subframe. Then, the data fields designated for NMA are assigned by the authentication data. Thereafter, the bit stream is converted back into symbols. The output of this tool is also a text-based nav-file in the same format but now with authentication data. The implementation is done in Matlab R2017a.

The second tool evaluates the authentication data and returns a successful authentication per subframe or a failed one. The input interface is the same as for the first authentication tool. Thus, the navigation symbols are read-in, transformed into bits and then the authentication data are evaluated. If the authentication is successful, a respective message is displayed on the computer screen. Otherwise, if the authentication fails for any subframe, the user is informed, too. The implementation is also done in Matlab.

III. Settings for the Case Studies

A. NMA settings

The NMA provides authenticity by (1) the MAC (2) the current key and (3) the signature. In this implementation, one MAC and one current key are broadcasted per subframe. Each subframe of the navigation message within Galileo E1B INAV consists of 15 even and 15 odd pages [7]. Each even page and its subsequent odd page contains amongst others a word between 1 and 10 or a spare word. The words are assigned to the field "data k" of the even page and the filed "data j" of the odd page, cf. Fig. 2.

Each subframe contains words 1 to 6 and either words 7 and 8 or words 9 and 10 besides the spare words. The MAC authenticates the words 1 to 5 of the navigation message. These words contain the ephemeris, clock correction, ionospheric correction and the Galileo system time [7]. All authentication data, i.e., the MAC, the current key and the signature are assigned to the 40 bit reserved space of odd pages (framed in red in Fig. 2). The transmission of the signature requires several subframes in sequence due to its size. In contrast to that, the MAC and current key corresponding to one subframe are transmitted within this subframe (in the reserved bit fields).

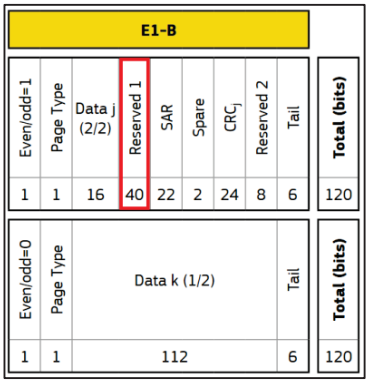

Fig. 2. Even and odd page of Galileo E1B INAV [7].

As mentioned before, the MAC authenticates the words 1 to 5. Using the current key, the MAC can be reconstructed. If the reconstructed MAC and the received MAC are identical, the MAC is said to be authentic. Moreover, the current key needs to be related to the key of the preceding subframe. If the derivation of the key of the preceding subframe is possible using the current key, then the current key is said to be authentic, too. Last, the signature of the KROOT needs to be checked. However, this step is omitted here since a warm start is assumed, i.e., the KROOT (= key of the first subframe) is assumed to be authentic.

IV. Case Study A: Proof of Concept

A. Setup of Case Study

In the first case study, a spoofer will not be involved. Instead, this case study serves as a proof of the total workflow shown in Fig. 1. To this end, real Galileo signals are recorded by the MuSNAT and afterwards processed. The navigation symbols are extracted and written to a text file. Then, the first authentication tool includes the authentication data based on NMA and saves the symbols (including authentication) in a text file. Afterwards, the Galileo signal transceiver generates the Galileo signal with the authenticated symbols.

The generated Galileo signal sample stream can then be processed directly by the MuSNAT, displayed in Fig. 1 as 'Path 1: Data Level'. But it is also possible to transmit the sample

stream file via a software defined radio (SDR) over-the-air and record a new sample stream file containing the transmitted signal using again antenna, front-end and the MuSNAT. The second way is also displayed in Fig. 1 as 'Path 2: Over-The-Air'. Path 1 allows an easy way for verification on the signal, path 2 enables to mimic real world scenarios with fading, multipath and signal blocking. The setup is displayed in Fig. 3. For transmitting the signal a sampling rate of 10 MHz was chosen with an additional carrier frequency offset of +750 kHz to avoid unintentional spoofing of other receivers.

According to path 1 or 2, the sample stream file is processed with MuSNAT which again extracts the (this time authenticated) navigation symbols and writes them into a text file. Finally, the second authentication tool reads in the text file and evaluates the authentication. Since a spoofer was not involved, each subframe should be successfully authenticated.

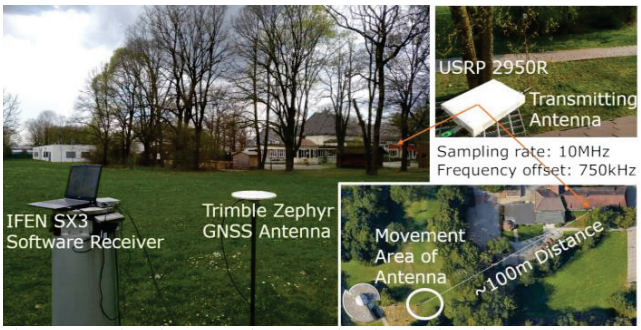

Fig. 3: Over-The-Air setup at the Universität der Bundeswehr München campus. With the USRP 2950R and a helix antenna as signal transmitter and a Trimble Zyphyr antenna with an IFEN SX3 front-end for receiving and recording. The distance is approximately 100 meter with an antenna movement area of ~10 meter in diameter.

B. *Results of Case Study: Data Level*

The antenna for receiving and recording the true Galileo signals was mounted on the roof of a building at the university campus at Neubiberg, Germany (open sky conditions). The recording was done at the 14.02.2018 between 15:00 and 16:00 o'clock, four Galileo satellites were in view: PRN 2, 7, 8 and 30. The authentication data were added to all satellites. The total recorded length is about 1800 seconds which corresponds 60 completed subframes. A power and Doppler analysis for the original received signals is shown in Fig. 4.

After the re-generation of the Galileo signals with the authenticated navigation massage, the stream sample file was again processed. The power and Doppler analysis for this re-generated signals (processed only on 'Data Level') is shown in Fig. 5. The signals were re-generated so that the power of the four satellites show a C/N0 difference of 2 dB-Hz from one satellite to the other. The power order is accordingly to the PRN number, so PRN 2 is the weakest and PRN 30 is the strongest. This was done to be able to test the signals over a broader power range in one scenario. Additional white Gaussian noise (WGN) was added to the signals to achieve a realistic intermediate frequency (IF) sample stream file.

The authentication of all fully received subframes was checked. The authentication of all MACs and keys was successful for all satellites and subframes.

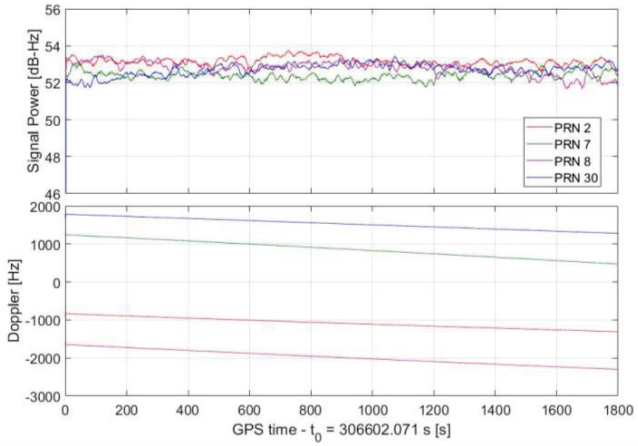

Fig. 4: Original Power (top) and Doppler (bottom) plots of Galileo E1 signals of PRN 2, 7, 8 and 30. The record was done at the 14.02.2018 between 15:00 and 16:00 o'clock.

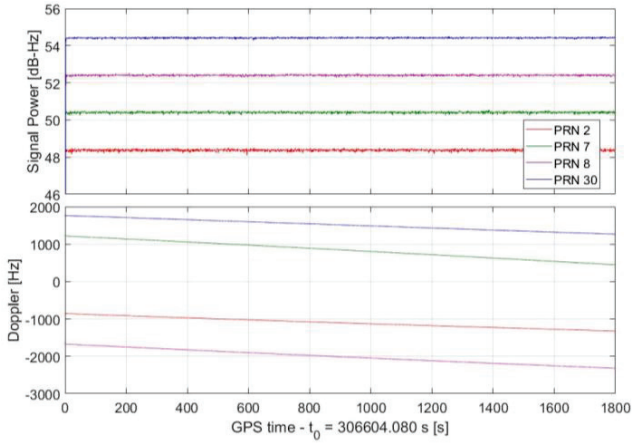

Fig. 5: Re-generated and processed on 'Data Level' Power (top) and Doppler (bottom) plots of Galileo E1 signals of PRN 2, 7, 8 and 30.

C. *Results of Case Study: Over-The-Air*

For the Over-The-Air tests, the same signal conditions were used in the re-generation of the signals, however no WGN was added to the signals.

The position of the antenna was static for the first eleven minutes of the recording. Thereafter the antenna was moved closer to the transmitting antenna. In a next step the antenna was moved behind trees and wooden huts to cause fading and signal blocking. Towards the end of the recording, the antenna was moved back to its starting position.

The fading and blockading can be nicely seen in Fig. 6 (top). In the second plot of Fig. 6, it is visible that the clock error of the USRP induces an additional Doppler offset but otherwise

the same Doppler behavior can be observed. In the third plot of Fig. 6, the true symbols were compared with the received symbols. Due to the movement of the antenna with multipath and fading symbol errors were caused followed by a total signal loss. Only a few symbol errors can be compensated by the viterbi decoder and cause no fail in the MAC and key authentication. Moreover, if the symbol error occurs in word 8, for example, the message is still classified as authentic since the MAC only protects words 1-5 and not word 8. A closer discussion of bit errors follows in Case Study B. As the current implementation require 9 subframes in a row to extract the root key from the navigation massage to verify the subframe key, it was not possible to authenticate the last three keys.

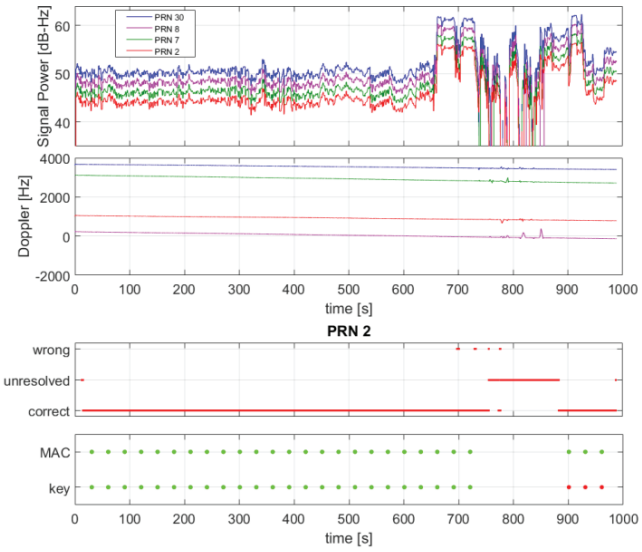

Fig. 6: Power (first) and Doppler (second) plots of Galileo E1 signals of PRN 2, 7, 8 and 30 for re-generated and 'Over-The-Air' transmitted signals. The third plot shows the occurens of errors in the received symbols for PRN 2. The bottom plot shows the authentication of MAC and key in the navigation massage for PRN 2. Each dot represents one subframe, where green stands for a succesful authentication and red identifies not authentic subframes.

V. Case Study B: Symbol Errors

A. Setup of Case Study

The authenticated navigation data from case study A within the 29 subframes was used here, too. The step of the signal regeneration and re-receivement was omitted because they have no influence on the effect of bit errors. Thus, arbitrary symbol errors were introduced in the authenticated navigation message. Therefore, the 14th subframe was selected because it is in the middle of the subframe chain. Afterwards, the authentication of the MACs and the keys was checked.

B. Results of the Case study

First, no symbol errors are introduced. In this case, all MACs and keys turned out to be authentic.

Afterwards, 60 random symbols of the first even page related to a spare word in the 14th subframe were changed. This corresponds to a change of 50% of the symbols. Although the number of symbol errors is very high, all MACs and keys were authentic. This makes sense because the MAC does only authenticate words 1 to 5 and none of the spare words. This means that errors in the spare words cannot be detected by the present implementation of the NMA. Moreover, the symbols corresponding to the MAC were also not changed because the MAC is assigned to odd pages whereas here only the bits of an even page were manipulated.

Then, 10 random symbols, i.e., ca. 8 %, of the even page related to word 2 of the 14th subframe were changed. This lead to a failed authentication of the MAC of subframe 14. This behavior was also expected since the MAC authenticates words 1 to 5, i.e., also word 2. The authentication of the current key was successful. This is because the key is stored in odd pages that were not spoofed here. The same result was obtained if only 5 random symbols, i.e., about 4 %, of the even page related to word 2 were changed. If up to 3 symbols are randomly changed in the even page related to word 2, the authentication of both, the MACs and the keys, were successful. This was tried out by 30 Monte Carlo iterations. The result suggests that the Viterbi corrected the symbol errors in these cases. When changing 4 random bits in the even page related to word 2, the MAC authentication was successful in at least 80 % of all Monte Carlo cases. The authentication of the key was always successful.

Last, 5 random symbols, i.e. about 4 % of the odd page related to word 2 of the 14th subframe were changed. In this case, both, the MAC and key authentication failed in about 40 % of all Monte Carlo cases. The reason for the failed authentication of the key is that the key is assigned to the odd page, thus the key of the previous subframe could not be reconstructed with the current manipulated key.

VI. Case Study C: Symbol-estimation Attack

A. Setup of Case Study

In this case study, the impact and usability of the authentication is tested under a symbol-estimation-attack. In this scenario, the villain aims, in the first phase, to mimic the genuine signal and synchronously (with respect to time) transmit it to the victim. Secondly, the power of the mimic signal is increased until it is stronger than the genuine signal. Afterwards, the villain shift the positon or time slowly as desired. For this attack, however, the villain needs to know the symbol before it is received by the victim to generate and transmit the mimicked signal. Therefore, the villain estimates the symbol by correlating over a fraction of the beginning of the genuine symbol. In the estimation time δt_{est}, the villain transmits only noise for the symbol (symbol value equals 0). After the estimation time, the villain knows the genuine symbol and transmits a correct mimicked signal. To imitate this scenario, a symbol estimation time is defined, e.g. 10% of the symbol time, $\delta t_{est} = 0.10 * t_{symbol}$. During the signal generation the symbol value is set to 0 for the time δt_{est} and after this time, the true symbol value is set. Three different generation approaches were tested. First, only the E1-B data symbol is set to zero. In this case, the correlation values in the data channel are smaller than in the pilot channel which can be easily detected by a receiver. Therefore, in the second case, the pilot channel was also set to zero during

the symbol estimation time. In the third case, only the data channel was set to zero but the second part of the symbol was generated with an increased power to compensate the correlation value reduction due to the first zero (noise) part. The receiver response and the authentication to this attack is evaluated for a symbol estimation time of 10%, 20%, 30%, 40%, 50% and 60% of the total symbol time.

B. Results of the Case study

The following results are gathered by analyzing only the generated spoofing signal. For all three cases (correlation compensation yes/no; Data- and Pilot-Channel estimation), it is shown that the receiver tracks and decodes the signal without any problem or symbol errors for 10%, 20%, 30% and 40% of estimation time. Therefore, all the received massages were recognized as authentic, even position and time could be modified by the villain. For estimation times of 50% and 60%, the receiver could still track the signal but was not able to decode the symbols. The signal was consecutive not authentic.

For the symbol estimation without compensation of correlation degradation:

If the power in the I- and Q-component of the unmodified tracking is compared (see Fig. *8*) with the power of the tracking of the sample stream with the symbol estimation time of 40% (Fig. 9) and 50% (Fig. 10), it can be observed that the power of the Data-channel is reduced compared to the Pilot-channel. This reduction is proportional to the estimation time. This behavior could be easily be detected by a receiver. In Fig. *10*, it is also clearly visible that the receiver is not able to decode the symbols.

For the symbol estimation with compensation of correlation degradation:

If again the power of I- and Q-component of unmodified and symbol estimated tracking (compare Fig. 11 and Fig. 12) are compared with each other, the power of Data- and Pilot-channel matches much better. However, there is still a small difference which is increasing with the estimation time. A better compensation model could even reduce this difference. Also for 50% estimation time, the symbols could not be decoded.

For the symbol estimation in Data- and Pilot-channel:

The power comparison in Fig. 13 and Fig. 14 shows that the power in I- and Q-component are for each estimation time equal. But compared to the unmodified tracking the total power reduces with the estimation time. For the symbol estimation of 50% and 60% the receiver was unable to track the signal for more than 3 seconds.

The C/N0 behavior for the three cases and the different estimation times is shown in Fig. 7. The C/N0 drops significantly if data- and pilot-channel is set to zero. Also, for the case of no correlation compensation, a reduced C/N0 is visible, compared to the case with power compensation.

VII. CONCLUSIONS

In this work, the capability and vulnerability of NMA-authenticated Galileo E1B INAV signals are evaluated by means of several case studies. The first study showed the proof of the correct workflow of the demonstration platform which was tested on data level as well as with Over-The-Air measurements. The second study evaluated the influence of symbol errors on the authentication. It turned out that less than 5 symbol errors in odd pages or in even pages whose information are incorporated in the MAC do not have a negative effect on the authentication. In the third case study, it turned out that the NMA authentication is not appropriate to detect symbol-estimation attacks. In future work, a wider range of spoofing attacks will be investigated.

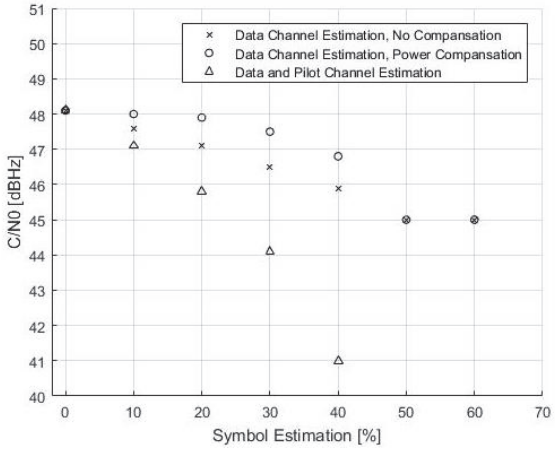

Fig. 7. C/N0 behavior for Data-channel estimation without compensation, data-channel estimation with power compensation and data- and Pilot-channel estimation over the estimation time in percent of the total symbol time.

REFERENCES

[1] K.D. Wesson, M.P. Rothlisberger, and T.E. Humphreys, "A proposed navigation message authentication implementation for civil GPS anti-spoofing", Proceedings fo the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, Portland, Oregon, 2011.

[2] J.T. Curran, M. Paonni, and J. Bishop, "Securing the open-service: a condidate navigation message authentication scheme for Galileo E! OS", European Navigation Converence, 2014.

[3] M. Yuan, Z. Lv, H. Chen, J. Li, and G. Ou, "An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing", China Satellite Navigation Conference, vol. II, 2017.

[4] I.F. Hernández, V. Rijmen, G.S. Granados, J. Simón, I. Rodríguez, and J.D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service", Proceedings of the ION GNSS+ Meeting, 2014.

[5] C. Sarto, O. Pozzobon, S. Fantinato, S. Montagner, I.F. Hernández, J. Simón, J.D. Calle, S.C. Díaz, P. Walker, D. Burkey, G. Seco-Granados, and E. Göhler, "Implementation and testing of OSNMA for Galileo", Proceedings of the ION GNSS+ Meeting, 2017.

[6] C. Stöber, M. Anghileri, A. Sicramaz Ayaz, D. Dötterböck, I. Krämer, V. Kropp, D. Sanromà Güixens, J.-H. Won, B. Eissfeller, and T. Pany, "ipexSR: a real-time multi-frequency software GNSS receiver", ELMAR, IEEE Proceedings, 2010.

[7] Galileo SIS ICD, "Galileo open service signal in space interface control document", OS SIS ICD, issue 1, revision 1, 2010.

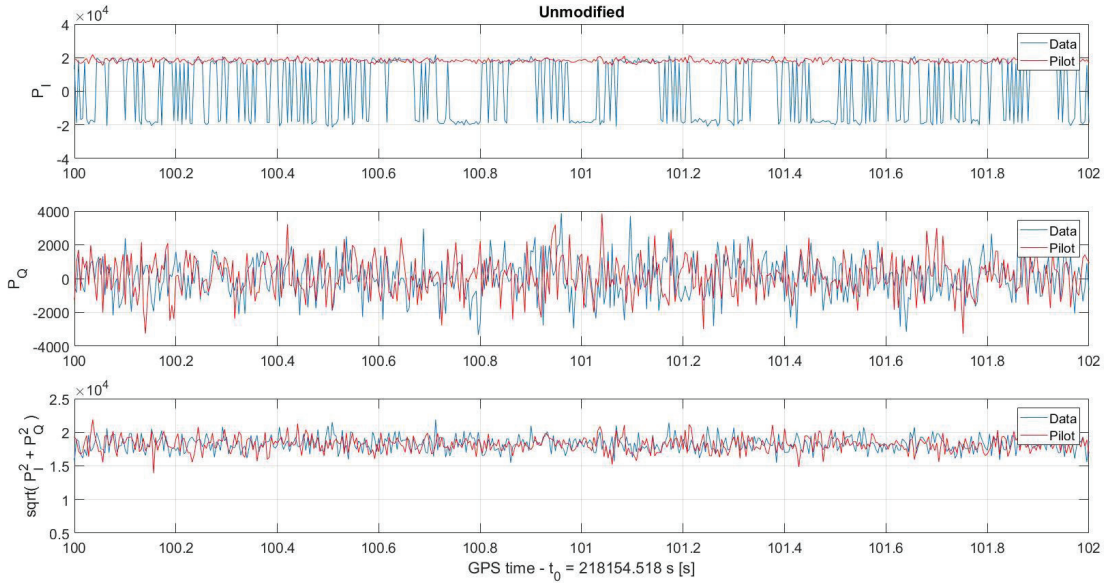

Fig. 8. Power of I-component, Q-component and the absolute value of the sample file without symbol estimation.

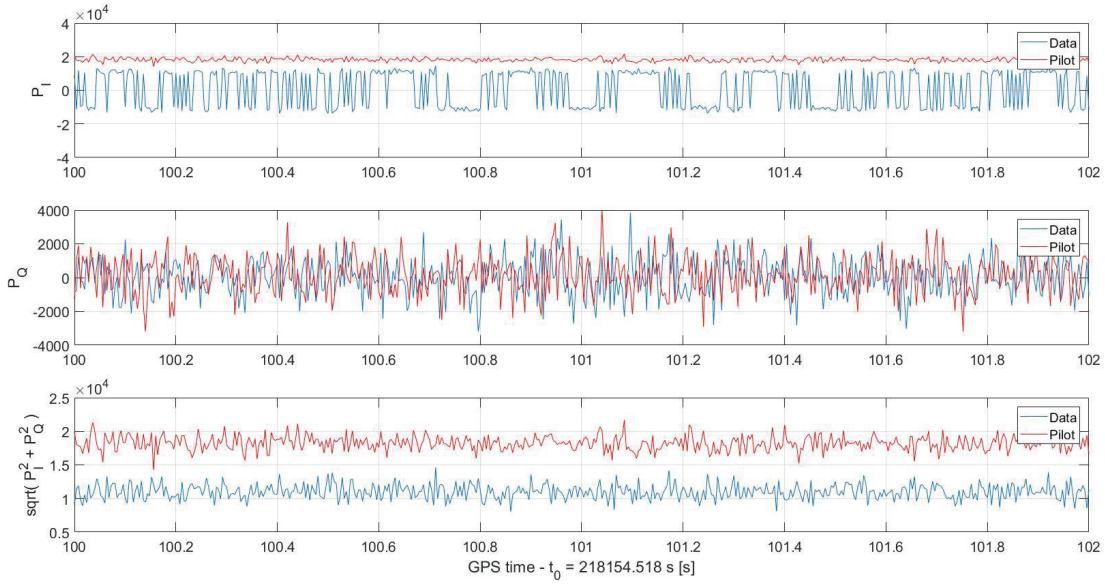

Fig. 9: Power of I-component, Q-component and the absolute value of the sample file with a symbol estimation time of 40% of the total symbol time. No compensation of correlation degradation was applied.

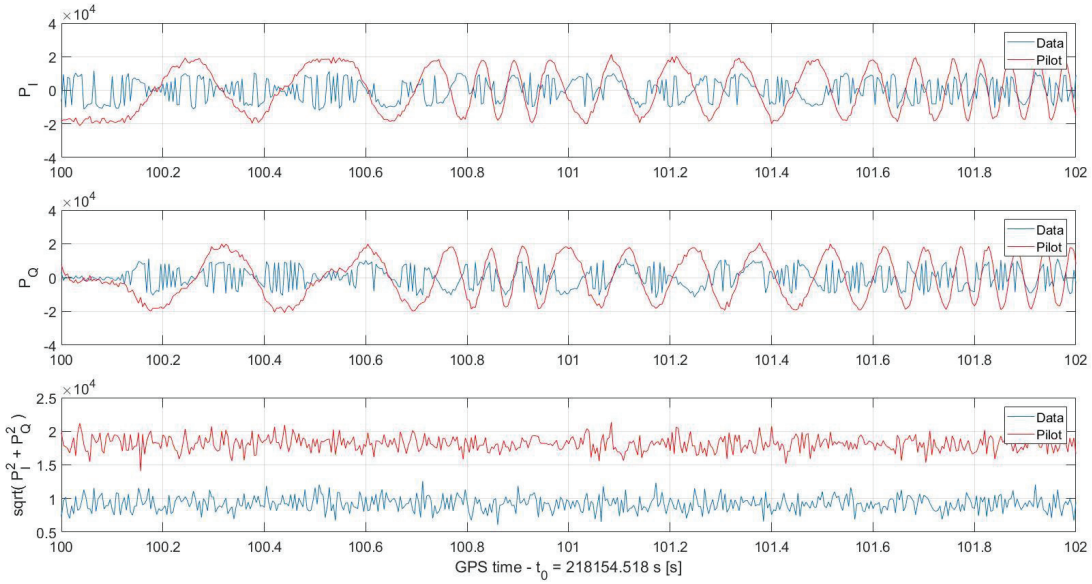

Fig. 10: Power of I-component, Q-component and the absolute value of the sample file with a symbol estimation time of 50% of the total symbol time. No compensation of correlation degradation was applied.

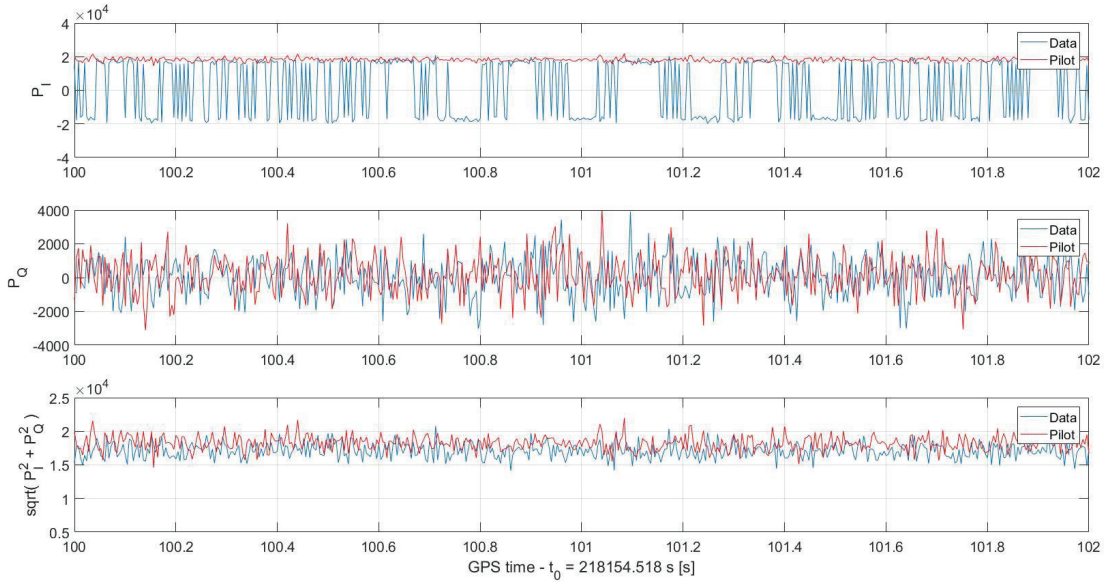

Fig. 11: Power of I-component, Q-component and the absolute value of the sample file with a symbol estimation time of 40% of the total symbol time. The power of the second part of the symbol was increased to compensate the correlation degradation.

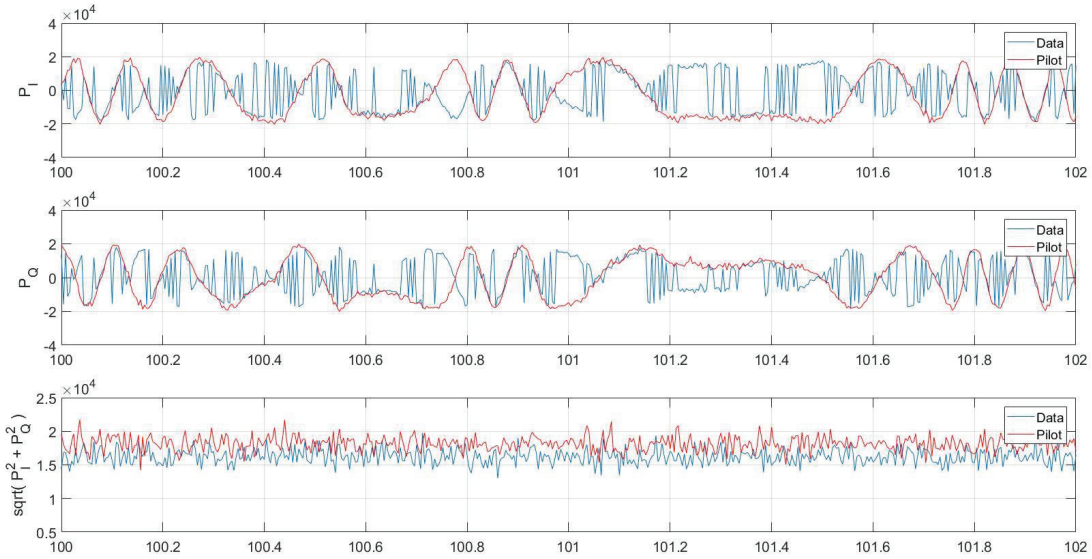

Fig. 12: Power of I-component, Q-component and the absolute value of the sample file with a symbol estimation time of 50% of the total symbol time. The power of the second part of the symbol was increased to compensate the correlation degradation.

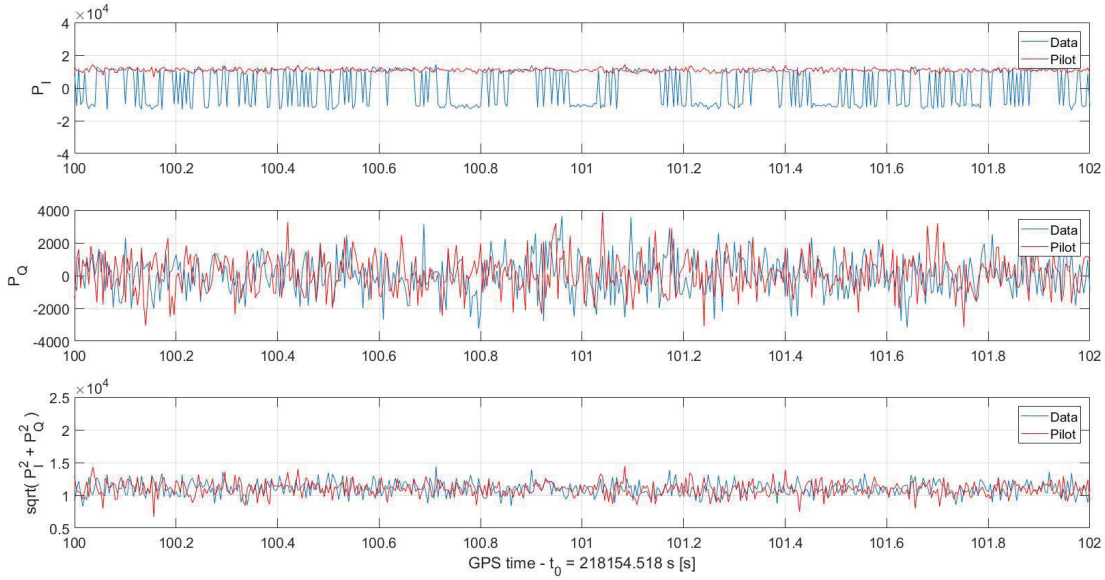

Fig. 13: Power of I-component, Q-component and the absolute value of the sample file with a symbol estimation time of 40% of the total symbol time. The symbol estimation was applied to Data- and Pilot-Channel.

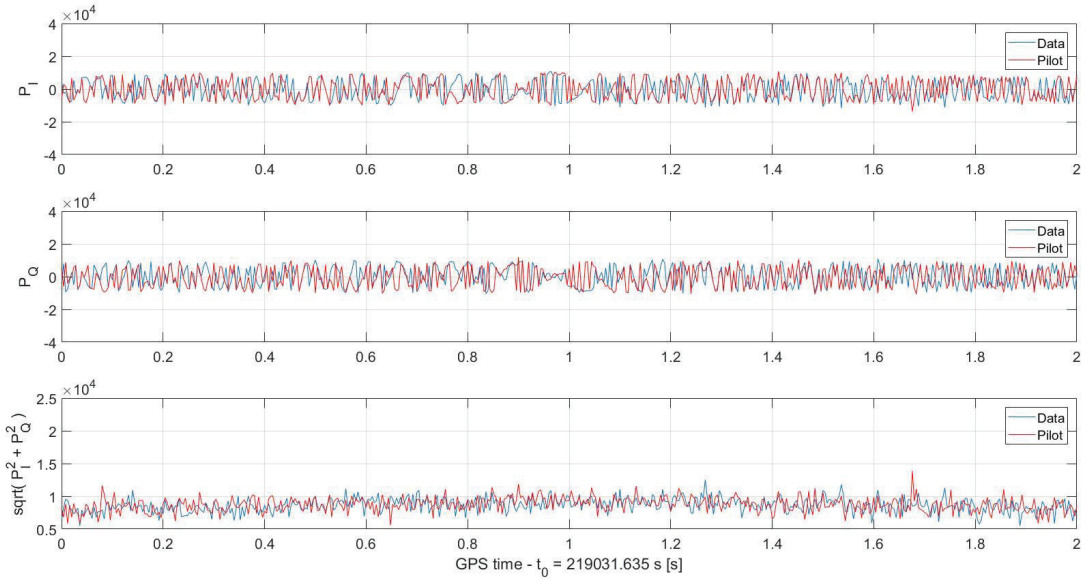

Fig. 14: Power of I-component, Q-component and the absolute value of the sample file with a symbol estimation time of 50% of the total symbol time. The symbol estimation was applied to Data- and Pilot-Channel.