JPNT 9(2), 43-50 (2020)
https://doi.org/10.11003/JPNT.2020.9.2.43

JPNT Journal of Positioning, Navigation, and Timing

Assessment of a Low Power Offset BPSK Component for Spreading Code Authentication

Daniel S. Maier†, Thomas Pany

Institute of Space Technology and Space Applications, Universität der Bundeswehr München, Germany

ABSTRACT

In this paper a low power Spreading Code Authentication (SCA) sequence with a BPSK(1) modulation at a frequency offset of +7.161 MHz is tested for authentication purposes, the Galileo E1OS is used as base signal. The tested signals comprise a Galileo constellation with 5 satellites including the Galileo OS Navigation Message Authentication (OSNMA) and a low power offset BPSK (OBPSK(7,1)) as SCA component. The signals are generated with the software based MuSNAT-Signal-Generator. The generated signals were transmitted Over-The-Air (OTA) using a Software-Defined-Radio (SDR) as pseudolite. With a real-environment-testbed the performance of the SCA in real channel conditions (fading and multipath) was tested. A new SCA evaluation scheme is proposed and was implemented. Under real channel conditions we derive experimental threshold values for the new SCA evaluation scheme which allow a robust authentication. A Security Code Estimation and Replay (SCER) spoofing attack was mimicked on the real-environment-testbed and analyzed with the SCA evaluation scheme. It was shown that the usage of an OBPSK is feasible as an authentication method and can be used in combination with the OSNMA to improve the authentication robustness against Security SCER attacks.

Keywords: GNSS, authentication, OSNMA, SCA

1. INTRODUCTION

The importance of GNSS as a backbone technology increases in many areas and applications. The need of an authentic position, velocity and timing information is a key feature for future public GNSS services, especially for applications like road toll systems, autonomous driving or geofencing and surveillance. This and the increasing number of spoofing and jamming incidences (Wendel et al. 2018, C4ADS 2019) whether intended or not, made the research on authentication possibilities in public GNSS services necessary and mandatory. The European GNSS Agency (GSA) decided to implement a Navigation Message Authentication (NMA) scheme into the Galileo Open Service (OS, E1-B) (Fernandez et al. 2016). The first transmission tests are planned for the first quarter of 2020 (Gutierrez 2020). The GPS system also considers to implement a SCA authentication method called Chimera (Anderson 2017).

The Galileo OSNMA uses the TESLA protocol (Perrig et al. 2000), which uses a one-way keychain and adding signed data with a message authentication code (MAC). In this way random bits are induced into the navigation message and are used to authenticate the message. An attacker is not able to know the transmitted symbols in total in advance. This approach works well against record and replay attacks as well as against signal generator attacks who can generate real-time signals but are now unable to produce a navigation message consistent with the already received keychain. More sophisticated attacks as a Security Code Estimation and Replay (SCER) attack (Humphreys 2013) is however not detectable with a NMA approach as the navigation message is estimated in real time and so are the induced random bits. The SCER attack exploits the circumstance that a symbol

Received Apr 2, 2020 **Revised** Apr 22, 2020 **Accepted** Apr 23, 2020
†**Corresponding Author**
E-mail: daniel.maier@unibw.de
Tel: +49-89-6004-3553
Daniel S. Maier https://orcid.org/0000-0002-5862-6634
Thomas Pany https://orcid.org/0000-0002-8456-5679

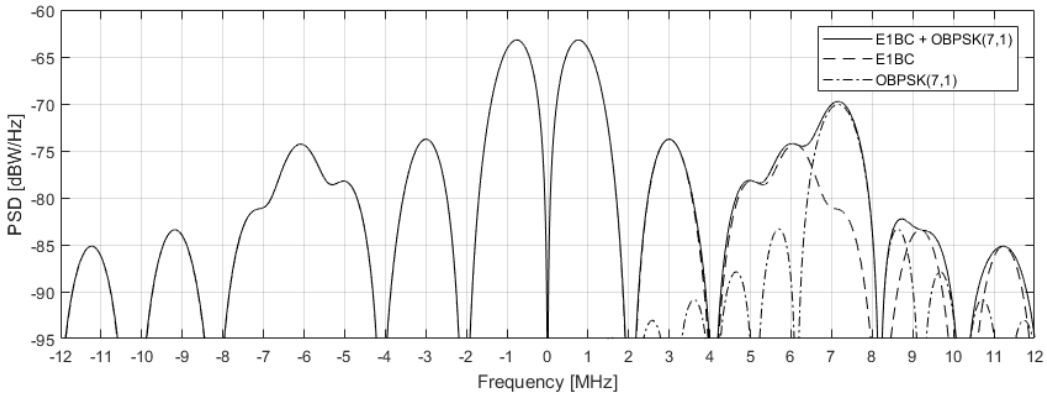


Fig. 1. Power spectral density (PSD) of E1-BC, the studied SCA OBPSK(7,1) and the combination of both.

can be estimated much faster than the symbol transmitting time using a high gain GNSS antenna. After the symbol is estimated a spoofing signal with correct navigation message can be transmitted. Meaconing, on the other hand, is a special class of spoofing attack. Here the true signal-in-space (SIS) is received and re-transmitted by a repeater. The spoofing signal is perfectly consistent with the true line-of-side (LOS) signal. That means, that any authentication technique based on the signals in space, be it NMA or SCA, is incapable of detecting this kind of attack. However, NMA and/or SCA can help receiver based detection methods to increase the detection probability.

In the following an additional encrypted low power spreading code component is analyzed to validate, if this low power SCA can help to strengthen the OSNMA against these attacks and how the receiver implementation can be realized. In the first part the additional signal is described and how the SCA evaluation scheme works with a look at receiver memory considerations. The second part describes the test setup and the execution of the test, followed by the results section where the measurement and authentication results are presented. At the end the conclusion section summarizes the findings.

2. SCA IMPLEMANTATION

The tested SCA implementation is based on the Galileo OS consisting of the data signals E1-B and the pilot signal E1-C. Additionally it is assumed that the Galileo OS NMA proposed by the GSA is implemented.

2.1 New Low Power Offset SCA Component

For a low power SCA component we study a BPSK(1) modulation at a frequency offset of +7.161 MHz. This offset BPSK (OBPSK(7,1)) is reduced in power by -10dB compared

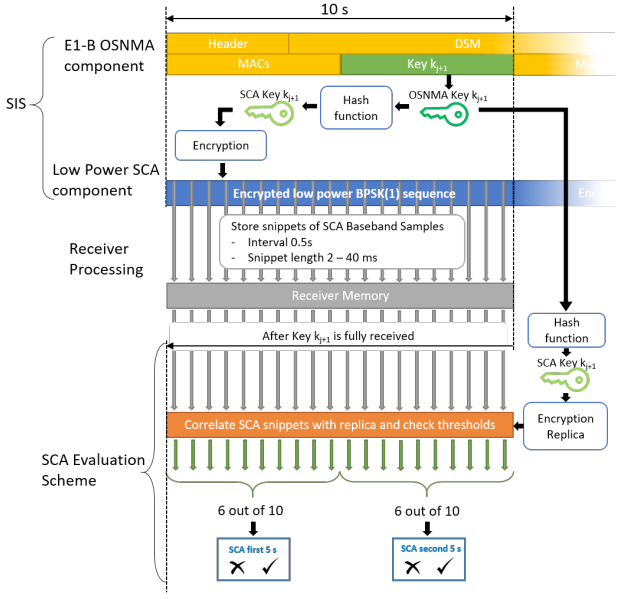


Fig. 2. SIS definition with E1-B OSNMA and a low power SCA component and the memory usage for the SCA evaluation scheme.

to the combined E1-BC signal power. The power spectral density (PSD) of E1-BC, the SCA OBPSK(7,1) and the combination of both is displayed in Fig. 1.

The fastest configuration of the Galileo OSNMA allows to receive all 10 s a new key of the keychain at each satellite. Approximately the first half (~5 s) of the OSNMA includes the MAC of key k_{j+1}^{NMA}, in the second half (~5 s) the key k_{j+1}^{NMA} is transmitted. With the OSNMA key k_{j+1}^{NMA} and a hash function a new SCA key k_{j+1}^{SCA} can be derived. This key is then used to encrypt the 10 s of the SCA spreading code. This can be done with symmetric encryption e.g. the advanced encryption standard or with a stream cipher approach e.g. ChaCha20 (De Santis et al. 2017). A detailed encryption approach is not part of this work. The SIS configuration with OSNMA, SCA key generation and SCA encryption is sketched at the top of Fig. 2.

https://doi.org/10.11003/JPNT.2020.9.2.43

2.2 Storing SCA Baseband Samples in Memory

The SCA sequence is unknown at receiving time. Due to the low power and the high chip rate it is also very hard for an attacker to estimate the chips in real time even with a high gain antenna. These features make it also impossible for the user to evaluate the SCA component in real time. The receiver has to save the raw IF samples until he receives the key and is able to generate the right SCA replica to lift the SCA component out of the noise due to the correlation. However, saving 10s of an IF signal stream with an minimum sampling rate of 12 MHz (required due to the OBPSK(7,1)) requires a significant amount of memory in the receiver. To overcome the need of saving the whole 10 seconds the following approach was chosen:

1. With the help of tracking the E1-BC component the IF raw samples were transformed into a SCA baseband signal. This means that the IF carrier and the Doppler for the specific Satellite as well as the frequency offset of the OBPSK(7,1) component were removed from the raw samples. This has to be done for each satellite in tracking separately. This comes with the disadvantage that for each satellite a separate baseband snippet has to be stored.
2. Snippets of the baseband samples are saved in receiver memory with a time tag synchronized to E1-B. During the 10 s twenty snippets were saved. The snippet interval is therefore 0.5 seconds. The saved snippet length is between 2 and 40 ms depending on the signal strength of the E1-BC component.

With this approach we don't have to store the whole 10 s and we saved the samples in an easy way for the latter correlation task as the snippets are already in the SCA baseband. The snippets can be correlated directly with the replica, without acquisition or Doppler removing.

The memory usage is reduced by adapting the snippet length to the satellite signal power. As the SCA component is -10 dB below the E1-BC power we can easily calculate the SCA power and therefore the needed coherent integration time t_coh to lift the SCA signal above a certain signal-to-noise-ratio (SNR). The SNR can be calculated with

$$SNR = C/N_0 \; t_{coh} \tag{1}$$

The Galileo OS E1-BC has an SNR_{BC} of 26 dB if the signal power is $C/N_0 = 50$ dB-Hz and $t_{coh} = 4$ ms (For Eq. (1), the dB values need to be converted into natural units). As our SCA signal is -10 dB lower we assume a SNR_{SCA} of 16 dB with the same integration time. To achieve this SNR for all satellites no matter the satellite power, we can rearrange Eq. (1) and determine the coherent integration time depending on the power of the E1-BC component. Coherent integration times for a selection of C/N_0 values are displayed in Table 1. The memory (MEM) needed for a total constellation with N_SV satellites in view and the whole 10 s (20 snippets) can now easily be calculated by

$$MEM = \sum_{sv=1}^{N_{SV}} 20 \; t_{coh}^{sv} \; f_S \; M_S \tag{2}$$

where M_S equals the memory needed for each baseband sample and f_S is the sampling rate.

Table 1. Coherent integration time and memory per snippet for different signal powers.

C/N_0 for E1-BC [dB-Hz]	C/N_0 for E1-SCA [dB-Hz]	SNR_{SCA} [dB]	t_{coh} [ms]	Memory per sample [byte/S]	Sampling rate [MS/s]	Memory per snippet [MB]
52	42	16	2.5	4	100	0.95
50	40	16	4.0	4	100	1.53
48	38	16	6.3	4	100	2.4
45	34	16	15.8	4	100	6.03
42	32	16	25.1	4	100	9.57
40	30	16	40.0	4	100	15.26

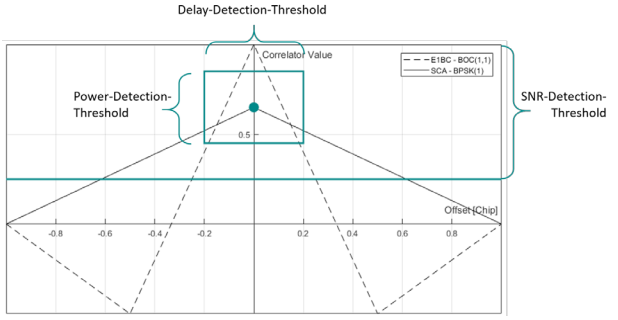


Fig. 3. SCA detection thresholds, illustrated with the correlator peaks of the Galileo E1-BC (BOC(1,1)) and the SCA (BPSK(1)) component. The y-axis is, for illustration purpose, arbitrarily normalized for SNR and C/N0 values.

2.3 SCA Evaluation

For the evaluation of the above defined and stored SCA component the following workflow was used:

1. After the OSNMA key k_{j+1}^{NMA} is fully received the SCA key can be derived and the SCA replicas for the SCA snippets can be created.
2. The SCA replicas are correlated with the stored snippets. With the correlation peak the SCA signal power C/N_0, the SNR_{SCA} and the time delay Δt between E1-BC and E1-SCA can be determined.
3. These 3 values are used to detect presence, position, and power of the SCA component in each SCA snippet separately. The detection principle is illustrated in Fig. 3 and will be explained in more detail below.

4. The 10 binary values of the first 5 seconds and the second 5 seconds, if the SCA component is correctly present or not, are evaluated separately in the following. In our evaluation we confirmed the 5 s segment for valid if 6 out of the 10 SCA snippets could be detected correctly, see Fig. 2. The 6 out of 10 allows a maximum of 4 SCA detection outliers in the 5 s. This makes the SCA detection more robust against short fading and blockage.
5. The total SCA verification is valid if the first and the second 5 s are valid. The separation into the first 5 s and the second 5 s is done because in the first 5 seconds there is no information about the OSNMA key present. So a possible advanced attacker has no additional information to estimate the SCA chips. In the second 5 s there is already some information about the key present. Not the whole key but parts of it. So the attacker is, maybe, capable of estimating the SCA chips with higher probability.

The correlator output of the SCA snippet is used to detect if the SCA component is present and coherent with the open signal E1-BC component. The following 3 parameters are analyzed for the SCA detection (compare Fig. 3):

1. SNR-Detection: The SNR value is assumed to be in the range of 16 dB as defined above and ensured due to the stored SCA snippet length (t_coh). If the SNR value is not above this 16 dB plus error margin, the SCA signal is assumed to be too weak for further tests. It cannot be confirmed that the correlation peak is a real peak or only noise.
2. Power-Detection: The SCA signal power C/N0 is by definition -10 dB below the E1-BC signal power. Therefore we check if this power offset is correct in a defined error range. With this test we can check if an attacker tries to hijack the signal by mimicking the open signal with increased spoofing power. The E1-BC (spoof) power is increased but the SCA power will stay on the real level, the increased power gap can be detected by using this detection.
3. Delay-Detection: The SCA snippets were stored with a specific time tag synchronized to the E1-B component. Therefore the position of the SCA correlator peak is known. If the SCA correlator peak is centered within a certain error range to the E1-BC correlator peak, one can detect if an attacker has hijacked the E1-BC signal and drags the spoofing signal away, in position or time.

For all three parameters threshold values have to be defined which allow a robust authentication in real environments and fail the authentication under spoofing attacks.

3. EXPERIMENTAL SETUP

3.1 Signal Generation

To verify the usability of the new SCA component and determine the Detection-Thresholds the real-environment-testbed (Maier et al. 2018b) was used and further developed for this propose. On the testbed a SCER attack was simulated. Therefore, the MuSNAT-Signal-Generator (Maier et al. 2018a) was used to generate the 'genuine' SIS at data level as IF sample stream with a sampling rate of 100 MS/s and IQ-Int16 samples. The genuine signal includes a Galileo constellation with 5 satellites, each satellite transmitting the signal components E1-B, E1-C and E1-SCA. The navigation message was supplemented with the OSNMA component. The test case is a static position. In a second step the 'spoofing' signal was generated with the same approach: MuSNAT-Signal-Generator, sampling rate, sample type, IF sample stream, data level. The spoofing signal consists of the same Galileo constellation but the generated signal components are now only the E1-B and E1-C. It was assumed that the attacker is able to estimate the navigation symbols in real time, therefore, the correct OSNMA was modulated on the spoofing signal.

The spoofing attack was implemented as following:

1. The spoofing signal starts at 1 224 429 119s GPS time with a 60 seconds long power increase from 0 dB-Hz until the spoofing signal power is +6 dB stronger than the genuine signal. The spoofing signal arrives at the receiver antenna with approx. zero delay compared to the genuine signal.
2. After the 60 second power ramp (1 224 429 179s GPS time) a Doppler shift, common to all satellite signals, is applied. This induces a clock drift in the receiver. During the spoof signal generation this simulated receiver clock drift also produces a small pseudorange drift depending on the satellite elevation.
3. 60 seconds after the Doppler shift the receiver position is dragged away (1 224 429 239s GPS time).

3.2 Transmitting Over-The-Air

The generated (data level) genuine and spoofing signal were converted to HF via a Software Define Radio (SDR). Therefore the National Instrument SDR 'USRP 2950R' was used. The genuine signal was transmitted with a passive GNSS antenna located at the rooftop of the institute building. The spoofing signal was transmitted with the same type of antenna but positioned at a window of the institute building. The setup is illustrated in Fig. 4. The transmitted signals travel over-the-air (OTA) approx. 130 m to the receiver antenna. The environment

https://doi.org/10.11003/JPNT.2020.9.2.43

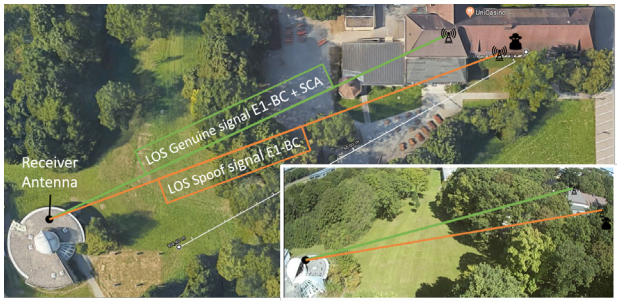


Fig. 4. Illustration of the geometrical and environmental setup of the SCER spoofing attack.

is quite challenging as trees are in LOS and multipath reflections from the rooftop and the buildings are present.

3.3 Receiving and Processing the Signal

The received signal was recorded with a sampling rate of 100 MS/s with the IFEN SX3 Front-End. The recorded signal was then processed with the MuSNAT-Receiver (Pany et al. 2019). A SCA snippet logging method was implemented into the MuSNAT-Receiver to store the SCA baseband samples as described above. For the evaluation the baseband samples were stored as complex int16 values (M_S=4 Byte per Sample) with a sampling rate of f_S=100 MS/s. The memory usage per snippet for these storage values are displayed in Table 1. The used values for baseband sample type and sampling rate are very high and could easily be reduced. An additional header was saved for each SCA snipped to store the E1-BC power, time tag, code phase and code phase rate. These values are needed for the post-processing correlation and evaluation.

For the SCA evaluation a Matlab tool was implemented which performs the SCA evaluation. Therefore, the logged SCA snippets with header as well as the SCA replica were read in. It was assumed the correct SCA replica could be derived from the OSNMA key. Afterwards, the SCA baseband snippet was correlated with the SCA replica. The correlation height and position was determined and the SCA power as well as the SCA SNR was calculated. With these values the 3 detection parameters could be evaluated and the authentication evaluation was executed as described in Section 2.3.

It should be mentioned here, that the receiver requires, apart from memory storage, the capability to correlate and evaluate the additional SCA snippets in real time. The SCA correlation and evaluation process is similar to the standard satellite signal tracking process. State-of-the-art receivers have the processing capability to track dozens of satellites of all different constellations in parallel. Therefore, it can be assumed that the SCA correlation and evaluation process can be integrated into the GNSS-chipsets. But, as the SCA will be most likely only a minor application, it can become an issue for mass market chipsets. The memory demand is assumed to be the more severe issue as current GNSS-chipsets don't need significant storage space. This could be overcome by transferring the sample storage to the chipsets host system, therefore however, some kind of memory interface is needed.

4. RESULTS

With the performed experiments, it was possible to derive threshold values regarding the 3 detection parameters. The following Detection-Thresholds with error range, as it turned out, allow a robust tracking under the tested conditions with a reliable indication under the spoofing attack:

- SNR-Detection-Threshold: Target SNR = 16 dB, Error margin = -6 dB
- Power-Detection-Threshold: Target SCA C/N_0 = E1-BC C/N_0 -10 dB; Error margin = ±5 dB
- Delay-Detection-Threshold: Target delay = 0 Chip, Error margin = ±0.2 Chip

The derived Detection-Thresholds were used to process the SCA evaluation scheme as described in Section 2.3. In the following the so achieved SCA authentication results for 3 of the 5 satellites are presented. The selected satellites cover a power range from 51 to 41 dB-Hz and a simulated elevation angle from 70.1 to 18.6°. The satellites with the corresponding figures are listed below:

- PRN 3: with a generated E1-BC signal power of ~51 dB-Hz, Elevation 70.1°, Fig. 5
- PRN 24: with a generated E1-BC signal power of ~45 dB-Hz, Elevation 24.2°, Fig. 6
- PRN 5: with a generated E1-BC signal power of ~41 dB-Hz, Elevation 18.6°, Fig. 7

In the three figures the following plots are shown

- First plot shows the signal power C/N_0 of the E1-BC component.
- Second plot shows the SNR of the SCA component with a SNR-Detection-Threshold at 10 dB.
- Third plot shows the signal power difference $\Delta C/N_0$ between the SCA and the E1-BC component with a Power-Detection-Threshold of ±5 dB-Hz.
- Fourth plot shows the correlator peak time delay Δt between the SCA and the E1-BC component with a Delay-Detection-Threshold on ±0.2 Chips.
- Fifth plot shows the SCA detection for each 5-second-segment.

In all 3 figures the same time period is shown, starting at

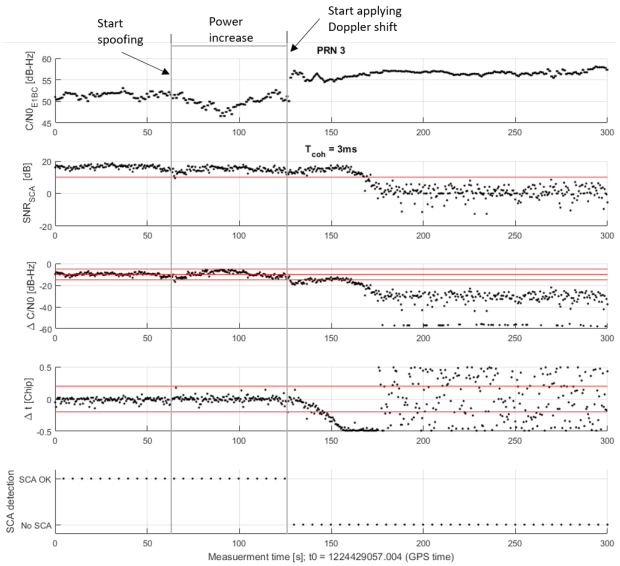


Fig. 5. SCA results for PRN 3: with a generated E1-BC signal power of ~51 dB-Hz an elevation 70.1° and a t_{coh}=3 ms. The first plot shows the signal power C/N_0 of the E1-BC component. The second plot shows the SNR of the SCA component with a SNR-Detection-Threshold at 10 dB. The Third plot shows the signal power difference $\Delta C/N_0$ between the SCA and the E1-BC component with a Power-Detection-Threshold of ±5 dB-Hz. The fourth plot shows the correlator peak time delay Δt between the SCA and the E1-BC component with a Delay-Detection-Threshold of ±0.2 Chips. The fifth plot shows the SCA detection for every 5 s segment. Compare Fig. 3 for the Detection-Threshold illustration.

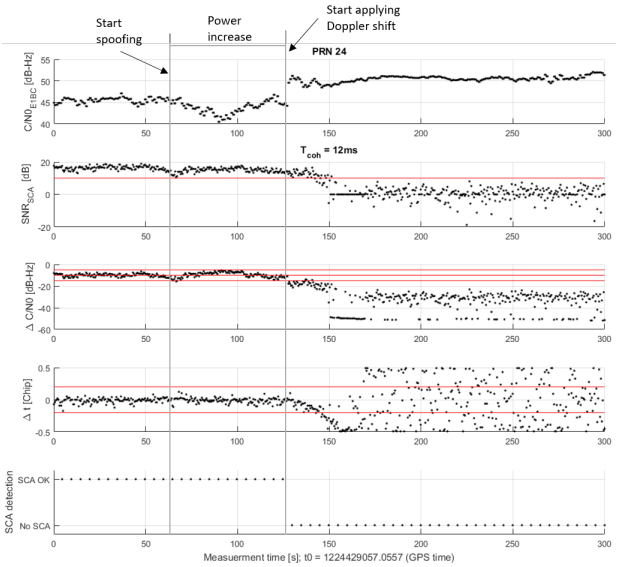


Fig. 6. SCA results for PRN 24: with a generated E1-BC signal power of ~45 dB-Hz an elevation 24.2° and a t_{coh}=12 ms. The first plot shows the signal power C/N_0 of the E1-BC component. The second plot shows the SNR of the SCA component with a SNR-Detection-Threshold at 10 dB. The Third plot shows the signal power difference $\Delta C/N_0$ between the SCA and the E1-BC component with a Power-Detection-Threshold of ±5 dB-Hz. The fourth plot shows the correlator peak time delay Δt between the SCA and the E1-BC component with a Delay-Detection-Threshold of ±0.2 Chips. The fifth plot shows the SCA detection for every 5 s segment. Compare Fig. 3 for the Detection-Threshold illustration.

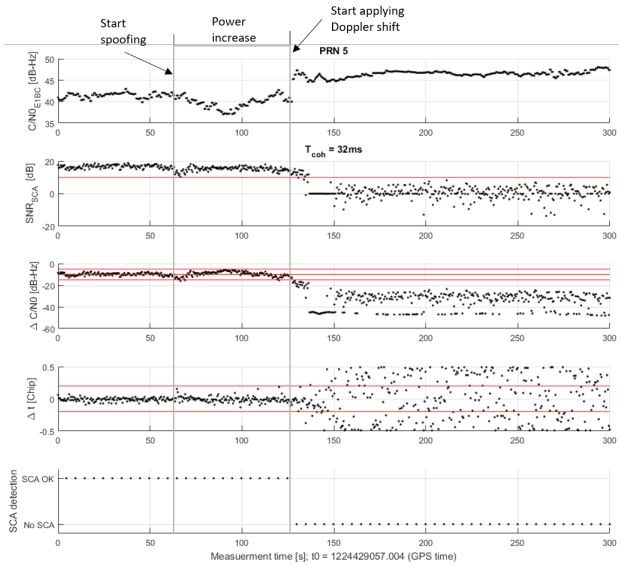


Fig. 7. SCA results for PRN 5: with a generated E1-BC signal power of ~41 dB-Hz an elevation 18.6° and a t_{coh}=32 ms. The first plot shows the signal power C/N_0 of the E1-BC component. The second plot shows the SNR of the SCA component with a SNR-Detection-Threshold at 10 dB. The Third plot shows the signal power difference $\Delta C/N_0$ between the SCA and the E1-BC component with a Power-Detection-Threshold of ±5 dB-Hz. The fourth plot shows the correlator peak time delay Δt between the SCA and the E1-BC component with a Delay-Detection-Threshold of ±0.2 Chips. The fifth plot shows the SCA detection for every 5 s segment. Compare Fig. 3 for the Detection-Threshold illustration.

the GPS time 1 224 429 057 s. From 0 - 62 s only the genuine signal is present. The SCA evaluation shows a reliable detection of the low power SCA component without any false alarm.

At time tag 62 s the spoofing signal starts to increase its power beginning at 0 and reaching 60 s later (time tag 122 s) a signal power which is +6 dB-Hz above the genuine signals. In the first half of this time period a drop in the tracked signal power is visible. Due to the incoherent addition of genuine and spoofing signal at the receiving antenna the spoofing signal behaves like a multipath signal. In the second half of the power increase period the spoofing signal overpowers the genuine signal and the track signal power increases again. Now the genuine signal acts as multipath signal. The SCA evaluation scheme shows here still a valid SCA detection. This behavior is expected and plausible, the receiver tracks now the spoofing signal but the spoofing signal matches the genuine signal perfectly and causes no harm to the receiver. As a remainder the spoofing signal mimics a SECR attack, so the navigation message and the OSNMA is also present on the spoofing signal.

At time tag 122 s the Doppler shift starts, to all spoofing satellite signals a common and slowly increasing Doppler shift is applied. This means the signals are dragged off in the frequency space. This common Doppler shift results in a

constant clock drift in the receiver. During the spoof signal generation this simulated receiver clock drift produces also a small pseudorange drift depending on the satellite elevation. In all three plots the tracked power increases now to its full spoofing maximum as the genuine signal and spoofing signal does not interfere anymore. The SCA SNR validation is still valid at the beginning as the correlator peak is still present in the Power-Detection- and Delay-Detection-Threshold box, compare Fig. 3. The Power-Detection drops immediately below the threshold because the tracked signal power does not match the SCA power anymore. This of course depends on the applied spoofing signal power. The time delay detection moves slowly out of the Delay-Detection-Threshold box. The speed of the movement depends on the Doppler shift speed and the satellite elevation because of the changing pseudorange mentioned above. As soon as the spoofed signal changes the Doppler or pseudorange the SCA detection failed. Or put it another way as soon as the spoofed signal tries to change receiver time or position the SCA evaluation scheme raises the alarm.

5. CONCLUSIONS

In this work we presented a SCA evaluation scheme in combination with the Galileo OS NMA. Therefore, we defined an additional low power SCA component based on an OBPSK(7,1). To obtain experimental threshold values and test the evaluation scheme a Security SCER attack was mimicked under real channel conditions. Therefore, the genuine and the spoofing signals were generated on data level and are afterwards transmitted via a SDR OTA. The recorded samples were processed with the MuSNAT software receiver. During processing, baseband snippet samples of the SCA components were stored in memory and were evaluated later with a Matlab tool accordingly to the proposed SCA evaluation scheme.

It was shown that the usage of an OBPSK is usable as an authentication method and can be used in combination with the OSNMA to improve the authentication robustness against SCER attacks. The proposed SCA verification scheme enables robust authentication under real and challenging channel conditions using the experimentally defined Detection-Thresholds. The Detection-Thresholds have a crucial influence on the performance of the SCA evaluation scheme and need to be verified and optimized in the future for different conditions and environments. Therefore, more and longer tests need to be conducted to achieve a more general statement on the robustness of the SCA authentication.

ACKNOWLEDGMENTS

This work is funded by the German Federal Ministry for Economic Affairs and Energy on the basis of a decision by the German Bundestag. It is administrated by the German Aerospace Center in Bonn, Germany (FKZ: 50 NA 1703).

AUTHOR CONTRIBUTIONS

The contribution is distributed as following: conceptualization, Daniel S. Maier; methodology, Daniel S. Maier; software, Daniel S. Maier; validation, Daniel S. Maier; formal analysis, Daniel S. Maier; investigation, Daniel S. Maier; data curation, Daniel S. Maier; writing—original draft preparation, Daniel S. Maier; writing—review and editing, Thomas Pany; visualization, Daniel S. Maier; supervision, Thomas Pany; project administration, Daniel S. Maier; funding acquisition, Thomas Pany.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Anderson, J. M., Carroll, K. L., DeVilbiss, N. P., Gillis, J. T., Hinks, J. C., et al. 2017, Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals, Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017), Portland, Oregon, September 25-29, 2017, pp.2388-2416. https://doi.org/10.33012/2017.15206

C4ADS, Above us only stars: Exposing GPS spoofing in Russia and Syria, March 2019, [Internet], cited 2020 March 10, available from: https://c4ads.org/reports

De Santis, F., Schauer, A., & Sigl, G. 2017, ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications, Design, Automation & Test in Europe Conference & Exhibition (DATE), 27-31 March 2017, Lausanne, Switzerland, pp.692-697. https://doi.org/10.23919/DATE.2017.7927078

Fernandez, I, Rijmen, V., Ashur, T., Walker, P., Seco, G., et al. 2016 (GSA), Galileo Navigation Message Authentication Specification for Signal-In-Space Testing, Version 1.0, November 2016. [Internet], cited 2018 May 31, available from: https://www.gsa.europa.eu/development-supply-

and-testing-galileo-open-service-authentication-user-terminal-os-nma-gsa (Annex I - Tender Specifications/AD1) (10.2019).

Gutierrez, P. 2020, Galileo to Transmit Open Service Authentication, InsideGNSS, January/February 2020, 15, 24-27. https://insidegnss.com/galileo-to-transmit-open-service-authentication/

Humphreys, T. E. 2013, Detection strategy for cryptographic GNSS anti-spoofing, IEEE Transactions on Aerospace and Electronic Systems, 49, 1073-1090. https://doi.org/10.1109/TAES.2013.6494400

Maier, D. S., Frankl, K., & Pany, T. 2018a, The GNSS-Transceiver: Using Vector-tracking Approach to Convert a GNSS Receiver to a Simulator; Implementation and Verification for Signal Authentication, ION GNSS+ 2018, September 24-28, 2018, Hyatt Regency Miami, Florida, pp.4231-4244. https://doi.org/10.33012/2018.16083

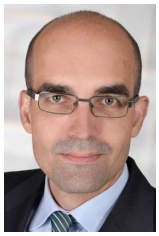
Maier, D. S., Kraus, T., Sánchez, D. E., Blum, R., & Pany, T. 2018b, Real-Time Real-World Testbed for New GNSS Signals – an Update on the Feasibility Study of Using UAVs as GNSS Satellites, Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation, ION GNSS+ 2018, September 24-28, 2018, Hyatt Regency Miami, Florida, pp.3530-3543. https://doi.org/10.33012/2018.15869

Pany, T., Schütz, A., Maier, D., Sharma, H., Arizabaleta, M., et al. 2019, The Multi-Sensor Navigation Analysis Tool (MuSNAT) as an Enhanced GNSS Software Radio to Face Current Navigation Challenges, ION GNSS+ 2019.

Perrig, A., Canetti, R., Tygar, J. D., & Song, D. 2000, Efficient authentication and signing of multicast streams over lossy channels, In Proceeding 2000 IEEE Symposium on Security and Privacy, S&P 2000, 14-17 May 2000, Berkeley, CA, USA, pp.56-73. https://doi.org/10.1109/SECPRI.2000.848446

Wendel, J., Rügamer, A., & Heue, R. 2018, GNSS Jamming and Spoofing: Hazard or Hype?, Space of Innovation, [Internet], cited 2018 June 4, available from: http://www.space-of-innovation.com/gnss-jamming-and-spoofing-hazard-or-hype/

Daniel S. Maier received a bachelor in Physics in 2015 and a master in Applied and Engineering Physics in 2017 from the Technical University of Munich (TUM), Germany. Since 2017 he has been a research associate at the Institute of Space Technology and Space Applications of the "Universität der Bundeswehr München." His current research interests include GNSS signal generation, signal authentication, and signal performance analysis.



Prof. Thomas Pany is professor at the "Universität der Bundeswehr München" at the faculty of aerospace engineering where he teaches satellite navigation. His research includes all aspects of navigation ranging from deep space navigation over new algorithms and assembly code optimization. Currently, he focuses on GNSS signal processing for Galileo second generation, GNSS receiver design and GNSS/INS/LiDAR/camera fusion. To support these activities, he is developing a modular GNSS testbed for advanced navigation research. Previously, he worked for IFEN GmbH and IGASPIN GmbH and is the architect of the ipexSR and SX3 software receiver. He has around 200 publications including patents and one monography.

https://doi.org/10.11003/JPNT.2020.9.2.43