Hindawi
Mobile Information Systems
Volume 2021, Article ID 8812333, 11 pages
https://doi.org/10.1155/2021/8812333

Research Article

Impact of GPS Interference on Time Synchronization of DVB-T Transmitters

Juraj Machaj,[1,2] **Peter Brida**,[1,2] **Norbert Majer**,[3] **and Roman Sčehovič**[3]

[1]*Department of Multimedia and Information-Communication Technology, Faculty of Electrical Engineering and Information Technology, University of Zilina, Žilina 010 26, Slovakia*
[2]*University Science Park, University of Zilina, Žilina 010 26, Slovakia*
[3]*Research Institute of Posts and Telecommunications, Banská Bystrica 974 05, Slovakia*

Correspondence should be addressed to Juraj Machaj; juraj.machaj@fel.uniza.sk

Received 17 September 2020; Revised 5 October 2020; Accepted 31 March 2021; Published 15 April 2021

Academic Editor: Adrian Kliks

Nowadays, the Global Positioning System (GPS) is widely used in all aspects of our lives. GPS signals are not used only in positioning and navigation applications and services in transport and military, but, thanks to quite precise information about time, also for synchronization of world trade and synchronization of wireless transmitters. However, with the recent spread of location-based services, a large number of GPS jammers had appeared. Use of these jammers is prohibited by law; however, their use is gaining popularity especially in the transport segment since jammers can be used to trick vehicle onboard units and help avoid paying toll fees on highways or avoid tracking of company cars when used privately. In this paper, we will investigate the impact of GPS interference caused by jamming and spoofing on the synchronization of Single Frequency Network (SFN) Digital Video Broadcasting–Terrestrial (DVB-T) transmitters. Since GPS signals are used in the DVB-T SFN to provide synchronization which is crucial for the correct network operation, the interference of GPS signals can cause problems with signal distribution. Thus, signals received from a DVB-T SFN network might be out of synchronization and disrupt the service for users.

1. Introduction

Recently Global Navigation Satellite System (GNSS) positioning systems are being widely implemented in all areas of our lives. GNSS systems are only not used for positioning and navigation purposes anymore but also for purposes of time synchronization in different applications. However, the GNSS and mainly GPS applications are widespread in all aspects of our daily life, for example, monitoring of company cars movement of tolling systems [1, 2]. Therefore, some people are trying to trick the system and are using GPS jammers. Although the use of GPS jammers is prohibited by the law in the majority of countries, it is relatively easy to get one shipped into any country and start using it.

The use of GPS jammers can potentially cause significant problems in various applications, for example, GPS-like signals are used at airports for air traffic control and navigation of planes during critical parts of the flight, like landing procedure for example. There have been reported cases when GPS jammer, used to hide the use of company vehicle for personal purposes, has caused disruption of airport services.

Moreover, GPS signals are widely used for time synchronization purposes in wireless networks as well as fixed networks, transport system, and financial transaction systems nowadays.

Recently, there has been a lot of studies focusing on the detection and mitigation of jamming and spoofing interference on GPS signals. A handful of solutions was proposed to detect the interference caused by jammers and spoofers. Jamming detection can be performed relatively easily as jammers transmit signals in the same band as GPS but with a higher amplitude, thus causing higher error rates in the received data or loss of GPS signals.

On the other hand, the detection of spoofing attacks is more complicated since the interference signal is mimicking the signals transmitted by GPS satellites. The solutions for the detection of GPS spoofing are based on monitoring of received power [3], spatial processing [4], Time of Arrival (TOA) Discrimination [5], Signal Quality Monitoring [6], distribution analysis of the correlator output [7], or consistency checks [8, 9]. Nevertheless, these solutions are not widely implemented in the GPS receivers since some special capabilities of the receiver, for example, L2 reception, correlators, multiple antennas, and so forth, are usually required [10].

However, the impact of GPS signal interferences caused by jamming and spoofing on systems used for time synchronization was not studied to a large extent yet. Therefore, we will focus on the impact of GPS attacks on the time synchronization of DVB-T transmitters in SFN configuration in this paper. In DVB-T SFN, it is important to have good synchronization of transmitters so signals can be considered as multipath copies of the same signal. Tight synchronization of the transmitters can be achieved using GPS signals, which can provide time synchronization with accuracy up to nanoseconds, while synchronization required by the DVB-T SFN networks is in microseconds. For the specific implementation of DVB-T SFN in Slovakia, the required synchronization accuracy is 224 μs, due to the physical separation of transmitters in the range of 64 km as well as setting of the guard interval in OFDM signals.

The main contribution of the paper is the analysis of the DVB-T SFN operation in a situation when one of the transmitters is affected by the interference of GPS signal used for synchronization. The analysis of the results shows that the implementation of some spoofing detection algorithms is required in order to make the system functionality reliable under a spoofing attack. It is important to note here that spoofing attack may be aimed on other applications which, however, can also affect the operation DVB-T SFN network that can be considered a part of the safety infrastructure, as in case of emergency, it can be used to spread safety information among citizens.

The rest of the paper is organised as follows: Section 2 provides an overview of DVB-T SFN networks as well as GPS interferences, Section 3 describes the testing setup, achieved results will be presented in Section 4, and Section 5 will conclude the paper.

2. Related Work

With the increased use of GPS systems in our daily life, also the number of so-called attacks on GPS services has increased. These attacks are commonly caused by devices causing interference of GPS signals. Due to increased interference of GPS signals, the attention of the research community was drawn to the development of solutions that are able to detect GPS interferences and thus provide some kind of warning to the users affected. In this section, we will provide an overview of GPS interferences and approaches of their detection, time synchronization using GPS, and a description of the DVB-T SFN network.

2.1. GPS Interference. GPS signals are vulnerable to many signals, which is caused by the low power level of signals received by the device. In civil code GPS L1 C/A, the power of the received signal can be as low as −158.5 dBW [11]. The GPS signals can therefore be affected by any transmitter operating at frequencies near to the GNSS bands with high transmission power or because of imperfections of implementation or malfunction of wireless systems [12]. Such interferences are considered to be unintentional and can be caused for example by DVB-T transmitters [13]. A method to assess the robustness of GPS signal in the presence of unintentional interference has been proposed in [14].

Unfortunately, unintentional interference is not the only problem GPS receivers have to face. Intentional GPS jamming can be caused by jammers that transmit noise-like signals on frequencies in the same frequency band as the GPS signals, thus causing loss of GPS signal reception. Jamming can be performed using different types of signals, the most common types of jamming are pulse jamming, spot jamming, barrage noise jamming, sweep jamming, and repeater jamming [15]. However, from the work presented in [16], it seems most of the publicly available jammers use swept tone method for jamming the GPS signals. From the tests, it was also concluded that the effective range of GPS jammers can be from 300 m up to 8.7 km.

On top of these relatively simple jamming approaches, it is possible to perform spoofing attacks on GPS services. Spoofing attacks can be performed in two ways, by rebroadcasting GPS signals recorded at another place or time (called meaconing) and by generating and transmitting modified satellite signals. Spoofing attacks can be much harder to detect since the receiver is still able to decode all GPS data without significant errors; however, these data are faulty. To detect spoofing of the GPS signals, additional features of the GPS receiver have to be implemented. Among approaches proposed to detect GPS spoofing methods like detection of unusual values in power-related parameters, monitoring of time-related parameters, spatial processing, and use of hybrid navigation, for example, GNSS + INS (Inertial Navigation System) in case of navigation services are used [17]. However, these are not suitable for static implementation with a single GPS receiver.

2.2. Time Synchronization Using GPS. The GPS signals not only are used for tracking purposes but can provide accurate time information as well. This can be done thanks to the fact that all GPS satellites are tightly synchronized to national and international standards. Therefore, GPS signals can be processed by the master clock, time servers, or reference clocks and thus provide accurate time synchronization to a variety of applications. The accuracy of the GPS synchronization is typically in the range of nanoseconds if devices are synchronized directly by GPS signals, up to milliseconds with accuracy depending on the protocol used to distribute the timing information among the devices [18].

Since GPS can provide accuracy close to atomic clocks and eliminates manual clock setting, it allows correlating events that are time-stamped by different clocks. There is a

vast number of applications that rely on GPS time synchronization including, legally validated time stamps, operational efficiency, regulatory compliance, and secure networking.

Characteristics of the GPS timing modules for accurate time synchronization were investigated in [19]. The authors have used M12M timing receivers to measure relative time error between generated PPS (pulse per second) and 100 PPS signals. The achieved mean timing offset between two receivers was 14 ns with a standard deviation of 13 ns without the implementation of data correction. The authors conclude that the difference might be higher for receivers placed further apart, as in such case, signals from different satellites will be received.

The GPS time synchronization with nanosecond accuracy with receivers in a region within 10 km was described in [20]. The authors were evaluating the impact of imprecise position in fixed position timing application and proposed a weighting algorithm that allowed them to achieve nanosecond level timing accuracy using GPS L1CA signals.

Based on data in [20–23], the influence of different error sources on the timing synchronization is summarized in Table 1.

From the table, it can be seen that the most important sources of errors are user clock bias and the impact of the ionospheric delay [21]. The user clock bias can be solved in the receiver for example by the implementation of advanced signal processing and carrier phase measurements [22].

Table 1: Sources of timing errors in GPS.

Source of error	Timing error
User clock bias	10–50 ns
Receiver noise	<1 ns
Residual satellite clock error	<7 ns
Residual of broadcast ephemeris	<7 ns
Residual of tropospheric delay	0.3–2 ns
Residual of ionospheric delay	3–15 ns

2.3. DVB-T SFN Network. The DVB-T standard specifies characteristics of channel coding, modulation, and framing structure for transmission of digital television signals [24]. The Coded Orthogonal Frequency Division Multiplex (COFDM) with a large number of subcarriers is used to transfer video data streams since it delivers robust signal able to deal with complex radio channel conditions affected by signal fading and multipath propagation.

The use of COFDM with guard interval allows a network of DVB-T transmitters to operate in the SFN mode. The SFN operation allows covering an area with signals transmitted from different geographical sites at the same frequency and this way enhances coverage of the area. When the SFN signals, synchronized at both time and frequency domain, are received by the DVB-T receiver, they can be considered to be "echoes" of the same signal if the time delay between signals is shorter than the guard interval of the OFDM signal. On the other hand, when the delay between signals is higher than the guard interval, the received signal will be affected by ISI (Inter Symbol Interference) resulting in noticeable noise in the receiver [25] causing increased bit error rate (BER).

3. Experimental Scenario

Experiments were performed in laboratory conditions. We have used two DVB-T transmitters in a single frequency setup with OFDM modulators being synchronized using GPS receivers. In the experiments, two DVB-T modulators PRO Television TV-05D were used. The main reason for using these modulators was their implementation in a real network operating in Slovakia. Real GPS signals were used in the experiments and one of the GPS receivers was affected by an interference signal, caused either by jamming or by spoofing. The block diagram of the experimental setup is shown in Figure 1.

To gather data from the experimental setup and monitor the achieved results, all devices were connected to the network and managed from a PC (Figure 2). In the SFN, it is important to have transmitters synchronized using, for example, GPS receivers. The transmitted data stream was created using camera and data stream coder and Megaframe Initializing Packet (MIP) inserter to provide MIP information required for synchronization of DVB-T modulators.

Measurements of parameters of DVB-T SFN signal was performed on receiver HD TAB 9 which allows measuring received power strength, bit error rate, modulation error ratio, and visualisation of the received signal characteristics including constellation diagram of the modulated signal, the spectrum of the signal, and delay between signals in SFN network.

In the experiment, the video data was transmitted in the MPEG-2 stream to the MIP inserter since MIP information is crucial for the correct operation of DVB-T/H SFN transmitters. To achieve correct operation of the network, MIP has to be tightly synchronized using 10 MHz frequency normal as well as PPS signals derived from GNSS signals. In the experiment, both 10 MHz and PPS signals were generated in the DVB-T transmitter 1, which was not affected by the interference, that is, jamming and spoofing, of GPS signals.

The PPS signal consists of periodic impulses which are shorter than 1 s and repeat every second. The accuracy of the PPS signals generated by internal clocks of the selected DVB-T transmitters is in the range from 12 ps up to microseconds per second, or 2 ns up to a few milliseconds per day. The accuracy of the signal depends on the resolution and accuracy of the signal generator. An example of the PPS signal is shown in Figure 3.

The web interface of the modulators is shown in Figure 4. It can be seen that the data stream with MIP as well as GPS signals are available, that is, highlighted with green colour. The same settings were applied to the second transmitter. Both transmitters operated at the 490 MHz frequency, which represents the TV23 channel. The DVB-T modulators were operating in 8k IFFT OFDM mode with 64 QAM modulation scheme and 1/8 guard interval. The signal was transmitted from both DVB-T modulators with a power of 0 dBm and attenuated by 7 dB in the inserter. Therefore, the signal should be received with the same amplitude from both DVB-T transmitters.

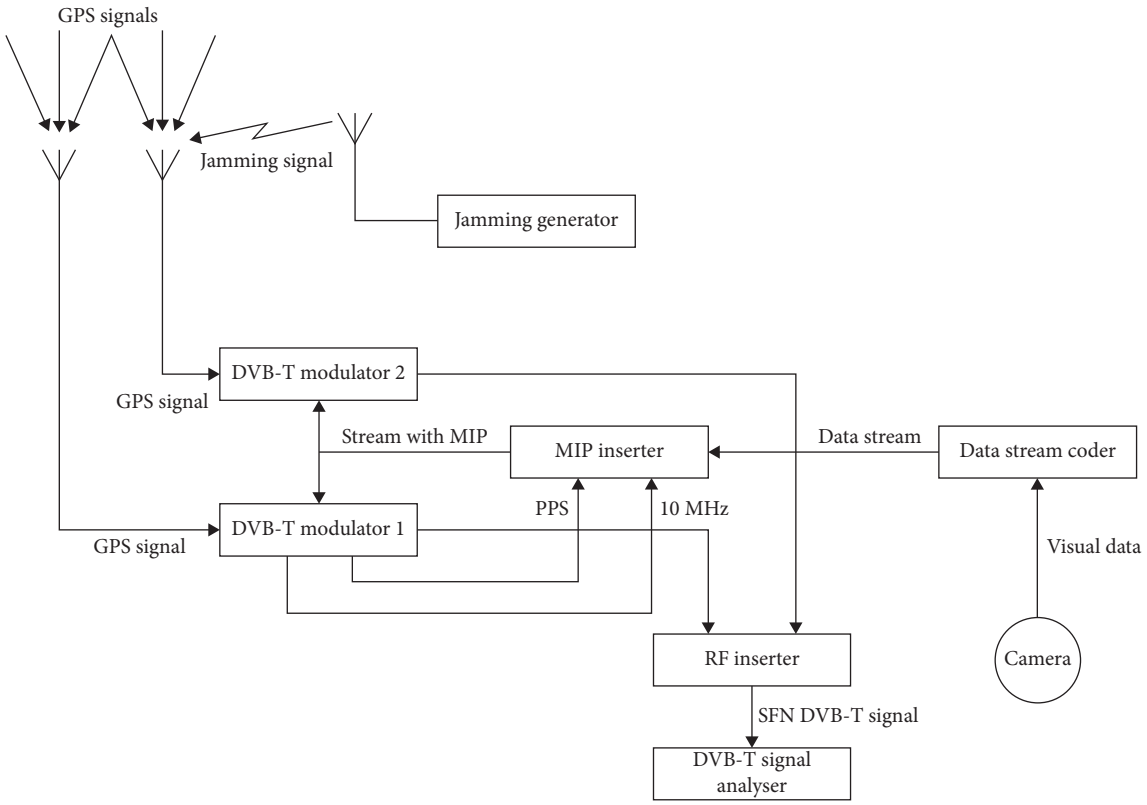


Figure 1: Block diagram of the experimental setup.

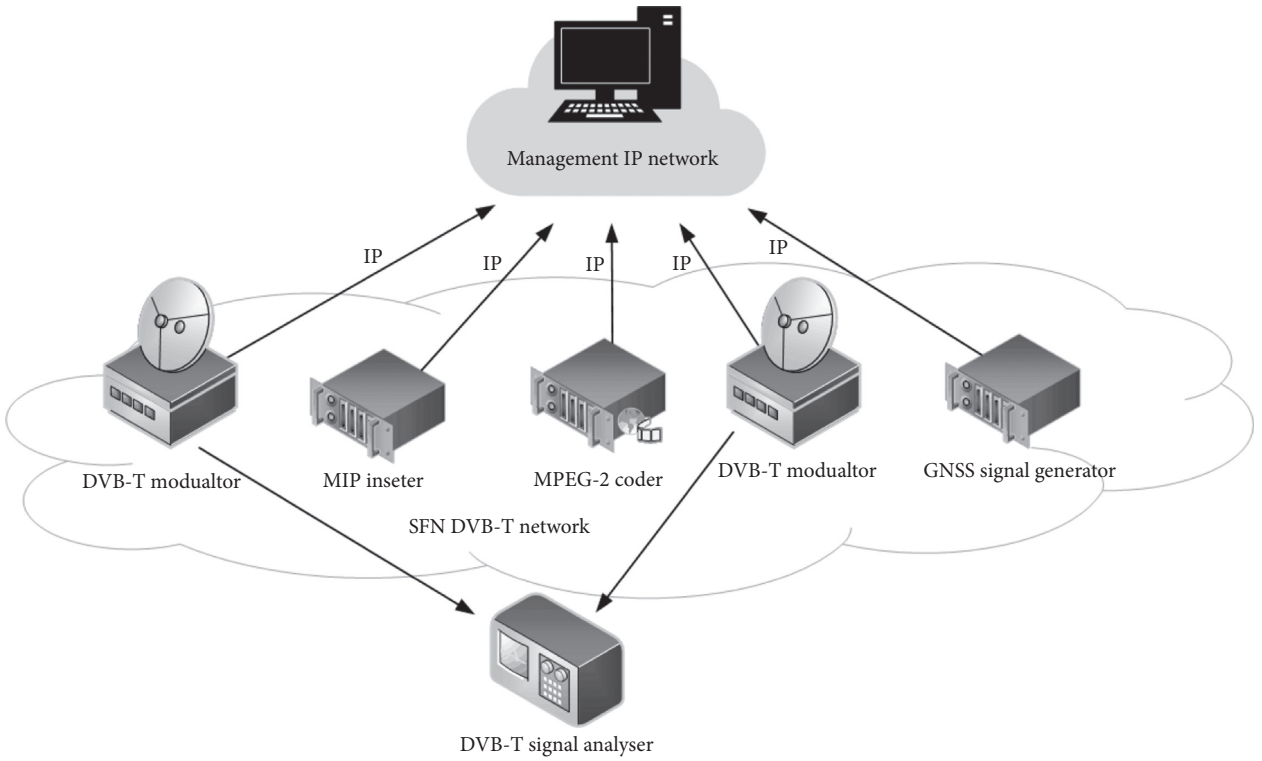


Figure 2: Connection of devices into the management network.

The correct function of SFN was verified at the receiver which was used during the experiments. The values shown in Figure 5 are based on signals received from both transmitters. Without the interference to GPS signals used for synchronization of the second transmitter, the received power is 98.9 dBuV, modulation error ratio is MER >42 dB,

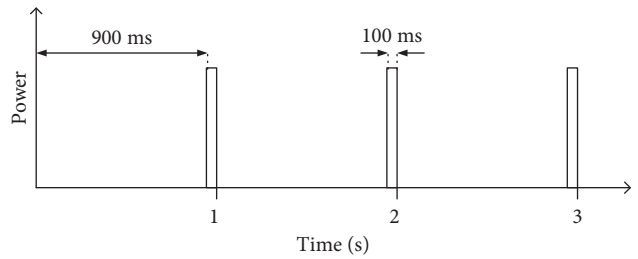
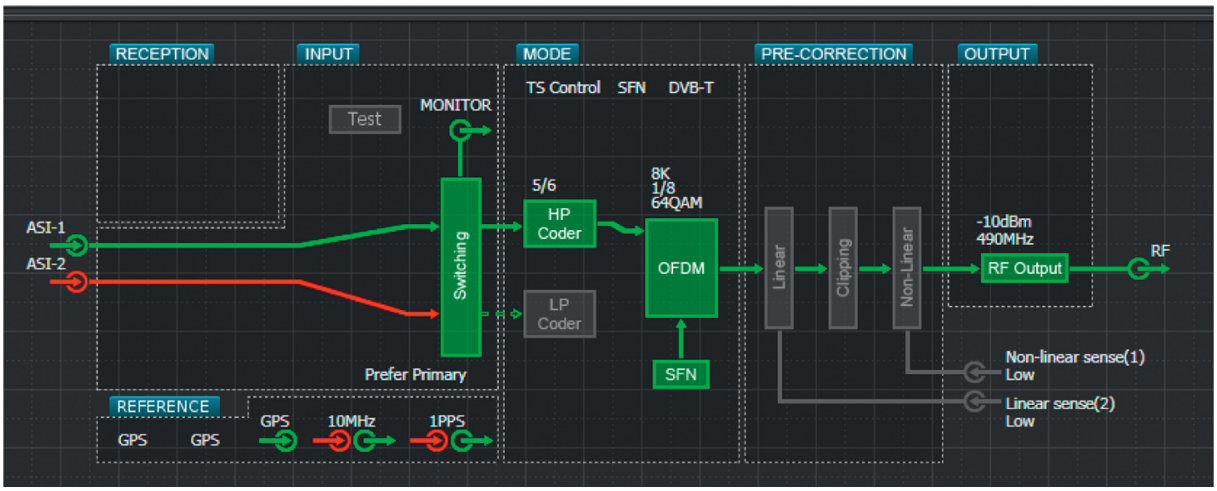
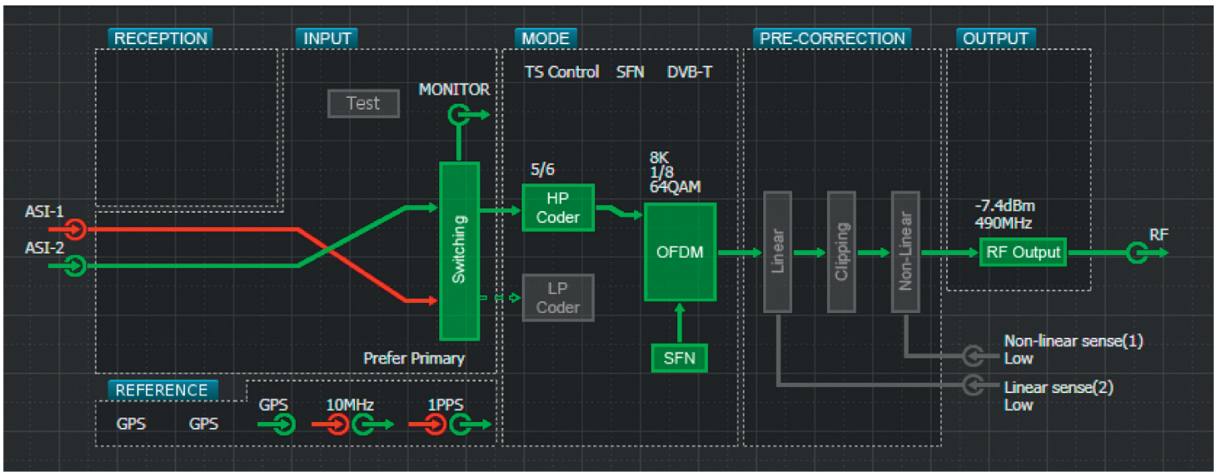


Figure 3: Principle of PPS signal timing.



(a)



(b)

Figure 4: Web interface of DVB-T modulators.

and the bit error rate after decoding and before correction bBER and bit error rate for evaluation of quality aBER are less than $10e-6$ and less than $10-8$, respectively.

In the experiment, we have considered two scenarios for GPS interference. In the first scenario, a simple GPS jammer was used to interfere with GPS signals, while in the second scenario, a GNSS signal generator was used to generate GPS signals and perform a spoofing attack on the GPS receiver used for the synchronization of the second DVB-T transmitter.

In the beginning, the impact of different power levels of the jammer and distance between the jammer and GPS receiver on detection of GPS jamming was tested. The achieved results can be seen in Figure 6. The blue line in the figure highlights the threshold level of the field strength of the jamming signal equal to 0.77 mV/m that will be detected by the GPS receiver and thus cause an outage of the GPS clock synchronization.

From the figure, it can be seen that a jammer with the 1 mW transmit power can affect the receiver up to the distance of

Figure 5: Screenshot from the DVB-T analyser without GPS jamming.

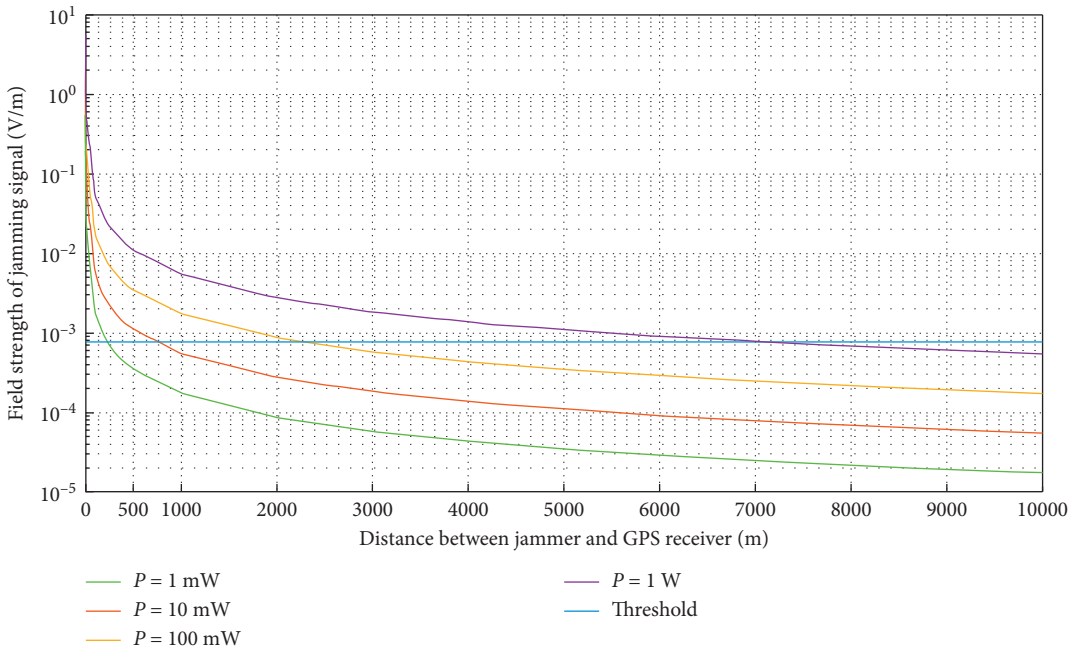


Figure 6: Impact of the power level of jammer and distance between jammer and GPS receiver on detection of GPS jamming.

250 m, while with increasing transmit power, the distance between the jammer and GPS receiver can grow up to more than 7 km in the case when transmitting power of the jammer was 1 W. Therefore, using jammers with high transmit powers can disrupt GPS services in a significant range.

In the first scenario, the jamming signal, depicted in Figure 7, was generated by GPS jammer model DHM3659. The antenna of the GPS jammer was deployed in the proximity of the GPS antenna of the second DVB-T transmitter. The power of the GPS jammer was set to value which caused the loss of GPS signals at the DVB-T transmitter.

In the second scenario, the GNSS simulator Spirent GSS6700 was used instead of a jammer to generate fake

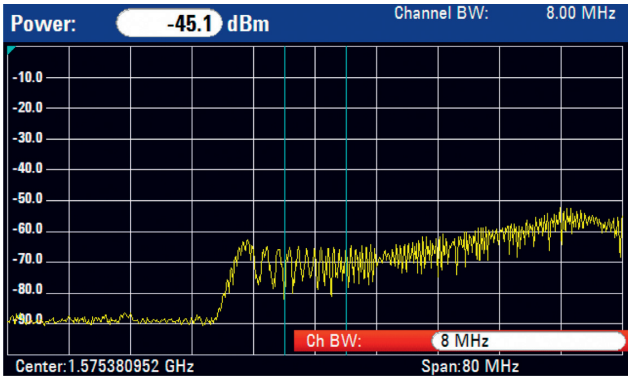


Figure 7: Frequency spectrum of the jamming signal.

signals from GPS satellites. The transmitting antenna was placed 1 m from the GPS antenna of the second DVB-T transmitter, similarly to the first scenario. Parameters of the generated GPS signals were chosen as close to real signals as possible. The GPS satellites were simulated with satellite constellation shown in Figure 8, and GPS simulation time was shifted by 1 minute compared to real GPS clocks; therefore, the constellation of satellites in the simulations was close to the real situation.

In this scenario, the power of the spoofing signals was at the beginning set to value 49 dB below the real GPS signals, the power was gradually increased up to the point when the GPS receiver at the DVB-T transmitter picked up the spoofing signal and used it for synchronization purposes. The spoofing signal was picked by the GPS receiver when the received power of the signal was −127 dBm, which is close to the power of the real GPS signals received from the GPS satellites.

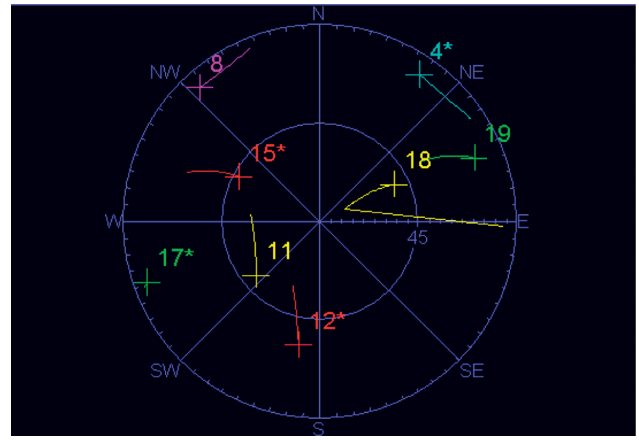


Figure 8: Constellation of GPS satellites used for spoofing purposes.

4. Discussion of Achieved Results

In the first scenario, the GPS signal used to synchronize the second DVB-T transmitter was affected by a jammer. In this case, the DVB-T modulator is able to detect the problem with GPS signals as can be seen from the yellow label next to GPS input in the web interface of the modulator shown in Figure 9. The yellow colour indicates that the status of the GPS receiver is unlocked; therefore, it cannot be used for synchronization of the transmitter.

The measurements of the quality of the received signal were performed over time to evaluate the impact of GPS jamming on the performance of SFN DVB-T. The impact of GPS jamming on signal parameters can be seen in Table 2. Measurements were performed for a 60-minute period after the start of jamming, since the transmitter will automatically shut down after 60 minutes of running on internal clocks only, in order to prevent interference in the network.

From the table, it can be seen that, with increasing time, the SNR, MER, and BER parameters were negatively affected, and the quality of the received signal was decreasing gradually. The fact that signal parameters are better after 60 minutes from the start of jamming is given by the fact that the transmitter affected by GPS jamming automatically muted the transmission which can be seen from Figure 10 where GPS input, as well as the output of the transmitter, is marked with the red colour. This is given by the fact that the transmitter is set up to mute output in case it lost the time synchronization for a certain period of time, in this case, 60 minutes, in order to avoid interferences in the SFN broadcasting.

Figure 11 shows constellation diagrams of the received signals in time 0 (without GPS jamming) after 30 minutes of jamming and after 50 minutes of jamming. It can be seen that modulation symbols were affected by lack of synchronization in the network; however, the resulting signal was still decoded with minimum errors since the SNR of the received signal is well above the threshold [26] required for successful decoding.

From the results achieved during the first experimental scenario, it can be concluded that when the GPS receiver at the DVB-T transmitter is affected by jamming, the transmitter switches automatically to internal synchronization; however, this is not sufficient for operation over a long period of time. The longer the period without external synchronization, the higher is the interference caused by the transmitter in the SFN network. However, the transmitter will automatically mute after a certain period of time, before it will cause significant interference and loss of signal in the area covered by the affected transmitter. Since the loss of GPS signals was reported in the web interface of the DVB-T transmitter, it is relatively easy to detect the problem thru the management network.

In the second scenario, a spoofing attack on the GPS receiver of the second transmitter was performed. In this case, measurements were performed when spoofing signals were below the power level of real GPS signals and when spoofing signals were higher compared to real signals and therefore were picked up by the GPS receiver. The spoofing signal was picked by the GPS receiver when the received power of the signal was −127 dBm.

When spoofing signals were picked up by the DVB-T transmitter, there was not any indication of a problem, synchronization seems to work fine, and the transmitter is broadcasting at full power, as can be seen from Figure 12. However, from the results below, we can conclude that the SFN network is not working properly as can be seen from the results presented in Figure 13.

From Figure 13, it can be seen that the signal is received with the power of 103.7 dBuV; however, there is no image at the output and values of SNR, MER, bBER, and aBER are signalling that there is significant interference in the received signal since bBER is only 10^{-2}.

In Figure 14, a constellation diagram of the received signal is presented; it can be seen that there is a huge noise in the signal and it is not possible to detect symbols of QAM modulation, which is resulting in high BER and lack of image data at the receiver.

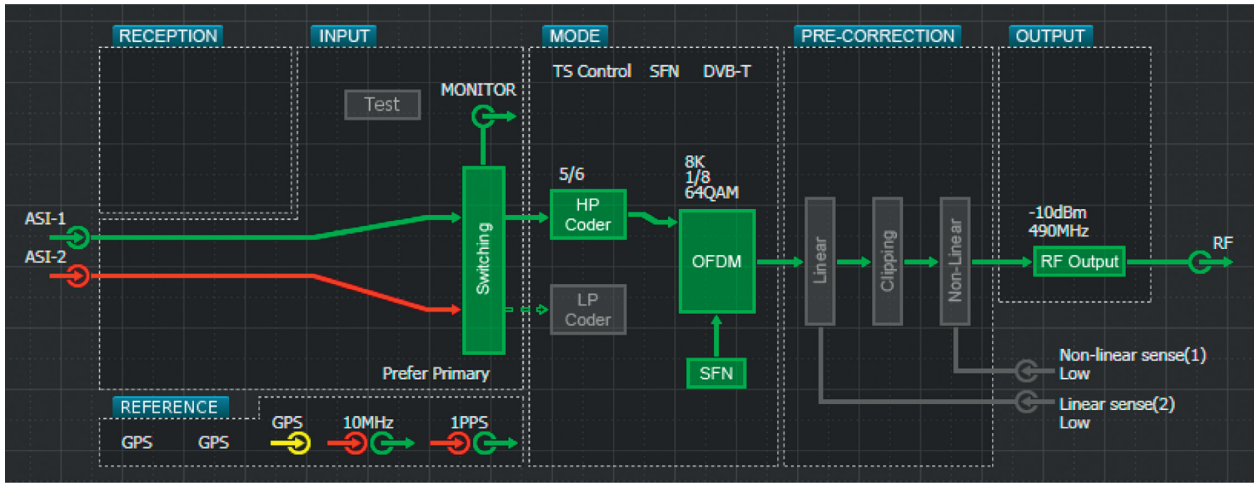


Figure 9: Web interface of DVB-T modulator affected by GPS jamming.

Table 2: Sources of timing errors in GPS.

Signal parameter	Time (minutes)						
	0	5	10	30	40	50	60
Power (dBuV)	98.9	100.2	105.4	99.1	103.2	103.4	101.6
SNR (dB)	>42	34	35	35	33	28	38
MER (dB)	>42	34.3	34.9	35.3	33.1	28.5	37.7
bBER	$<10e-6$	$2e-4$	$2e-4$	$2e-4$	$3e-4$	$6e-4$	$<10e-6$
aBER	$<10e-8$	$<10e-8$	$<10e-8$	$<10e-8$	$<10e-8$	$5e-07$	$<10e-8$

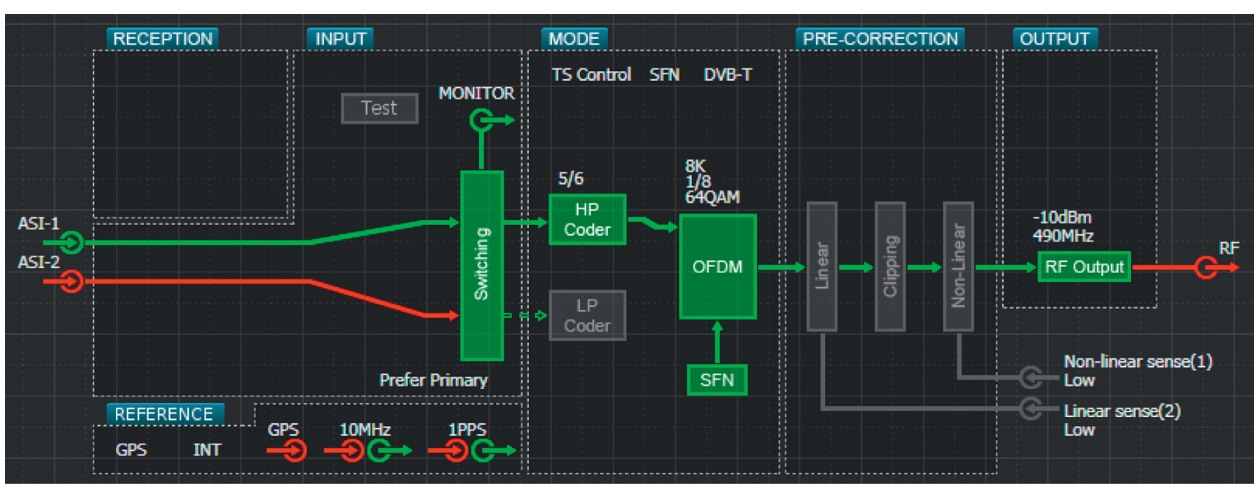
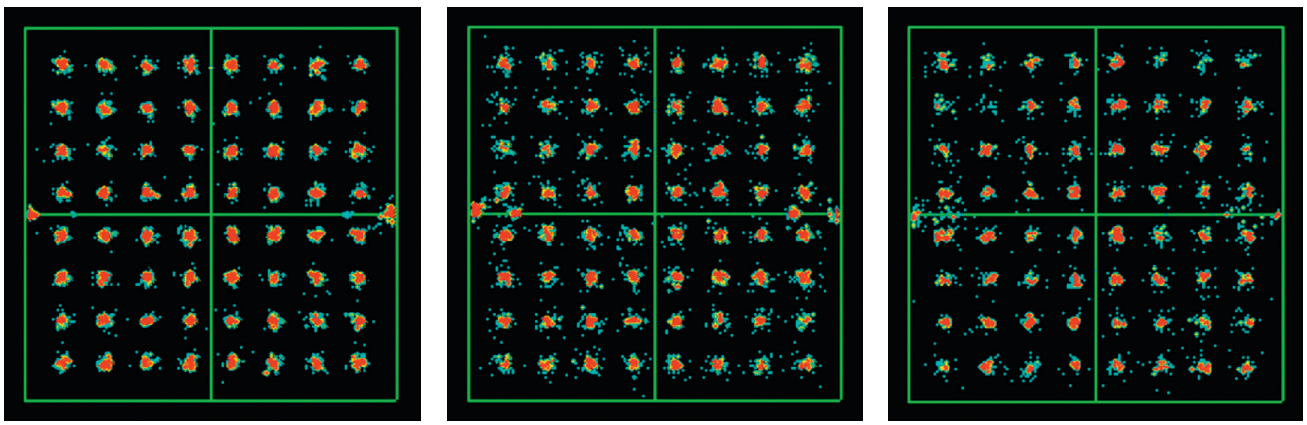


Figure 10: Web interface of DVB-T modulator affected by GPS jamming after 60 minutes.

In Figure 15, the time delays of DVB-T signals from transmitters in the SFN are shown. If delays of individual signals are smaller than the guard interval of the signal, then these signals do not cause intersymbol interference and the SFN network is operating correctly.

However, in the second scenario, the DVB-T transmitter affected by spoofed GPS signal caused interference in the whole SFN network. Moreover, it was not possible to detect this problem from the monitoring and management tools as the affected transmitter was not showing any issues with the synchronization and was showing a correct operation in the management web interface.

To reduce the vulnerability of the DVB-T SFN network to GPS spoofing, some algorithms for spoofing detection and spoofing mitigation should be implemented in the GPS receivers. In order to implement spoofing detection with good performance, a GPS receiver with the support of multiple antennas should be implemented. This would help to estimate the direction of arrival of the GPS signal and thus easily detect the spoofing signal since this signal is usually terrestrial [4]. The advantage of multiple GPS receiver antennas is also a possibility to implement spoofing mitigation solutions based on Multiantenna Beam Forming and Null Steering [27] or Vestigial Signal Detection [28].



(a) (b) (c)

Figure 11: Constellation diagrams of received DVB-T signal (a) without GPS jamming, (b) after 30 of GPS jamming, and (c) 50 minutes of GPS jamming.

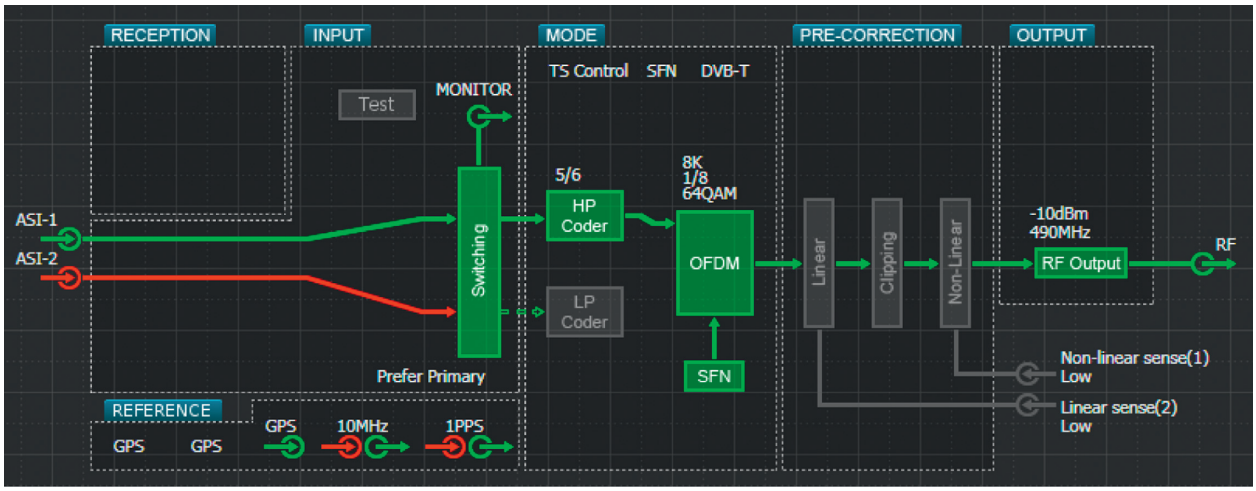


Figure 12: Web interface of DVB-T modulator affected by GPS spoofing.

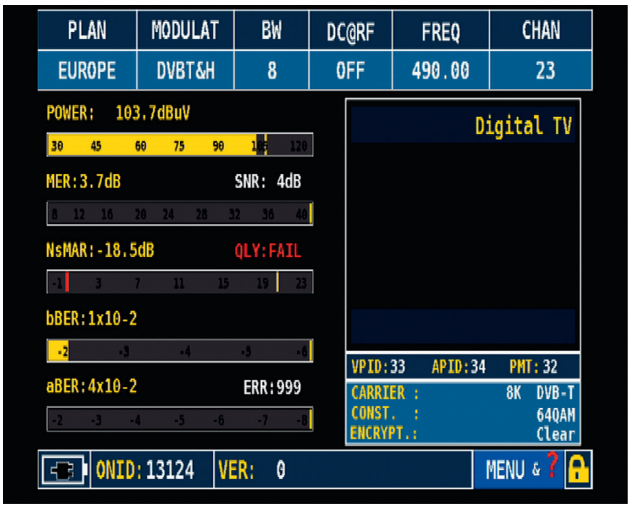


Figure 13: Screenshot from the DVB-T signal analyser with active GPS spoofing.

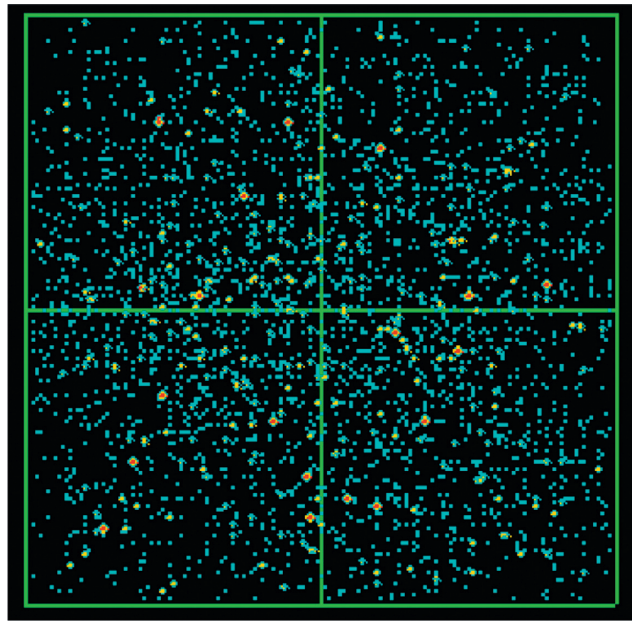


Figure 14: Constellation diagrams of the received DVB-T signal with GPS spoofing.

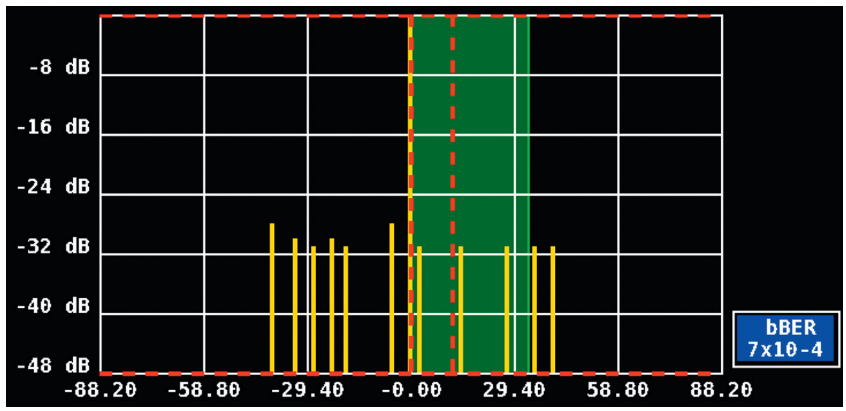


Figure 15: Timeshift of received DVB-T signals during GPS spoofing.

5. Conclusion

In the paper, the impact of the GPS interference caused by jamming and spoofing on the function of the DVB-T SFN network was investigated. The transmitters in DVB-T SFN use GPS signals for synchronization of data in the network, to avoid interference and sustain the quality of received signals. With an increased number of GPS interference caused by jammers, it is required to understand how DVB-T transmitters can cope with the affected GPS signals. We have performed experiments in two scenarios: in the first scenario, the GPS receiver at one of the transmitters was affected by jamming and in the second scenario by spoofing of GPS signals.

Based on achieved results, it can be concluded that the DVB-T SFN network is able to cope with the jamming of GPS signals, in case that it does not last too long. From the results it is obvious that the SNR of the received DVB-T signal was reduced, resulting in increased BER. However, the receiver was still able to decode the video stream without any significant decrease in quality.

Moreover, jamming of the GPS signal used for synchronization of the transmitter could be easily detected thru the management interface. On the other hand, when one of the transmitters was affected by GPS spoofing, the situation was much worse. The transmitter was out of synchronization, which caused that it was not possible to decode the signal at the receiver. On top of that, the management interface of the affected transmitter did not show any errors since the GPS receiver was receiving a spoofing signal which was decoded correctly, although the time information in the signal was tempered.

Data Availability

The data supporting the results are presented in the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the Slovak Vega grant agency, project no. 1/0626/19, "Research of Mobile Objects Localization in IoT Environment" and Operational Program Integrated Infrastructure 2014–2020 of the project: Innovative Solutions for Propulsion, Power and Safety Components of Transport Vehicles, code ITMS 313011V334, cofinanced by the European Regional Development Fund.

References

[1] J. Ristvej, M. Lacinák, and R. Ondrejka, "On smart city and safe city concepts," *Mobile Networks and Applications*, vol. 25, no. 3, pp. 836–845, 2020.

[2] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, "Future trends and current state of smart city concepts: a survey," *IEEE Access*, vol. 8, pp. 86448–86467, 2020.

[3] H. Wen, P. Y. R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '05)*, pp. 1285–1290, Long Beach, CA, USA, September 2005.

[4] C. E. McDowell, "GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling," Rockwell Collins, Cedar Rapids, IA, USA, US Patent 7250903 B1, 2007.

[5] S. C. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts," in *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS'10)*, pp. 708–717, Indian Wells, CA, USA, May 2010.

[6] J. Nielsen, A. Broumandan, and G. Lachapelle, "Spoofing detection and mitigation with a moving handheld receiver," *GPS World*, vol. 21, no. 9, pp. 27–33, 2010.

[7] N. A. White, P. S. Maybeck, and S. L. DeVilbiss, "Detection of interference/jamming and spoofing in a DGPS-aided inertial system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 4, pp. 1208–1217, 1998.

[8] A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attack on a vector based tracking GPS receiver," in *Proceedings of the International Technical Meeting of the Institute of Navigation*, Newport Beach, CA, USA, January 2012.

[9] S. Moshavi, "Multi-user detection for DS-CDMA communications," *IEEE Communications Magazine*, vol. 34, no. 10, pp. 124–136, 1996.

[10] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, Article ID 127072, 16 pages, 2012.

[11] Interface Specification, IS-GPS-200 Rev.D, IRN-200D-001, 7. March 2006.

[12] A. Novák, F. Jůn, F. Škultéty, and A. N. Sedlačková, "Experiment demonstrating the possible impact of GNSS interference on instrument approach on RWY 06 LZZI," *Transportation Research Procedia*, vol. 43, pp. 74–83, 2019.

[13] D. Borio, S. Savasta, and L. L. Presti, "On the DVB-T coexistence with Galileo and GPS systems," in *Proceedings of the 3rd ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC '06), ESA/ESTEC*, pp. 1–13, Integrated Navigation Systems, Noordwijk, The Netherlands, December 2006.

[14] S. S. BeatriceMotella and F. D. DavideMargaria, "A method to assess robustness of GPS C/A code in presence of CW interferences," *International Journal of Navigation and Observation*, vol. 2010, Article ID 294525, 8 pages, 2010.

[15] E. Elezi, G. Cankaya, B. Ali, and S. Yarkan, "The effect of electronic jammers on GPS signals," in *Proceedings of the 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD'19)*, Istanbul, Turkey, March 2019.

[16] R. H. Mitch, "Signal characteristics of civil GPS jammers," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, pp. 1907–1919, Portland, OR, USA, September 2011.

[17] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *Journal of Applied Research and Technology*, vol. 13, no. 1, pp. 45–57, 2015.

[18] H. Puttnies, P. Danielis, A. R. Sharif, and D. Timmermann, "Estimators for time synchronization-survey, analysis, and outlook," *IoT*, vol. 1, no. 2, pp. 398–435, 2020.

[19] P. Vyskocil and J. Sebesta, "Relative timing characteristics of GPS timing modules for time synchronization application," in *Proceedings of the 2009 International Workshop on Satellite and Space Communications*, pp. 230–234, Siena, Italy, September 2009.

[20] W. Liu, H. Yuan, and J. Ge, "Local-area nanosecond-accuracy time synchronisation based on GPS L1 observations," *IET Radar, Sonar & Navigation*, vol. 13, no. 5, pp. 824–829, 2019.

[21] B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, *Global Positioning System: Theory and Applications*, American Institute of Aeronautics andAstronautics, Washington, DC, USA.

[22] Q. Zhu, Z. Zhao, and L. Lin, "Real time estimation of slant path tropospheric delay at very low elevation based on singular ground-based global positioning system station," *IET Radar, Sonar & Navigation*, vol. 7, no. 7, pp. 808–814, 2013.

[23] M. Olynik, "Temporal variability of GPS error sources and their effect on relative positioning accuracy," in *Proceedings of the Institute of Navigation NTM 2002*, San Diego, CA, USA, January 2002.

[24] ETSI EN 300 744 v1.4.1 (2001-01). European Standard (Telecommunications series). Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television. ETSI and EBU, 1/2001.

[25] T. Kratochvil and V. Ricny, "Simulation and experimental testing of the DVB-T broadcasting in the SFN networks," in *Proceedings of the 2008 18th International Conference Radioelektronika*, pp. 1–4, Prague, Czech Republic, April 2008.

[26] ETSI TR 101 290 v1.2.1, "Digital video broadcasting (DVB); measurement guidelines for DVB systems ETSI and EBU, 5/2001," Technical report, 2001–2005, ETSI, Sophia Antipolis, France.

[27] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low complexity gnss spoofing mitigation technique using a double antenna array," *GPS World Magazine*, vol. 22, no. 12, pp. 44–46, 2011.

[28] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: development of a portable gps civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS '08)*, pp. 2314–2325, Savannah, GA, USA, September 2008.