2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) | 978-1-6654-2652-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/UkrMiCo52950.2021.9716665

Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio

Invited Paper

Mahyar TajDini
Dept. of Inform. and Cyber Security
Borys Grinchenko Kyiv University
Kyiv, Ukraine
ORCID: 0000-0001-8875-3362

Volodymyr Sokolov
Dept. of Inform. and Cyber Security
Borys Grinchenko Kyiv University
Kyiv, Ukraine
ORCID: 0000-0002-9349-7946

Pavlo Skladannyi
Dept. of Inform. and Cyber Security
Borys Grinchenko Kyiv University
Kyiv, Ukraine
ORCID: 0000-0002-7775-6039

***Abstract*—This paper discusses the aviation Automatic Dependent Surveillance-Broadcast Vulnerabilities such as Sniffing and Spoofing over it with the help of Software Defined Radio (SDR) by looking at data frame structure and no encryption on this kind of message, we were able to capture 1090 MHz and 978 MHz signals and decoding them and gather all necessary information from it. Then we tried to have visual information by using VirtualRadar and online aviation databases. So we successfully could regenerate and encode messages with our data input and resend them at the same frequency as we captured 1090 MHz. That led us to a spoofing attack, which we could confirm by receiving our own generated messages. And in the end, we had an idea to use Long Short-Term Memory (LSTM) neural network to detect such spoofing attacks.**

Keywords—sniffing, spoofing, ADS-B, Mode S, software-defined radio, SDR.

I. Introduction

Modern aircraft use a Mode S Automatic Dependent Surveillance-Broadcast (ADS-B) transponder, which regularly sends position and altitude information to air-to-ground (air traffic controllers) and air-to-air (other aircraft). Simply ADS-B is a format that works on top of Mode S.

ADS-B supported aircraft using two frequencies to exchange information between each other's, the most popular frequency is 1,090 MHz. Sometimes they use 978 MHz, known as Universal Access Transceiver (UAT). At the same time, 1,090 MHz frequency is associated with Mode A, C, S transponder operation, and in case 1090 MHz equipment integrated with ADS-B functionality extends the transponder messages, known as Extended Squitter messages. It's referred to as 1090ES, and generally, aircraft as operators flying above 18,000 ft (~5.5 km, counted as Class A airspace) are required to have 1090ES equipment, and the rest which passes under 18,000 ft may have UAT or 1090ES equipment.

The paper is structured as follows. Section II gives an overview of related works. Section III Data Retrieval method and formats. Sections IV Comparing Downlink Format and Section V showing Sniffing Method on ADS-B. Section VI ads-b attack approach and Section VII talks about the ADS-B sniffing process, Section VIII spoofing results, Section IX spoofing detection methods, and finally Section X conclusions and future work.

II. Related Works

We have already covered spoofing on mobile networks [1] using SDR in previous publications [2, 3]. By looking at other research similar to our topic, we can mention a paper [4] by Daniel Howell and Jennifer King that showed that ADS-B usage in General Aviation influences the overall rate of aviation accidents. However, it is considered that the data are too sparse for the results to be statistically significant in assessing the impact on the index.

ICAO summarized the potential security problems associated with open systems such as ADSB and concluded that "distributing encryption keys to a large number of ADSB receivers can be problematic and a solution will not be helpful in the short and medium-term." Deployed all over the world. If the ground station is a passive receiver, internet-based encryption strategies are not applicable [5].

In another scientific paper shows possible authentication strategies without encryption in the protocol. They come with their solution called ADSBT ("T" for timestamp), which considers the signal propagation and internal hardware time delay when examining incoming ADSB packets. Suppose the disconnect time must be accurate for multiple frames, making it more difficult for an attacker to spoof the message. If a discrepancy is found, the message will be rejected [6].

ADSB is just a tiny piece of the aviation and cybersecurity puzzle. In an article on assessing security vulnerabilities in aviation systems, the authors discuss the importance of increasing cybersecurity research as the attack surface of cyber-physical computer systems increases due to technological advances in recent decades. They present their rating system for wired and wireless networks and techniques that may exist on board. Modern airliners have complex and integrated systems that create a larger attack surface, such as in-flight, aviation information, and entertainment. The researchers concluded that these services offer many significant benefits to the aviation industry and have disadvantages in introducing new security threats [7].

III. Data Retrieval Method

ADS-B can improve surveillance for the air-to-air and air-to-ground even and primarily where radars don't function like it's prohibited or not practical. Each ADS-B aircraft is programmed at installation with a unique International Civil Aviation Organization (ICAO) address that is 24 bit and broadcast by ADS-B equipment. Multiple aircraft informed with the same ICAO address while the ADS-B network may not track the targets correctly. As a result, the target loses full tracking sight on one or both targets.

ADS-B-equipped aircraft on the UAT data link has a function that allows broadcasting an anonymous 24-bit ICAO

address. The UAT system creates a random address that does not match the actual ICAO address already assigned to the aircraft by getting to this mode. The 24-bit anonymous address of the UAT can only be used in cases in which the operator has not submitted an Instrument Flight Rules flight plan and does not request Air Traffic Control (ATC) services. In anonymous mode, the aircraft beacon code should be set to 1,200, and depending on the manufacturer's implementation, the aircraft's FLT-ID may not be transmitted at all.

ADS-B equipment broadcast a lot of helpful information like GPS location, ground speed, altitude, and much more almost every single second, a random time between 0.8 to 1.2 seconds [8, Parag. 3.1.2.8.5.2], and compared to radar technology that sweeps for position between 5 to 12 seconds, ADS-B is much more reliable, faster, and gives more precise information to another ADS-B enabled equipment or ground station. And as mentioned before, radars in the mountains and between other types of solid objects may not work correctly and need a tower and other equipment installed at the place, while ADS-B are mode adaptive and smaller stations can capture them.

ADS-B information usually shows in cockpit weather display in graphical format or textbase. Anyway, according to the Federal Aviation Administration reference Aeronautical Information Manual, there are three forms of ADS-B in surveillance [9, ch. 4, sect. 5]. And there is one more piece of the puzzle, Traffic Information Service-Broadcast, broadcasting from a ground station to every ADS-B equipment regardless of whether it uses 1090ES or UAT data link.

Each ADS-B frame contains 112 bits of information in five sections:

DF	**CA**	**ICAO**	**ME**	**PI**
5 bit	3 bit	24 bit	56 bit	24 bit

IV. Downlink Format Comparison

There are different downlink formats for other purposes. For example, DF17 is used for 1090 Extended Squitter as for ADS-B. Nowadays, for civil aviation, these downlink formats, DF0, DF4, DF5, DF11, DF16, DF20, DF21, DF24, are in use. And there, we have got the format DF0 which provides information about Airborne Collision Avoidance System (ACAS). And replies with ACAS can be responses to ACAS or Traffic Alert and Collision Avoidance System (TACAS). For Long Air-to-Air ACAS or TACAS, aircraft use DF16, and DF4 is designed to respond to a ground station.

The message field is set to 56 bits of 112-bit frame length, but by using DF24, message length can extend to 80 bits. DF24 is known as Extended Length Message (ELM). DF22 is unique for military use only (see Table I) [10].

TABLE I. Downlink Format and Contents

Format	**Content**
DF0	Short Air-to-Air ACAS
DF4	Surveillance (roll call) Altitude
DF5	Surveillance (roll call) IDENT Reply
DF11	Mode S. Only All-Call Reply (Acq. Squitter if II=0)
DF16	Long Air-to-Air ACAS
DF17	1090 Extended Squitter
DF18	1090 Extended Squitter, Supplementary
DF19	Military Extended Squitter
DF20, DF21	Comm. B. Altitude, IDENT Reply
DF22	Military Use Only
DF24	Comm. D. ELM

The second field called capability, which is just 3 bit and it has eight different variants, 0 is set to level one Transponders, 1 to 3 are Reserved, four is set to Level 2 Transponders which are capable of developing Transponder Capability (CA) to 7 on the ground, five is set to Level 2 Transponders which are capable of setting CA to 7 for airborne, 6 is a combination of 4 and 5, which means this is also for level 2 transponders but with the ability of set CA to 7 for both on-ground and airborne and finally 7 shows the downlink request set to 0 or flight status indicates between 2 to 5 for both on-ground or airborne.

The following field is the ICAO address, a standard 24bit address assigned by ICAO regulations, and it does not change till the last day of that aircraft working. Still, it has two exceptions. As usual, military usages are the exception, and they can reprogram and change it. Still, according to FFA privacy, this ICAO Address can be reprogrammed for private aircraft.

V. Sniffing on ADS-B

And message field, which usually is 56 bit, starts with the first 5 bits as message type code; as we can see here, "a6ab00f4ccfbea76792aa92a4391" is an example of content in the message field. If we convert this hex to bits, we will get something like

"10100110101010110000000011110100110011001111101111101010011101100111100100101010101010010010101000100001110010001,"

and the first 5 bits are 10101, which is equivalent to decimal value 21. The message type code 20 to 22 indicates the airborne position (w/GNSS Height), and if this code would be identical to message type, code 19 indicates airborne velocities. In another example, "84524f299ade215028a 7b7e2ca7e," the first 5 bits of the message field in decimal is equal to 10, which demonstrates the airborne position (w/Baro Altitude). Fig. 1 captured the ADS-B frame, showing some of the ADS-B frames which we captured.

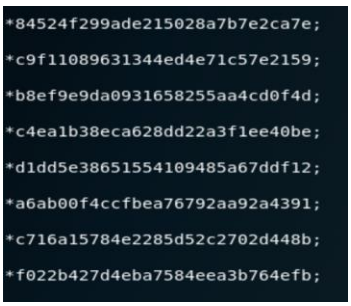

Fig. 1. Captured ADS-B Frame.

And if we want to make all these easier, we can use pyModeS library (in Python v. 3), and we get decodes the frame and get helpful information from it as in Fig. 2, we decided our first example. And it has shown it was a DF20 message which captured and should show the altitude as it shows 380 ft (~116 m).

```
>>> import pyModeS as modes
>>> modes.tell("a6ab00f4ccfbea76792aa92a4391")
           Message: a6ab00f4ccfbea76792aa92a4391
      ICAO address: 000000
    Downlink Format: 20
          Protocol: Mode-S Comm-B altitude reply
          Altitude: 380 feet
               BDS: None
```

Fig. 2. Decoding ADS-B frame in Python.

VI. ADS-B Attack Approach

Since ADS-B messages are not encrypted, from an attacker's point-of-view, much more accessible, we can perform different types of attacks on ADS-B in and out both sides. If there were some level of encryption still, we would be able to have a more sophisticated plan. In this paper, we want to focus on two principal vulnerabilities and show it's possible to take advantage of them.

1. Sniffing as a passive kind of attack.

2. Jamming, inject into replies/spoofing as active kind of attacks.

VII. ADS-B Sniffing Approach

Using dump1090 [11], we can create a network connection by default on port 30003 to feed other applications to process the data captured by BladeRF. We decided to use VirtualRadar as freeware to map captured data to ICAO databases and visualize ADS-B Messages information. As shown in Fig. 3, under the options menu, we can define a receiver and set how to find the data feed. In this example, we ran our dump1090 on a Kali Linux with IP address 192.168.0.121 and mentioned before on default port 30003.

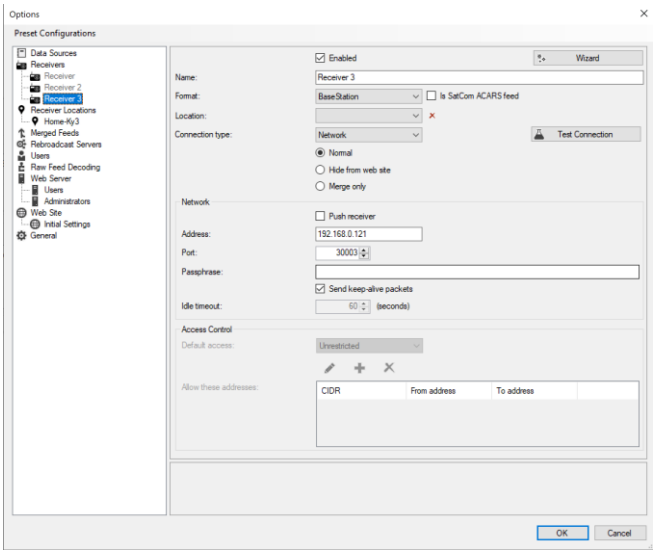

Fig. 3. VirtualRadar receiver settings.

We also run gr_air_modes, as shown in Fig. 4, we decode ADS-B Messages. Here in this figure, we can see a different type of message, for example, type 21.

So, at this point, we have our sniffing lab, and we can capture ADS-B frames and decode them. Also, we can visualize the result in VirtualRadar and have a graphical view of the map and aircraft information.

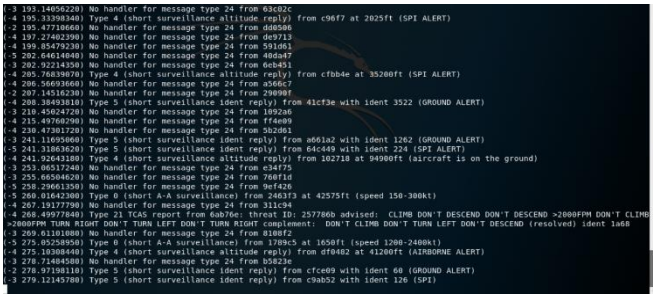

Fig. 4. gr_air_modes decoded ADS-B messages.

To encode or decode position in ADS-B Protocol, the Compact Position Reporting (CPR) Algorithm by checking bit 51 in the frame F of data that can be 0 or 1 representing the frame is even or odd find out the Latitude and Longitude. Without CPR, the accuracy could differ even more than 300 m. CPR merging F frame with 17th bit of every latitude/longitude and with this method have better accuracy to 5 m or even better.

Controller Pilot Data Link Communications(CPDLC) has two known formats: Aeronautical Telecommunication Network (ATN-B1) and Future Air Navigation System (FANS-1/A). Still, despite what the name shows now, it's old and used worldwide, and that's the only format that can be used for all aviation radio with Aircraft Communication Addressing and Reporting System (ACARS) capability. This experiment focuses more on FANS-1/A to have an encoding/decoding method for ADS-B and FANS-1/A.

ACARS Address	Imbedded Message Identifier (IMI)	Aircraft Registration Number	Byte String	Cyclic Redundancy Check (CRC)

There are two categories of messages in CPDLC carried between aircraft and ATC equipment, known as UP-LINK MESSAGES (uM), ground to Air Messages, and Downlink Message (dM) for air to ground messages.

Since there are a lot of online sources about CPDLC, FANS-1/A, ADS-B, we decided not to include them in this research and focus more on the operation part by focusing on how this kind of attack works and can be performed in real-world. By looking at Fig. 5, we can see how a sniffing attack works in our scenario and which devices and tools were used to capture and decode the ADS-B for our experiment.

Fig. 5. Sniffing ADS-B flowgraph.

To generate a file with encoded ADS-B message, we used ADSB_Encode.py with a syntax like the following lines to generate a file as "FILENAME"

ADSB_Encode.py "ICAO" "LATITUDE" "LONGITUDE" "ALTITUDE" "FILENAME"

As an example, for ICAO ID 508EEE and latitude 48.978, longitude 30.975 with altitude 967 and creating an "iq8s" file aligned with the size of the buffer as 256 Kb, shown below:

python ADSB_Encoder.py 0x508eee 48.978 30.975 967.0 sampleTest01

dd if=sampleTest01.iq8s of=sampleTest01_256K.iq8s bs=4k seek=63

Now that output with HackRF can be transmitted over 1090 MHz and 2 Mhz sample rate like below:

hackrf_transfer -t sampleTest01.iq8s -f 1090000000 -s 2000000 -x 47 -R

Which flags -x for Gain in dB and -R to recursive signal is used. And again, in another hand side with dump1090, we can capture our self-generated signal as shown below.

./dump1090 --interactive --net --freq 1090000000

Now we have another goal to create a FANS-1/A message described in ARINC622 Data Communication [12]. Since its syntax is complicated, we were using "ASN.1 Studio" to generate ASN.1 encoded or decoding without additional coding and then passing to a Packed Encoding Rules (PER) Encoder and create a byte string as PER encoded as the message for FANS-1/A. as previously mentioned in this paper, there should be a CRC for FANS-1/A which calculated by IMI and aircraft Registration ID, and PER encoded Message. To generate this CRC, we were using an open-source library called "libacars."

After generating all these, it's time to transmit them, and in this paper, as shown in Fig. 6, HackRF is connected to an Antenna used to send FANS-1/A messages. Since we got everything ready and had an output file from the previous step, we could utilize it in GNU Radio.

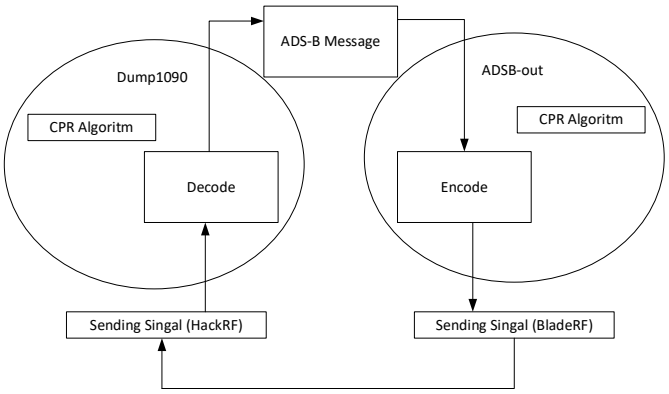

Fig. 6. ADB-B implementation.

As shown in Fig. 7, a GMSK mod component converted bytes into signals, and that complex signal was sent to be transferred with HackRF.

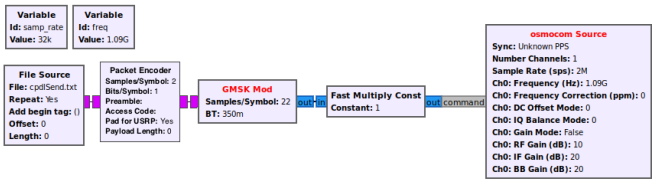

Fig. 7. gr_air_modes decoded ADS-B messages.

In this experiment, since we take care of regulation and do all these in a laboratory environment with our antenna, we could transfer signals maximum of up to 50 m.

VIII. Spoofing Results

In conclusion, we could show that ADS-B and Air traffic control systems are vulnerable to Spoofing and Sniffing attacks, which could be dangerous in the real world. And since it's possible to spoof GPS signals, this combination is likely to confuse aircraft about other aircraft and even send wrong alerts, leading them into a more significant danger and even a crash. And the things which make it scarry that with a grand station or with a movable and portable drone or attacked to another aircraft all these are possible because having all required devices together for both kinds of attacks are less than a kilogram and small as a candy box. Around two years ago, on a flight we had been I just tried to sniff on the aircraft's signal we were sitting inside, and I could get as shown in Fig. 8.

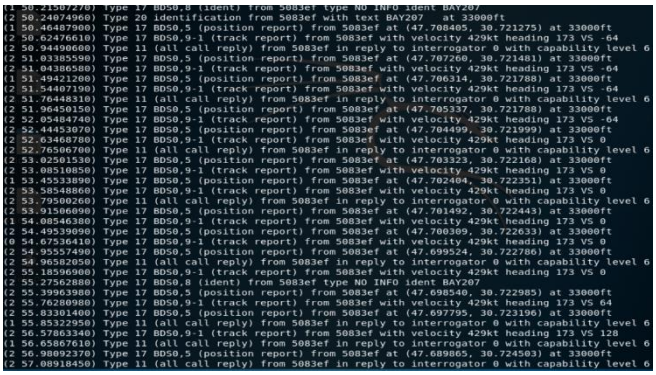

Fig. 8. Sniffing against BAY207.

That aircraft has ICAO ID 5083EF, and the flight number was BAY207. We can find that it was a Boing-737; as Fig. 9 shows, it is registered for Ukraine [13]. And at the moment I was sniffing on ADS-B Signals, we had 429 kt equivalent to almost 794 km/h speed and an Altitude of 33,000 ft (~10 km), nearly 10 km far from the earth. And you can see a bunch of Type 17 and type 11 messages I could receive. And that's the dangerous point in the middle of nowhere and has no access to data sources. A transmitter could perform a spoofing attack, and of course, according to protocols, pilot and aircraft would react based on the data they would receive in their panel.

Fig. 9. 5083EF aircraft information.

IX. Spoofing Detection Methods

These methods have some problems, such as low computing efficiency, difficulty in equipment upgrading, and limited application scenarios [14]. With the help of LSTM neural network, we can collect different ADS-B data and by having LSTM based neural network for prediction, measure their threshold, and calculate residuals of predicted values and actual values, when we see any point more than the actual value, this is a fake signal [15]. But first, we need to preprocess data and then train the model and have feature extraction related to aircraft ADS-B messages, including longitude, latitude, heading, speed, and climb rate, and sort it based on aircraft information ICAO. As Fig. 10 shows on that example threshold line after scoring was standing around 100 while we can see some spikes between 250–400, and this shows those serial numbers, which means each of them to belong to different ICAO are spoofed are fake. As [16] in their research, using recurrent neural networks based on LSTM for anomaly detection works well and in such cases could be a solution.

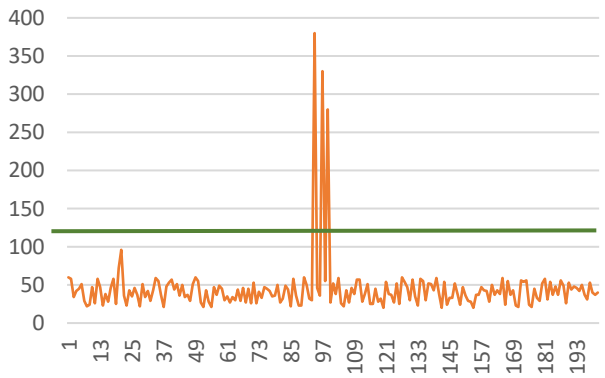

Fig. 10. Abnormal score.

X. Conclusions and Future Work

This paper shows different vulnerabilities in the aviation system, mainly focusing on Sniffing and spoofing ADS-B messages. And shows the current system needs an update, and protocols need to change at least a little to be more secure; otherwise, with newer technologies, we can wait for more aviation incidents.

In future work, we may publish how it's possible to detect and prevent such attacks. While nowadays aircraft are not equipped to detect these attacks, most likely aircraft are so old. For instance, according to reports [17], the average age for Ukrainian planes is around 23 years. Of course, we cannot expect they can detect spoofing against their ADS-B, and that's the challenge because the technology itself needs to review again, updated, and maybe have a rule on an international flight to have new devices based on the new standard. But as we researched detection based on noise and signals by measuring them, maybe in future work, we publish how it's possible to detect it, and then it would be possible by some integration prevent it too.

Also, we are working on a new method to detect such kind attacks faster and more reliable at the same time cheaper and easier to implement. And we will publish more technical details about how possible to use machine learning to train the machine and detect spoofing attacks on ADS-B. Using a double-stage layer deep neural network and classifying messages and aircraft, we expect more than 90% accuracy on detection and less than 0.5% having False Positive, which could be a very efficient result compared to current methods.

References

[1] V. Buriachok, V. Sokolov, and M. TajDini, "Research of Caller ID Spoofing Launch, Detection, and Defense," Cybersecurity: Education, Science, Technique, vol. 3, no. 7, pp. 6–16, 2020. DOI: 10.28925/2663-4023.2020.7.616.

[2] M. TajDini, V. Sokolov, and V. Buriachok, "Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio," SSRN Electronic Journal, pp. 287–296, 2019. DOI: 10.2139/ssrn.3455453

[3] M. Taj Dini and V. Sokolov, "Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio," Modern Information Protection, vol. 1, pp. 82–89, 2018.

[4] D. Howell and J. King, "Measured Impact of ADS-B In Applications on General Aviation and Air Taxi Accident Rates," 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), Sep. 2019. DOI: 10.1109/dasc43569.2019.9081643.

[5] ICAO (2018, Jul.). ADS-B implementation and operations guidance document. [Online]. Available: https://www.icao.int/APAC/Documents/edocs/AIGD%20Edition%2011.pdf.

[6] Y. Kim, J.-Y. Jo, and S. Lee, "ADS-B vulnerabilities and a security solution with a timestamp," IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 11, pp. 52–61, Nov. 2017. DOI: 10.1109/MAES.2018.160234.

[7] S. A. P. Kumar and B. Xu, "Vulnerability Assessment for Security in Aviation Cyber-Physical Systems," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), Jun. 2017. DOI: 10.1109/CSCloud.2017.17.

[8] International Civil Aviation Organization (2014, Jul.). Aeronautical Telecommunications Surveillance and Collision Avoidance Systems. Annex 10 to the Convention on International Civil Aviation, Vol. IV. [Online]. Available: https://www.spilve.lv/library/law/Annex%2010%20Volume%20IV.pdf

[9] U. S. Department of Transportation, Federal Aviation Administration, Aeronautical Information Manual Official Guide to Basic Flight Information and ATC Procedures (2017, Oct.). [Online]. Available: https://www.faa.gov/air_traffic/publications/media/aim.pdf.

[10] RTCA Inc., "Proposed Change to DO-181D and ED-73C for Higher Squitter Rates at Lower Power," Special Committee 209 ATCRBS / Mode S Transponder MOPS Maintenance, Apr. 2007.

[11] dump1090-fa Debian/Raspbian packages (2021, Aug.). [Online]. Available: https://github.com/flightaware/dump1090.

[12] RTCA SC-189/EUROCAE WG-53 (1998, Nov.). [Online]. Available: http://www.asas-tn.org/library/standardisationsbodies/eurocae/g1-019.pdf.

[13] ADS-B Exchange (2021, Oct.). [Online]. Available: https://globe.adsbexchange.com.

[14] S. Wang, J. Wang, C. Su, and X. Ma, "Intelligent Detection Algorithm Against UAVs' GPS Spoofing Attack," 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), pp. 382–389, 2020. DOI: 10.1109/icpads51040.2020.00058.

[15] J. Wang, Y. Zou, and J. Ding, "ADS-B Spoofing Attack Detection Method based on LSTM," EURASIP Journal on Wireless Communications and Networking, vol. 2020, no. 1, Aug. 2020. DOI: 10.1186/s13638-020-01756-8.

[16] R. Calvo-Palomino, A. Bhattacharya, G. Bovet, and D. Giustiniano, "Short: LSTM-based GNSS Spoofing Detection Using Low-cost Spectrum Sensors," 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Aug. 2020. DOI: 10.1109/wowmom49955.2020.00055.

[17] M. Mamayeva, The average age of aircraft in Ukraine is 23 years—the State Aviation Service [Seredniy vik litakiv v Ukrayini stanovyt 23 roky—Derzhaviasluzhba] (2018, Dec.). [Online]. Available: https://www.unn.com.ua/uk/exclusive/1770081-seredniy-vik-litakiv-v-ukrayini-stanovit-23-roki-derzhaviasluzhba. (In Ukrainian).