EPiC Series in Computing

Volume 67, 2019, Pages 97–108

Proceedings of the 7th OpenSky Workshop 2019

Detecting GPS Jamming Incidents in OpenSky Data

Ala' Darabseh, Evangelos Bitsikas, and Brice Tedongmo

New York University Abu Dhabi, UAE
afd8,eb173,bdt2@nyu.edu

Abstract

GPS is used widely to determine the location of objects across the world. Getting an accurate position is a must, however, jamming signals can adversely affect the precision of received GPS signals. Thus, countermeasures are required to detect such attacks. In this paper, a new GPS jamming detection scheme is proposed to explore real-world GPS jamming incidents on air traffic data. The approach utilizes and investigates on the Automatic Dependent Surveillance-Broadcast (ADS-B) data from OpenSky receivers to detect the jamming attacks. To our knowledge, this work is the first to address GPS jamming detection based on ADS-B quality metrics. The core idea behind this scheme is based on observing the distribution of received data from aircraft under normal situation and use it later to check if there is a jamming attack. More precisely, we consider the Navigation Accuracy Category for position (NACp) parameter, whose value ranges from 0 to 15 and is indicative of the aircraft's Estimated Position Uncertainty (EPU), as a basis to build the distribution of normal traffic across all NACp categories. In addition, we build the distribution of NaNs values of received location from aircraft for all covered OpenSky receivers at a specific location. Lastly, the distribution for each aircraft at this location is also observed and analyzed. After that, we evaluate the proposed approach by using real incidents to check its effectiveness.

1 Introduction

Automatic Dependent Surveillance-Broadcast (ADS-B) is considered consequential in modern aviation. It is an important part of the Next Generation Air Transportation that will be mandatory for all aircraft in Europe and U.S.A. by 2020 according to FAA. The main benefits of ADS-B are easily noticeable. First, it dramatically improves the situational awareness and control of the pilots, since they have access to real-time traffic information. Second, the aircraft determine their position and the position of others without relying on external mechanisms and procedures. Finally, it provides a solid coordinates resolution which will lead to air-traffic optimizations in terms of use.

In ADS-B each aircraft obtains its coordinates from the global navigation satellites. Then, by using the ADS-B avionics transmits the ADS-B messages to the ground-based receivers over the 1090MHz band. These messages contain important information related to the aircraft; coordinates, velocity, a unique identifier (ICAO) and other ATC related data, which will be assessed by the ADS-B sensors on the ground. However, these messages are broadcasted unencrypted and unsigned through the airspace, giving the change to possible attackers to exploit

their weaknesses. As a matter of fact, multifarious attacks exist against ADS-B. For instance, eavesdropping, spoofing attacks, message modifications attacks, message injection attacks and jamming attacks are discussed extensively in the literature. The attacker's main objective is to cause confusion or damage to the aircraft and to the ground-based systems.

In this paper, we focus on ADS-B jamming attacks discussing how these attacks can be detected on the application layer. Traditional (reactive) jamming detection methodologies in the literature rely on evaluations of the Packet Delivery Ratio PDR [42]. On the other hand, we present numerous GPS jamming detection schemes to explore real-world GPS jamming incidents on air traffic data. All approaches discussed are based on using ADS-B [33] data from OpenSky [44] receivers. More specifically, one of the approaches is to analyse the distribution of the NACp indicator over a long observation period to uncover patterns within the normalized instantaneous count of messages with either 'good' or 'bad' NACp received by each sensor. To our knowledge this work is the first to investigate GPS jamming detection based on ADS-B quality metrics. The other proposed approach is also to analyse the patterns of the NULL values in ADS-B, sent by the aircraft. Of course, the above metrics can be combined taking into consideration all the sensors' results to bolster our accuracy.

Therefore, in this work we make the following contributions:

- First, we gather all available real GPS jamming incidents from several blogs/reports/news from past years, and we order them in a table with some related information.
- Then, we propose an approach to detect GPS jamming attacks in aviation network using the navigation accuracy information by observing the pattern of such information. Also, we show how OpenSky network data can be used as a tool to figure such type of attacks.
- Lastly, we propose another approach to detect such attacks by analyzing the pattern of NULL values in OpenSky data for each senor on ground.

1.1 Problem Statement

Jamming GPS signals is a Denial-of-Service (DoS) type attack and can cause erroneous navigation system information, which may result in aircraft being grounded, delayed or misled. The jamming incident at the Nantes Atlantique airport two years ago was no exception to this [18]. If aircraft are affected during a flight, these errors can build up quickly and as a consequence, they will affect the performance of the system and even its safety. The fact that there is a wide variety of jamming attacks that can utilized by an attacker to damage the communications necessitates a robust detection scheme which will take into account different metrics/features of the traffic and analyse them.

We address this problem of GPS jamming event detection from a single or multiple static and/or moving sources based on ADS-B-Out messages received by ground sensors. As mentioned previously, we focus on the application layer characteristics to solve the problem. Specifically, we try to determine suspicious ADS-B traffic for each aircraft based on their history of transmissions. These transmissions indeed create a pattern that can be investigated, therefore any newly received transmission that deviates from normal can be rendered suspicious. The application layer metrics that we use to unearth potential anomalies are the frequency of NACp values and NULL values. We can determine jamming attacks using the distributions of these two metrics and comparing them with the received frequency values.

2 Preliminaries

2.1 ADS-B System

ADS-B is a new Air Traffic Control (ATC) surveillance technology. It is part of the Next Generation Air Transportation System (NextGen) plan as launched by the American Federal Aviation administration (FAA) as a replacement of the radar systems. It operates at 1030 MHz for the active interrogation and 1090 MHz for the active response or normal broadcasts. Furthermore, according to the ADS-B data link standards, ADS-B's frequencies for the extended Squitter is 1090MHz and for Universal Access Transceiver is 987 MHz. In ADS-B system architecture there can a receiver, refereed as ADS-B IN and a transmitter, refereed as ADS-B OUT. Normally, all aircraft are considered broadcast transmitters equipped with ADS-B OUT hardware.

In our work, we comply with OpenSky's ADS-B message structure and dataset. Table 1 lists the main blocks from each message that we used.

Data field	Meaning
icao24	Aircraft identification number assigned by the International Civil Aviation Organization (unique ID for each aircraft)
lat,lon,alt	Aircraft location at the time when the ADS-B message is transmitted in terms of latitude, longitude, and altitude
NACp	Value ranges from 0 to 15 and is representative of the real-time GPS location accuracy, where 0 is the least accurate one
serials	The database allows to obtain sensor information by an inner join with the serials field in this table, thus combining all sensors that received a message

Table 1: ADS-B data used from the OpenSky database.

Each aircraft obtains its location from navigation satellite systems (GPS) and broadcasts messages periodically to ATC stations on ground and to other surrounding aircraft to provide better location awareness and self-separation [43]. ADS-B messages contain information about the broadcasting aircraft as well as its navigation quality metrics. Since the ADS-B protocol is encapsulated in Mode-S frames, it uses pulse-position modulation (PPM) and the replies/broadcasts are encoded by a certain number of pulses, each pulse being 1 μs long. Each message contains a 8 μs preamble for synchronization purposes and a short 56-bit or a extended 112-bit data block.

2.2 OpenSky

OpenSky is a non-profit association and network of receivers launched in 2012 [44]. It is a collaborative research project aiming to improve security, reliability, and efficiency of the air space usage by providing public access to real-world air traffic control data. The OpenSky network consists of a large number of connected sensors that are operated by volunteers, academic

organizations, and industrial supporters; these sensors collect real-time traffic from ADS-B aircraft.

2.3 Threat Model

We consider an external ground-based attacker, who is able to use specialized hardware to disrupt ADS-B communications. The attacker's proximity to the sensors depends on the capabilities of his/her hardware. Consequently, we assume that his/her transmit power is sufficient to make the attack possible. This also means that the adversary is aware of the location of the sensors and the structure of the ground-based system. Low-cost SDRs, such as USRP family equipment, may of course be used if the attacker believes that they are suitable. Furthermore, we assume that the adversary has a full knowledge of the ADS-B system, network and its protocols. Finally, we speculate that the attacker is familiar with the following types of jamming attacks:

- Constant Jamming. The attacker selects a frequency band and transmits random values continuously without necessarily complying with the ADS-B protocol structure. This is a trivial attack without the need of ADS-B, but it is costly in terms of energy for the attacker.
- Deceptive jamming. The attacker selects a frequency band and emits false ADS-B messages continuously to confuse the sensors. He/She uses legitimate messages instead of random values, so the detection of such signals is straightforward and requires further evaluation.
- Adapting Jamming. The attacker can use either Constant or Deceptive jamming, determine the proper order of their use, implement energy-saving algorithms and choose when the jamming should stop and continue based on detection evasion.
- Channel-hopping Jamming. The attacker is capable of jamming the target with random values or legitimate ADS-B messages by hopping between different channels and detecting multiple frequency bands. It may be used to counter Frequency Hopping Spread Spectrum (FHSS).
- Smart jamming. The use of multiple jamming devices (more than one) and their coordination to inflict damage is considered. Of course, the jamming devices may hop to different channels and use energy-saving algorithms. The main point of this kind of jammers is to achieve a considerable balance between effectiveness and cost.

The goal of the attacker is to abuse the GPS communications and cause confusions that may lead to dangerous situations.

2.4 Assumptions

To derive the proposed approaches we use the following assumptions:

- Aircraft send ADS-B messages from the beginning till the end of trip.
- All aircraft send GPS accuracy indication (NAC) values for each message.
- The locations of sensors on ground are fixed.
- There is no location spoofing attack while collecting the data for analysis and getting the patterns.

3 Real Incidents

In order to evaluate the effectiveness of the proposed approaches to detect GPS spoofing attacks, we need to make use of real GPS jamming incidents. Thus, we collected a large set of reports of real-world jamming attacks from several available reports, news, and blogs and organize them in Table 2. We provide information about the location, date, interference period, number of recorded reports (frequency), and from where we got this information. As not all information is available for all incidents, we report the information we were able to find and leave the fields empty if we were not able to extract further information.

Table 2: Real GPS jamming incidents.

	Location	**Date**	**Interference Time/ Period/Frequency**
1	Piraquara [27]	Oct 15, 2019	10:00
2	Helsink [19]	August 21, 2019	Half hour
3	Gulf, Strait of Hormuz, Gulf of Oman [25]	August 7, 2019	
4	Syria, near Iran [32]	August 1, 2019	
5	Strait of Hormuz, Gulf [5, 6]	August 8, 2019	Two incidents
6	Sabratha Oilfield - Offshore Libya [27]	July 24, 2019	16:00 GMT
7	New Zealand [27]	July 18, 2019	03:00 UTC
8	Port of Shanghai [26]	July 17, 2019	
9	Shanghai [3]	July 16, 2019	
10	Strait of Hormuz Gulf of Oman[4]	July 16, 2019	
11	US [1]	June 19, 2019	09:01:40 - 09:04:00
12	US [12]	June 19, 2019	09:12:31 - 10:04:30
13	Haifa, Ashdod ports [7]	June, July 2019	Two months
14	Oman [25]	June, 13 2019	Two incidents
15	Ben Gurion Airport Tel Aviv [23]	June 2019	Three weeks
16	Larnaca, Cyprus [27]	May 15, 2019	13:00
17	Crimea, Black Sea, Russia, Syria[15]	April-June 2019	1,311 ships 9,883 reports Three months
18	North Norway [11]	Early 2019	
19	Abilene [27]	April 15, 2019	13:30 CST
20	Friedman Memorial Airport [8]	April 2019	
21	Southwest of Eielson base [21]	May 25, 2019	
22	Fujairah [25]	May 12, 2019	4 commercial vessels
23	Russia-Norway border [22]	Jan 9 and 10, 2019	
24	Strait of Hormuz [27]	Oct 29, 2018	7:00
25	Finland, Norway [2]	Oct 16 - Nov 7 2018	
26	Kabul [27]	Sep 11, 2019	03:30

27	Victoria Harbour Hong Kong [20]	August 25, 2018	46 drones
28	Norway [13]	August 2018	
29	Kerch Bridge (from Russia to Crimea) [16]	May 2018	24 ships
30	Middle East, Syria Larnaca Airport [9]	spring of 2018	
31	Syria [30]	Jan-Apr 2018, main Apr	Weeks
32	Orlando, Florida [27]	April 30, 2018	11:00 EST
33	Middle East [28]	2018	147 events reported 24 incidents
34	Addison [27]	Oct 18, 2017	00:41 UTC
35	Charlotte [27]	June 24, 2017	11:00 EST
36	Nantes airport (France) [18]	April 20, 2017	
37	Chandler [27]	Feb 8, 2017	07:45 MT
38	San Angelo Airport [27]	Jan 3, 2017	11:00 AM
39	Latvia, Norway, Sweden [10]	2017	
40	Manila, Philippines [14]	July-August 2016	50 interference reports Two months
41	Zone that separates North,South Korea [29]	April 1, 2016	962 planes
42	Syria [31]	Sep 30, 2015	
43	Newark Airport [24]	August 2013	
44	List of incidents [27]	2017-2019	
45	Worldwide Database [17]	Any Time	

4 Proposed Methodology

4.1 Approach-1: NAC Values Pattern

The jamming detection scheme we propose works by firstly specifying the coordinates of the area to be monitored for eventual incidents, then all sensors which cover this area are observed. After that, the received packets by these sensors are categorized and grouped based on NACp which is assigned to each packets. Finally, the distribution of NACp categories for the observed sensors are built and accordingly are analyzed over several time windows. Getting the pattern of such type of attack would be useful to detect jamming in the future by noticing the variation on this pattern.

Getting the Pattern:

Given a subnetwork of N ADS-B receivers. The monitoring time is subdivided into K observation windows of size w each. Let $A = \{0, \ldots, 15\}$ be the set of all possible NACp values and $A_s \subset A$ represent the subset of NACp values to be processed for spotting anomalous events that may be brought about by a jamming device, and let P list of aircraft on space and $P_s \subset P$ that sensor s^{th} receives messages from. We define the following functional time series to track

changes in NACp values under consideration.

$$m_{ip}(j) = m_{ipj} = \frac{c_{ip}(j)}{n_{ip}(j)}, \tag{1}$$

where $c_{ip}(j)$ is the count of messages with NACp values falling in A_s as received by the i^{th} sensor for aircraft p^{th} during the j^{th} time window, and $n_{ip}(j)$ the number of messages collected by the same receiver and for the same aircraft during the same time frame. Each of the K time series $\{m_{ip}(j)\}_{1\leq j\leq K}$ is then obtained to define distribution/pattern of each sensor to use them later for anomaly detection. Equation 2 computes the mean μ for each sensor for each aircraft across all K time windows, and then use it to get the pattern of this sensor against this aircraft in equation 3.

where $c_{ip}(j)$: the count of messages with NACp values falling in A_s as received by the i^{th} sensor for aircraft p^{th} during the j^{th} time window

$n_{ip}(j)$: the number of messages collected by the same receiver and for the same aircraft during the same time frame.

Each of the K time series $\{m_{ip}(j)\}_{1\leq j\leq K}$ is then obtained to define distribution/pattern of each sensor to use them later for anomaly detection.

$$\mu_{ip} = \frac{1}{K}\sum_{j=1}^{K} m_{ip}(j) \tag{2}$$

$$\sigma_{ip} = \sqrt{\frac{1}{K-1}\sum_{j=1}^{K} |m_{ip}(j) - \mu_{ip}|^2} \tag{3}$$

Anomaly Detection:

Assume there is a jamming attack in the given subnetwork. Also, the N receivers receive a set of ADS-B message from aircraft a within w time window. The NACp value of these messages are observed and then the distribution of the received messages are compared with the observed one from equation 3. The distribution is formed based on equations 1 and 2. Each sensor i will calculate how much does the received value deviate D_i from the distribution using equation 4. More specifically, we evaluate how the received ratio differs from each window of the distribution. Then, given a threshold, we can finally conclude if the value is indeed normal ($H_i = 0$) for the distribution or not ($H_i = 1$) as defined in 5

$$D_i = \frac{\sum_{j=1}^{K}\left(\frac{|m_{ipj} - m_a^{'}|}{m_{ipj}}\right)}{K} \tag{4}$$

$$H_i = \begin{cases} 0, & 0 \leq D_i < threshold_i \\ 1, & threshold_i \leq D_i \leq 1 \end{cases} \tag{5}$$

where m_{ipj} represents each value in the distribution and $m_a^{'}$ the received calculated ratio using equation 1. The greater the value of D_i (closer to 1), the greater the deviation meaning that this specific value is probably unusual for the distribution. Otherwise, if it is closer to zero, it means that the received value is probably usual for this distribution.

If more than one sensors receive the message then the cross match will be applied for all of these sensors to get more precise results. Ideally, if there are more aircraft affected by the jamming attack this means the probability to catch such attack is getting increase, i.e more up-normal distribution are observed by several sensors and aircraft, hence this gives an indication for jamming incident.

To achieve an accurate result we have to set the threshold appropriately. Each sensor will have each own threshold since their distribution is different. We can determine the threshold by practically executing experiments and assessing the data. In addition, by increasing the window size and consequently reducing the number of windows, we can minimize possible inaccuracies. Again, the number of windows can be determined by the data.

4.2 Approach-2: NaN/NULL Values Pattern

Getting the Pattern:

Given a subnetwork of N ADS-B receivers. The monitoring time is subdivided into K observation windows of size w each, exactly like the NACp values in the previous section.

We define the following functional time series to track the NULL values in ADS-B messages.

$$u_i(j) = u_{ij} = \frac{c_i(j)}{n_i(j)}, \tag{6}$$

where $c_i(j)$ is the count of messages with NULL values as received by the i^{th} sensor during the j^{th} time window, and $n_i(j)$ the number of messages collected by the same receiver

during the same time frame. Each of the K time series $\{m_i(j)\}_{1\leq j\leq K}$ of NULL values is then obtained to define distribution/pattern of each sensor as we did for NAC values to use them later for anomaly detection. Equation 7 computes the mean μ for each sensor for each aircraft across all K time windows, and then use it to get the pattern of NULL values of this sensor against in equation 3.

$$\mu_i = \frac{1}{K}\sum_{j=1}^{K} u_i(j) \tag{7}$$

$$\sigma_i = \sqrt{\frac{1}{K-1}\sum_{j=1}^{K} |u_i(j) - \mu_i|^2} \tag{8}$$

Anomaly Detection:

$$D_i = \frac{\sum_{j=1}^{K}(\frac{|u_{ij} - u_a^{'}|}{u_{ij}})}{K} \tag{9}$$

$$H_i = \begin{cases} 0, & 0 \leq D_i < threshold_i \\ 1, & threshold_i \leq D_i \leq 1 \end{cases} \tag{10}$$

The process of anomaly detection is identical with the anomaly detection in NACp values. For each sensor i, we have the distribution of the NaN/NULL values based on 7 and 8 accordingly and we measure the received ratio based on equation 6. Then, the level of deviation is calculated using 9. Finally, given a specific threshold we can infer if the received ratio is usual or unusual for the distribution with equation 10. It has to be mentioned that $u_a^{'}$ represents each value in the distribution and u_{ij} represents the received calculated ratio of the NaN values (from 6). Of course, the measurements of the sensors may be fused again together to give a more accurate prediction.

5 Experiments and Findings

In order to detect jamming occurrences near the Nantes Atlantique airport during the month of April 2017, we examine the ADS-B traffic from a subnetwork of $N = 64$ ground ADS-B receivers deployed around the airport and all covering the geographic coordinates 46.6 to 47.6 latitude and -2.1 to -1.1 longitude. We then build the distribution of NACp categories as recorded by individual sensors in order to analyse their variation under the effect of real jamming incidents.

For assessing the detection performance of our proposed scheme we choose observation windows of size $w = 1$ hour. The response of the jamming detector for different time frame sizes will be examined subsequently.

5.1 First Findings

The m_{ij} follow a half-normal distribution with mean $\mu = 0.04$, standard deviation $\sigma = 0.05$, lower and upper quartile values $Q_1 = 0.01$ and $Q_3 = 0.06$ respectively as shown in Figure 1. The inter quartile range is $IQR = 0.06 - 0.01 = 0.05$ and the upper outlier limit $Q_3 + 1.5 \times IQR = 0.135$. These outliers values potentially represent actual GPS jamming incidents degrading ADS-B quality metrics.

Although this computed cut-off limit can readily be used for jamming detection, another possibility for classifying a given event or a change point in the time series shown in Figure 2 as jamming attack may be based on a threshold computed through training after which a low detector's equal error rate has been reached.

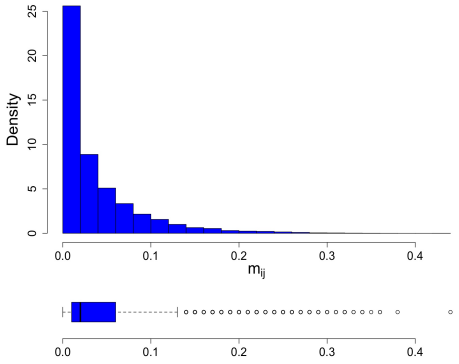

Figure 1: Distribution of the m_{ij} for the sub-network of 64 sensors

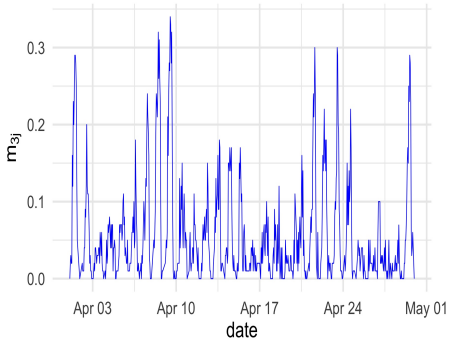

Figure 2: Monthly variations in 'bad' NACp values ($A_s = \{0\}$) at the 3^{rd} sensor ($i = 3$)

5.2 Testing Limitations

Evaluating the proposed approaches faces a couple of limitation which make the evaluation process in an experimental way not fruitful.

- The information of some of the observed incidents in table 2 is not sufficient enough to limit the actual location/time of such incidents. We are looking for an accurate reports for these incidents to make sure the proposed approaches are applicable.
- The NAC value of ADS-B message is not recorded for each received messages which makes the evaluation process impossible with such low level of data.
- Taking into account the low level of data, as previously mentioned, it is remarkably difficult to further enhance our accuracy by using machine learning or other more advanced mathematical techniques. For instance, the aforementioned approaches combined appropriately with deep learning may yield significant results.

6 Related Works

Researchers have realized the weaknesses of ADS-B and tried to provide solutions or defense mechanism assessments concerning the ADS-B jamming attacks in order to possibly reduce their severity or detect and suppress them. A research study [36] shows the impact of the jamming

attacks through multiple experiments and propose signal separation methods as a potential solution. [39] and [38] provide a comprehensive understanding of ADS-B threats, solid risk assessment and defense in depth mechanisms, however there is no decisive solution for ADS-B jamming. In addition, [34] includes many details about ADS-B threats but again with no focus on jamming. [41] discusses multifarious ADS-B exploits and possible solutions. It states that wireless jamming is indeed hard to eliminate but it can be scaled down by degrading ADS-B based coverage to secondary surveillance radar based coverage. Moreover, other proposals work on the physical layer too harvesting the features of the receivers [37] and the cross-antenna array [45]. On the other hand, Habler et al. [35] tries to detect anomalies in ADS-B message using LSTM, but the work chiefly focuses on spoofing. Finally, [40] elaborates on the integrity of ADS-B IN messages and studies the disruptions of ADS-B communications due to jamming.

7 Conclusion

In this work, the issue of real-world GPS jamming detection from avionics datasets is addressed. We proposed a scheme where each sensor is able to determine possible jamming attacks relying on the distribution of its received data in a specific time period. The preliminary results are promising and further experiments need to be carried out utilizing also more advanced statistical techniques combined with the suggested metrics. By eliminating the aforementioned limitations in the future, we are confident that we can produce considerable results on identifying jamming attacks based on ADS-B's application layer.

8 Acknowledgements

The authors gratefully acknowledge the financial support of and research interaction with Armasuisse Science & Technology and Abu Dhabi Department of Education and Knowledge (ADEK).

References

[1] Telcon gps/ads-b failure. https://www.fly.faa.gov/adv/adv_otherdis.jsp?advn=11&adv_date=06092019&facId=DCC&title=ADS-B%20AND%20GPS%20ANOMALIES&titleDate=06/09/19. Accessed: 2019-11-18.

[2] Finland, norway press russia on suspected gps jamming during nato drill. https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/. Accessed: 2019-11-18.

[3] Gps jamming and spoofing reported at port of shanghai. https://maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai. Accessed: 2019-11-18.

[4] U.s. coast guard warns of cyber-attack & electronic interference threats to commercial vessels. https://www.ajot.com/insights/full/ai-u.s-coast-guard-warns-of-cyber-attack-electronic-interference-threats-to-commercial-vessels. Accessed: 2019-11-18.

[5] Iran is reportedly jamming ship gps navigation systems to get them to wander into iranian waters. https://www.businessinsider.com/iran-is-jamming-ship-gps-navigation-systems-to-seize-them-2019-8. Accessed: 2019-11-18.

[6] Us government warns of iranian threats to commercial shipping, including gps interference. https://edition.cnn.com/2019/08/07/politics/us-warns-of-iranian-threats-to-shipping/index.html. Accessed: 2019-11-18.

[7] Israeli ports confronting gps jamming. https://i-hls.com/archives/93375. Accessed: 2019-11-18.

[8] Passenger aircraft nearly crashes due gps disruption. https://www.gpsworld.com/nasa-report-passenger-aircraft-nearly-crashes-due-gps-disruption/. Accessed: 2019-11-18.

[9] Russia is disrupting gps signals and it's spilling into israel. https://www.popularmechanics.com/military/weapons/a28250133/russia-gps-signals-israel/. Accessed: 2019-11-18.

[10] Russian naval jamming. https://www.gpsworld.com/jammers-at-dachas-add-to-russias-ability-to-silence-gps/. Accessed: 2019-11-18.

[11] Russian jamming for nato exercises. https://www.gpsworld.com/jammers-at-dachas-add-to-russias-ability-to-silence-gps/. Accessed: 2019-11-18.

[12] Blanket waiver for all flights having gps/ads-b issues. https://www.fly.faa.gov/adv/adv_otherdis.jsp?advn=29&adv_date=06092019&facId=DCC&title=GUIDANCE+FOR+ADSB&titleDate=06/09/19. Accessed: 2019-11-18.

[13] Russians tried to jam nato exercise; swedes say they've seen this before. https://breakingdefense.com/2018/11/russians-tried-to-jam-nato-exercise-swedes-say-theyve-seen-this-before/. Accessed: 2019-11-18.

[14] Gps interference/signal degradation in manila. https://www.icao.int/APAC/Meetings/2017%20RPGITUWRC19/WRC19RPG42-GNSS_Interference_Philippines_CharlemagneGilo.pdf. Accessed: 2019-11-18.

[15] Russia hacks global satellite navigation systems to confuse planes and ships. https://www.ibtimes.com/russia-hacks-global-satellite-navigation-systems-confuse-planes-ships-2785410. Accessed: 2019-11-18.

[16] Their gps systems told their captains they were anchored more than 65 kilometers away, on dry land at the anapa airport inside russia. https://www.ibtimes.com/russia-hacks-global-satellite-navigation-systems-confuse-planes-ships-2785410. Accessed: 2019-11-18.

[17] Asrs database online - aviation safety reporting system. https://titan-server.arc.nasa.gov/ASRSPublicQueryWizard/QueryWizard_Filter.aspx. Accessed: 2019-11-18.

[18] Forgotten' gps jammer costs motorist 2,000 euro. https://www.connexionfrance.com/French-news/Forgotten-GPS-jammer-costs-motorist-2-000. Accessed: 2019-11-18.

[19] Free pass for putin, gps jamming and climate change anxiety. https://yle.fi/uutiset/osasto/news/thursdays_papers_free_pass_for_putin_gps_jamming_and_climate_change_anxiety/10932777. Accessed: 2019-11-18.

[20] one million dollar in damage caused by gps jamming that caused 46 drones to plummet during hong kong show. https://www.scmp.com/news/hong-kong/law-and-crime/article/2170669/hk13-million-damage-caused-gps-jamming-caused-46-drones. Accessed: 2019-11-18.

[21] Military to again briefly jam gps signal during alaska exercise. http://www.newsminer.com/news/alaska_news/military-to-again-briefly-jam-gps-signal-during-alaska-exercise/article_c84c72c4-777e-11e9-9906-d7806df214ea.html. Accessed: 2019-11-18.

[22] Gps jamming in the arctic circle. https://aerospace.csis.org/data/gps-jamming-in-the-arctic-circle/. Accessed: 2019-11-18.

[23] Israel hit by mysteriously recurring gps disruptions in its airspace. https://www.haaretz.com/israel-news/israel-says-gps-mysteriously-disrupted-in-its-airspace-but-planes-secure-1.7413357. Accessed: 2019-11-18.

[24] Truck driver has gps jammer, accidentally jams newark airport. https://www.regulus.com/blog/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/. Accessed: 2019-11-18.

[25] Sabotage operations iranian gps jamming. shipping industry faces gps jamming in persian gulf. https://www.satellesinc.com/shipping-industry-faces-gps-jamming-in-persian-gulf/. Accessed: 2019-11-18.

[26] Gps jamming and spoofing reported at port of shanghai. https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai. Accessed: 2019-11-18.

[27] Gps problem reports status. the navigation center of excellence. https://navcen.uscg.gov/?Do=

gpsreportstatus. Accessed: 2019-11-18.

[28] Gps jamming suspected in steep rise of dp incidents. https://www.rivieramm.com/news-content-hub/news-content-hub/gps-jamming-causes-dp-incidents-and-endangers-lives-56229. Accessed: 2019-11-18.

[29] North korea is jamming gps signals. https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/. Accessed: 2019-11-18.

[30] The russians are jamming us drones in syria because they have every reason to be. https://www.thedrive.com/the-war-zone/20034/the-russians-are-jamming-us-drones-in-syria-because-they-have-every-reason-to-be. Accessed: 2019-11-18.

[31] Jamming the jihad: Russian electronic warfare systems spotted in syria. https://sputniknews.com/world/201510051028033057-syria-russia-electronic-warfare-systems/. Accessed: 2019-11-18.

[32] Massive investments in electronic warfare and turned cell phone towers into gps jammers. https://www.yoursurvivalguy.com/future-weapons/how-vulnerable-are-vital-u-s-military-systems-to-gps-jamming-spoofing/. Accessed: 2019-11-18.

[33] W Blythe, H Anderson, and N King. Ads-b implementation and operations guidance document. *International Civil Aviation Organization. Asia and Pacific Ocean*, 2011.

[34] Andrei Costin and Aurélien Francillon. Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices. *Black Hat USA*, pages 1–12, 2012.

[35] Edan Habler and Asaf Shabtai. Using lstm encoder-decoder algorithm for detecting anomalous ads-b messages. *Computers & Security*, 78, 11 2017.

[36] M. Leonardi, E. Piracci, and G. Galati. Ads-b vulnerability to low cost jammers: Risk assessment and possible solutions. In *2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*, pages 41–46, Sep. 2014.

[37] Mauro Leonardi, Emilio Piracci, and Gaspare Galati. Ads-b jamming mitigation: A solution based on a multichannel receiver. *IEEE Aerospace and Electronic Systems Magazine*, 32:44–51, 11 2017.

[38] W. Li and P. Kamal. Integrated aviation security for defense-in-depth of next generation air transportation system. In *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, pages 136–142, Nov 2011.

[39] Donald McCallie, Jonathan Butts, and Robert Mills. Security analysis of the ads-b implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*, 4:78–87, 08 2011.

[40] K. Sampigethaya and R. Poovendran. Visualization assessment of ads-b security for green atm. In *29th Digital Avionics Systems Conference*, pages 3.A.3–1–3.A.3–16, Oct 2010.

[41] Krishna Sampigethaya, Radha Poovendran, and Linda Bushnell. Assessment and mitigation of cyber exploits in future aircraft surveillance. *2010 IEEE Aerospace Conference*, pages 1–10, 2010.

[42] M Spuhler, D Giustiniano, V Lenders, M Wilhelm, and J B Schmitt. Detection of reactive jamming in dsss-based wireless communications. *IEEE Transactions on Wireless Communications*, 13(3):1593–1603, 2014.

[43] M Strohmeier, V Lenders, and I Martinovic. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys Tutorials*, 17(2):1066–1087, Secondquarter 2015.

[44] M Strohmeier, I Martinovic, M Fuchs, M Schäfer, and V Lenders. Opensky: A swiss army knife for air traffic security research. In *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, pages 4A1–1. IEEE, 2015.

[45] R. Wu, G. Chen, W. Wang, D. Lu, and L. Wang. Jamming suppression for ads-b based on a cross-antenna array. In *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, pages K3–1–K3–9, April 2015.