ADS-B spoofing attack detection method based on LSTM

Jing Wang
Civil Aviation University of China
Yunkai Zou (zouyunkaicauc@qq.com)
Civil Aviation University of China https://orcid.org/0000-0003-2399-1532
Jianli Ding
Civil Aviation University of China

Research

Keywords: ADS-B, attack detection, LSTM, sliding window, security threat

Posted Date: April 9th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-19635/v1

Version of Record: A version of this preprint was published on August 12th, 2020. See the published version at https://doi.org/10.1186/s13638-020-01756-8.

ADS-B spoofing attack detection method based on LSTM

Jing Wang[1], , Yunkai Zou [2]*, Jianli Ding[1]

1. College of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China

2. Sino-European Institute of Aviation Engineering, Civil Aviation University of China, Tianjin 300300, China

**Correspondence: zouyunkaicauc@qq.com*

Abstract: The open and shared nature of the ADS-B protocol makes its messages extremely vulnerable to various security threats, such as jamming, modification, and injection. This paper proposes an LSTM-based ADS-B spoofing attack detection method from the perspective of data. First, the message sequence is preprocessed in the form of a sliding window, and then a long short-term memory (LSTM) network is used to perform prediction training on the windows. Finally, the residual set of predicted values and true values is calculated to set a threshold. As a result, we can detect a spoofing attack and further identify which feature was attacked. Experiments show that this method can effectively detect 10 different kinds of simulated manipulated ADS-B messages without further increasing the complexity of airborne applications. Therefore, the method can respond well to the security threats suffered by the ADS-B system.

Keywords: ADS-B; attack detection; LSTM; sliding window; security threat

1 Introduction

With the significant increase in airspace density, traditional surveillance technologies such as primary surveillance radar (PSR), secondary surveillance radar (SSR), and multilateration (MLAT) technology will have increasing difficulty meeting

the future need for the development of air traffic management (ATM) systems. Because Automatic Dependent Surveillance-Broadcast (ADS-B) technology has the advantages of high accuracy, large coverage, support for data sharing and air surveillance, it has become an important part of the next-generation (NextGen) air transport system.

However, since the protocol of ADS-B has the characteristics of open sharing, its security faces great challenges. Specifically, the protocol does not provide any relevant data encryption and authentication, and its messages are broadcast in a simple and open format, which is very vulnerable to eavesdropping, jamming, modification and injection. In addition, authorized aircraft and ATC (Air Traffic Controller) stations do not perform identity authentication before sending ADS-B messages, and the protocol cannot distinguish authorized entities from unauthorized ones. All these factors make the ADS-B system extremely vulnerable to various spoofing attacks. At present, many studies have successfully verified the possibility of attacking the ADS-B system [1,2]. Therefore, concerns about its safety will continue to increase with the development of air traffic and the further popularization and application of ADS-B.

In recent years, researchers have carried out related research on the security issues of the ADS-B system and have given suggested security measures and solutions, mainly including the following aspects: (1) Prevent eavesdropping and modification by encrypting ADS-B messages [3]. Because this method needs to change the existing ADS-B protocol structure, it is difficult to implement. (2) An aircraft is authenticated through a challenge response [3], and additional sensors are added in the airspace to verify the security of the transmitted data [4-6]. However, the ADS-B system has been

deployed on most aircraft, and software and hardware installations and changes require strict airworthiness certifications, so they are difficult to implement at this stage. (3) Position-based verification methods [7-10]: These methods usually perform a secondary check on the position claimed by the aircraft or other ADS-B users. The principle is to establish a mechanism that can find the exact position of the message sender, which is essentially different from the verification of the broadcast source and the message. The advantage of this method is that it can be used as a primary navigation system or even a GPS backup system because it can generate additional position data, which can be combined with ADS-B and radar systems. However, such methods usually require synchronization of multiple ground stations or receiving devices, and the complexity is high. (4) Methods of antenna verification DOA (Direction of Arrival) [11-13]: These methods can avoid problems such as time synchronization and data fusion and do not need to change the existing ADS-B protocol. However, this approach requires spatial search direction finding, has high computational complexity and is sensitive to array errors. (5) From the perspective of data, a machine learning method is used to reconstruct the ADS-B message sequence, and the reconstruction error is used to detect anomalous messages. Based on the original features contained in an ADS-B message, Habler et al. calculated the distances from all points on the track to four special nodes and the distances between two adjacent track points, for a total of 5 parameters, as additional training features to perform anomaly detection [14]. Our research group statistically expands the original features based on the strong temporal correlation of ADS-B messages so that the model can better capture the time

dependence of the data [15]. Although such methods can detect abnormal data, they cannot further determine the specific cause of the abnormality, that is, which data items (features) in the ADS-B message have been modified. In addition, these methods need to further expand the features of the original data to a certain extent, that is, perform more complicated feature engineering. These data processing steps undoubtedly increase the complexity of the application in the actual process.

Therefore, this paper proposes an ADS-B spoofing attack detection method based on a long short-term memory (LSTM) network [16]. The core idea of this method is prediction. Specifically, the ADS-B message sequence data are first preprocessed in the form of a sliding window, and then a neural network composed of LSTM units is used for predictive training. Finally, a threshold is set by calculating the predicted data residual set to determine whether there is an abnormality in the ADS-B data. By setting corresponding thresholds for different features, we can further identify the specific features under attack. In this paper, anomalous data (abnormality) refer to data that have been manipulated and need to be detected.

The main contributions of this paper are the following:

1. By analyzing the ADS-B attacks, we construct a neural network made up of LSTM units to detect different types of anomalous data we simulate. Compared with the existing machine learning methods [14,15], our method does not require complicated feature engineering.

2. We set different thresholds for different features, so that we can determine the specific features containing anomalies. In addition, the experiments show that when a

single feature is attacked, it can trigger the overall anomaly threshold (that is, the average of the anomaly thresholds of all features) and does not affect the abnormal scores of other features. The advantage is that in actual applications, the overall threshold can be used to determine whether an abnormality occurs first, and then use the thresholds of different features to determine the specific features that contain anomalies.

The rest of the paper is organized as follows. In Section 2, we analyze different types of attacks. Then in Section 3, we describe the process and detailed steps of the anomaly detection method. Using this method, we perform detection experiments on different simulated anomalous data, analyze and discuss the results in Section 4. Finally, we conclude in Section 5.

2 Types of ADS-B Attacks

The ADS-B system is a new paradigm of air traffic control and does not require manual operation or inquiries. It can automatically obtain parameters from relevant airborne equipment and broadcast the flight status information of the aircraft to other aircraft or ground stations for controllers. According to the direction of aircraft information transmission, the system functions can be divided into two categories, ADS-B IN and ADS-B OUT [17]. The former is an optional service that enables the aircraft to receive and display detailed information broadcast by other aircraft operating in the same area. The latter is the basic function of the on-board ADS-B equipment. It sends the aircraft's position information and other additional information to other aircraft or controllers at a certain period, mainly including aircraft identification

information, speed, heading, climb rate, etc. Ground stations can monitor air traffic by receiving this information.

The risks faced by the ADS-B system are essentially derived from the broadcast nature of radio frequency communications and the fact that messages are broadcast as unencrypted plain text [18]. The importance and strong attackability of the aircraft operating status information that these messages contain make them the main target for malicious attackers.

At present, the types of attacks that exist for the ADS-B system are mainly divided into eavesdropping, jamming, message injection, message deletion, and message modification [19]. Among them, eavesdropping will not directly harm the air traffic control system, so the impact is minimal. Message deletion will have an impact on the surveillance system, causing the aircraft to temporarily disappear from the ATC map, but it can be identified by surveillance systems such as radar and multilateration systems. Message modification is a typical spoofing attack. For example, if an attacker continuously changes the aircraft position information in ADS-B messages by small amounts, that is considered a "frog boiling"-type spoofing attack [20]. At this time, other surveillance technologies (such as radar surveillance systems) and positioning technology will have difficulty detecting these small differences due to accuracy issues, resulting in incorrect guidance to air traffic controllers or delaying the response of the collision avoidance system. This has a great impact on the ATC system.

Table 1 ADS-B packet attack types

Serial number	Attack type	Purpose of attack	Way of attack
1	Eavesdropping	Eavesdrop operating status information of aircraft (Aircraft Reconnaissance)	Obtain ADS-B data of corresponding airspace through ADS-B IN device
2	Jamming	Jam the transmission of an ADS-B message in a specific airspace (Ground Station Flood Denial, Aircraft Flood Denial)	By using an ADS-B transmitting device with sufficiently high transmit power in the relevant frequency band
3	Message Injection	Inject fake aircraft into specific flight scenarios, confusing air traffic control systems (Aircraft Target Ghost Injection/Flooding)	By using a transmitting device with sufficient high transmit power in the relevant frequency band and capable of generating correct modulation and conforming to the ADS-B message format
4	Message Deletion	Delete some or all of the information contained in a message (Aircraft Disappearance)	By implementation at the physical layer through constructive or destructive interference
5	Message Modification	Modify the information contained in a message (Virtual Trajectory Modification)	Realized by overshadowing and bit-flipping at the physical layer of the system and can also be achieved by combining two attack methods: false message injection and message deletion

3 ADS-B Spoofing Attack Detection Method

3.1 Overall Process

Figure 1 shows the overall flowchart of the method proposed in this paper. First, we analyze and preprocess the original ADS-B series and then use the LSTM-based neural network to predict the ADS-B data in the form of a sliding window. Finally, anomaly thresholds are determined by calculating the residuals between predicted values and true values to complete the detection.

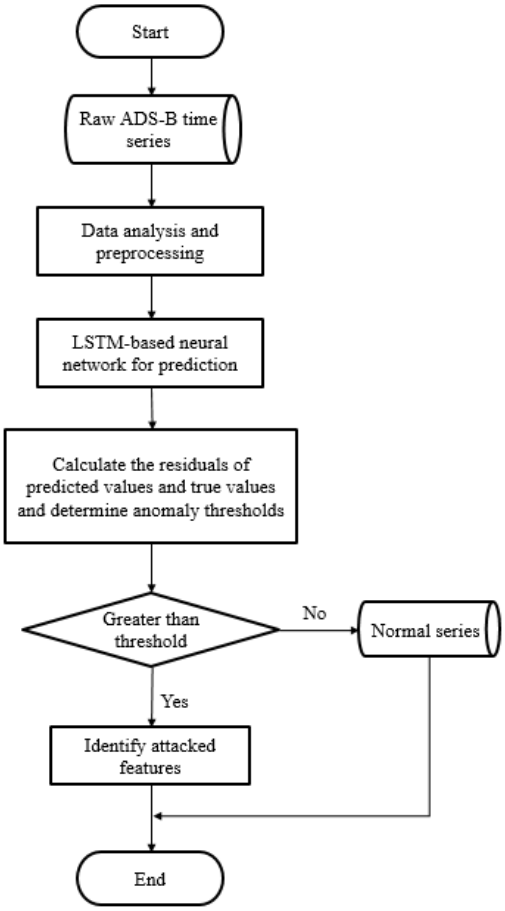

Fig. 1 Overall process

3.2 Data Preprocessing

The ADS-B protocol format is shown in Figure 2. Before model training, the data set needs to be preprocessed according to the steps shown in Figure 3. First, the features related to the aircraft operating status information are extracted from the ADS-B message, including the aircraft's longitude, latitude, altitude, speed, heading, and climb rate. Then, the data are sorted according to the ICAO code (the unique identifier of each aircraft) so that the data set is sorted according to different flights; the form is shown in Figure 4. Next, the data set is normalized so that the scaling transformation of different feature dimensions makes the features comparable between different measures without changing the distribution of the original data. Finally, the data are processed into

window form according to the time-dependent relationship between ADS-B data features.

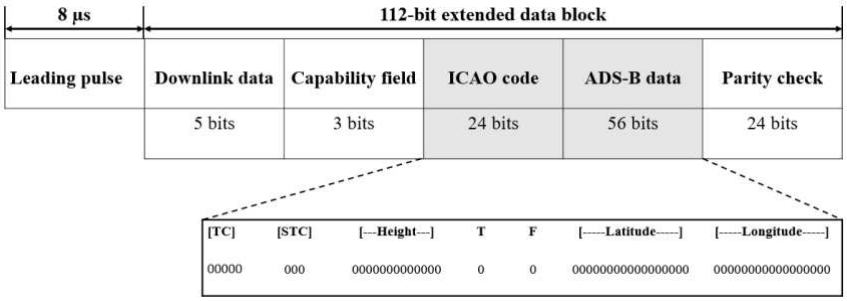

Fig. 2 ADS-B protocol

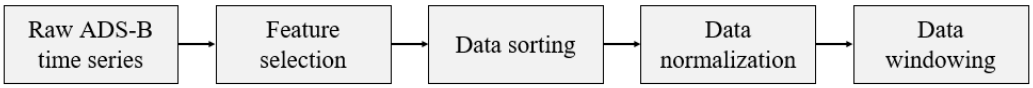

Fig. 3 Data preprocessing steps

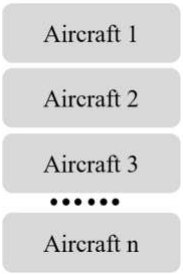

Fig. 4 Data set arrangement

3.3 Sliding Window

Define an n-dimensional time series $S = \{S_1, S_2, ..., S_C\}$ to represent the ADS-B sequence window, which is composed of a series of n-dimensional vectors, where C is the length of the time series. $S_i = \{s_1, s_2, ..., s_n\}$ is an n-dimensional vector, and each dimension corresponds to a feature. Specifically, S represents a window composed of continuous C pieces of an ADS-B message, and each vector S_i contains the features extracted from the corresponding ADS-B message, namely, the longitude, latitude, altitude, speed, heading, and climb rate. Figure 5 shows a sample data diagram, including the timestamp, ICAO, latitude, longitude, altitude, speed, heading, and climb rate from left to right. The data are in CSV format.

	Timestamp	ICAO	Lat	Lon	Alt	Speed	HDG	ROC
2	1483255284	400802	51.75096	-0.17326	17575	402	60.2	3648
3	1483255284	400802	51.75152	-0.17166	17600	402	60.2	3648
4	1483255296	400802	51.76076	-0.14089	18225	405	67.7	3008
5	1483255301	400802	51.76404	-0.12672	18475	407	70.6	2816
6	1483255301	400802	51.76442	-0.12501	18500	407	70.6	2816
7	1483255303	400802	51.76538	-0.1204	18575	407	71.8	2624
8	1483255305	400802	51.76625	-0.1158	18625	408	72.9	2496
9	1483255312	400802	51.76972	-0.09529	18875	407	76.4	1984
10	1483255316	400802	51.7717	-0.08166	19025	408	76.8	1984
11	1483255322	400802	51.77414	-0.06447	19225	409	77	1984
12	1483255334	400802	51.7793	-0.02813	19625	411	77.1	1984
13	1483255335	400802	51.77973	-0.02518	19675	411	77.1	1984
14	1483255336	400802	51.78017	-0.02212	19700	411	77.1	1984
15	1483255344	400802	51.78331	0	19975	412	77	2368

Fig. 5 Data sample

Considering the time correlation of ADS-B data, the data are processed into the form of a sliding window. For example, a window with a length of 10 is selected, and the training phase first uses the data with the serial number [1,10] to predict the 11th data; then, by sliding the window, the data with the serial number [2,11] are used to predict the 12th data, and the rest of the data all follow this pattern. Figure 6 shows a schematic diagram of the sliding window.

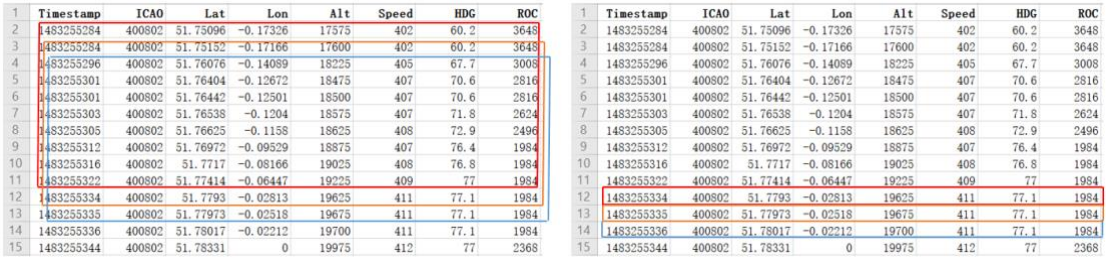

Fig. 6 Illustration of the sliding window

3.4 Model Structure and Parameter Settings

This paper uses an LSTM network to predict an ADS-B sequence. The network is a sequential model consisting of a layer of LSTM units and a fully connected layer. An LSTM unit is a memory unit for learning long-term patterns, including the current state and three nonlinear gates: a forget gate, input gate, and output gate. The forget gate is responsible for determining how much information to remember. It is determined by a

nonlinear function and outputs a number between 0 and 1, where 0 means forgetting all the information in memory and 1 means keeping all the information in memory. The input gate is responsible for deciding how to update the old unit status; that is, the new information is selectively recorded into the unit status. The output gate is responsible for deciding how much memory information is passed to the next unit.

The loss function for training uses the mean square error, the number of LSTM units is 14, and the number of fully connected layer units is 7, which is the dimension of the ADS-B vector (ICAO is used for flight sequencing and does not participate in model training).

3.5 Threshold Setting

The total data set is defined as M, and M is divided into three subsets, M1, M2, and M3, where the ratio is approximately 8:1:1. Among them, M1 is used for model training, M2 is used for determination of thresholds, and M3 is modified according to the descriptions of different attack types; then the model is tested.

After the model is trained, M2 is input into it to obtain a set of predicted values P. The set of true values corresponding to P is V, and the residual set of P and V is defined as D. For di∈D, we have

$$d_i = | p_i - v_i |$$

where pi∈P, vi∈V, and i is the index coefficient. Then, the mean and standard deviation of set D are calculated and recorded as μ and σ; that is, E(D)=μ and D(D)=σ2. Then, we can define the threshold as follows:

$$t = 3\sigma$$

In the test phase, the corresponding residual set D' is obtained by using the model and the data set M3 in the same manner as described above. The anomaly score can be defined as:

$$a = |d_i' - \mu|$$

where $di' \in D'$ and μ is the mean of set D.

In addition, the threshold used to detect modifications of multiple features is the average of their residuals. In practical applications, the average threshold of all features can be used first to determine whether an attack has happened. Furthermore, if the predicted residual of a certain feature exceeds the corresponding threshold, it can be determined that an abnormality has occurred in this specific feature.

4 Results and Discussion

4.1 Attack Data Simulation

The data used in the experiments in this paper were obtained from a GitHub project [21]. The data were decoded from real ADS-B messages with a total length of approximately 220,000. This paper focuses on 10 different types of attack data for jamming, modification, and injection, as shown in Table 2.

Table 2 ADS-B attack data simulation methods

Attack type	**Simulation data**	**Simulation method**	
Jamming	Random noise	Multiply the flight value obtained in the original ADS-B message by a random value between 0 and 2.	
Injection	Route replacement	Given certain route information, inject different correct route information to replace the sequence for the selected ADS-B sequence segment.	
Modification	Fixed offset(+)	Increase the flight value (except time characteristics) obtained in the ADS-B message by 10%.	
	Fixed offset(-)	Decrease the flight value (except time characteristics) obtained in the ADS-B message by 10%.	
	Height	Use 400 feet as	In the selected ADS-B sequence, increase the altitude

Attack type	Simulation data	Simulation method	
	offset(+)	multiples to gradually change the altitude characteristics of ADS-B messages.	feature of the first vector by 400 feet, the second by 800 feet, and so on.
	Height offset (-)		In the selected ADS-B sequence, decrease the altitude feature of the first vector by 400 feet, the second by 800 feet, and so on.
	Speed offset(+)	Use 5 knots as multiples to gradually change the speed characteristics of ADS-B messages.	In the selected ADS-B sequence, increase the speed feature of the first vector by 5 knots, the second by 10 knots, and so on.
	Speed offset(-)		In the selected ADS-B sequence, decrease the speed feature of the first vector by 5 knots, the second by 10 knots, and so on.
	Heading change	Change the value of the heading information contained in the ADS-B message to the opposite of the original value.	
	Climb rate change	Change the value of the climb rate information contained in the ADS-B message to the opposite of the original value.	

4.2 Results Visualization

An independent flight or sequence segment is selected and the sequence segments with serial numbers [100, 105] are injected with the different types of attacks described in Table 2. Figure 7 shows the abnormal score for a certain flight after modification, where the abscissa is the data serial number and the ordinate is the abnormal score.

Different subgraphs represent attacks against different features in the following order: random noise, fixed offset (+), fixed offset (-), route replacement, altitude offset (+), height offset (-), speed offset (+), speed offset (-), heading change, and climb rate change. It can be seen that for different data features, the method can effectively detect the attack using the corresponding threshold.

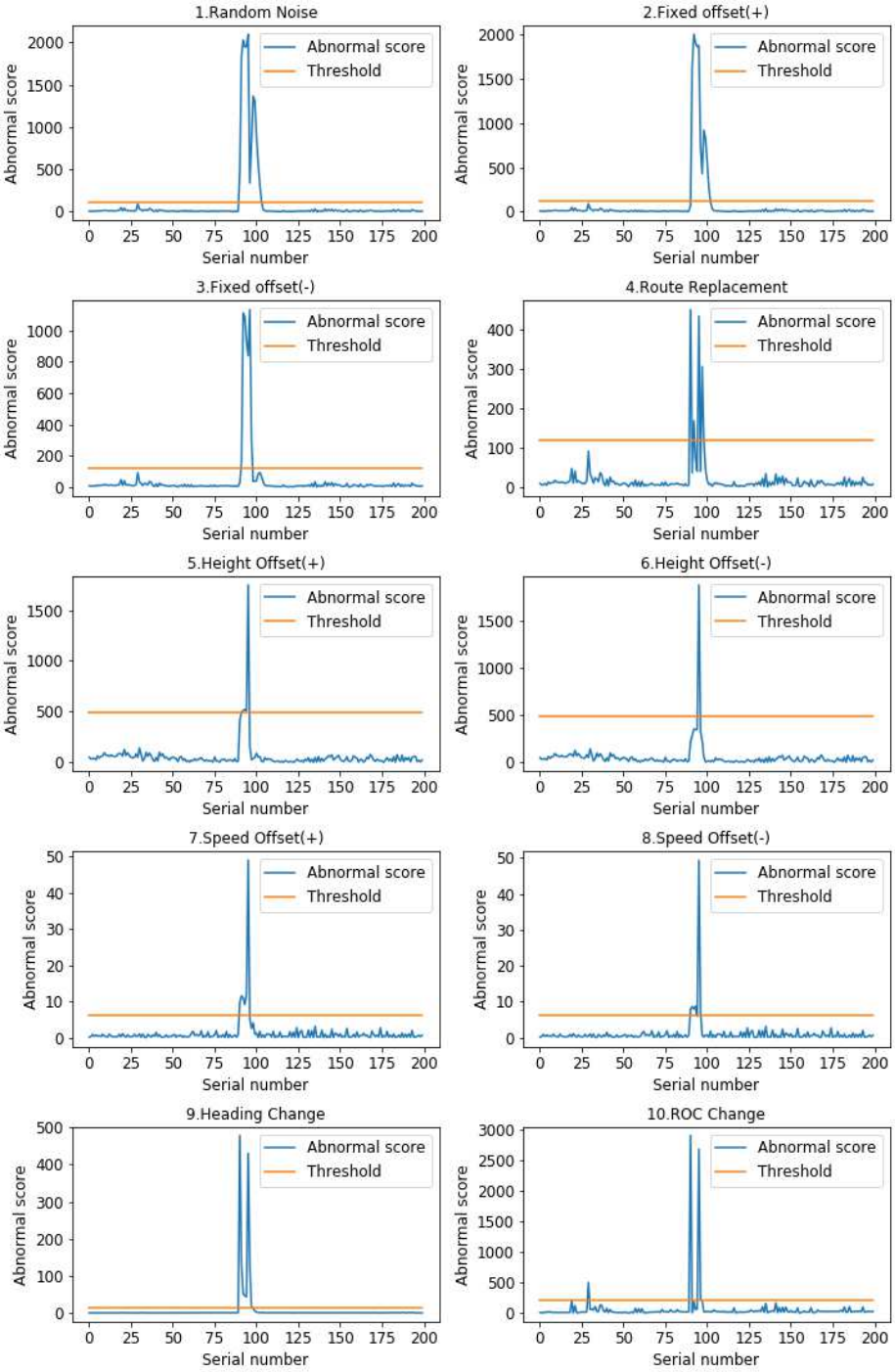

Fig. 7 Abnormal score figures

4.3 Evaluation Metrics

To evaluate the method more accurately, this paper uses precision, recall and the F1-score as metrics. They are defined as follows:

Precision: Precision is the ratio of correctly predicted positive observations to the total predicted positive observations.

$$P = TP / (TP + FP)$$

Recall: Recall is the ratio of correctly predicted positive observations to all observations in the actual class.

$$R = TP/ (TP + FN)$$

F1-score: The F1-score is the weighted average of precision and recall.

$$F1\text{-}Score = 2 \times (R \times P) / (R + P)$$

TP, FP, and FN refer to true positive, false positive, and false negative, respectively. We might fail to detect potential anomalies if we only pay attention to precision. However, some false positives might be received when we focus only on recall. The F1-score provides a balance of precision and recall and is therefore used as the main evaluation metric in our experiments.

4.4 Effect of sliding window length

Before statistical analysis of all attack detection results, fixed offset (+) is first taken as an example to study the effect of different sliding window lengths on the detection effect.

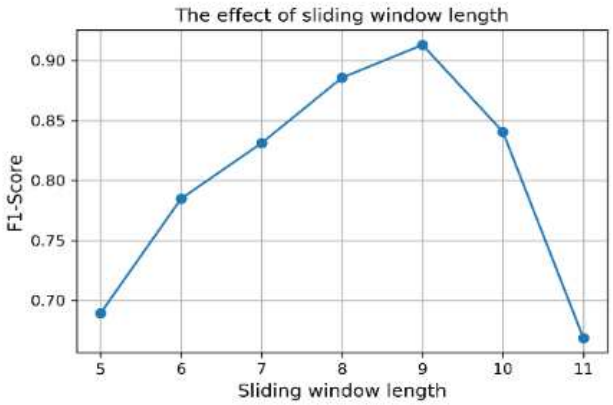

Fig. 8 Effect of sliding window length on the detection effect

For the data set used in this paper, the detection result is best when the sliding

window length is 9. By continuing to increase the window length, the detection effect gradually becomes worse because a longer window will mask the time change in a short time.

4.5 Comprehensive Test Results

Test set composition: 20 flight segments are selected, and attacks are injected into two sequence segments, [100,105] and [140,145], for different flight phases.

A training model with a window length of 9 is selected to test various anomalous attack types, as shown in Table 3 for the comprehensive test results.

Table 3 Average precision, recall, and F1-score

Attack type	Precision	Recall	F1-score
Random noise	0.9136	0.8902	0.8932
Fixed offset +	0.9667	0.8655	0.9109
Fixed offset -	0.9674	0.9242	0.9415
Route	0.9772	0.5751	0.6844
Height offset +	0.8656	0.5947	0.6824
Height offset -	0.8518	0.5284	0.6316
Speed offset +	0.9768	0.5341	0.6901
Speed offset -	0.9809	0.5530	0.7058
Heading	0.9788	0.4583	0.5914
Climb rate	0.8698	0.1856	0.3032

As shown in Table 3, this method has a low recall rate in regard to some more difficult attacks (warm-water boiled frog attacks). This is because the results are calculated from separate points when calculating these metrics. For example, in Figure 6, for attacks such as "height offset", although the attacked data were successfully detected, only one point located in the attacked sequence segment exceeded the

threshold. In this case, the recall rate is only 1/5 = 0.2. However, in the actual situation, the data enter the model in the form of sliding windows. Therefore, when an anomalous point is detected, we reasonably suspect that all sliding windows containing that point have the possibility of containing the attacked data. If further analysis is performed, the attacked sequence segment can be accurately detected. The specific method is to change the statistical unit of the recall rate to the number of attacks; that is, the detection target becomes two sequence segments. In this way, the recall rate index is significantly improved. Table 4 shows the results after changing the statistical method.

Table 4 Average precision, recall, and F1-score (after changing the detection target)

Attack type	Precision	Recall	F1-score
Random noise	0.9136	1.0000	0.9548
Fixed offset +	0.9667	1.0000	0.9830
Fixed offset -	0.9674	1.0000	0.9834
Route	0.9772	1.0000	0.9885
Height offset +	0.8656	1.0000	0.9280
Height offset -	0.8518	1.0000	0.9200
Speed offset +	0.9768	1.0000	0.9883
Speed offset -	0.9809	1.0000	0.7058
Heading	0.9788	1.0000	0.5914
Climb rate	0.8698	0.8958	0.3032

4.5 Consideration of influencing factors

In addition, this paper also considers whether an attack on one feature will affect other features when attacked, that is, whether it will increase the false alarm rate. Figure 9 shows the latitude anomaly score graph when the altitude is modified. Figure 10 presents a partially enlarged view of the latitude anomaly score.

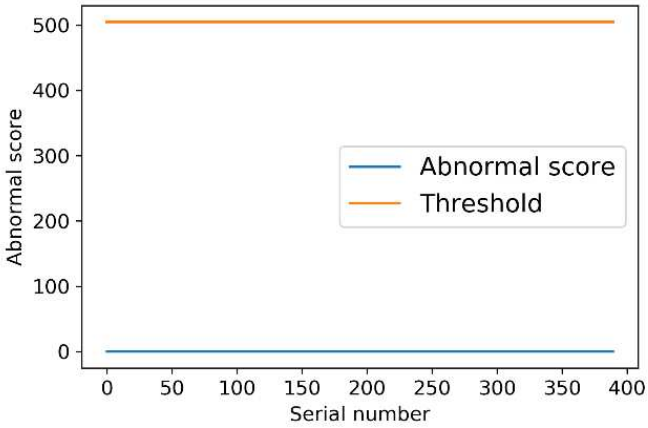

Fig. 9 Latitude anomaly score

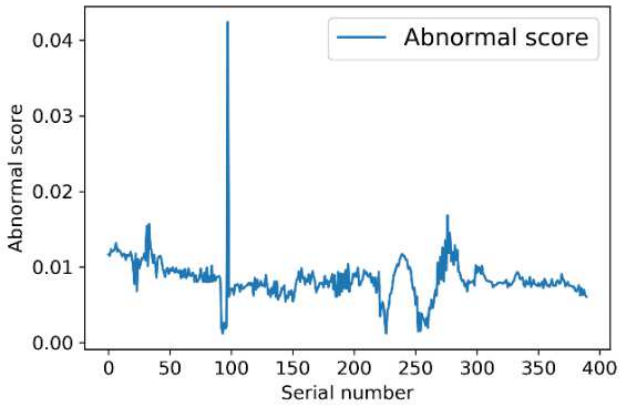

Fig. 10 Partially enlarged view of latitude anomaly

Figures 9-10 show that the latitude anomaly score exhibits only a small fluctuation in the attacked sequence segment ([100,105]), and the magnitude is much smaller than the anomaly threshold. A large number of tests show that when a feature is manipulated, the effect on the abnormal scores of other features is negligible.

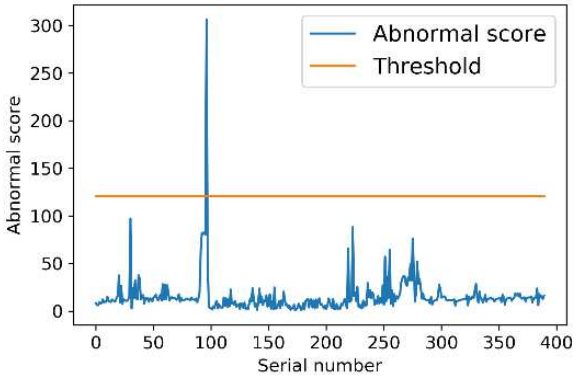

Fig. 11 Triggering effect of latitude change on the average threshold of all features

Figure 11 presents the triggering effect of modified latitude on the average threshold of all features. Similar tests for each feature modification show that a single feature modification will exactly trigger the overall threshold; that is, in practical applications, we can set the overall threshold first, and if anomalous data are detected using this threshold, then the specific feature threshold is used to identify the exact manipulated feature in a further step.

4.6 Discussion

In this work, we use public datasets in evaluation. It is possible that they contain a small degree of noise. Furthermore, their data volume is also limited. We will experiment with larger scale datasets in our future work. For the simulated anomalous data, the modified granularity needs to be further refined. Besides, this method can only find anomalies from a data perspective and cannot further lock the attacker.

On the other hand, although the proposed method cannot completely solve the security problem of the ADS-B system, it will certainly increase the difficulty for attackers to attack the system. Moreover, this method can be easily extended to other aeronautical data, such as GPS signals, radar data, etc.

5 Conclusion

Addressing typical security threats that ADS-B systems may currently suffer, this paper proposes a method for detecting ADS-B spoofing attacks based on LSTM. We use a neural network composed of LSTM units to predict an ADS-B message in the form of a sliding window and set a threshold value by calculating the residual of predicted values and true values to further detect attack data. The detection of 10 kinds

of simulated attack data in ADS-B messages shows that this method can effectively detect attack data and further identify the specific features under attack. Since this method does not require complicated feature engineering, the participation of additional nodes, and modification of the existing protocol, it has strong operability in future practical applications.

Declarations

Abbreviations

ADS-B: Automatic Dependent Surveillance-Broadcast

LSTM: Long short-term memory

PSR: Primary surveillance radar

SSR: Secondary surveillance radar

MLAT: Multilateration

ATC: Air Traffic Controller

NextGen: next-generation

DOA: Direction of Arrival

Acknowledgements

This work is supported by the National Natural Science Foundation of China (NSFC) (U1833114), and Central University Foundation of Civil Aviation University of China (3122019124)

Authors' contributions

JW conceived of the study, participated in the summary of the types of attacks and helped to draft the manuscript. YZ participated in its design and coordination, carried

out the training and testing of the method and helped to draft the manuscript. JD participated in the study of related work, and helped to draft the manuscript. All authors read and approved the final manuscript.

Funding

National Natural Science Foundation of China (NSFC) (U1833114)

Central University Foundation of Civil Aviation University of China (3122019124)

Availability of data and materials

The datasets analyzed during the current study are available in https://github.com/junzis/meteo-particle-model.

Competing interests

The authors declare that they have no competing interests.

References

[1] COSTIN A, FRANCILLON A. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices[C]. Black Hat USA, 2012: 1-12.

[2] SCHÄFER M, LENDERS V, MARTINOVIC I. Experimental analysis of attacks on next generation air traffic communication[C]//International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2013: 253-271.

[3] FINKE C, BUTTS J, MILLS R, et al. Enhancing the security of aircraft surveillance in the next generation air traffic control system[J]. International Journal of Critical Infrastructure Protection, 2013, 6(1): 3-11.

[4] COSTIN A, FRANCILLON A. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices[J]. Black Hat USA, 2012: 1-12.

[5] BAEK J, HABLEEL E, BYON Y J, et al. How to protect ADS-B: confidentiality framework and efficient realization based on staged identity-based encryption[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 18(3): 690-700.

[6] KACEM T, WIJESEKERA D, COSTA P, et al. Key distribution mechanism in secure ADS-B networks[C]//2015 Integrated Communication, Navigation and Surveillance Conference (ICNS). IEEE, 2015: P3-1-P3-13.

[7] JOHNSON J, NEUFELDT H, BEYER J. Wide area multilateration and ADS-B proves resilient in Afghanistan[C]//2012 Integrated Communications, Navigation and Surveillance Conference. IEEE, 2012: A6-1-A6-8.

[8] WANG W Y, LI W J, LU D, et al. ADS-B Spoofing Detection Method Using TDOA Correlation Coefficient[J]. Journal of signal processing, 2019, 35(11):1784-1790 (in Chinese)

[9] KAUNE R, STEFFES C, RAU S, et al. Wide area multilateration using ADS-B transponder signals[C]//2012 15th International Conference on Information Fusion. IEEE, 2012: 727-734.

[10] STROHMEIER M, MARTINOVIC I, Lenders V. A k-NN-based localization approach for crowdsourced air traffic communication networks[J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 54(3): 1519-1529.

[11] NAGANAWA J, TAJIMA H, MIYAZAKI H, et al. ADS-B anti-spoofing performance of monopulse technique with sector antennas[C]//2017 IEEE Conference on Antenna Measurements & Applications (CAMA). IEEE, 2017: 87-90.

[12] CHEN L, WU R B, LU D. ADS-B spoofing detection method using doppler effect[J]. Journal of Signal Processing, 2018, 34(6):722-728.

[13] WANG W, CHEN G, WU R, et al. A low-complexity spoofing detection and suppression approach for ADS-B[C]//2015 Integrated Communication, Navigation and Surveillance Conference. Piscataway, NJ: IEEE Press, 2015: K2-1-K2-8.

[14] HABLER E, SHABTAI A. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages[J]. Computers & Security, 2018, 78: 155-173.

[15] DING J L, ZOU Y K, WANG J et al. ADS-B anomaly data detection model based on deep learning [J] Acta Aeronautica et Astronautica Sinica. 2019, 40(12)：167-177.

[16] GRAVES A, SCHMIDHUBER J. Framewise phoneme classification with bidirectional LSTM and other neural network architectures [J]. Neural Networks, 2005, 18(5-6): 602-610.

[17] RTCA Special Committee. Minimum aviation system performance standards for automatic dependent surveillance broadcast (ADS-B) [R]. Technical report, January, 1998.

[18] STROHMEIER M, LENDERS V, MARTINOVIC I. On the security of the automatic dependent surveillance-broadcast protocol [J]. IEEE Communications Surveys & Tutorials, 2014, 17(2): 1066-1087.

[19] MANESH M R, KAABOUCH N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system[J]. International Journal of Critical Infrastructure Protection, 2017, 19: 16-31.

[20] CHAN-TIN E, HEORHIADI V, HOPPER N, et al. The frog-boiling attack: Limitations of secure network coordinate systems [J]. ACM Transactions on Information and System Security, 2011, 14(3): 27.

[21] Junzi Sun, Meteo-Particle model for wind and temp-erature field construction using Mode-S data[DB/OL], https://github.com/junzis/meteo-particle-model, 2018-01-30.

Figures

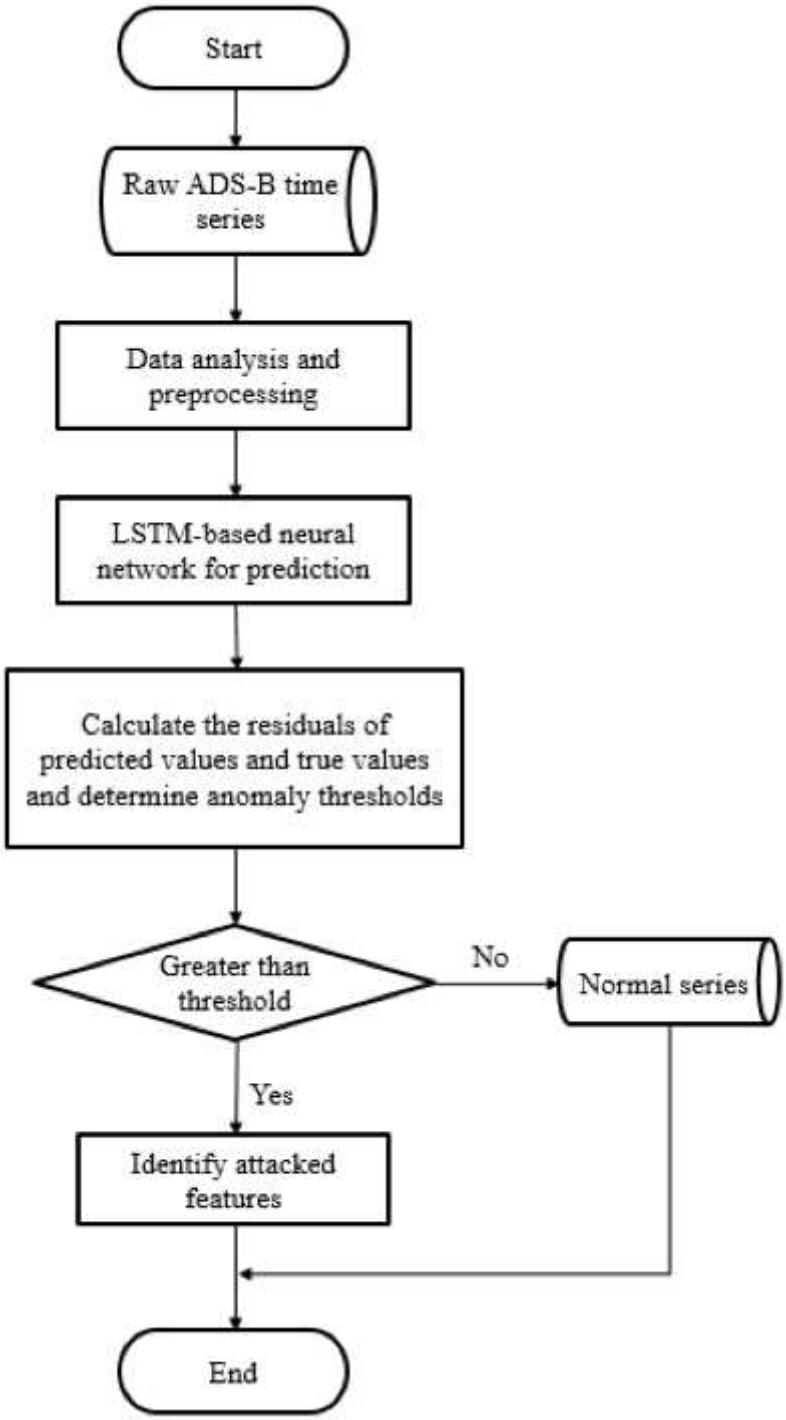

Figure 1

Overall process

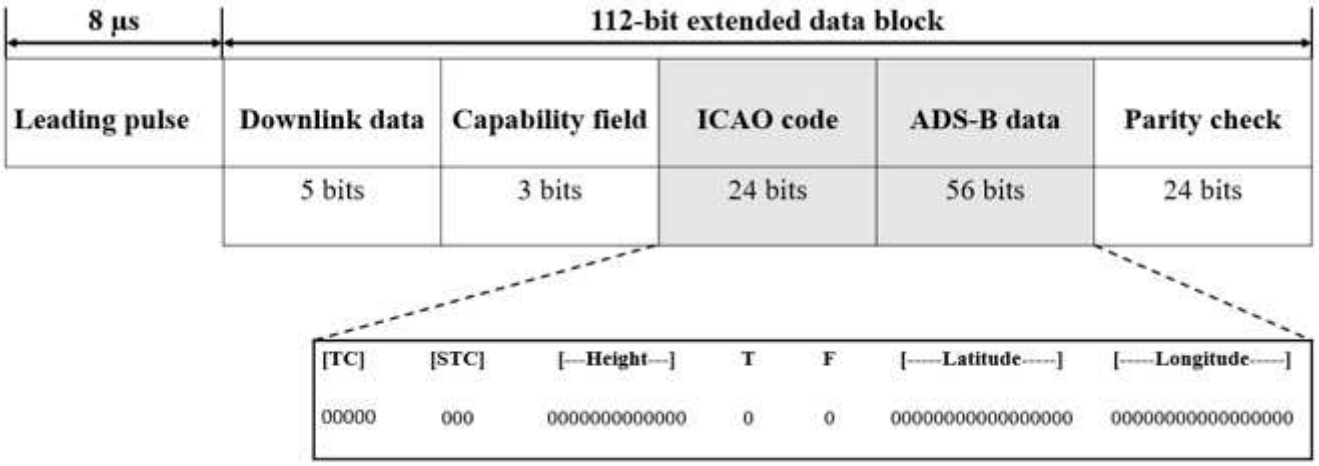

Figure 2

ADS-B protocol

Figure 3

Data preprocessing steps

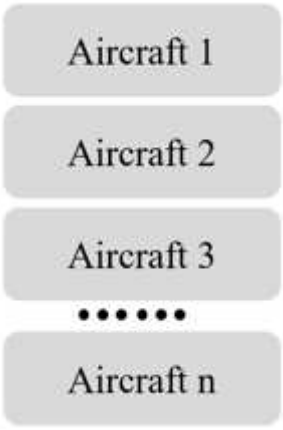

Figure 4

Data set arrangement

	Timestamp	ICAO	Lat	Lon	Alt	Speed	HDG	ROC
2	1483255284	400802	51.75096	-0.17326	17575	402	60.2	3648
3	1483255284	400802	51.75152	-0.17166	17600	402	60.2	3648
4	1483255296	400802	51.76076	-0.14089	18225	405	67.7	3008
5	1483255301	400802	51.76404	-0.12672	18475	407	70.6	2816
6	1483255301	400802	51.76442	-0.12501	18500	407	70.6	2816
7	1483255303	400802	51.76538	-0.1204	18575	407	71.8	2624
8	1483255305	400802	51.76625	-0.1158	18625	408	72.9	2496
9	1483255312	400802	51.76972	-0.09529	18875	407	76.4	1984
10	1483255316	400802	51.7717	-0.08166	19025	408	76.8	1984
11	1483255322	400802	51.77414	-0.06447	19225	409	77	1984
12	1483255334	400802	51.7793	-0.02813	19625	411	77.1	1984
13	1483255335	400802	51.77973	-0.02518	19675	411	77.1	1984
14	1483255336	400802	51.78017	-0.02212	19700	411	77.1	1984
15	1483255344	400802	51.78331	0	19975	412	77	2368

Figure 5

Data sample

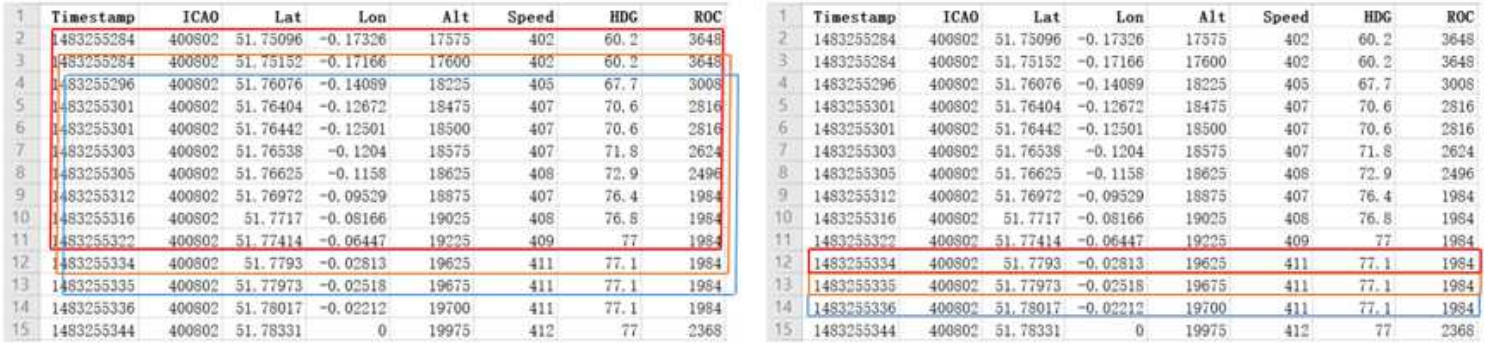

Figure 6

Illustration of the sliding window

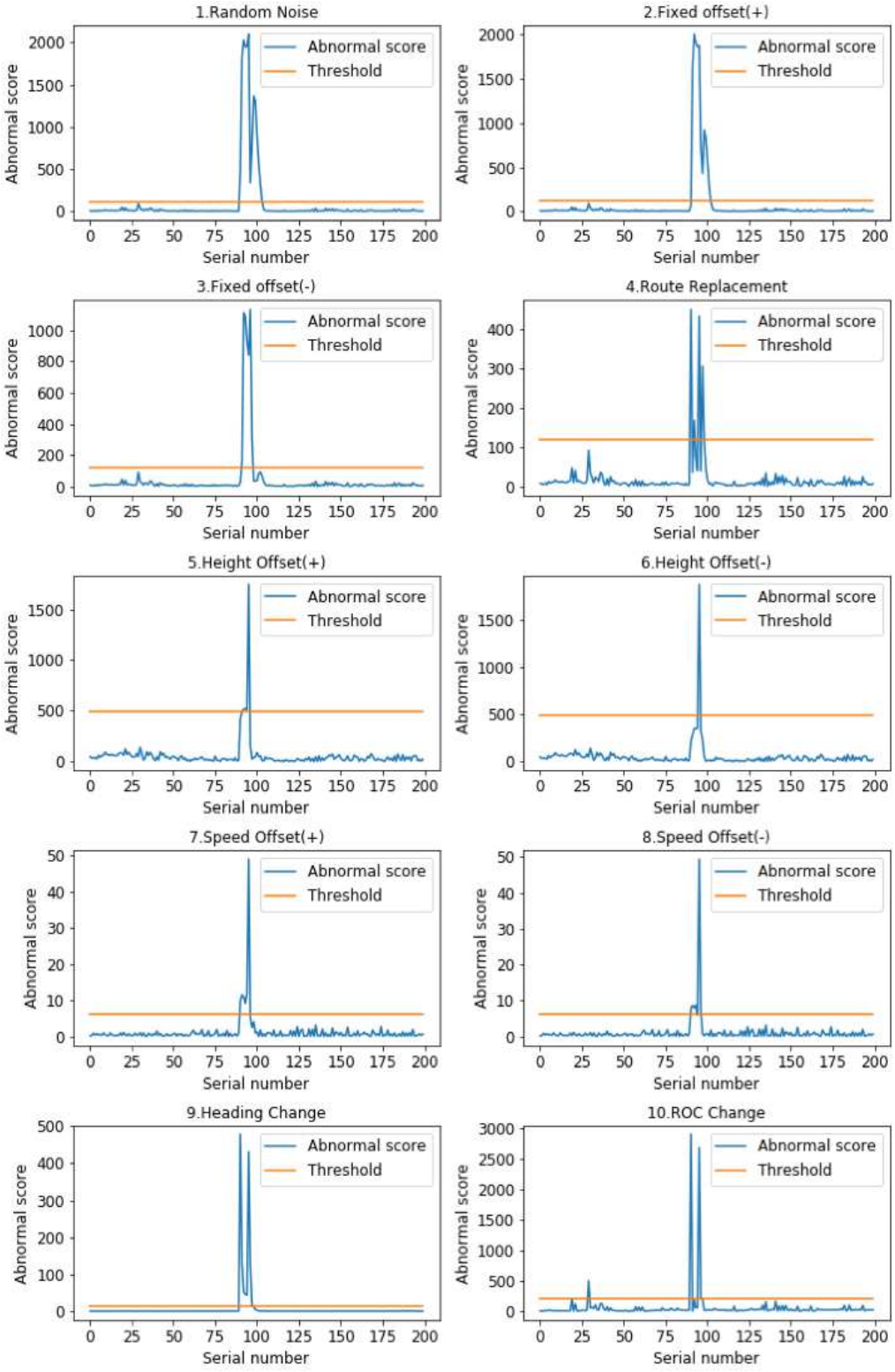

Figure 7

Abnormal score figures

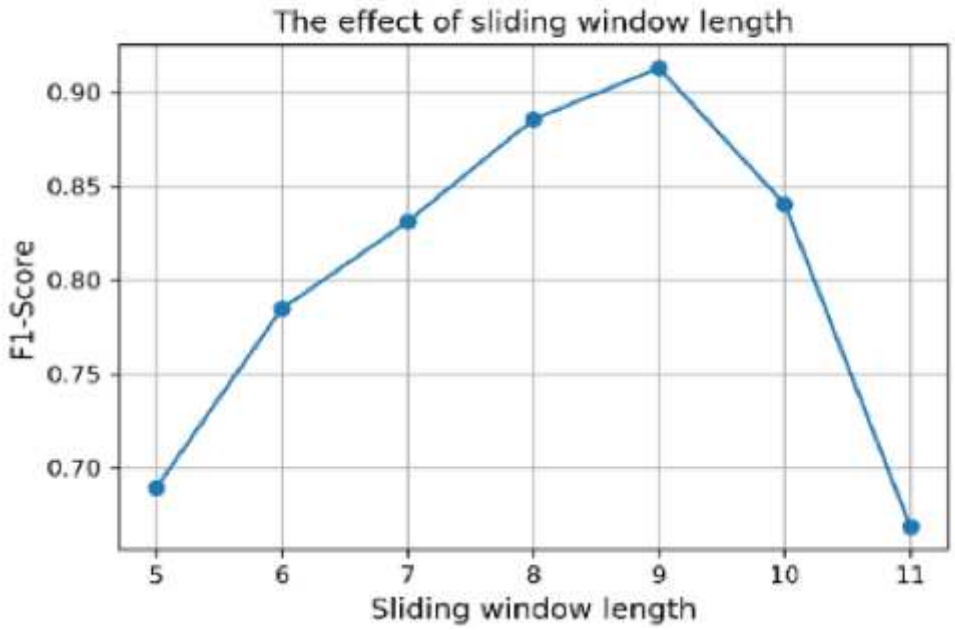

Figure 8

Effect of sliding window length on the detection effect

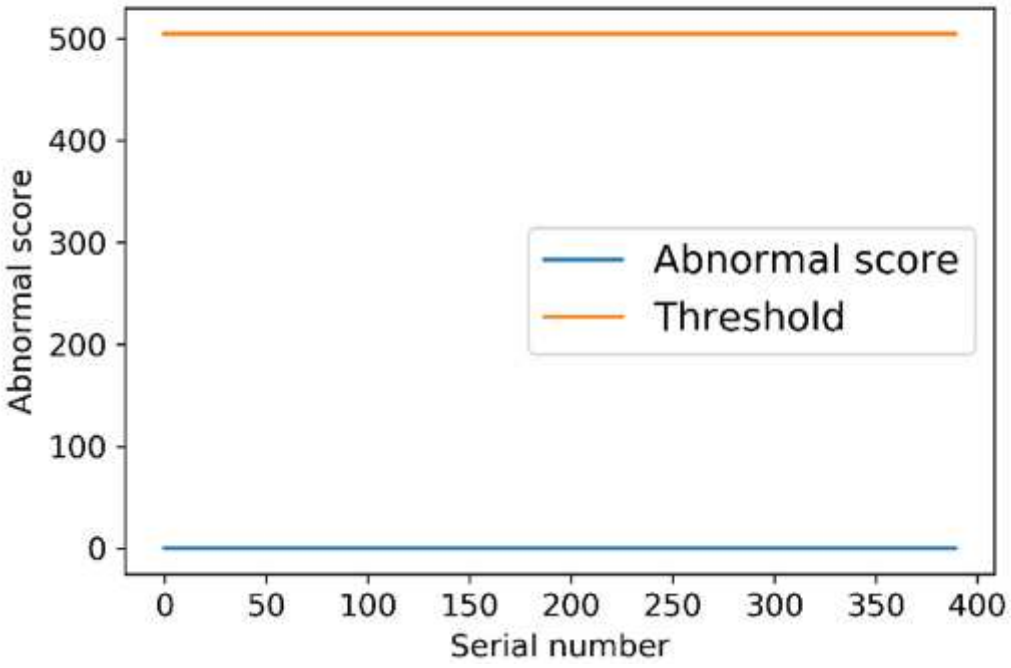

Figure 9

Latitude anomaly score

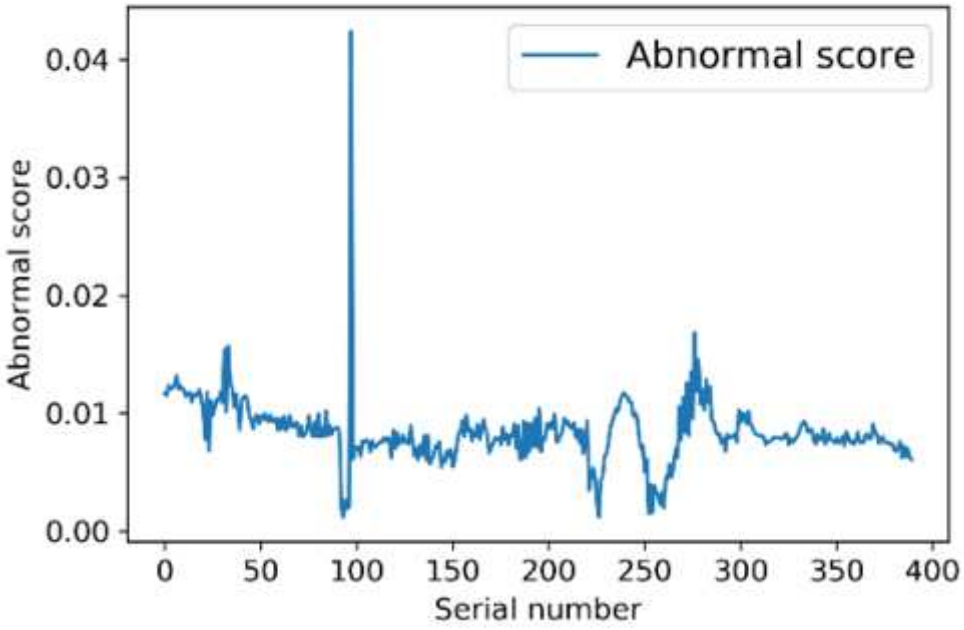

Figure 10

Partially enlarged view of latitude anomaly

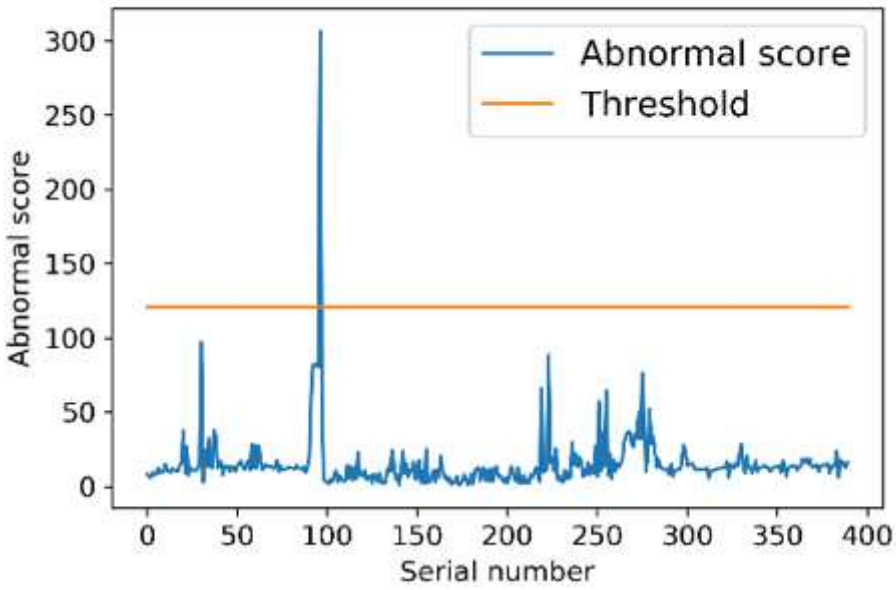

Figure 11

Triggering effect of latitude change on the average threshold of all features