Computers & Security 141 (2024) 103840

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

TTSAD: TCN-Transformer-SVDD Model for Anomaly Detection in air traffic ADS-B data

Peng Luo *, Buhong Wang, Jiwei Tian

Information and Navigation College, Air Force Engineering University, Xi'an, Shanxi Province, China

ARTICLE INFO

Keywords:
ADS-B
Anomaly detection
Deep learning
TCN
Transformer

ABSTRACT

ADS-B (Automatic Dependent Surveillance-Broadcast) is a key technology in the new generation air traffic surveillance system. However, it is vulnerable to various cyber attacks because it broadcasts data in plaintext format and lacks authentication mechanism. Previous research has rarely considered the application scenarios of ATM (Air Traffic Management) in commercial air transport, and there are the problems of low anomaly detection rate and the non-lightweight model. This paper focuses on ADS-B anomaly detection under the background of ATM. We propose the TTSAD (**T**CN-**T**ransformer-**S**VDD Model for **A**nomaly **D**etection) model, which aims to address the problems of existing ADS-B anomaly detection methods including inadequate considerations of long-term dependencies and distribution characteristic, the non-lightweight model and the poor adaptive threshold. First, ADS-B time series is input into TCN (Temporal Convolutional Network) prediction module which predicts data in an accurate and quick way using causal convolution and dilated convolution. Then, the predicted ADS-B time series is input into Transformer reconstruction module which reconstructs data accurately and quickly based on Self-Attention and Multi-Head Attention mechanism. Finally, the difference values between the reconstructed values and the real values are input into SVDD (Support Vector Data Description) threshold determination module for an optimal threshold. Experimental results show that the TTSAD model can detect ADS-B anomaly data generated from attacks such as altitude slow offset and DOS (Denial of Service). The TTSAD model is superior to other machine learning methods in terms of recall rate, detection rate, accuracy rate, missing detection rate and false alarm rate. Furthermore, compared with other deep learning methods including LSTM, GRU and LSTM-AE, the TTSAD model has a shorter training time and a lightweight characteristic. This approach guarantees the information security of ADS-B, thereby improving the operational security of ATM.

1. Introduction

With the advantages of high surveillance accuracy, large surveillance range, support for information sharing and low cost, ADS-B has become a key technology for the new generation ATM surveillance system (Sampigethaya et al., 2011). ADS-B data is considered an essential data source for ATM system. It has a critical impact on the ATM subsystems such as flight separation management, air traffic flow management and traffic collision avoidance (Strohmeier et al., 2017; Strohmeier et al., 2014). However, ADS-B data is broadcast in plaintext format and lacks authentication mechanism, making it vulnerable to various attacks carried out with cheap SDR (Software Defined Radio) devices (Costin and Francillon, Jul. 2012; Schafer et al., 2013). In our previous work, a lot of types of attacks on ADS-B data are modeled (Li and Wang, 2019). If ADS-B data are attacked, the security of the entire ATM system will be threatened. Therefore, it is crucial to research security methods for solving ADS-B vulnerabilities.

At present, security solutions for ADS-B vulnerabilities mainly include encryption schemes and non-encryption schemes. Encryption schemes encrypt ADS-B data before it is attacked (Baek et al., 2017). However, it is difficult to implement encryption schemes because encryption schemes are not compatible with the existing ADS-B standardized protocol. Non-encryption schemes detect ADS-B anomaly data by using physical layer information (Strohmeier and Martinovic, 2015), multilateration (Nijsure et al., 2016) and machine learning (Habler and Shabtai, 2018). Recently, machine learning, with the advantage of fast and intelligent processing of big data, has been gradually applied to the field of ADS-B anomaly detection. Machine learning method usually detects ADS-B anomaly data based on the prediction errors and the reconstruction errors (Habler and Shabtai, 2018; Li et al., 2019; Luo

* Corresponding author.
E-mail address: bluebird690212@163.com (P. Luo).

https://doi.org/10.1016/j.cose.2024.103840
Received 3 July 2023; Received in revised form 23 February 2024; Accepted 30 March 2024
Available online 31 March 2024

et al., 2021). In our previous work, HTM (Hierarchical Temporal Memory) model is built to predict ADS-B data and detect ADS-B anomaly data by analyzing prediction errors (Li et al., 2019). Also, VAE (Variational AutoEncoder) model is used to detect ADS-B anomaly data based on the reconstruction errors in our previous work (Luo et al., 2021). Machine learning method makes full use of the temporal correlation of ADS-B data to establish anomaly detection model, which has the advantages of not modifying ADS-B protocol, not adding ground station nodes and detecting ADS-B anomaly data quickly.

However, there are still some problems to be solved when using machine learning to detect ADS-B anomaly data. First, existing methods have not fully considered the context information and the distribution characteristic of ADS-B time series, resulting in that the performance of recall rate, detection rate, missing detection rate and false alarm rate still need to be improved. Second, the disadvantage of existing methods is that the training time is too long and the model is not lightweight. Third, the threshold determined by manual analyzing the prediction errors or the reconstruction errors has a poor adaptability.

In order to solve the above problems, this paper proposes the TTSAD model for ADS-B anomaly data detection which considers a variety of attack styles including random position deviation, fixed position deviation, altitude slow offset, velocity slow offset and DOS attack. The major contributions of this research are generalized as follows:

(1) The temporal correlation of ADS-B time series is fully considered based on TCN causal convolution. Also, it is able to capture the long-term temporal dynamics of ADS-B time series since the perceptual field can be extended using TCN dilated convolution.
(2) In addition to parallel computing and training ADS-B time series, the problem of gradient disappearance can be alleviated based on one-dimensional convolutional network in the TCN prediction module and Self-Attention mechanism in the Transformer reconstruction module. Therefore, it can train ADS-B data with lightweight characteristic and detect ADS-B anomaly data in real time.
(3) The context information and the distribution characteristic of ADS-B time series can be fully learned based on Multi-Head Attention mechanism in the Transformer reconstruction module. As a result, ADS-B anomaly data can be reconstructed and detected accurately.
(4) In order to determine an optimal threshold, the difference values between ADS-B reconstructed values and ADS-B real values are input into the SVDD threshold determination module for secondary training. Therefore, an optimal threshold is obtained which can improve recall rate, detection rate and accuracy rate.

The paper is organized as follows. Section 2 introduces the working principle of ADS-B and previous solutions for ADS-B vulnerabilities. Section 3 provides the problem definition of ADS-B anomaly detection. Section 4 constructs the TTSAD model for detection ADS-B anomaly data and describes each sub-module. Section 5 shows the experimental results and compares the TTSAD model with other machine learning methods. Section 6 makes conclusions.

2. Related works

2.1. ADS-B

ADS-B has become a key technology for the new generation ATM surveillance system. Fig. 1 depicts the working principle of ADS-B. The aircrafts obtain precise position information from GNSS (Global Navigation Satellite System) and other information such as heading and velocity from the onboard devices, which is encapsulated in ADS-B data format. The aircrafts equipped with ADS-B Out broadcast the ADS-B data over the 1090ES (1090 MHz Extended Squitter) or UAT (Universal Access Transceiver) communication channel. The nearby aircrafts

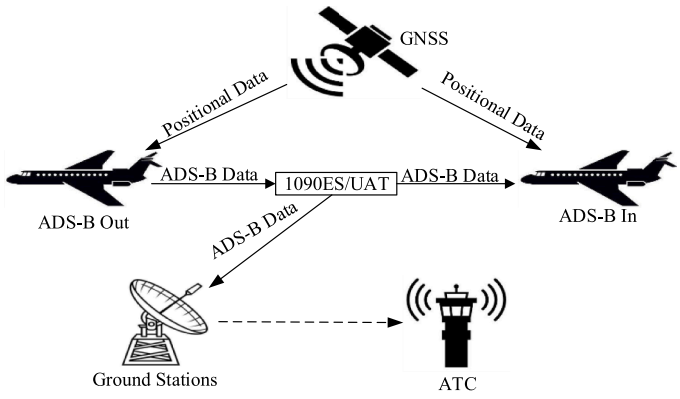

Fig. 1. working principle of ADS-B.

equipped with ADS-B In can receive ADS-B data. The ground stations receive and process ADS-B data which is then sent to the ATC (Air Traffic Control) system for further decision analysis. ADS-B messages can contain the following aircraft attributes. (1) icao24: the 24-bit aircraft transponder identifier. (2) time: the UNIX timestamp. (3) longitude: east–west position on the Earth's surface. (4) latitude: north–south position on the Earth's surface. (5) altitude: the altitude above sea level. (6) velocity: the speed over ground of the aircraft. (7) heading: the direction of movement.

However, ADS-B broadcasts data in plaintext format. Therefore, ADS-B data is vulnerable to eavesdropping, jamming, message injection, message modification, and message deletion. Table 1 shows the way and effect of ADS-B attack.

Eavesdropping: ADS-B data can be easily eavesdropped because it is sent in plaintext format. However, eavesdropping will not cause harm directly. It is the basis for other attacks. The attackers can obtain status information of aircraft through eavesdropping.

Jamming: Jamming is a problem common to all wireless communication. The attackers can implement the attacks by sending jamming signals with sufficiently high power in the relevant frequency band. The attacks can jam the transmission of ADS-B messages in a specific airspace through jamming.

Message Injection: Since the ADS-B system does not have an authentication mechanism, the attackers implement message injection attacks by constructing a transmitter that can generate the correct modulated and formatted ADS-B messages. Due to message injection, a large number of false tracks appear in the air traffic surveillance system, which disrupt the safety and order of air traffic. Therefore, the severity level of message injection is relatively high.

Table 1
Way and effect of ADS-B attack.

Attack type	Way of ADS-B attack	Effect of ADS-B attack
Eavesdropping	Obtain ADS-B data through ADS-B IN device	Eavesdrop status information of aircraft
Jamming	Send ADS-B jamming signals with sufficiently high power in the relevant frequency band by using an ADS-B transmitting device	Jam the transmission of ADS-B messages in a specific airspace
Message injection	Generate correct modulated and formatted ADS-B messages by using an ADS-B transmitting device	Inject fake aircraft into specific flight scenarios and confuse air traffic control systems
Message Deletion	Launch this attack through constructive or destructive interference at the physical layer	Cause the disappearance of the tracks in the air traffic control systems
Message Modification	Launch this attack by overshadowing and bit-flipping at the physical layer	Modify the tracks and confuse air traffic control systems

Message Deletion: The attackers launch the attacks through constructive or destructive interference at the physical layer (Strohmeier et al., 2014). Message deletion causes the disappearance of the tracks in the air traffic surveillance system.

Message Modification: Message modification is implemented by injecting deviations into the actual ADS-B data, which has high severity level. The attackers launch the attacks by overshadowing and bit-flipping at the physical layer (Strohmeier et al., 2014). The difficulty of implementing message modification is high because it requires strict time synchronization.

2.2. Security solutions for ADS-B vulnerabilities

At present, the security solutions for ADS-B vulnerabilities mainly include four categories. The four categories are encryption, physical layer information, multilateration and machine learning. Table 2 provides a comparison of the existing four types of research methods.

2.2.1. Encryption

ADS-B encryption method uses keys to directly encrypt ADS-B plaintext or generate corresponding integrity information, so as to provide information basis for ADS-B security reinforcement (Yang et al., 2019). In order to make up for the authenticity and integrity defects of the previous ADS-B agreement, HMAC (hash message authentication code) method is used to prevent and detect multiple ADS-B attacks (Kacem et al., 2018). An ADS-B message authentication method based on certificateless short signature is proposed to study the authenticity and integrity of information by signing messages (Wu et al., 2020). This proposed method does not require certificate management and has the efficient performance. A novel and efficient pairing-free ADS-B authentication batch verification scheme is presented in ID-based setting (Thumbur et al., 2019). The proposed scheme is proved to be unforgeable against chosen message and identity attack in the random oracle model under the hardness of elliptic curve discrete logarithm problem. However, encryption method needs to modify the original ADS-B protocol, which hinders system compatibility and international interoperability.

2.2.2. Physical layer information

When ADS-B data is transmitted by wireless communication, the data is attached with physical fingerprint information, which is the basis to analyze the probability of attack behaviors (Strohmeier and Martinovic, 2015; Li et al., 2020). Hypothesis testing is used to detect attacks on ADS-B according to the negative correlation between the received signal strength and the distance (Strohmeier et al., 2015a). A realistic jamming threat model is developed for the ADS-B communication and a physical level ADS-B security solution based on a signal separation method is proposed in a multichannel receiver (Leonardi et al., 2021; Leonardi and Galati, 2017). However, when the attackers obtain the prior knowledge of physical layer information through statistical analysis, the applicability of the method still needs to be further verified for sophisticated ADS-B data attacks.

Table 2
Summary of related work.

Methods	Protocol modification required or additional nodes required	Advantages and Disadvantages
Encryption	Requires modifying the original ADS-B protocol.	Disadvantages: Encryption methods need to modify the original ADS-B protocol, which hinders system compatibility and international interoperability.
Physical layer information	Requires ground stations and other entities.	Disadvantages: When attackers obtain the prior knowledge of physical layer information through statistical analysis, the applicability of the method still needs to be further verified for sophisticated ADS-B data attacks.
Multilateration	Requires more than one sensor or entity.	Disadvantages: The locations of ground stations need to be near airports and air routes.
Machine learning	Does not require modifying protocol and additional nodes.	Advantages: Machine learning method makes full use of ADS-B time series to detect anomaly data quickly and accurately.

2.2.3. Multilateration

Multilateration method usually uses TDOA (Time Difference of Arrival) to measure the position of the aircrafts and compares it with the parsed ADS-B position (Monteiro et al., 2015). If the difference between the two position is too large, the ADS-B message is illegal (Shang et al., 2019). Comparing the position calculated by TDOA, AOA (Angle of Arrival), FDOA (Frequency Difference of Arrival) with the parsed position can judge whether attack behaviors happen (Nijsure et al., 2016). A method for location verification is proposed by tracking of the different sensors' clocks using the measured TDOA of the ADS-B messages (Leonardi, 2019). However, multilateration method requires deploying multiple ground stations, which is not economical. Moreover, the locations of ground stations need to be near airports and air routes.

2.2.4. Machine learning

Machine learning method usually detects ADS-B anomaly data based on the prediction errors and the reconstruction errors (Habler and Shabtai, 2018). LSTM (Long Short-Term Memory) is usually used to predict ADS-B data and determine whether ADS-B data is anomalous based on the prediction errors (Wang et al., 2020). In our previous work, HTM is used to detect ADS-B anomaly data by analyzing the prediction error (Li et al., 2019). It has the advantage of learning and predicting ADS-B data at the same time, so the online performance of anomaly detection is better. However, HTM is not suitable for detecting long duration attacks. Encoder-Decoder is used to reconstruct ADS-B data and determine whether ADS-B data is anomalous based on the reconstruction errors (Akerman et al., 2019; Habler and Shabtai, 2022). Encoder-Decoder generally uses RNN (Recurrent Neural Network) as the hidden layer to preserve the temporal correlation of ADS-B data. In order to make full use of temporal correlation of ADS-B data, VAE is used to detect ADS-B anomaly data based on the reconstruction errors (Luo et al., 2021). Machine learning method makes full use of the temporal correlation of ADS-B data to establish anomaly detection model, which has the advantages of not modifying ADS-B protocol, not adding ground station nodes and detecting ADS-B anomaly data quickly.

With the scale of ADS-B data increasing, utilizing machine learning to analyze ADS-B is feasible. However, there are still some problems to be solved when using machine learning to detect ADS-B anomaly data. First of all, existing methods have not fully considered the context information and the distribution characteristic of ADS-B time series. In the second place, the training time of existing methods is too long and the model is not lightweight. In the end, the threshold determined by manual analyzing the prediction errors or the reconstruction errors has a poor adaptability.

3. Background

3.1. Problem definition

Define time series $\boldsymbol{X} = \langle X_1, X_2, \cdots, X_L \rangle$ as the original ADS-B data received by the model, and L is the length of time series. $X_j = [t, id, lon, lat, alt, vel, f_7, \cdots, f_n]$ is a n-dimensional vector, and j is not greater than L. t denotes the time, iddenotes the 24-bit ICAO (International Civil Aviation Organization) transponder identity number, lon denotes the longitude, lat denotes the latitude, alt denotes the altitude, vel denotes the velocity, and $[f_7, f_8, \cdots, f_n]$ denotes other features of ADS-B data.

Fig. 2 shows the general flow chart of anomaly detection method in this paper. At first, ADS-B time series $X = \langle X_1, X_2, \cdots, X_L \rangle$ is input. The normalized time series $Y = \langle Y_1, Y_2, \cdots, Y_L \rangle$ is obtained after data preprocessing. Then, the TTSAD model processes time series Y in two steps. Firstly, TCN prediction module and Transformer reconstruction module process ADS-B time series to obtain the reconstructed time series $\overline{Y} = \langle \overline{Y_1}, \overline{Y_2} \cdots, \overline{Y_L} \rangle$. Secondly, the difference value $\{D_j | D_j = \overline{Y_j} - Y_j\}$ is put into the SVDD threshold determination module to obtain the center a of SVDD hypersphere and the threshold R. Finally, if the distance from the difference value D_j to the center a is greater than the threshold R, X_j is ADS-B anomaly data. If the distance from the difference value D_j to the center a is smaller than the threshold R, X_j is ADS-B normal data.

3.2. Data preprocessing

Data preprocessing includes four parts: lost packet complement, feature selection, normalization and sliding window selection. Due to the influence of wireless channel noise, there is a certain packet loss rate of ADS-B data. In this paper, the interpolation method is used to complement the lost ADS-B data. If ADS-B data X_j is lost at the moment t_j, X_j can be expressed as follows:

$$\begin{cases} X_j = X_{j-1} + b \times (t_j - t_{j-1}) \\ b = \dfrac{X_{j+1} - X_{j-1}}{t_{j+1} - t_{j-1}} \end{cases} \tag{1}$$

X_{j-1}, X_j and X_{j+1} are ADS-B data at the moment t_{j-1}, t_j and t_{j+1}respectively. b is the slope.

There are two reasons why ADS-B data can be represented as$X_j = [t, id, lon, lat, alt, vel, f_7, \cdots f_n]$. (1) As a new ATM surveillance technology, the most important role of ADS-B is to monitor and track flight information

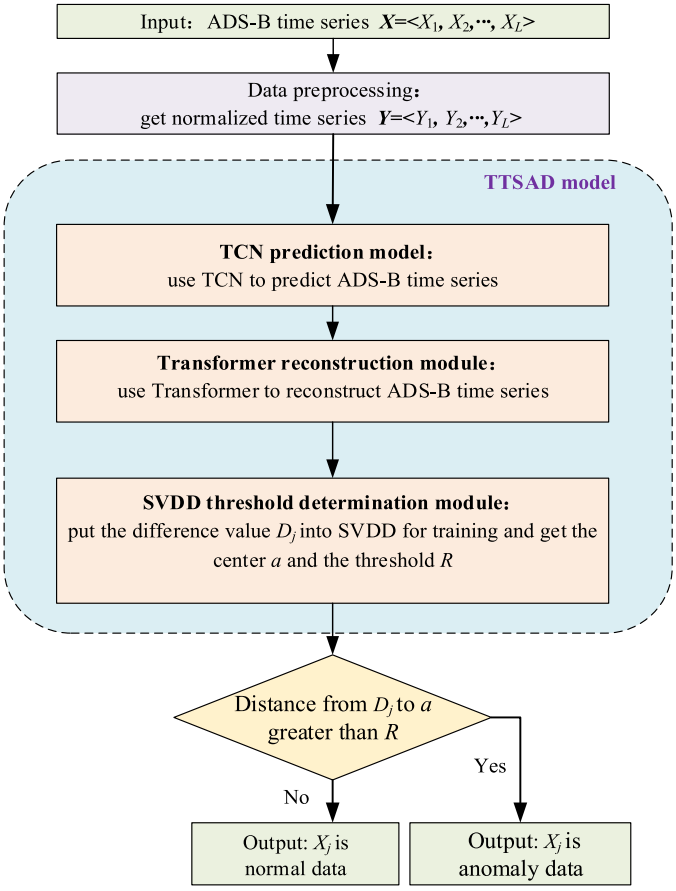

Fig. 2. Flow chart of anomaly detection.

such as position and velocity of aircraft in real time, and broadcast the information to the nearby aircraft and ground stations (Strohmeier et al., 2014). Therefore, the most used and important features in ADS-B data generally include time, aircraft identity number, longitude, latitude, altitude and velocity. (2) From the attacker's perspective, the intention is to disrupt the safety and order of air traffic through ADS-B data attack. Therefore, the attacker will choose the feature like longitude, latitude, altitude and velocity to launch message injection and tampering attacks (Li et al., 2019; Li et al., 2020). As a result, the aircraft will be in an unsafe flight state, such as the aircraft flying to the wrong position and the aircraft colliding with each other.

Fig. 3 shows the heatmap about a feature correlation analysis of ADS-B data from 10 different flights. The feature aircraft identity number is not included in the heatmap. Because the feature aircraft identity number of the same flight does not change at any time, there is no correlation between the feature aircraft identity number and the other features. According to the heatmap, except velocity and altitude, the correlation degree of time, longitude, latitude, velocity and altitude is weak. In order to locate the source of the attack and reduce computational complexity, time series $F = \langle F_1, F_2, \cdots, F_j, \cdots, F_L \rangle$ is selected to represent the feature sequence. Among them, F_j is a four-dimensional vector, and the selected four features represent latitude, longitude, altitude and velocity respectively. There are some reasons why latitude, longitude, altitude and velocity are chosen as the selected four features. (1) First of all, in terms of the high stealth of the attack, the attacker will choose the feature like the longitude, latitude, altitude and velocity to launch ADS-B data attack. If the feature is attacked with minor message tampering, it is difficult for air traffic controllers and pilots to discover and detect anomalies in real-time flight trajectories. (2) Secondly, in order to accurately locate the source of the attack, although the correlation between the feature altitude and velocity is high, both features need to be preserved. The reasons are as follows. The target of the attacker is usually the feature longitude, latitude, velocity and altitude. In order to accurately locate the source of the attack, the anomaly detection model usually predicts or reconstructs the feature of ADS-B data. For example, if the attacker launches ADS-B tampering attack on the feature velocity, the error between the predicted or reconstructed value and the real value of the velocity is obviously large. Therefore, the source of the attack can be located as velocity. Similarly, if the attacker launches ADS-B tampering attack on the feature altitude, the error between the predicted or reconstructed value and the real value of the altitude is obviously large. Therefore, the source of the attack can be located as altitude. (3) Thirdly, from the perspective of the impact of the attack on air traffic, the attacker usually chooses the feature like longitude, latitude, altitude and velocity as attack objects. As a result, the aircraft will be in an unsafe flight state, such as the aircraft flying to the wrong position and the aircraft colliding with each other. (4) Finally, the attacker usually does not select the feature time and aircraft identity number as attack objects. In terms of the stealth and success rate of the attack, the attack on time and aircraft identity number is easily discovered and detected immediately by the air traffic controllers and pilots because the attack obviously and clearly violates air traffic flight plans. As a result, the attacker rarely selects the feature time and aircraft identity number as attack objects in real air traffic environment.

Normalization is used to process time series F. The reasons for normalization are as follows. First, because different features have different value ranges and units, some features may be ignored if they are not normalized. Therefore, the result of anomaly detection may be affected. Second, the gradient oscillates because different features have different value ranges. As a result, the training process takes a long time to reach the global optimal value. The normalization process is as follows:

$$Y_j^i = \frac{F_j^i - \min(F^i)}{\max(F^i) - \min(F^i)}, \quad 1 \le i \le 4 \tag{2}$$

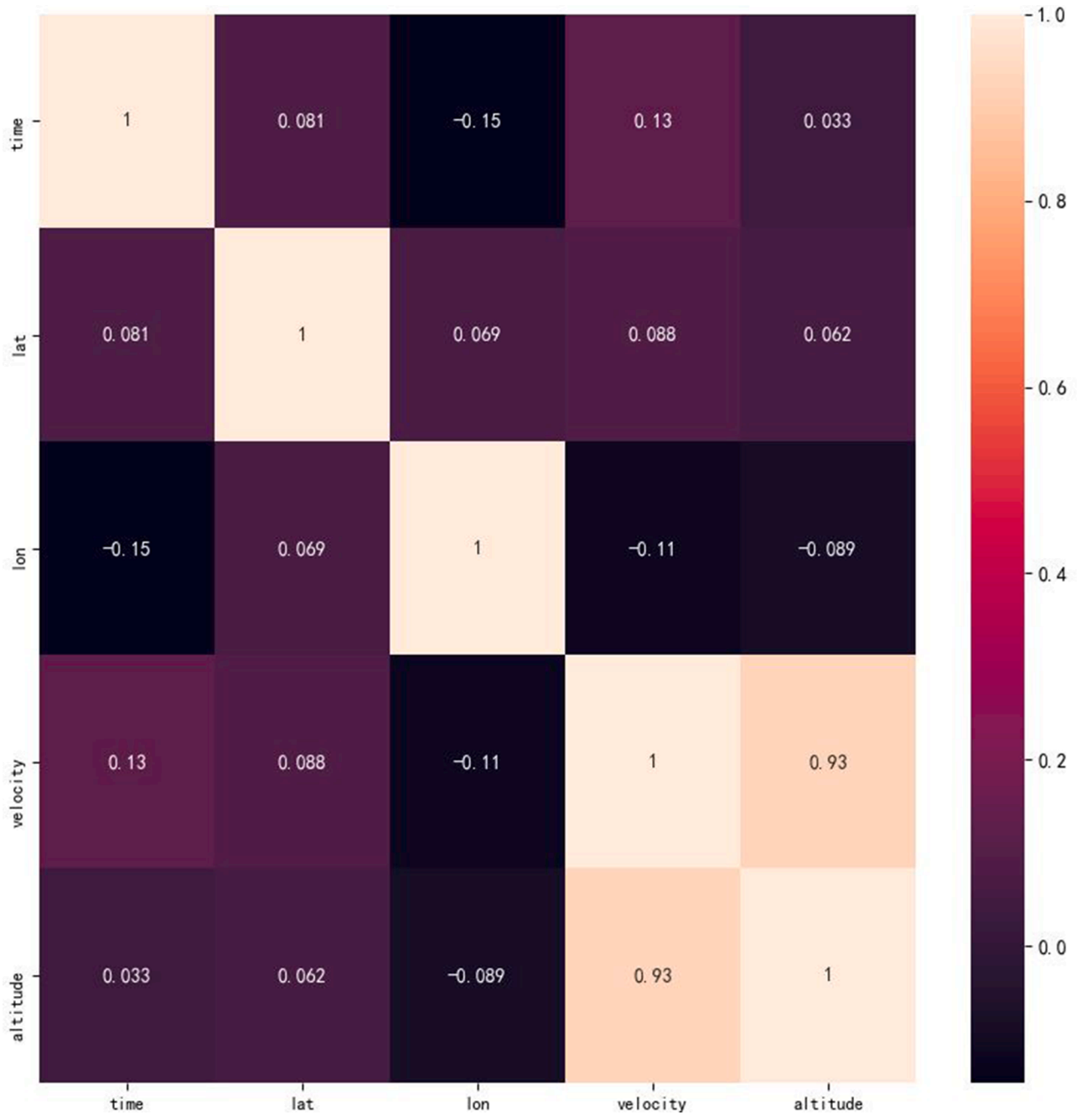

Fig. 3. Heatmap about feature correlation analysis.

The superscript i represents the ith feature. Because latitude, longitude, altitude and velocity are chosen as the four features, the maximum value of i is equal to 4. The subscript j represents the jth data, max() is the maximum function, and min() is the minimum function.

In order to make full use of the temporal correlation of ADS-B data, this paper uses the sliding window mechanism to input time series. As shown in Fig. 4, the sliding window $W_j = \langle Y_{j-S+1}, Y_{j-S+2}, \cdots, Y_j \rangle$ is defined as time series on the interval $[t_{j-S+1}, t_j]$. Here set the step of the sliding window to 1. Therefore, $W_{j+1} = \langle Y_{j-S+2}, Y_{j-S+3}, \cdots, Y_{j+1} \rangle$ is time series on the interval $[t_{j-S+2}, t_{j+1}]$.

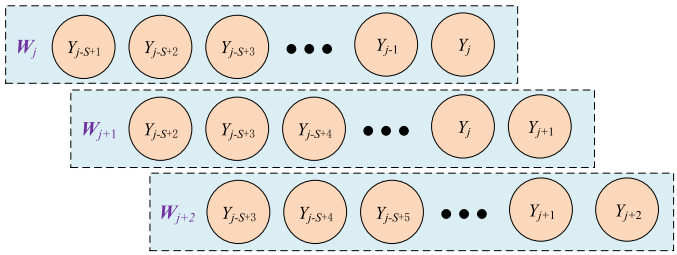

Fig. 4. Diagram of the sliding window.

4. The proposed TTSAD model

4.1. Model framework

Fig. 5 shows the overall architecture of the TTSAD model. The TTSAD model consists of three modules: TCN prediction module, Transformer reconstruction module and SVDD threshold determination module. First, TCN prediction module is based on one-dimensional convolutional network for fast computing and has the advantage of lightweight characteristic. Based on causal convolution and dilated convolution, TCN can accurately predict ADS-B time series by making full use of temporal correlation. Second, Transformer reconstruction module completes parallel computing based on the Self-Attention mechanism, so it can reconstruct ADS-B data in a quick way. The context information and distribution characteristic of ADS-B time series can be fully learned based on Multi-Head Attention mechanism in Transformer reconstruction module. As a result, ADS-B anomaly data can be reconstructed and detected accurately. Third, SVDD threshold determination module can improve the accuracy of anomaly detection by training the difference values, which make the determined threshold better.

4.2. TCN prediction module

TCN has been proven to be able to accurately and quickly detect anomaly time series (Thill et al., 2021; Cheng and Xu, 2019). It is necessary to make full use of temporal correlation for predicting and detecting ADS-B anomaly data. The advantages of using TCN are as follows: (1) ADS-B data is time series of aircraft trajectories, and the prediction of ADS-B data needs to be real-time and quick. TCN uses one-dimensional convolutional network instead of RNN, so it can avoid the gradient disappearance problem and can compute in parallel. As a result, it can quickly predict and detect ADS-B anomaly data. (2) TCN can predict ADS-B data accurately by taking temporal correlation into account based on causal convolution. (3) TCN gets a larger perceptual field based on dilated convolution. Thus, it can memorize long-term historical information of ADS-B time series. Fig. 6 depicts the architecture of TCN.

TCN can fully utilize temporal correlation of ADS-B data based on causal convolution and dilated convolution. Assuming that the number of layers is n, TCN convolution operation $F(t)$ can be defined as follows:

$$F(t) = \sum_{k=1}^{N} f_k x_{t-(N-k)d} \tag{3}$$

When d is the constant 1, $F(t)$ denotes causal convolution. The filter can be denoted as $f = (f_1, f_2, f_k, f_N)$. N denotes the size of the filter which is also convolution kernel. $x_{t-(N-k)}$ denotes the input data at time $t-(N-k)$.

When d is not the constant 1, $F(t)$ denotes dilated convolution. d is the dilation factor and can be denoted as $d = b^{i-1}$. b denotes the expansion base and usually takes the value 2. i takes the value range $i \in [1, n]$. $x_{t-(N-k)d}$ denotes the input data at time $t-(N-k)d$.

As shown in Fig. 6, when the dilation factor is d and the size of convolution kernel is N, the number of padding zeros can be expressed as:

$$padding = (N-1)d \tag{4}$$

Similarly, the size r of the perceptual field of each TCN convolutional layer can be expressed as follows:

$$r = (N-1)d + 1 \tag{5}$$

When the number of TCN convolutional layers is n, the whole perceptual field l can be expressed as follows:

$$l = 1 + \sum_{i=1}^{n} (N-1)b^{i-1} = 1 + (N-1)\frac{b^n - 1}{b-1} \tag{6}$$

In order to cover ADS-B input data by the perceptual field l, the length of sliding window T needs to satisfy the following inequality:

$$T \le 1 + (N-1)\frac{b^n - 1}{b-1} \tag{7}$$

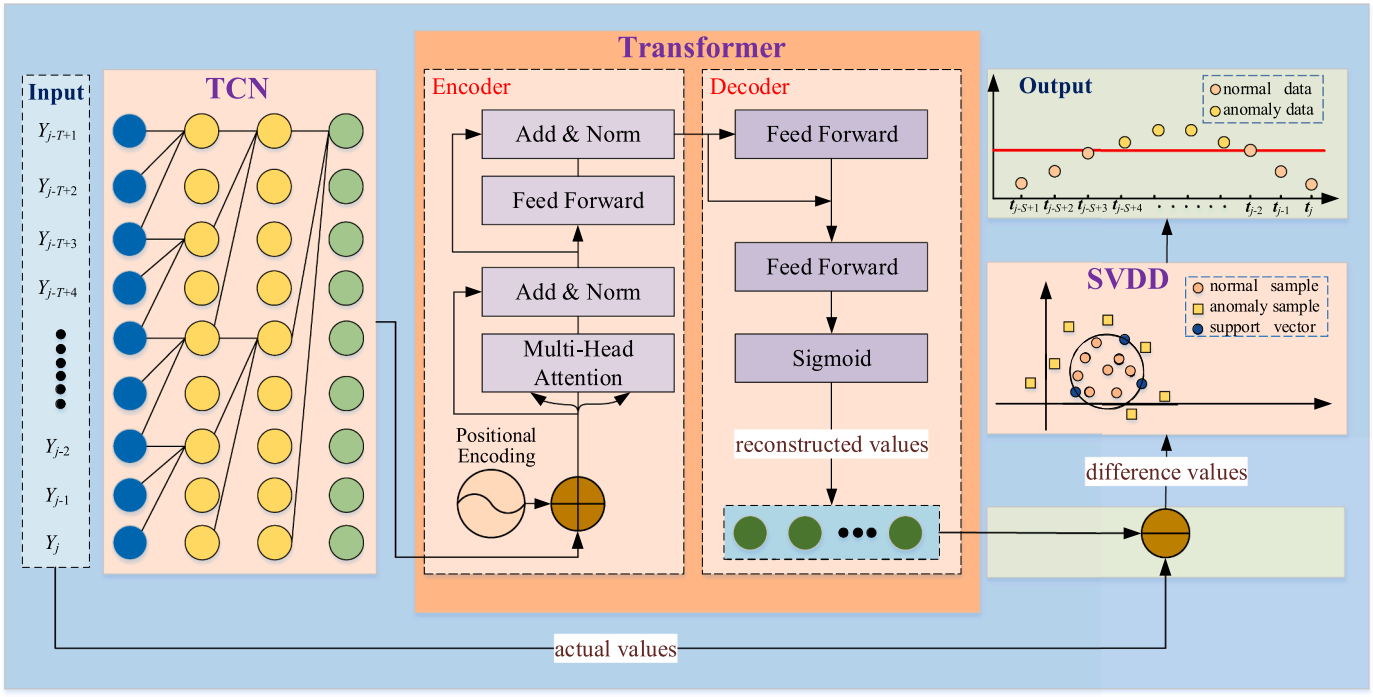

Fig. 5. Overall architecture of the TTSAD model.

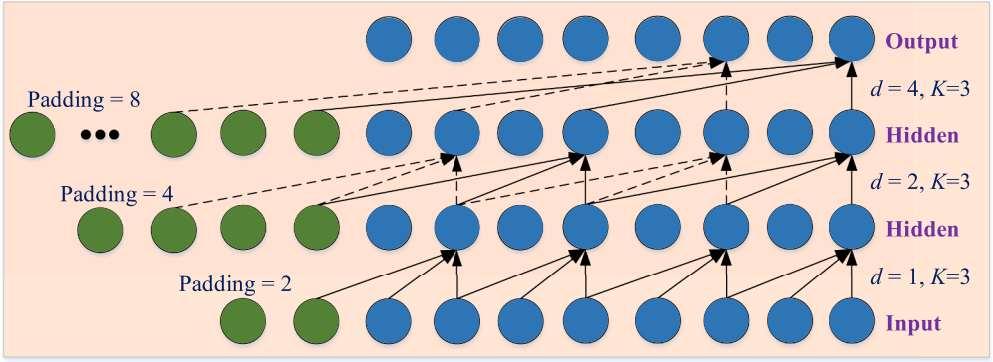

Fig. 6. Architecture of TCN.

4.3. Transformer reconstruction module

Transformer has been proven to be suitable for detecting anomaly time series (Chen et al., 2022; Tuli and Casale, 2022). As shown in Fig. 5, Transformer reconstruction module consists of two parts: Encoder and Decoder. The purpose of Transformer reconstruction module is to make the reconstructed value $\overline{Y}$ equal to the input value Y. In order to accurately reconstruct the ADS-B time series, Transformer reconstruction module needs to capture the contextual information of time series based on positional encoding. Positional encoding can be expressed as follows:

$$\begin{cases} PE_{(pos,2i)} = \sin\left(\dfrac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \\ PE_{(pos,2i+1)} = \cos\left(\dfrac{pos}{10000^{\frac{2i}{d_{model}}}}\right) \end{cases} \tag{8}$$

The input data in Transformer is obtained by adding embedding vector and positional encoding (Vaswan et al., 2017; Chu and Tian, 2021). Some parameters in Eq. (8) are described as follows. PE is the abbreviation of positional encoding.posdenotes the position of embedding vector in the input time series. d_{model} denotes the dimension of embedding vector. Positional encoding has the same dimension d_{model} as embedding vector, so that the two can be summed. i is the index of the dimension in the embedding vector. $2i$ and $2i+1$ are not greater than d_{model}. sin() and cos() are the abbreviation of sine and cosine functions. The wavelengths form a geometric progression from 2π to $10{,}000 \cdot 2\pi$. In summary, because the positional information of the ADS-B data can be added to embedding vector, Transformer can reconstruct ADS-B data based on positional encoding.

Unlike RNN, the Self-Attention mechanism allows Transformer to process ADS-B time series simultaneously without the need for sequential iterations. This means that Self-Attention enables parallel computing. The query matrix is denoted as Q. The key matrix is denoted as K. The value matrix is denoted as V. The column dimension of matrix K is denoted as d_k. Then the attention scoring matrix $Attention(Q, K, V)$ can be denoted as follows:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{9}$$

The Transformer uses the Multi-Head Attention mechanism to learn rich contextual information in different representation subspaces and thus is able to accurately reconstruct ADS-B data. Fig. 7 depicts the internal structure of the Multi-Head Attention. The matrices Q, K and V are linearly transformed using the weight matrices W_i^Q, W_i^k and W_i^v respectively. Then the attention scoring matrix is calculated to obtain $head_i$.

$$head_i = Attention\left(QW_i^Q, KW_i^k, VW_i^v\right) \tag{10}$$

The range of i is $1 \le i \le h$. h denotes the number of heads. $MultiHead$can be obtained when the heads are concatenated and a linear

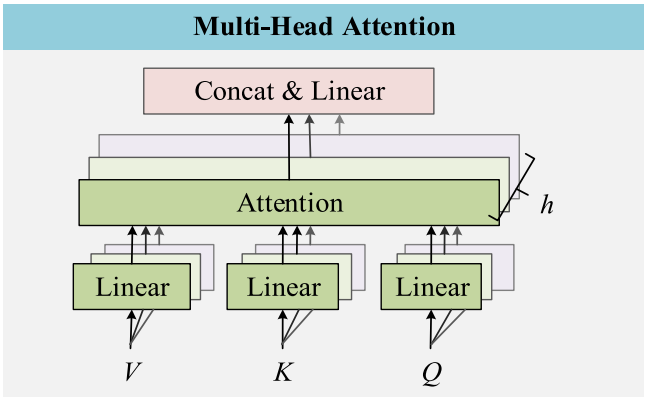

Fig. 7. Internal structure of Multi-Head Attention.

transformation W^o is performed:

$$MultiHead(Q, K, V) = Concat(head_1, head_h)W^o \tag{11}$$

I_1 is input to Multi-Head Attention. I_2 is obtained by residual connection and layer normalization. The output I_3 of Encoder can be obtained after I_2 is input to the Feed Forward network for residual connection and layer normalization:

$$\begin{cases} I_2 = LayerNorm(I_1 + MultiHead(I_1, I_1, I_1)) \\ I_3 = LayerNorm(I_2 + FFN(I_2)) \end{cases} \tag{12}$$

The process of Transformer Decoder can be divided into two steps. First, I_4 can be obtained after the output I_3 of Encoder is input into the Feed Forward network for residual connection. Second, the reconstructed value $\overline{Y}$ can be obtained after I_4 is input into the Feed Forward network for Sigmoid activation. The process can be represented as follows:

$$\begin{cases} I_4 = I_3 + FFN(I_3) \\ \widehat{Y} = Sigmoid(FFN(I_4)) \end{cases} \tag{13}$$

4.4. SVDD threshold determination module

SVDD is a one-classification machine learning method that can be used for anomaly detection (Tax and Duin, 2004; Zhou and Liang, 2021). In order to solve the threshold adaptive problem and achieve the optimal accuracy of anomaly detection, this paper uses SVDD to determine the threshold. Fig. 8 shows the diagram of SVDD. The difference value $\{D_j / D_j = \overline{Y_J} - Y_j 1 \le j \le L\}$between the reconstructed value $\overline{Y_j}$ and the real value Y_j is put into SVDD for training, and then the threshold of anomaly detection can be obtained. SVDD can be expressed as the following optimization problem:

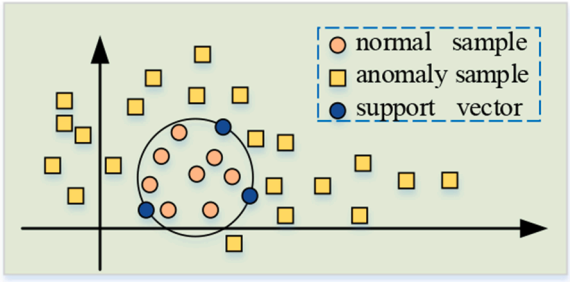

Fig. 8. Diagram of SVDD.

$$\min\ H(R,a)=R^2+C \times \sum_j^n \xi_j s.t.\ \begin{cases} \| D_j - a\text{AptCommand2016;}^2 \le R^2+\xi_j,\ (j=1,2,L) \\ \xi_j \ge 0 \end{cases} \tag{14}$$

R is the radius of SVDD hypersphere, which is the threshold of anomaly detection. a is the center of the hypersphere. ξ_j is the slack variable. C is the penalty factor, $0<C\le 1$. The Lagrange multiplier method can be used to solve this optimization problem. If the distance from D_j to the center a is denoted as $S(D_j)$, then $S(D_j)$ can be expressed as follows:

$$S(D_j) = \| D_j - a \| = \sqrt{(D_j, D_j) - 2\sum_{i=1}^{L}\lambda_i(D_i, D_j) + \sum_{i=1}^{L}\sum_{k}^{L}\lambda_i\lambda_k(D_i, D_k)} \tag{15}$$

It means that the sample D_j is the anomaly data when $S(D_j) > R$. It means that the sample D_j is the normal data when $S(D_j) \le R$. In this paper, Radial Basis Function (RBF) is used to map ADS-B data from the original space to the higher-dimensional feature space. RBF kernel function is expressed as follows:

$$K_{RBF} = \exp\left(-\frac{\| D_i, D_j\text{AptCommand2016;}^2}{gamma}\right) \tag{16}$$

D_i and D_j are two samples. *gamma* is the kernel parameter.

4.5. Evaluation metrics

The confusion matrix for sample classification is given in Table 3. *TP* (True Positive) indicates that real normal data is reconstructed as normal data. *FN* (False Negative) indicates that real normal data is reconstructed as anomaly data. *FP* (False Positive) indicates that real anomaly data is reconstructed as normal data. *TN* (True Negative) indicates that real anomaly data is reconstructed as anomaly data.

In this paper, *DE* (detection rate), *RC* (recall rate) and *ACC* (accuracy rate), *MDR* (missing detection rate), *FAR* (false alarm rate) are used as evaluation metrics for ADS-B anomaly detection. As shown in Eq. (17), *DE* is the proportion of data correctly reconstructed as anomaly data to real anomaly data. *RC* is the proportion of data correctly reconstructed as normal data to real normal data. *ACC* is the proportion of data correctly reconstructed to real whole data. *MDR* is the proportion of data incorrectly reconstructed as normal data to real anomaly data. *FAR* is the proportion of data incorrectly reconstructed as anomaly data to real normal data.

Table 3
confusion matrix for sample classification.

confusion matrix	reconstructed normal data	reconstructed anomaly data
real normal data	*TP*	*FN*
real anomaly data	*FP*	*TN*

$$\begin{cases} DE = \dfrac{TN}{FP+TN} \\ RC = \dfrac{TP}{TP+FN} \\ ACC = \dfrac{TN+TP}{TP+FN+FP+TN} \\ MDR = \dfrac{FP}{FP+TN} \\ FAR = \dfrac{FN}{TP+FN} \end{cases} \tag{17}$$

5. Experiments

5.1. Experiments datasets

ADS-B data of 40 flights is collected as the training sample from OPENSKY (Strohmeier et al., 2015b). In addition, ADS-B data of 20 flights is collected as test samples. Each collected flight comes from the same geographical zone between New York LaGuardia Airport and Ronald Reagan Washington National Airport. Each collected flight includes the aircraft's take-off, climb, cruise and descent phase. Moreover, each flight contains ADS-B data from 200 to 400. Considering the limitations of actual environments, ADS-B attack data is difficult to obtain. The attack data in the testing dataset is generated by simulation. The simulated attack styles include random position deviation, fixed position deviation, altitude slow offset, speed slow offset and DOS attack. Considering the stealth and effectiveness, the five types of attacks are constructed based on original ADS-B data which is shown in Table 4. The training ADS-B dataset and the testing ADS-B dataset can be downloaded from https://github.com/erlibanyanyi/air-traffic-anomaly-detection/tree/master/dataset-ATM. Some of the code can be downloaded from https://github.com/erlibanyanyi/air-traffic-anomaly-detection. Anyone who needs the whole code can contact the authors by sending emails and the code can be given after evaluation.

An example test flight containing 243 ADS-B data is selected. The attack data is generated specifically as follows. (1) **Random position deviation**: As shown in Fig. 9, the first 50 and the last 102 ADS-B data is not tampered. For the middle 100 data, Gaussian noise with the mean of 0 and standard deviation of 0.5 is added to the longitude and latitude. The attacker makes the trajectory fluctuate randomly around the real trajectory by random position deviation attack. (2) **Fixed position deviation**: As shown in Fig. 10, the first 50 and last 102 ADS-B data is not

Table 4
Experimental testing dataset.

Data attack	Data construction methods
Random position deviation	Attack data: Inject Gaussian noise with the mean of 0 and standard deviation of 0.5 into the original longitude and latitude for the 51st-150th ADS-B data. Authentic data: Include authentic ADS-B data from the first 50 and after the 150th.
Fixed position deviation	Attack data: Inject the constant 1 into the original longitude and latitude for the 51st-150th ADS-B data. Authentic data: Include authentic ADS-B data from the first 50 and after the 150th.
Altitude slow offset	Attack data: Enlarge the altitude with a multiple of 50 m gradually for the 51st-150th ADS-B data. Authentic data: Include authentic ADS-B data from the first 50 and after the 150th.
Velocity slow offset	Attack data: Enlarge the velocity with a multiple of 2 m/s gradually for the 51st-150th ADS-B data. Authentic data: Include authentic ADS-B data from the first 50 and after the 150th.
DOS attack	Attack data: The aircraft track disappears in the air traffic surveillance system for the 51st-150th ADS-B data. Authentic data: Include authentic ADS-B data from the first 50 and after the 150th.

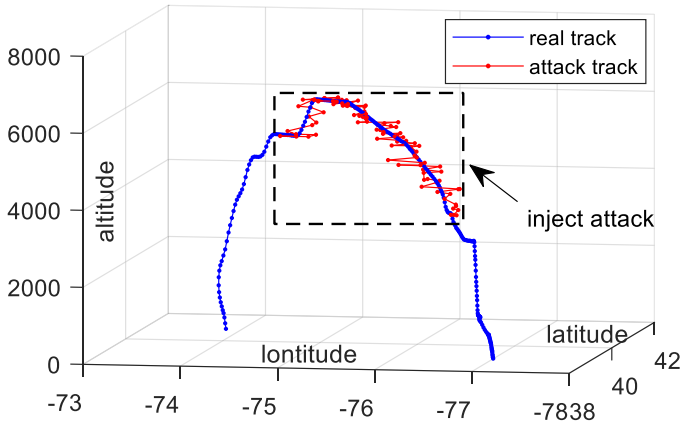

Fig. 9. Random position deviation.

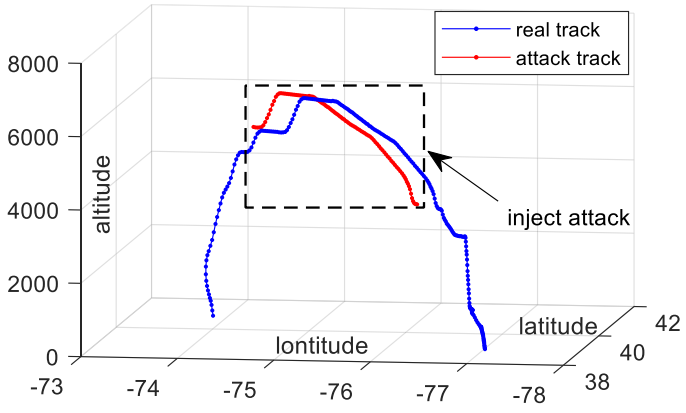

Fig. 10. Fixed position deviation .

tampered. For the middle 100 data, the constant 1 is added to the longitude and latitude. (3) **Altitude slow offset**: As shown in Fig. 11, the first 50 and last 102 ADS-B data is not tampered. For the middle 100 data, the altitude is gradually changed in multiples of 50 m. Specifically, the altitude of the 51st data is increased by 50 m. The altitude of the 52nd data is increased by 100 m, and so on. (4) **Velocity slow offset**: As shown in Fig. 12, the first 50 and last 102 ADS-B data is not tampered. For the middle 100 data, the velocity is gradually changed in multiples of 2 m/s. Specifically, the velocity of the 51st data is increased by 2 m/s. The velocity of the 52nd data is increased by 4 m/s, and so on. (5) **DOS attack**: As shown in Fig. 13, the first 50 and last 102 ADS-B data is not tampered. For the middle 100 data, the attacker launches DOS attack so

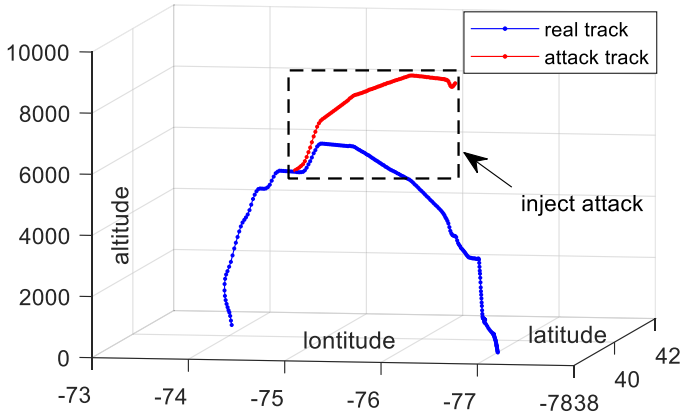

Fig. 11. Altitude slow offset .

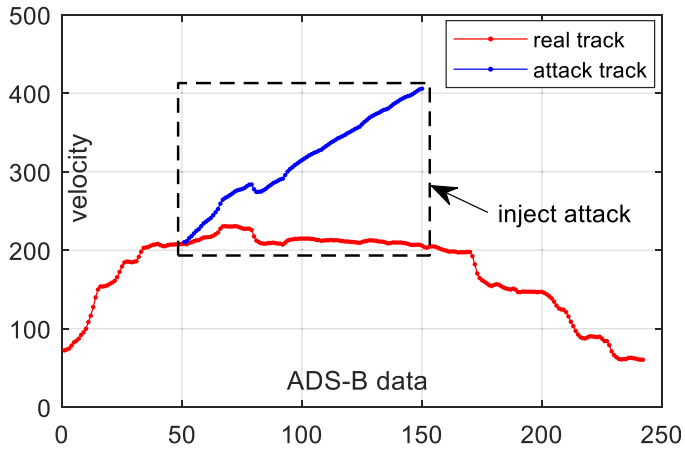

Fig. 12. Velocity slow offset .

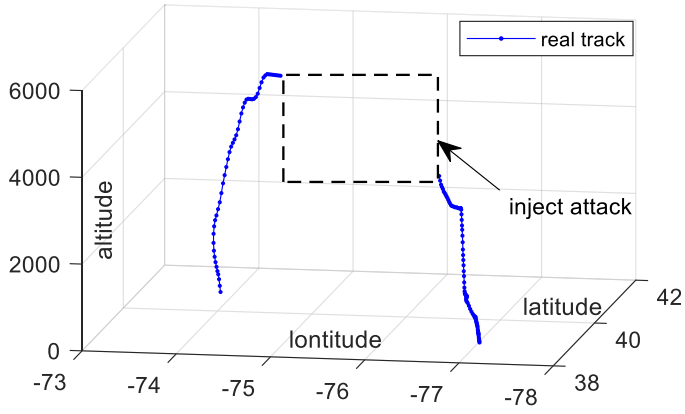

Fig. 13. DOS attack.

that ADS-B message cannot be received. The aircraft track disappears in the air traffic surveillance system due to DOS attack.

5.2. Sliding window selection

In order to make full use of temporal correlation of ADS-B data, it is necessary to select an appropriate length of sliding window. If the length of the sliding window is too short, the TTSAD model will lose a lot of ADS-B time-related information and reduce the accuracy of anomaly detection. If the length of the sliding window is too long, the training time of TTSAD model will be too long. In order to select an appropriate length of sliding window, the training loss and training time are compared under different lengths of sliding window (Tian and Wang, 2022). The function used by the training loss is MAE (Mean Absolute Error) function. After analyzing Fig. 14, the following conclusions can be drawn: (1) When the length of sliding window is 2, the training loss is relatively large. It shows that the short length of sliding window can't make full use of temporal correlation, which leads to poor anomaly detection performance. (2) When the length of sliding window is 8 and 10, the training loss is relatively small. It shows that temporal correlation of ADS-B data is fully utilized, and the anomaly detection performance is better. (3) As the length of sliding window increases from 2 to 10 and the training epochs is 50, the training time keeps increasing at a nearly linear rate. (4) Considering the training loss and training time comprehensively, the selected length of sliding window is 8.

5.3. Anomaly detection experiment results

Similarly, considering the training loss, anomaly detection accuracy

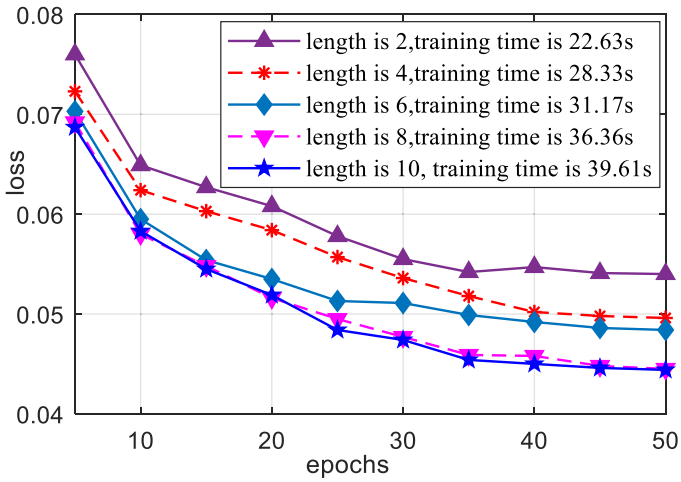

Fig. 14. Sliding window selection.

and training time, the hyperparameters of the TTSAD model are set as follows. The size of TCN convolutional kernel is 3. The number of TCN hidden layers is 3. TCN dilated factor of each layer of is set to 1, 2 and 4 respectively. The number of Transformer Multi-Head is 4. The penalty factor C in SVDD is 4, and the kernel parameter *gamma* in SVDD is 50. The training batch size *batch_size* is set to 32, the learning rate *lr* is set to 0.01, and *epochs*is set to 50. Figs. 15–19 show the anomaly detection results for the above five attack styles.

Fig. 15 depicts the anomaly detection results for random position deviation. The threshold for anomaly detection is 0.9167. A total of 139 data has a distance less than the threshold for the 1st-50th and 151st-242nd ADS-B data. Thus, the recall rate is 97.89 %. For the 51st-150th ADS-B data, a total of 93 data has a distance greater than the threshold. Thus, the detection rate is 93 %. For the 1st-242nd ADS-B data, a total of 232 data is correctly classified. Thus, the accuracy rate is 95.87 %. For the 51st-150th ADS-B data, a total of 7 data has a distance less than the threshold. Thus, the missing detection rate is 7 %. A total of 4 data has a distance greater than the threshold for the 1st-50th and 151st-242nd ADS-B data. Thus, the false alarm rate is 2.11 %.

Fig. 16 depicts the anomaly detection results for fixed position deviation with the recall rate of 92.96 %, the detection rate of 94 %, the accuracy rate of 93.39 %, the missing detection rate of 6 %, and the false alarm rate is 7.04 %. Fig. 17 depicts the anomaly detection results for altitude slow offset with the recall rate of 92.25 %, the detection rate of 93 %, the accuracy rate of 92.56 %, the missing detection rate of 7 %, and the false alarm rate is 7.75 %. Fig. 18 depicts the anomaly detection results for velocity slow offset with the recall rate of 93.67 %, the

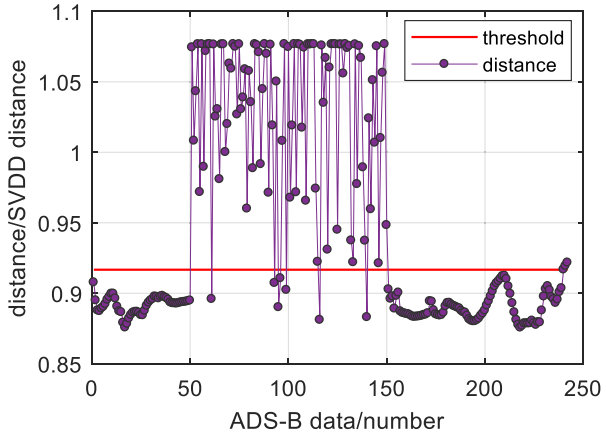

Fig. 15. Detection of random position deviation.

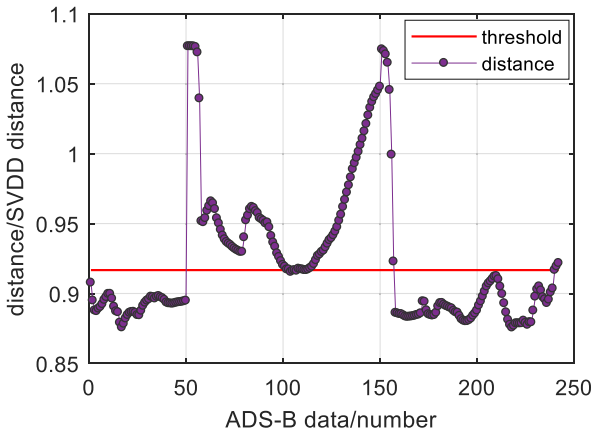

Fig. 16. Detection of fixed position deviation.

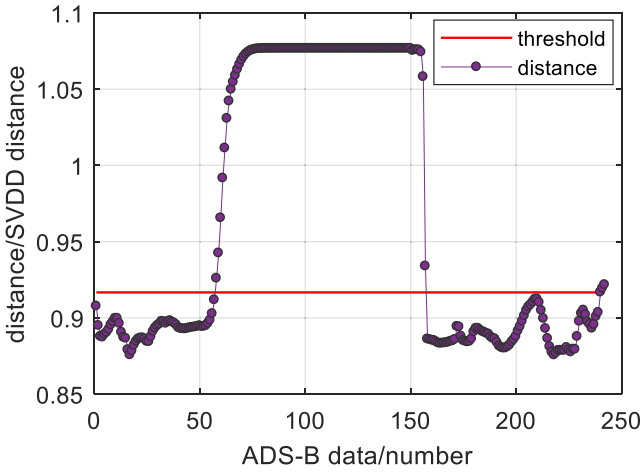

Fig. 17. Detection of altitude slow offset.

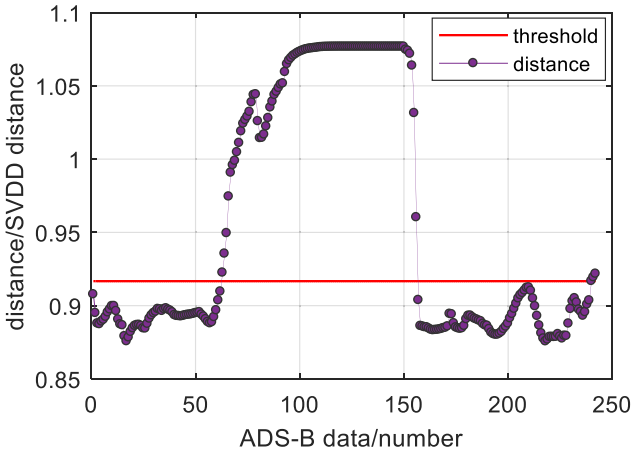

Fig. 18. Detection of velocity slow offset.

detection rate of 88 %, the accuracy rate of 91.32 %, the missing detection rate of 12 %, and the false alarm rate is 6.33 %. Fig. 19 depicts the anomaly detection results for DOS attack with the recall rate of 92.96 %, the detection rate of 100 %, the accuracy rate of 95.47 %, the missing detection rate of 0 %, and the false alarm rate is 7.04 %.

Anomaly detection experiments are conducted on the ADS-B data of 20 test flights. The average value is taken as the final anomaly detection result. Table 5 depicts the anomaly detection results of the five attack

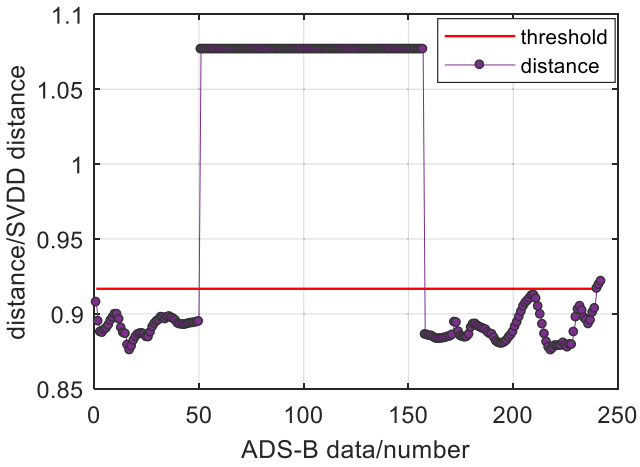

Fig. 19. Detection of DOS attack.

Table 5
Detection results of five attack styles.

Evaluation metrics	Random position deviation	Fixed position deviation	Altitude slow offset	Velocity slow offset	DOS
RC	97.23	92.67	92.39	93.98	92.58
DE	96.62	91.95	93.20	88.57	100
ACC	97.03	92.14	93.33	92.19	95.36
MDR	3.38	8.05	6.80	11.43	0
FAR	2.77	7.33	7.61	6.02	7.42

styles. The following conclusions can be drawn:

(1) The accuracy rate of the TTSAD models is all above 92 %. It shows that the TTSAD model can accurately classify the ADS-B normal and anomaly data. The performance of anomaly detection is superior.

(2) For the recall rate and false alarm rate, the recall rate and false alarm rate of random position deviation has the best performance. The tampering magnitude of this attack style is not obvious. Therefore, once the attack is over, the TTSAD model can quickly and accurately classify ADS-B normal data.

(3) For the detection rate and missing detection rate, the DOS attack has the highest detection rate of 100 % and the lowest missing detection rate of 0 %. This is because DOS attack causes the disappearance of the trajectory. Therefore, this attack can be detected most accurately. The detection rate for the velocity slow offset is 88.57 % which is the lowest due to the high concealment of this attack. Especially at the beginning of the attack, velocity slow offset is not obvious enough and thus difficult to detect.

5.4. Comparison experiments

In order to verify the superiority of the TTSAD model, five other representative methods for detecting ADS-B anomaly data are selected in this paper. These five methods are IForest (Isolated Forest), OCSVM (One Class Support Vector Machine), neural network composed of LSTM (Long Short-Term Memory), neural network composed of GRU (Gated Recurrent Unit) and LSTM-AE (LSTM AutoEncoder). (1) IForest considers that the region with sparse distribution indicates that the probability of data falling in this region is low. Therefore, the data falling in the sparse region can be considered as anomaly data. We set the number of IForest trees to 100. (2) OCSVM is an anomaly detection algorithm based on kernel functions. The input only needs to have normal data and the labels. This method learns the decision boundaries of normal observations. We set the kernel function as radial basis kernel function. (3) Neural network composed of LSTM/GRU performs ADS-B anomaly detection based on the prediction errors. It consists of a 3-layer LSTM/GRU network and a fully connected layer. The threshold is determined by the cosine similarities. (4) LSTM-AE performs ADS-B anomaly detection based on the reconstruction errors. Both the Encoder and Decoder consist of a single layer LSTM. The threshold is determined by the cosine similarities. Experimental results show that the six methods, including the TTSAD model, can detect each ADS-B data in less than 1 ms. Thus, all the six methods have good performance for real-time detection. The average values of recall rate, detection rate, accuracy rate, missing detection rate and false alarm rate for the five attack styles are given in Fig. 20 and Table 6. The time required to train ADS-B data of 40 flights is given in Table 7. After analyzing Fig. 20, Tables 6 and 7, the following conclusions can be drawn:

(1) As shown in Fig. 20 and Table 6, compared to state-of-the-art ML-driven solutions, TTSAD has the highest recall rate of 93.77 %, the highest detection rate of 94.07 %, the highest accuracy rate of 94.01 %, the lowest missing detection rate of 5.93 % and the lowest false alarm rate of 6.23 %. This is because TCN can accurately predict ADS-B time series by making full use of temporal correlation of ADS-B data based on causal convolution and dilated convolution. Transformer can accurately reconstruct ADS-B data by fully capturing the context information based on the Multi-Head Attention mechanism. Moreover, SVDD can further improve the performance of anomaly detection by training the difference value to make the determined threshold better.

(2) As shown in Table 7, the training time of TTSAD is 141.05 s, which is shorter than other deep learning solutions including LSTM, GRU and LSTM-AE. This is because TCN is based on one-dimensional convolutional network for fast computing, and thus has the advantage of being lightweight. Moreover, Transformer completes parallel computing based on Self-Attention mechanism, thus it can reconstruct ADS-B data quickly.

(3) As traditional machine learning methods, although IForest and OCSVM have the shorter training time, they have the worst performance of recall rate, detection rate, accuracy rate, missing detection rate and false alarm rate which can be seen in Tables 6 and 7.

(4) As shown in Fig. 20 and Table 6, LSTM, GRU, LSTM-AE and TTSAD have higher recall rate, detection rate, accuracy rate and lower missing detection rate, false alarm rate than IForest and OCSVM. These four types of deep learning methods take full advantage of temporal correlation of ADS-B data. Therefore, the anomaly detection performance of these four methods is superior.

(5) The recall rate, detection rate and accuracy rate of LSTM-AE are higher than those of LSTM and GRU which can be seen in Fig. 20 and Table 6. It indicates that the anomaly detection methods based on the reconstruction errors outperform the methods based on the prediction errors when temporal correlation of ADS-B data is fully utilized.

6. Conclusion

Based on the adequate consideration of temporal correlation of ADS-B data, this paper proposes the TTSAD model for detecting ADS-B anomaly data. First, TCN prediction module makes full use of temporal correlation of ADS-B data based on causal convolution and dilated convolution and supports parallel computation to accurately and quickly predict ADS-B time series. Then, Transformer reconstruction module completes parallel computing and fully captures the context information of ADS-B data based on Self-Attention mechanism and Multi-Head Attention mechanism, which can reconstruct ADS-B data in an accurate and quick way. Finally, SVDD threshold determination module further improves the performance of anomaly detection by training the difference value to make the determined threshold better.

In the future, we consider using the ATM knowledge graph for ADS-B anomaly detection. The ATM knowledge graph provides the prior knowledge such as entities and relations for ADS-B anomaly detection. Therefore, we can accomplish more types of ADS-B anomaly detection. Moreover, we will consider the interpretability of ADS-B anomaly detection. This will provide pilots and controllers with explanations and

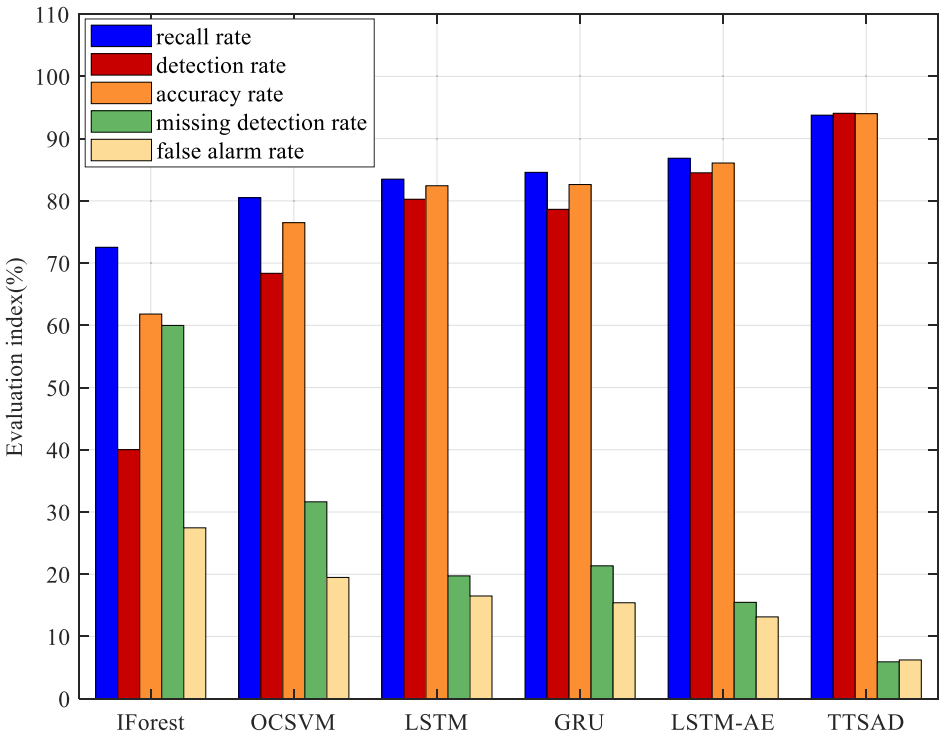

Fig. 20. Comparison chart of six anomaly detection methods.

Table 6
Comparison results of six anomaly detection methods.

Evaluation metrics	IForest	OCSVM	LSTM	GRU	LSTM-AE	TTSAD
recall rate	72.54	80.51	83.49	84.58	86.85	93.77
detection rate	40.02	68.36	80.26	78.64	84.51	94.07
accuracy rate	61.81	76.49	82.43	82.62	86.08	94.01
missing detection rate	59.98	31.64	19.74	21.36	15.49	5.93
false alarm rate	27.46	19.49	16.51	15.42	13.15	6.23

Table 7
Comparison of training time.

Evaluation metrics	IForest	OCSVM	LSTM	GRU	LSTM-AE	TTSAD
Training time (s)	13.07	7.34	484.02	462.04.	270.92	141.05

descriptions of anomaly detection under various attack patterns.

CRediT authorship contribution statement

Peng Luo: . **Buhong Wang:** . **Jiwei Tian:** Validation, Writing – review & editing, Formal analysis, Methodology, Supervision.

Declaration of competing interest

The authors declare that they do not have any financial or non-financial conflict of interest in this paper.

Data availability

No data was used for the research described in the article.

References

Akerman, S., Habler, E., and Shabtai, A., "VizADS-B: analyzing sequences of ADS-B images using explainable convolutional LSTM encoder-decoder to detect cyber attacks," 2019, arXiv:1906.07921.

Baek, J., Hableel, E., Byon, Y., Wong, D.S., Jang, K., Yeo, H., 2017. How to protect ADS-B: confidentiality framework and efficient realization based on staged identity-based encryption. IEEE Trans. Intell. Transp. Syst. 18 (3), 690–700.

Chen, Z., Chen, D., Zhang, X., Yuan, Z., Cheng, X., 2022. Learning graph structures with transformer for multivariate time-series anomaly detection in IoT. IEEE Internet Things J. 9 (12), 9179–9189. https://doi.org/10.1109/JIOT.2021.3100509.

Cheng, Y., Xu, Y., et al., 2019. HS-TCN: a semi-supervised hierarchical stacking temporal convolutional network for anomaly detection in IoT. In: 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), pp. 1–7.

Chu, X., Tian, Z., et al., 2021. Conditional positional encodings for vision transformers. In: 2021 *International Conference on Learning Representations*.

Costin, A., Francillon, A., 2012. Ghost in the air traffic: on insecurity of ADS-B protocol and practical attacks on ADS-B devices. In: Proceedings of Black Hat USA. Las Vegas, USA, pp. 1–12.

Habler, E., Shabtai, A., 2018. Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B Messages. Comput. Secur. 78, 155–173.

Habler, E., Shabtai, A., 2022. Analyzing sequences of airspace states to detect anomalous traffic conditions. IEEE Trans. Aerosp. Electron. Syst. 58 (3), 1843–1857. https://doi.org/10.1109/TAES.2021.3124199.

Kacem, T., Wijesekera, D., Costa, P., 2018. ADS-Bsec: a holistic framework to secure ADS-B. IEEE Trans. Intell. Veh. 3 (4), 511–521.

Leonardi, E.P.M., Galati, G., 2017. ADS-B jamming mitigation: a solution based on a multichannel receiver. IEEE Aerosp. Electron. Syst. Mag. 32 (11), 44–51.

Leonardi, M., 2019. ADS-B anomalies and intrusions detection by sensor clocks tracking. IEEE Trans. Aerosp. Electron. Syst. 55 (5), 2370–2381.

Leonardi, M., Strohmeier, M., Lenders, V., 2021. On jamming attacks in crowdsourced air traffic surveillance. IEEE Aerosp. Electron. Syst. Mag. 36 (6), 44–54.

Li, T., Wang, B., 2019. Sequential collaborative detection strategy on ADS-B data attack. Int. J. Crit. Infrastruct. Prot. 24, 78–99.

Li, T., Wang, B., Shang, F., Tian, J., Cao, K., 2019. Online sequential attack detection for ADS-B data based on hierachical temporal memory. Comput. Secur. 87 https://doi.org/10.1016/j.cose.2019.101599.

Li, T., Wang, B., Shang, F., Tian, J., Cao, K., 2020. Dynamic temporal ADS-B data attack detection based on sHDP-HMM. Comput. Secur. 93 https://doi.org/10.1016/j.cose.2020.101789.

Luo, P., Wang, B., Li, T., Tian, J., 2021. ADS-B anomaly data detection model based on VAE-SVDD. Comput. Secur. 104 https://doi.org/10.1016/j.cose.2021.102213.

Monteiro, M., et al., 2015. Detecting malicious ADS-B broadcasts using wide area multilateration. In: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). Prague, Czech Republic, pp. 4A3-1–4A3-12. https://doi.org/10.1109/DASC.2015.7311413.

Nijsure, Y.A., Kaddoum, G., Gagnon, G., Gagnon, F., Yuen, C., Mahapatra, R., 2016. Adaptive air-to-ground secure communication system based on ADS-B and wide-area multilateration. IEEE Trans. Veh. Technol. 65 (5), 3150–3165.
Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C., 2011. Future E-enabled aircraft communications and security: the next 20 years and beyond. Proc. IEEE 99 (11), 2040–2055.
Schafer, M., Lenders, V., Martinovic, I., 2013. Experimental analysis of attacks on next generation air traffic communication. In: International Conference on Applied Cryptography and Network Security. Berlin, Germany, pp. 253–271.
Shang, F., Wang, B., Yan, F., Li, T., 2019. Multidevice false data injection attack models of ADS-B multilateration systems. Secur. Commun. Netw. 2019 https://doi.org/10.1155/2019/8936784.
Strohmeier, M., Lenders, V., Martinovic, I., 2014. On the security of the automatic dependent surveillance-broadcast protocol. IEEE Commun. Surv. Tutor. 17 (2), 1066–1087.
Strohmeier, M., Lenders, V., Martinovic, I., 2015a. Intrusion detection for airborne communication using PHY-layer information. In: Proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 9148, pp. 66–77.
Strohmeier, M., Martinovic, I., 2015. On passive data link layer fingerprinting of aircraft transponders. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, 2015.
Strohmeier, M., Martinovic, I., Fuchs, M., Schäfer, M., Lenders, V., 2015b. OpenSky: a swiss army knife for air traffic security research. In: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). Prague, Czech Republic, pp. 4A1-1–4A1-14.
Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., Martinovic, I., 2017. On perception and reality in wireless air traffic communication security. IEEE Trans. Intell. Transp. Syst. 18 (6), 1338–1357.
Tax, D., Duin, R., 2004. Support vector data description. Mach. Learn. 54, 45–66.
Thill, M., Konen, W., Wang, H., Bäck, T., 2021. Temporal convolutional autoencoder for unsupervised anomaly detection in time series. Appl. Soft Comput. 112.
Thumbur, G., Gayathri, N.B., Reddy, P.V., Rahman, M.Z.U., Lay-Ekuakille, A., 2019. Efficient pairing-free identity-based ADS-B authentication scheme with batch verification. IEEE Trans. Aerosp. Electron. Syst. 55 (5), 2473–2486.
Tian, J., Wang, B., et al., 2022. Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles. IEEE Internet Things J. 22399–22409.
Tuli, S., Casale, G., et al., 2022. TranAD: deep transformer networks for anomaly detection in multivariate time series data, 2022. Proc. VLDB Endowment 15 (6), 1201–1214. https://doi.org/10.14778/3514061.3514067.
Vaswani, A., Shazeer, N., et al., 2017. Attention Is All You Need. https://doi.org/10.48550/arXiv.1706.03762.
Wang, J., Zou, Y., Ding, J., 2020. ADS-B spoofing attack detection method based on LSTM. EURASIP J. Wirel. Commun. Netw. 2020 (1), 1–12.
Wu, Z., Guo, A., Yue, M., Liu, L., 2020. An ADS-B message authentication method based on certificateless short signature. IEEE Trans. Aerosp. Electron. Syst. 56 (3), 1742–1753.
Yang, H., Zhou, Q., Yao, M., Lu, R., Li, H., Zhang, X., 2019. A Practical and compatible cryptographic solution to ADS-B SEcurity. IEEE Internet Things J. 6 (2), 3322–3334.
Zhou, Y., Liang, X., et al., 2021. VAE-based deep SVDD for anomaly detection. Neurocomputing 453, 131–140.

Peng Luo was born in Yancheng, Jiangsu, China in 1995. He received his BS and MS degrees in Air Force Engineering University, China, in 2018 and 2020, respectively. Now, he is a PhD candidate at Air Force Engineering University, China. His current research interest is machine learning and anomaly detection on air traffic ADS-B data.

Buhong Wang received the MS and PhD degrees in signal and information prcessing from Xidian University, Xi'an, China, in 2000 and 2003, respectively, where his PhD degree thesis "On Some Crucial Aspects of High-Resolution Direction of Arrival Estimation" was honored as the "Excellent Doctoral Dissertation of Shaanxi Province." From 2003 to 2005, with the support of the National Post-Doctoral Science Foundation, he was a Post-Doctoral Fellow with the Post-Doctoral Technical Innovation Center, Nanjing Research Institute of Electronics Technology, Nanjing, China. From 2006 to 2008, he was an Associate Professor with the School of Electronic Engineering, Xidian University. From 2009 to 2010, he was a Research Fellow with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. Since 2012, he has been a Professor with the Information and Navigation College, Air Force Engineering University, Xi'an. His current research interests include cyber security and cyber physical system.

Jiwei Tian received the MS degree in information and communication engineering from Air Force Engineering University, in 2017 and is pursuing for the PhD degree in Air Force Engineering University. His current research interest is machine learning and adversarial attack on cyber physical system.