An Adaptive-Data-Driven Attack Detection Framework on ADS-B Data

Tengyao Li

Information and Navigation College, Air Force Engineering University, Xi’an, Shaanxi Province, China

ABSTRACT

With the variety and quantity of flights increasing, accurate and efficient surveillance methods are in great demands for the next generation air traffic management. Relying on high accuracy, wide coverage, low deployment cost and data share support, Automatic Dependent Surveillance - Broadcast (ADS-B) is becoming the primary surveillance method in 2020. However, ADS-B data is lacking of sufficient security measures to ensure data integrity and authentication, which makes it face with various attack threats. To detect the malicious data caused by attack behaviours accurately, an adaptive-data-driven attack detection framework is proposed, which is utilized to establish the consistent framework for predictive discriminant detection methods. It is composed of sequential predictor, behaviour discriminator and dynamic updater, enhancing adaptive sequential detection performances. According to the framework, an effective implementation is designed to improve attack detection accuracy: (I) The sequential predictor identifies flight phases to predict sequential data effectively and accomplish model fusion to generate ADS-B predictive data sequences. (II) The behaviour discriminator utilizes value differences and contextual information to distinguish attack data from ADS-B data sequences. (III) The dynamic updater is designed to update the training data sets and discriminate threshold dynamically, improving the adaptation in face of concept drifts for ADS-B data. By experiments on real ADS-B data with diverse attack patterns, the feasibility and efficiency of the framework are validated.

1. Introduction

Nowadays, the density of airspaces and types of flights are growing fast in terms of emerging requirements for air traffic transportation, which promote the air traffic management (ATM) into intelligent, automatic and networked systems. The security, safety and reliability are regarded as the foundation to ensure the developments of the next generation air transportation systems[12]. With the deep interactions between physical components and information components, ATM system is involved with cyber physical systems (CPS)[11]. As a result, the attack surfaces and entrances are extended to make the systems more vulnerable. Cyber security is becoming the key to ensure the availability and efficiency of the whole system. Once the systems are attacked from cyber domain, attack effects may be transmitted to physical functional subsystems with high probabilities, which threaten the aviation safety and reliability [14]. Hence, the cyber security is of great significance to defend against various attack patterns[8]. For the next generation ATM systems, surveillance data is the foundation to establish situation awareness capabilities, which enables ATM to set up decision support systems based on large scale data. When the data is manipulated maliciously by attackers, it is impossible to ensure the availability of situation awareness and maintain high performances of the system. Therefore, surveillance data security is becoming the vital part to support cyber security.

Recently, Automatic Dependent Surveillance - Broadcast (ADS-B) is becoming the primary surveillance method to obtain surveillance data, which is superior with the traditional primary surveillance radar (PSR) and secondary surveillance radar (SSR) mechanisms on accuracy, deployment cost and information share support [21]. In 2020, ADS-B out is mandated for the majority of countries, which offers the opportunities to establish global ADS-B surveillance capabilities [22]. However, ADS-B protocol is designed without sufficient security measures [19]. In particular, the integrity and authentication of ADS-B data are much more vulnerable to various attack patterns. According to the protocol, ADS-B data is transmitted with plain texts, which gives rise to a variety of attack patterns, including ghost flood attack, false data injection attack, data manipulation attack, replay attack, De-nial of Service (DoS) attack and so on[10]. Different attack behaviours create, modify, replace or delete ADS-B data sequences in terms of attack intentions, which destroy the situation awareness on air traffic. Without the data security of ADS-B, the whole ATM system is absent of reliable surveillance data seriously[16]. As a result, the safety is eliminated due to the absence of effective and reliable ADS-B data to obtain safe operations and managements.

During ADS-B data collecting and processing, attack detection is the primary and essential method for the whole defence strategy. Traditionally, it is dependent on location validations to detect attack data sequences. The estimation locations are obtained from other surveillance methods or based on the motion laws for the specific targets. However, the traditional attack detection methods are dependent of another surveillance data or prior system knowledge. When the amount of ADS-B data is increasing fast with concept drifts, the detection time delay, accuracy and adaptation are
eliminated. When only ADS-B data sequences are available, the difficulty to establish effective attack detection solution is challenging. To deal with the challenge, attack detection methods based on deep learning are proposed to support online, dynamic and sequential detections. Among them, the predictive discriminant methods are widely applied and validated with high detection performances. The predictive data is used to generate reconstruction error, which is designed as the metrics to support attack behaviour analyses. The discriminant model is used to determine attack data sequences from stream data with thresholds. When the quantity of ADS-B data is sufficiently large, the detection performances of methods with deep learning are improved further. However, the methods are lacking of consistent framework to support full design flow to support more effective attack behaviour analysis and dynamic discriminant thresholds.

To establish the consistent framework, an adaptive-data-driven attack detection framework is proposed to set up the formal model, which offers the baseline for predictive discriminant detection methods. With the framework, an effective implementation is designed to improve the accuracy and adaptation of attack detection on ADS-B data. The main contributions of our paper are:

1. An adaptive data driven framework for predictive discriminant detection methods on ADS-B data is proposed to establish the formal model as baseline for such methods.
2. To improve the prediction accuracy, the flight phases are separated to accomplish prediction with model fusion.
3. To decrease the false alarm ratio, the contextual information is integrated with normal data bound to establish reasonable behaviour analysis model.
4. To enhance the adaptation for data concept drift, the discriminant threshold is configured dynamically to set up effective feedbacks.

The rest of paper is organized as following: the current developments of attack detection on ADS-B data are presented in Section 2, the attack detection framework is designed in Section 3, the sequential predictor for ADS-B data is designed and implemented in Section 4 to improve the prediction performances, the behaviour discriminant is designed and implemented in Section 5 to improve detection accuracy, the dynamic updater is designed and implemented in Section 6 to enhance the dynamic detection adaptation, the experimental analyses are implemented in Section 7 to validate the efficiency of the proposed framework, the pros and cons of the proposed framework are presented in Section 8 and Section 9.

2. Related Works

With the mandated deployment deadline coming, ADS-B is becoming the primary surveillance method in the next air traffic transportation systems. The traditional surveillance methods such as PSR, SSR, MLAT and so on act as the supplement technologies for ADS-B. The ADS-B data will help establish the data foundation for situation awareness to facilitate effective and reliable decision supports[20]. The security of ADS-B data is essential to ensure the reliable awareness capabilities and correct control commands. To improve ADS-B security, ADS-B data attack detection is the vital measure to enable accurate detection and robust system against various attack patterns.

2.1. ADS-B

ADS-B is the promising technology for the next generation air traffic surveillance, which is standardized with RTCA 260B[13]. With the airspace density and variety of flights growing fast, ADS-B is regarded as the core surveillance method to enhance situation awareness capabilities. Currently, lots of key projects focus on ADS-B to improve the traffic surveillance, including Single European Sky Advanced Research (SESAR), The Next Generation Air Transportation System (NextGen), China Next Generation Air Traffic Management System (CNGATM) and so on. In 2020, ADS-B out is mandated to be deployed in the majority of countries. In the near future, ADS-B data is becoming one of the most important data source for the whole air traffic management system.

ADS-B data enriches the attributes of surveillance data, including ICAO identification, latitude, longitude, altitude, velocity, heading and so on. As illustrated in Fig. 1, the current flights obtain flight state data from Global Navigation Satellite System (GNSS) and airborne navigation system. The state data is encapsulated into ADS-B data format to broadcast periodically. The neighbour flights receive the ADS-B data to support local situation awareness. And the corresponding ground stations receive the ADS-B data from the specific airspace to set up the whole situation awareness. To meet the compatibility and offer various data support, ADS-B data is rebroadcast towards the airspace with ADS-B Data Rebroadcast (ADS-R) or Traffic Information Surveillance - Broadcast (TIS-B) protocols. In addition, ADS-B data is pushed to Air Traffic Control (ATC) center to support air traffic management.

![Figure 1: ADS-B Transmission Flow](image-url)
 ADS-B data is sequential data with specific data features to represent flight states, which influences on the attack detection designs and implementations.

- **Multiple Attributes.** The ADS-B data extends the dimension of surveillance data and enriches the descriptions of flight states. The attributes are related with each other and constricted with motion laws. Meanwhile, ADS-B data provides the feasibility to establish Trajectory Based Operations (TBO) capabilities, supporting accurate predictions.

- **High Update Frequency.** The locations decoded from ADS-B data are updated per second with high accuracy, which can be utilized to improve detection performances with low time delay.

- **Temporal and Spatial Correlation.** The ADS-B data is typical sequential stream data and there exist to be strong correlations between historical data and current data. With the control of flight separation laws and intrinsic broadcast feature of ADS-B data, the spatial constraints for each ADS-B data is explicit, which can be established with ADS-B data from the neighbour flights.

- **Large Scale.** With the airspace density growing fast, the volume of collected ADS-B data is becoming larger to set up the basis of big data analysis. Large scale historical data offers feasibility to apply with deep learning algorithms.

- **Noise Impacts.** When generating and transmitting ADS-B data, it is prone to being affected with the instability and interference from physical devices and electromagnetic environments. As a result, ADS-B data may be absent on some sample points and under randomized noise impacts.

    When detecting ADS-B attack data, the most important feature is the temporal and spatial correlation, which restricts the data sequences to specific ranges. When designing attack detection method, the data features of ADS-B are utilized to establish models to identify attack behaviours.

### 2.2. Attack Detection on ADS-B Data

For ADS-B data, attack detection is the primary way to ensure data security. Relying on fast and accurate detection on attack behaviours, the malicious data can be labelled in time to avoid false situation awareness and wrong control commands. In terms of ADS-B data vulnerability, attack detection is necessary to weaken attack intentions and keep malicious data away from normal data. Generally, ADS-B data is the representation of flight states, which is sequential stream data with the high dynamic feature. Hence, ADS-B data is in demand of online, sequential, dynamic detection methods to improve accuracy and false alarm ratio on attack detection.

(1) Attack detection based on physical features

When ADS-B data is generated and transmitted, the corresponding signals are attached with specific physical information, which provide the feasibility for attack detection based on physical features. When ADS-B data is generated with transmitters, the features of signals are related with the specific equipments. Strohmeier [18] utilized the probability distribution of time separations between two neighbour ADS-B messages as the basic metric, analysing the differences caused by attackers. The distribution rule is dependent on specific transmitters of ADS-B, which is difficult for attackers to tamper. When ADS-B data is transmitted by datalinks, the signals are related with the broadcast environments. Generally, the transmission distance is correlated negatively with the received signal strength. Based on the assumption, Strohmeier [15] proposed intrusion detection method to detect anomaly data with hypothesis tests. In face of detection methods based on physical features, it is difficult for attackers to construct fake messages to escape from specific detection rules. But such methods are dependent on the specific devices, which limit the application scopes. It is too difficult to coverage features of all devices.

(2) Attack detection based on location validations

The attack detection based on location validations are dependent on reliable location data to validate current data sequences. If the motion models of target flights can be obtained accurately, Kalman filter is practical to validate locations with one step predictions. Cho [3] utilized interacting multiple model (IMM) filter to keep accurate track of positions, setting up the foundation to obtain reliable prediction sequences. Based on the results, Kovel [5] proposed the ADS-B data verification method with Kalman filter. In comparison with prediction data, the deviations caused by attackers on ADS-B data can be detected. When the deviations are injected slowly enough with time, the efficiency of the detection method is eliminated. With TBO technology developing, the predictions based on four-dimensional trajectories [24] are used to make up with the model deviation for Kalman filter methods. Relying on the accurate motion model, it is possible to determine the maximum boundary for current flights. If the flights are beyond the areas for specific time windows, the data is regarded as attack data. But the method is short of sufficiently tight boundary, which results in low accuracy or high false alarm ratio when detecting.

To meet with accurate motion model requirements, data fusion is utilized to accomplish location validations, detecting attack data with SSR and MLAT. If the target flights are monitored by ADS-B and SSR simultaneously, it is practical to validate ADS-B data with reliable SSR data. Zhang [25] proposed bias estimation method with probability hypothesis density filter based on SSR and ADS-B data, which could be used to detect attack data in terms of anomaly bias distributions. Nijsure [9] proposed data fusion methods with multilaterations, analysing attack behaviours with the deviations between ADS-B and MLAT data. By obtaining ADS-B data with Time-Difference-of-Arrival (TDOA), Angle-of-Arrival (AOA), and Frequency-Difference-of-Arrival (FDOA), all the data for the same targets are compared with each other.
If the deviations are beyond the threshold, attack data is labelled. Strohmeier [17] applied the multilateration in the air to propose group validations. When the amount of neighbour flights is more than four, the method can be utilized to validate current data with the data of TDOA measurements. To get over the limitation of flight amount, Leonardi [6] proposed detection methods by tracking sensor clocks with different nodes.

The attack detection methods based on location validations are dependent on prior system knowledge or reliable data from the third party. It is difficult to establish accurate motion model for each flight target, which increases the instability of the detection performance. When utilizing SSR or multilateration to detect attack data, time synchronization, coordinate transformation and target association are vital constraints on detections. If only ADS-B data is available and less prior system knowledge is mastered, data-driven detection methods are in demands.

(3) Attack detection with deep learning

With the quantity of ADS-B data growing, data-driven methods based on deep learning for ADS-B attack data are emerging. Ying [23] proposed classification method based on neural networks to detect attack data sequences. By analysing the relationships between ICAO identification and signal features from historical data, the fake messages are detected from the whole data sets. Harbler [4] proposed attack detection method based on LSTM encoder and decoder mechanism. By reconstructing ADS-B data sequences with encoder, the similarity metric is set up to detect attack behaviours. To support online detection, Li [7] designed attack detection method based on hierarchical temporal memory (HTM). By transferring ADS-B data into sparse distributed representation (SDR) binary codes, the ADS-B data can be predicted online to support attack behaviour analysis. To make the most of multiple attributes of ADS-B data, Akerman [1] proposed attack detection method based on explainable LSTM algorithm. ADS-B data is mapped to the representative image, which is mined to extract attack vectors.

Data-driven detection methods with deep learning can be applied with sufficient amount of ADS-B data, which are without constraints with prior system knowledge and other surveillance data. In general, the methods tries to establish reference data sequences that are utilized to represent features of normal data. With the reference data sequences, the comparisons are conducted with collected ADS-B data to detect attack data. The reference data may be prediction data or transformation data sequences, which is determined by the detailed methods.

These days, attack detection methods based on deep learning are promising in terms of high accuracy, efficiency and low false alarm ratio. However, (a) the methods are lacking of consistent framework to the offer baseline, helping integrating and improving the performance of data-driven methods. Meanwhile, (b) current methods are short of dynamic and self-adaptive capability when detecting real ADS-B data. (c) The contextual information and adaptive threshold are not taken deep considerations to improve detection accuracy. Therefore, we propose an adaptive data-driven framework to establish consistent design framework and set up dynamic threshold configurations to improve the adaptation on complex attack patterns. In addition, contextual Information are utilized to enhance the attack behaviour analysis.

3. Attack Detection Framework

The attack detection framework is designed to consist of three modules as illustrated in Fig. 2: sequential predictor (P), behaviour discriminator (D) and dynamic updater (U), which is called as PDU Framework. The sequential predictor is designed to predict ADS-B data based on historical data, which establishes pairwise data sequences with the original data. The behaviour discriminator is designed to identify attack behaviours based on the differences between original data and predicted data. The dynamic updater is designed to update parameters in behaviour discriminator and extend the training set in sequential predictor, improving the capability to adapt with normal data concept drifts.

**Figure 2: Adaptive Data Driven Framework**

ADS-B data is temporal spatial data with multiple attributes, which is set as $\omega_i$ and its attribute sets are $\Lambda$. For $\Lambda$, ICAO identification, latitude, longitude, altitude, heading and velocity are selected as the essential information.

$$\begin{align*}
\Omega &= \{\omega_{t_1}, \omega_{t_2}, \ldots, \omega_{t_n}\} \\
\Lambda &= \{\omega_{t_1}^{icao}, \omega_{t_1}^{lat}, \omega_{t_1}^{lon}, \omega_{t_1}^{alt}, \omega_{t_1}^{heading}, \omega_{t_1}^{vel}\}
\end{align*}$$

The original ADS-B data is preprocessed to fill with estimations for the missing values and sampled within specific time cycles, which is chosen as the input data for the whole framework.

1. Sequential Predictor

Assuming training time window is $T_t$, predicted time window is $T_p$, the ADS-B data in $T_t + T_p$ is separated into two parts: historical data and predicted data. The historical data should ensure the reliability to abandon novelty data, which is kept with large enough volume in terms of prediction accuracy. For $\Omega = \{\omega_{t_1}, \omega_{t_2}, \ldots, \omega_{t_n}\}$, the following constraints
should be satisfied:

\[
\begin{align*}
    & \Omega = \{ \omega_i | t_i < t_j < t_n \} \\
    & \Psi = \{ \tilde{\omega_i} | t_n - T_p < t_i < t_n \} \\
    & |\Psi| = \left\lceil \frac{T_n}{T_p} \right\rceil \\
    & \Psi = f_p(\Omega, \zeta_p) \\
    & \Psi = f_p(\Omega, \zeta_p) \\
    & \psi = f_p(\Omega, \zeta_p)
\end{align*}
\]

For the sequential predictor, the prediction model is:

\[
\Psi = f_p(\Omega, \zeta_p) = \left\{ \begin{array}{ll}
    1, & \phi > \theta \\
    0, & \phi \leq \theta
\end{array} \right.
\]

where \( \Omega \) is the ADS-B sequential data as the model input, \( \zeta_p \) is the hyper parameter, \( f_p \) is the mapping function to predict ADS-B data based on the measurement sequences. Due to the dynamic features for ADS-B data, static \( f_p \) is not suitable with the model, which is prone to result in large deviations. Setting the prediction model update time cycle is \( T_u \):

\[
\hat{f}_p = F_p(f_p, \Omega)
\]

\[
\begin{align*}
    & s.t. \\
    & T_u > \alpha T_p \\
    & \alpha > 1
\end{align*}
\]

where \( \hat{f}_p \) is mapping functions to update the model, \( F_p \) is the update function and \( \alpha \) is the window size control factor. Relying on dynamic update procedure, the prediction accuracy is improved to obtain \( \Psi \) as the model outputs.

**II. Behaviour Discriminator**

When the predicted ADS-B data within \( T_p \) is obtained, the original data \( \Omega \) and the predicted data \( \Psi \) are pushed to the behaviour discriminator module. After matching with the pairwise data according to sample points, the deviations for two data sequences are utilized to distinguish normal behaviours and attack behaviours. To measure the deviations, the distance between two sequences is designed as the vital metric.

\[
\chi = f_d(\Omega, \Psi, \zeta_d)
\]

where \( \chi \) is the distance between the original and predicted ADS-B data, \( \zeta_d \) is the hyper parameter for the model, \( f_d \) is the distance measurement function. In terms of the deviations, the evaluation values of attack behaviours can be calculated as:

\[
\phi = f_b(\chi)
\]

where \( \phi \) is the evaluation metrics, \( f_b \) is the evaluation function to transform \( \chi \) into the metrics, analysing the attack behaviour probability. When the metrics are obtained, depending on discriminant thresholds, the behaviour labels \( f_l \) are acquired:

\[
f_l = \left\{ \begin{array}{ll}
    1, & \phi > \theta \\
    0, & \phi \leq \theta
\end{array} \right.
\]

where \( \theta \) is the threshold to classify behaviours on ADS-B data. With the stream data of ADS-B reaching, the label sequence \( \gamma \) is obtained as the module output:

\[
\gamma = \{ f_l^{\gamma} | t_n - T_p < t_j < t_n \}
\]

**III. Dynamic Updater**

After the data sequences are analysed with the behaviour discriminator, the attack behaviours are detected and the attack data ratio is obtained. Setting the update control time window is \( T_c \), the dynamic update procedure is applied to update key parameters: training time window \( T_t \) and attack behaviour threshold \( \theta \):

\[
\hat{T}_t = \eta T_t = f_\eta(T_t, \gamma)
\]

\[
\hat{\theta} = \delta \theta = f_\delta(\theta, \gamma)
\]

where \( \eta \) is the moving step, \( \delta \) is the adjustment factor. Both parameters are updated with \( f_\eta \) and \( f_\delta \) respectively, which determine \( \eta \) and \( \delta \).
4. Sequential Predictor

The sequential predictor is designed to predict the ADS-B data effectively to offer the reference sequence values. As depicted in Fig. 6, the module is composed of three parts: (1) Flight Phase Identification, (2) Deep Prediction Network and (3) Model Fusion. The flight phase identification is to identify the detailed flight phase to support more accurate prediction data, which relies on altitude attribute of ADS-B data to analyse. The deep prediction network is implemented with LSTM neural networks, which is the core component to obtain reliable prediction sequences. Based on flight phases, the predicted results for different phases are put into fusion to improve prediction efficiency.

4.1. Flight Phase Identification

There are three primary flight phases: climbing, cruising and descending. And there exist to be four transition states at the same time. To identify different flight phases, altitude is the vital data to support the flight phase analyses. As illustrated in Fig. 7, the support vector regression (SVR) is applied to determine the boundary of ADS-B sequence data, which is used to identify the phase switch point. In the neighbourhood of the phase switch point, the track point is marked with a little time delay.

In terms of the SVR boundary, we use $\gamma$ to measure the ADS-B fluctuations:

$$\gamma = |f_r(\alpha_{alt}^t) - \alpha_{alt}^p| \left( \frac{\alpha_{alt}^t - \alpha_{alt}^p}{\tau} \right) - \bar{s}^2$$

(12)

where $f_r$ is the SVR model to predict the ADS-B data, $\bar{s}$ is the average value of altitude for the specific time window, which is calculated as following:

$$\bar{s} = \frac{1}{T} \sum_{j=1}^{T} (\alpha_{alt}^t - \alpha_{alt}^p)$$

(13)

Assuming the fluctuation range of $\gamma$ is $\varepsilon$, when the deviation of $\gamma$ is beyond the normal range, there exist to be high probability to determine that the flight phase is switching. When $\text{sign}(\gamma - \varepsilon) = 1$, relying on the variances and mathematical expectations for $T_i$ and $T_p$, the flight phase switch points can be determined.

\[
\begin{array}{|c|c|c|c|c|}
\hline
\text{Status} & 1 & 2 & 3 & 4 \\
\hline
\text{sign}(D_{i_p} - D_{i}) & 1 & 1 & -1 & -1 \\
\text{sign}(E_{i_p} - E_{i}) & 1 & -1 & 1 & -1 \\
\hline
\end{array}
\]

Figure 8: Flight Transition Phase Switch Status Determination

As illustrated in Fig. 8, $D_{T_i}$, $D_{T_p}$ are the variances for $T_i$ and $T_p$ respectively, $E_{T_i}$, $E_{T_p}$ are the mathematical expectations for $T_i$ and $T_p$ respectively. $\text{sign}(D_{T_p} - D_{T_i})$ is utilized to measure the difference on data fluctuations between training data and prediction data with SVR. $\text{sign}(E_{T_p} - E_{T_i})$ is utilized to measure the difference on average value between training data and prediction with SVR. The transition phase switches are analysed in terms of $\text{sign}(D_{T_p} - D_{T_i})$ and $\text{sign}(E_{T_p} - E_{T_i})$, which determine four transition states. Based on the flight phase identification, the corresponding
flight state is obtained. For normal ADS-B data, there are seven states including three main states and four transition states. The four switch points on the transition states are vital to classify flight phases in order to obtain accurate ADS-B data predictions.

### 4.2. Sequence Prediction

![Sequence Prediction Based on LSTM](image)

Taking advantage of deep learning, the LSTM neural network is constructed to establish the predicted networks. As illustrated in Fig. 9, the prediction deep network consists of four layers, including two full-connected layers and two LSTM layers. The input data is the original ADS-B data sequence and the data is transformed into hidden status. The output is the predicted ADS-B sequence data based on current ADS-B data patterns. For each flight phase, it is important to establish the corresponding normal data model to accomplish predictions, which is utilized to improve the accuracy.

### 4.3. Model Fusion

Analysing the ADS-B data, when the flight is on stable continuous states, the prediction is obtained with the model for specific flight phase. If the flight is on transition states, the prediction is obtained with the fusion results. To improve model fusion, the fusion matrix $W_q$ is designed with relationships between seven states transition weights and four model patterns. Setting climbing, cruise and descending as $\{s_c, s_r, s_d\}$, the transition state set is $\{s_c, s_r, s_d \rightarrow s_c, s_r \rightarrow s_c, s_r \rightarrow s_d, s_d \rightarrow s_c\}$. Based on historical data, the model is established in terms of flight states, which is classified into four patterns: climbing, cruising, descending and the whole flight period. The historical data for the whole flight period model pattern is all the received data up to now. The other patterns utilize the historical data from the corresponding flight state data.

$$
W_q = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
\end{bmatrix}
\begin{bmatrix}
\alpha_1 & \beta_1 & 0 & \kappa_1 \\
\alpha_2 & \beta_2 & 0 & \kappa_2 \\
0 & \beta_3 & \gamma_3 & \kappa_3 \\
0 & \beta_4 & \gamma_4 & \kappa_4 \\
\end{bmatrix}
$$

(14)

where $\alpha_i, \beta_i, \gamma_i, \kappa_i$ are the weight vectors to integrate with different training deep models to make predictions. Assuming the prediction result set is $w_q^i$ and $|w_q^i| = 7$, the final model to predict ADS-B data is:

$$
\Psi = W_q^T \psi_q
$$

(15)

The module utilizes SVR to divide ADS-B data into different parts for different flight phases, supporting more accurate predictions. Relying on LSTM deep prediction networks, the temporal sequential features of data are analysed to construct predicted ADS-B data sequences. Based on different prediction model for different flight phases, the predicted sequences are fused to improve prediction accuracy and reliability.

### 5. Behaviour Discriminator

When the original and predicted ADS-B data are obtained, it is necessary to analyse the pairwise data sequence to identify attack behaviours. The behaviour discriminator module is designed to set up the metrics on attack behaviours and mark ADS-B attack data sequences.

![Behavior Discriminator](image)

As illustrated in Fig. 10, there are four essential parts to generate the behaviour labels: (1) Temporal Association, (2) Distance Measurement, (3) SVDD Discrimination and (4) Behaviour Analysis. The temporal association is designed to match the data sequences on the original and predicted ADS-B data according to the actual sample points. If ADS-B data for the specific sample points is missing, the data will be filled to accomplish data associations. The distance measurement is used to measure the differences between the original and predicted ADS-B data sequences, which offers the evaluation metrics on the attack probability. The SVDD discrimination is designed to analyse the novelty data in the ADS-B data sequences based on SVDD (Support Vector Data Description) methods, which provides the evidence for attack behaviour detections. The behaviour analysis extends the capability of SVDD discrimination, which takes the continuity of attack behaviours into considerations to decrease the false alarm ratio.

#### 5.1. Temporal Association

As illustrated in Fig. 11, the predicted ADS-B data sequence is generated based on historical data with the specific
sample separations. However, the data collected from the real airspaces may be missing due to signal interferences or noise influences. To fill with the original data sequence, the neighbour data is used to generate the full sequence data:

$$\omega_i = \frac{\omega_{i_a} - \omega_{i_b}}{t_{i_b} - t_{i_a}} (t_i - t_{i_a}) + \omega_{i_a}$$ (16)

where $l_m$ is the amount of missing sample points for specific time windows, $t_i$, $t_a$, $t_b$ are the neighbour data time point with available values for $\omega_{i_a}$. By linear interpolation, the missing data are filled with linear growth ratio. All the missing data is filled with equal intervals based on the neighbour reference data.

5.2. Distance Measure

To measure the distance between the original and predicted ADS-B data, the $p$ norm is calculated based on multiple attributes of ADS-B data. The weighted sum is adopted as the distance metric $L$:

$$L = \sum_{k \in A} \epsilon_k^p (\|\omega_{i_k}^a - \omega_{i_k}^b\|_p)$$ (17)

where $\epsilon_k^p$ is the weight variables for time $t_i$ on attribute $k$, the parameter $p$ can be selected from $\{1, 2, \infty\}$, which makes $L$ flexible to depict the differences on each sample point.

5.3. SVDD Discrimination

The SVDD methods are applied with slack variables to model the normal distance $L$ scope, which are dependent on the reliable historical data to construct the boundaries:

$$\min_{\epsilon_i, a} \quad F(R, a) = R^2 + C \Sigma_i \epsilon_i$$

s.t.

$$\|L_i - a\|^2 \leq R^2 + \epsilon_i, \epsilon_i \geq 0, \forall i$$ (18)

where $R$ is the radius to determine boundaries, $a$ is the center of the hyper sphere for SVDD, $L_i$ is the distance between current point and $a$, $\epsilon_i$ is the slack variable to enhance the robustness of SVDD.

To make a trade off between accuracy and false alarm ratio, the boundary is set up with two boundaries to put together. With the data reaching, the historical data can be divided into two time windows: older time window and newer time window. The size of newer time window is much shorter than the size of older time window, which is configured as stationary value to move with time. Based on ADS-B data within older time window, it is utilized to construct the compatible scope $R^c$. Based on ADS-B data within newer time window, it is utilized to construct the expanding scope $R^b$.

Two boundaries are joint to accomplish the final boundary for normal data distance measurements, which are used as the threshold to detect attack behaviours.

$$R^b = R^c + \frac{n_c}{n_e} (R^c - R^e)$$

$$= (1 - \frac{n_c}{n_e}) R^c + \frac{n_c}{n_e} R^e$$ (19)

where $R^b$ is the integrated radius boundary for SVDD methods, $n_e, n_c$ are numbers of sample points for the older and newer time window respectively. Relying on the time ratio, the boundaries are improved to avoid high false alarm ratio on concept drifts of ADS-B data.

5.4. Behaviour Analysis

To identify the attack behaviours, it is not sufficient to only rely on dependent points to make decisions. It is important to make the most of the sequential contextual information. Setting the detection time window is $T_d = \beta T_p$, within $T_d$ the differences between the two sequence data are compared on data probability distribution, which are used to detect attack behaviours on attack continuity. To analyse ADS-B data sequences with contextual information, Wasserstein distance is adopted as the analysis foundation. The definition of Wasserstein distance [2] is:

$$W_p(p(x), q(y)) = \inf \mathbb{E} (||X - Y||_p^2)$$ (20)

where $\mathbb{E}$ is the mathematical expectation function, $X \sim p(x)$ and $Y \sim q(y)$ are random variables, and the infimum is considered over all joint distributions of $X$ and $Y$. Relying on Wasserstein distance, the differences between two sequences on data distributions can be obtained.

Generally, the attack behaviours are identified with two obvious features: (I) the attack data should be beyond the configured thresholds, (II) the attack data should be marked for a long enough detection cycle. According to the analyses on attack behaviours, the attack behaviours are identified with improved rules:

$$z = \frac{\epsilon}{T_d} \sum_{j \in T_d} (L_j - a)^2 + \sigma W_p$$ (21)

where $z$ is the final decision metric on behaviour analysis, $L_j$ is the SVDD discrimination analysis result for time $j$ within $T_d$, $\sigma$ is the normalization variable to configure weights on the final decision for each part.

$$f^j_i = \begin{cases} 1, z_j > \theta_0 \\ 0, z_j < \theta_0 \end{cases}$$ (22)
where $\theta_0$ is initial threshold which is obtained from validations on reliable normal data sets. $Y = \{ f_t^i \}$ is the output of proposed framework, which consists of the decision results with binary sequences. When ADS-B data is marked with attack labels, it is excluded from the normal stream data to avoid attack effects penetrating into ADS-B systems.

6. Dynamic Updater

For ADS-B data, there are no explicit labels to distinguish normal data from attack data in real environments. If the data detected as normal data, it is useful to extend training sets with the validated data. With the procedure, the training data is becoming more reliable to improve prediction reliability. To improve the detection performances, the threshold is necessary with dynamic configurations in terms of detection results and data states. Generally, attackers is constricted with attack capabilities and equipments, which result in low percentage of attack flights for real attack behaviours. Based on the assumption, the threshold is updated periodically.

![Figure 12: Dynamic Updater](image)

As illustrated in Fig. 12, the dynamic updater is designed to establish update procedures, which consists of two modules: training set extension and threshold update module. The training set extension is implemented to enhance the capability of sequential predictor on accuracy. The threshold update is implemented to transfer the static models to dynamic flexible models.

For the dynamic updater, two parameters are chosen to update with current detection results: $T_c$ and $\phi$. Within $T_c$, the attack data number is $A_c$ and the normal data number is $N_c$, which are the key factors to coordinate. As illustrated in Fig. 13, there are three cases to process ADS-B data sequences. For the control time window $T_c$, the ADS-B data sequences can be separated into several parts in terms of behaviour labels. (a) If the attacked data accounts for a small number, it is abandoned to avoid influencing on the decision supports for air traffic. (b) If the attacked data emerges for a continuous time from a specific data time point, the threshold in behaviour discriminator module is updated to enhance the dynamics of the attack detection framework. (c) If the reached data is judged as normal data sequences for $T_c$, the training set in sequence predictor module is extended to enhance the accuracy of the attack detection framework.

![Figure 13: Sequence Updater for Different cases](image)

For case (a), the ADS-B data is hybrid with attacked and normal data. The moving step variable $\eta$ is configured with the percentage of normal ADS-B data. Considering the level of $T_c$ and $T_t$, the adjustment factor $\delta$ is set as 1, which keeps it as before.

$$\begin{align*}
\eta &= \frac{N_c T_c}{(N_c + A_c) T_c} \\
\delta &= 1
\end{align*}
$$

For case (b), the ADS-B data is marked with attacked data, which illustrates the high ratio for attacked data. In such case, there is no more valuable normal data to extend the training sets. However, to decrease the false alarm ratio, it is necessary to modify $\delta$ when the number of attack labels is increasing fast.

$$\begin{align*}
\eta &= 1 \\
\delta &= 1 - \frac{1}{\ln(1 + A_c)}
\end{align*}
$$

For case (c), the ADS-B data is marked with normal data, which illustrates the continuous reliable status on ADS-B data. In such case, the normal data is useful to extend the training sets. Hence, the moving step $\eta$ is increasing within a small range. The threshold is decreased with small fluctuations. The adjustment factor $\delta$ is set in the neighbourhood of 1.

$$\begin{align*}
\eta &= 1 + \frac{c N_c}{e^{T_t}} \\
\delta &= 1 - \frac{1}{e^{T_t}}
\end{align*}
$$

By implementing the dynamic updater, the attack detection performance is improved on efficiency and accuracy. The dynamic feature of the framework enables the system adapt to more attack patterns. The uncertainty and stealthy of attack behaviours are eliminated with dynamic detections.

7. Experimental Analysis

To validate the feasibility and efficiency of the proposed framework, the experiments based on ADS-B data that is
collected from real airspaces are designed and implemented. The initial collected data is crawled from OpenSky, which is preprocessed to deal with missing values. The average amount of flights for each day data reaches 6000, establishing the big data foundation for our framework. For the dataset, the data for each flight varies with the constriction of motion laws, including the intrinsic features for normal data models. The framework is utilized to capture and mine the normal features to distinguish attack behaviours from real stream data.

In terms of limitations of laws and environments, it is quite difficult to obtain attack data from real airspaces. Hence, to accomplish the experiments, attack data is constructed according to attacker intentions. At present, attack patterns for ADS-B data mainly include: data tampering attack, ghost injection attack, data replay attack and DoS attack. For each attack pattern, there are different implementations which result in different attack effects. For the experiments, six classical attack behaviours are used to validate performances of the proposed framework, which cover attack patterns except for ghost injection attack. Ghost injection attack is designed to construct fake messages to model ghost flight data. The ghost flight data is constructed approximately equivalent to the other attack patterns, which is used to create non-existed flights. The other attack patterns are implemented to modify current data itself while ghost attack behaviours are implemented to create new data sequences. Because the proposed framework is designed to focus on attack effect on data to detect attack behaviours, the validations on attack patterns without ghost injection attack are sufficient.

As depicted in Tab. 1, six classical attack behaviours are utilized to validate detection performances. For the whole dataset, the numbers of attack targets are limited within a low percentage, considering the actual capability and stealth of attackers. As illustrated in Fig. 14, the tracks of three flights are chosen to show attack effects on ADS-B data.

- Constant deviation injection attack is designed to inject constant values into current data sequences. When implementing constant deviation injection attack, the deviations are configured as constant static values, which are injected into one of latitude, longitude or altitude attributes randomly. For each iteration of experiments, the deviations for latitude, longitude and altitude are setting as 5%, 5%, 1% of the corresponding attributes respectively.

- Random deviation injection attack is designed to inject random values into current data sequences. When implementing random deviation injection attack, the deviations are configured as random sequences with Gaussian distributions, which are within 3.5% of the corresponding attributes.

- Increased deviation injection attack is designed to inject deviation sequences with a ratio. When implementing increased deviation attack, the deviations are configured as a initial value within 0.1% of the corresponding attributes. With time elapsing, the deviations increases with a small ratio around 0.05%.

- Flight replacement attack is designed to replace current data sequences with data of another flights. When implementing flight track replacement attack, the track data is replaced with another flight data that is randomly selected.

- Data replay attack is designed to put the previous data to take place with current data sequences. When implementing data replay attack, the historical data is utilized to replace current data with specific time delay. The time delay is configured as 5 minutes in the experiments.

- DoS attack is designed to block current data within specific time windows. When implementing DoS attack, the data for attack time window is configured as missing data.

For various attack patterns, the key to ensure the detection efficiency is to master the features of normal data and novelty data. Hence, with the PDU framework, the flight phases are analysed and the transition states are distinguished to enhance the prediction accuracy. As illustrated in Fig. 15, altitude datasets of five different targets are chosen to analyse the phase. The $\gamma$ is calculated to confirm the transition point. When the value of $\gamma > 0.5$, the phases of flight data are changed. In Fig. 15, there are state transitions in subfigure (a)-(d). For (a)-(c), the state transitions cause obvious increase for $\gamma$ to depict the switch between two states. For (d), $\gamma$ is fluctuated around the switch point which results in the time delay of decision on transition states. For (e), the flight phase remains unchanged, for which $\gamma$ is around the neighbourhood of 0.0.

When slicing the data into several parts based on phases, the prediction models are established on the corresponding

| No. | Attack Pattern                  | Attack Effects on ADS-B data                                      |
|-----|---------------------------------|------------------------------------------------------------------|
| ATK-1| Constant Deviation Injection Attack | Inject constant deviations into ADS-B data                       |
| ATK-2| Random Deviation Injection Attack | Inject random deviations into ADS-B data                         |
| ATK-3| Increased Deviation Injection Attack | Inject deviations that increase with time into ADS-B data        |
| ATK-4| Flight Track Replacement Attack | Replace current track data with another flight track             |
| ATK-5| Data Replay Attack              | Replay ADS-B data with some time delay                            |
| ATK-6| DoS Attack                      | Block ADS-B data for specific time window                        |
Figure 14: ADS-B Data with Attack Patterns
data for different phases. Especially, the ADS-B data located on the transition states is predicted with the fusion model to improve the accuracy.

As illustrated in Fig. 16, three representative targets are selected to show the prediction efficiency. The track of original data and prediction data are depicted and the corresponding deviations are analysed to illustrate the accuracy of predictions. For Fig. 16(a), the flight cruise with stable states, for which ADS-B data is with several noise data. The deviations are around $-0.04$ after initial model establishments. Around the noise data, there are mutations on limited numbers of data points. For Fig. 16(b), the flight is climbing with state transitions, for which ADS-B data is with missing data. The prediction deviation is around $-0.1$, which is fluctuated around missing data points. For Fig. 16(c), the flight is descending continuously, for which the prediction data is very accurate within $0.05$ deviations.

Considering the noise data and missing data, the deviations may occur mutations on data points with quite low percentages. For normal ADS-B data, the prediction data is around original data with low deviations, which depicts the efficiency of the Sequential Predictor.
When prediction data is acquired, the Behaviour Discriminator is utilized to analyse the attack behaviours. After temporal associations, the data is distinguished with SVDD discrimination module. As illustrated in Fig. 17, the reasonable boundaries for the normal data are established in terms of five example flights. The boundaries are set up based on the normal data and prediction data, which is utilized to cover normal data except for a small number of outlier points. To improve the adaptation of the boundaries, some slack variables are added to enlarge the scopes. Generally, only relying on SVDD boundaries, the normal data is not described fully for the temporal and spatial features. Hence, the comprehensive decision $z$ is necessary to make the most of contextual information, comparing data sequences within the specific time windows. In terms of attack detection results, Dynamic Updater is implemented to modify key parameters: $\eta$ and $\delta$ to improve attack accuracy. By 100 experiments, the accuracy and false alarm ratio of proposed framework are validated.

The metric of detection accuracy is defined as the ratio that detected attack targets account for the whole attack targets in data sets. If more attack targets are detected from the whole data sets, the attack data can be labelled in time to avoid it into decision flow. As illustrated in Fig. 18, the data of six classical attack patterns are detected with the framework. The red line is the average detection accuracy. For ATK-2, the random deviations destroy the correlations on temporal features, which result in high detection accuracy. For ATK-4, the selected flight data sequences are different with current data sequences, in which there exist to be obvious mutations for the replacement data points. For ATK-6, DoS attack increase the ratios of missing data, which is prone to being detected easily. Thus, detection accuracy results for random deviation injection attack (ATK-2), flight replacement attack (ATK-4) and DoS attack (ATK-6) are better than the others. For ATK-1, the values of constant deviations are related with the detection results. If the constant deviations are lower relatively, the difficulties of attack detection are increased, which cause the lower attack detection accuracy than detections on ATK-2. Similarly, for ATK-5, when the replay time is close to current time point, the detection performances are eliminated in terms of such attack pattern. The detection accuracy for ATK-1 and ATK-5 are approximate. For ATK-3, the deviations are increased with time which are configured with low initial values. Meanwhile, the deviations are changed with a relatively lower level to keep temporal correlations, which result in the lowest detection accuracy than others.

The metric of detection false alarm ratio is the value that normal targets account for the whole detected results. If more normal data is labelled with attack data, the detection performances are eliminated to influence on effective surveillance. As illustrated in Fig. 19, the false alarm ratio for six classical attack patterns are validated. False alarm ratios for ATK-2 and ATK-4 are relatively lower around 2.0% due to large differences for normal data and attack data. For ATK-1 and ATK-5, false alarm ratios are around 4.0%. For ATK-3, the false alarm ratio is higher, because the slowly increased deviations make attack features stealthy and reduce the differences between normal data and attack data. For ATK-6, the false alarm ratio is the highest, which is caused by missing data. In real environments, there are missing data in normal data sequences, which is approximate with attack data with ATK-6.

When attackers implement attack behaviours, different attack patterns may emerge at the same time, which increase the difficulties of detections. In terms of the complex scenarios, the efficiency of the framework is tested further. The attack data sets are constructed with six attack patterns (depicted in Tab. 1), in which attack patterns are randomly selected for each attack data sequences. The ratio of attack targets vary from 0% to 100%. As illustrated in Fig. 20, the accuracy and false alarm ratio of detections are validated. In Fig. 20(a), the accuracy reaches the maximum value when attack targets account for 8%. When the ratio of attack targets is lower, the normal data sets are sufficient to establish accurate model and the threshold is configured dynamically to the reasonable value. As a result, the detection accuracy remains a high value within 20% attack targets. When the ratio of attack targets is beyond 20%, the accuracy is fluctuated around 88%. For the scope of attack target ratio, the accuracy is improved with dynamic updater. When the ratio of at-
tack targets is more than 60%, the accuracy increase with the amount of attack data growing. In Fig. 20(b), the false alarm ratio descends within 20% attack targets when the proportion of normal data is decreasing. The discriminant threshold is gradually configured as a reasonable value. When the ratio of attack targets is beyond 25%, the false alarm ratio increases. With the ratio of attack targets increasing beyond 66%, the value of false alarm ratio descends to 0% fast due to the proportions of normal data are decreasing gradually.

In complex environments, the ratio of attack targets are limited within low percentages. When attack target ratio is within 20%, the detection of proposed framework is with higher accuracy and lower false alarm ratio relatively. Hence, the efficiency and feasibility of the framework are validated in face of complex attack scenarios.

8. Discussion

In real environments of air traffic, attack detections on various attack patterns are in face of lots of uncertainty and complexity. Although the feasibility and efficiency of the framework are validated by experiments for six classical attack patterns, there still exist to be challenges when developing in real environments and detecting complex ADS-B data sequences. As illustrated in Fig. 21, the data sequences are difficult to predict with high accuracy, which results in high false alarm ratio.

(1) When ADS-B data is changed fast and not continuous within short time, the prediction data sequences cannot be modelled accurately to capture intentional features of normal data. If the differences between original data and prediction data are too large, the basic assumptions for the framework are non-existent. As a result, the corresponding flight data is detected as attack data, which increases the false alarm ratio. If the complete track for the dynamic data can be obtained before several days, it is possible to learn data features to accomplish detections. However, if the historical data for the dynamic targets cannot be obtained before detections, the framework is in demand of accurate motion models to provide reliable prediction data sequences.

(2) When original data is mixed with noise data with large values, the collected data is novelty data even though the deviations are not caused by attackers. If the framework encounters such data sequences, the data is prone to being identified as random deviation attack data sequences. As a result, the data is labelled with attack data, which is abandoned with high probability. The data is detected as attack data by mistake, but the result is acceptable to keep novelty data away from surveillance systems.

(3) When original data is lacking of sufficient data points with missing data, the data is detected as DoS attack data sequences with the framework. The false alarm ratio is increased if the data sequences with missing data account for large ratios. As a result, detection performances of the framework are eliminated. The existed data points in the original data can not be utilized to improve situation awareness.

For the proposed framework, the quality of data is important. Meanwhile, the efficiency of each module is related tightly with the performances of detections. The prediction module utilizes LSTM as the core component, but it relies
on large volumes of historical ADS-B data and is in need of long time to obtain models. If the attack scenarios require online detection, the module should be improved with online prediction algorithms. The behaviour discriminator module utilizes SVDD as the core component to establish normal data boundaries, but it is dependent on reliable normal data. If normal data is mixed with attack data as the training data, the SVDD boundaries are extended to cover more attack data. As a result, more attack data cannot be detected in time. Thus, the discriminator module should ensure the reliability of prediction data sequences and original data sequences. The dynamic updater is only designed to improve two parameters and the rules are too empirical, which eliminate performances of the module. All in all, the framework offers baselines for predictive discriminative model to detect attack behaviours on ADS-B data, which should be improved according to more complex detection scenarios.

9. Conclusion

The PDU framework is proposed to offer baselines for detection solutions based on prediction methods on ADS-B data. Each component is replaceable with any other method to act as the same functions. Based on ADS-B data features, the practical methods under the framework are designed and implemented, which are validated on feasibility and efficiency. The proposed methods are integrated and established to improve adaptations in face of various attack patterns.

However, when encountering target data with high manoeuvrability and complicated noise impacts, the proposed methods lack of sufficient efficiency to detect and locate the attack data within low time delay. When there is not adequately reliable historical data to support normal data model construction, the framework will be confronted with challenges. Considering the uncertainty and dynamic features of attack behaviours, the self-learning capability of the framework should be paid more attention to improve.

CRediT authorship contribution statement

Tengyao Li: Conceptualization, Methodology, Formal Analysis, Software, Validation, Writing-Original Draft, Visualization.

References

[1] Akerman, S., Habler, E., Shabtai, A., 2019. Vizads-b: Analyzing sequences of ads-b images using explainable convolutional lstm encoder-decoder to detect cyber attacks. Arxiv.
[2] Assa, A., Plataniotis, K.N., 2018. Wasserstein-distance-based gaussian mixture reduction. IEEE Signal Processing Letters 25, 1465–1469. doi:10.1109/LSP.2018.2865829.
[3] Cho, T., Lee, C., Choi, S., 2013. Multi-sensor fusion with interacting multiple model filter for improved aircraft position accuracy. Sensors 13, 4122–4137. URL: <GotoISI>://WOS:000318036400009, doi:10.3390/s130404122.
[4] Habler, E., Shabtai, A., 2018. Using lstm encoder-decoder algorithm for detecting anomalous ads-b messages. Computers & Security 78, 155–173. URL: http://www.sciencedirect.com/science/article/pii/S0167404818303725, doihttps://doi.org/10.1016/j.cose.2018.07.004.
[5] Kovell, B., Mellish, B., Newman, T., Kajopaiye, O., 2012. Comparative Analysis of ADS-B Verification Techniques. Report. Department
Figure 20: Performances for Different Ratios of Attack Targets

(a) Accuracy for Different Ratios of Attack Targets

(b) False Alarm Ratio for Different Ratios of Attack Targets

Figure 21: Complex ADS-B Data

of Electrical, Computer and Energy Engineering, University of Colorado.

[6] Leonardi, M., 2018. Ads-b anomalies and intrusions detection by sensor clocks tracking. IEEE Transactions on Aerospace and Electronic Systems, 1–10. doi:10.1109/TAES.2018.2886616.

[7] Li, T., Wang, B., Shang, F., Tian, J., Cao, K., 2019. Online sequential attack detection for ads-b data based on hierarchical temporal memory. Computers & Security 87, 101599. URL: http://www.sciencedirect.com/science/article/pii/S0167404819301531, doi:10.1016/j.cose.2019.101599.

[8] Mahmoud, M.S.B., Pirovano, A., Larrieu, N., 2014. Aeronautical communication transition from analog to digital data: A network security survey. Computer Science Review s 11–12, 1–29.

[9] 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 Transactions on Vehicular Technology 65, 3150–3165. URL: <GotoISI>://WOS:000402724400002, doi:10.1109/TVT.2015.2438171.

[10] Riahi Manesh, M., Kaabouch, N., 2017. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ads-b) system. International Journal of Critical Infrastructure Protection 19, 16–31. URL: http://www.sciencedirect.com/science/article/pii/S1874548217300446, doi:10.1016/j.ijcip.2017.10.002.

[11] Sampigethaya, K., Poovendran, R., 2013. Aviation cyber-physical systems: Foundations for future aircraft and air transport. Proceedings of the IEEE 101, 1834–1855. doi:10.1109/JPROC.2012.2235131.

[12] Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C., 2011. Future e-enabled aircraft communications and security: The next 20 years and beyond. Proceedings of the IEEE 99, 2040–2055.

doi:10.1109/JPROC.2011.2162289.

[13] SC-186, R.F., 2011. Minimum Operational Performance Standards (MOPS) for 1090 MHz Extended Squitter Automatic Dependent Surveillance - Broadcast (ADS-B) and Traffic Information Services - Broadcast (TIS-B). Document (RTCA (Firm)), RTCA, Incorporated. URL: https://books.google.com/books?id=H69erQAeAAJ.

[14] Smith, M., Strohmeier, M., Harman, J., Lenders, V., Martinovic, I., 2019. Safety vs. Security: Attacking Avionic Systems with Humans in the Loop.

[15] Strohmeier, M., Lenders, V., Martinovic, I., 2015a. Intrusion detection for airborne communication using phy-layer information.

[16] Strohmeier, M., Lenders, V., Martinovic, I., 2015b. On the security of the automatic dependent surveillance-broadcast protocol. IEEE Communications Surveys & Tutorials 17, 1066–1087. URL: <GotoISI>://WOS:000354860000024, doi:10.1109/COMST.2014.2365951.

[17] Strohmeier, M., Lenders, V., Martinovic, I., 2016. A localization approach for crowdsourced air traffic communication networks. IEEE Transactions on Aerospace and Electronic Systems PP, 1–1.

[18] Strohmeier, M., Martinovic, I., 2014. Detecting false data injection attacks on air traffic control protocols. Planta 72, 371–384.

[19] Strohmeier, M., Schafer, M., Lenders, V., Martinovic, I., 2014. Realities and challenges of nextgen air traffic management: the case of ads-b. IEEE Communications Magazine 52, 111–118. doi:10.1109/MCOM.2014.6815901.

[20] Strohmeier, M., Schafer, M., Pinheiro, R., Lenders, V., Martinovic, I., 2017. On perception and reality in wireless air traffic communication security. Ieee Transactions on Intelligent Transportation Systems 18, 1338–1357. URL: <GotoISI>://WOS:0004027244000082, doi:10.1109/TITS.2016.2612584.

[21] Sun, J., H. V., Ellerbroek, J., Hoekstra, J.M., 2019. pymodes: Decoding mode-s surveillance data for open air transportation re-
Tengyao Li received the M.S. degree in computer science and technology from Air Force Engineering University, in 2016 and is pursuing for the Ph.D. degree in Air Force Engineering University. His current research interest is attack detection and resilient recovery on ADS-B data.