On Passive Data Link Layer Fingerprinting of Aircraft Transponders

Martin Strohmeier, Ivan Martinovic
University of Oxford, United Kingdom

ABSTRACT

In order to meet future demands in increasingly congested airspaces, the world's aviation authorities are currently upgrading their air-traffic management systems. The Automatic Dependent Surveillance-Broadcast (ADS-B) protocol is at the core of the Next Generation Air Transportation (NextGen) system, and an increasingly large number of aircraft use ADS-B to broadcast data to their surroundings.

In this paper, we use differences in the implementation of aircraft transponders to fingerprint their wireless drivers. In particular, without any modification to either aircraft or the off-the-shelf ADS-B receivers that we use, we develop a passive fingerprinting technique that accurately and efficiently identifies the wireless implementation by exploiting variations in their transmission behavior. We perform an evaluation of our fingerprinting technique that shows it both quickly and accurately fingerprints aircraft transponders using real-world aircraft data. Furthermore, through cross-referencing our fingerprints with open source aircraft databases, we are able to infer potential aircraft types and fleet combinations, as well as general market proliferation of different transponder implementations. Finally, we discuss implications for the security and privacy of our approach as well as potential mitigating factors.

1. INTRODUCTION

As commercial air traffic is set to double until 2030, currently used air traffic control (ATC) technologies are quickly reaching their capacity limits. To replace the traditional primary and secondary surveillance radar methods, the aviation authorities around the world have adopted a new protocol standard called Automatic Dependent Surveillance - Broadcast or ADS-B. It is one of the core pieces of the Next Generation Air Transportation (NextGen) upgrade to improve the world's air traffic management systems to cope with the increased traffic density in many airspaces.

ADS-B is a major shift in the way air traffic control works, changing from *independent* to *dependent* surveillance. With ADS-B, aircraft retrieve their own position using GPS or any other Global Navigation Satellite System (GNSS) and broadcast it periodically alongside other information such as velocity or identification to ATC ground stations and other aircraft. Compared to traditional dependent systems, that gauge the position and bearing of an aircraft using ground-based interrogations, the new approach offers much better accuracy and faster update rates. Along with lower maintenance costs, this achieves improved situational awareness for both controllers and pilots. It enables controllers to lower the minimum separation between aircraft and thus to increase airspace density, a crucial requirement to deal with take-offs and landings at crowded airports in the future. Consequently, the European authority Eurocontrol and the US-American Federal Aviation Administration (FAA) mandated the use of ADS-B by 2017 and 2020, respectively. Until then, many aspects of ADS-B still need evaluation to ensure a safe adoption, most importantly the lack of security and privacy of the protocol [4, 12, 16, 20]. As most aircraft in these airspaces are already equipped with the new technology and broadcasting ADS-B messages, this offers an opportunity for independent research on these problems using a large amount of potential data.

This paper makes the following contributions:

- We present a fingerprinting method for aircraft using their ADS-B transponders and evaluate it on real-world data.
- Through cross-referencing our fingerprints with open source aircraft databases, we are able to infer potential aircraft types and fleet combinations, as well as general market proliferation of different transponder implementations.
- Finally, we discuss implications of our approach for the security and privacy of air traffic communication as well as potential mitigating factors.

The remainder of this paper is structured as follows. Section 2 gives a brief introduction to current air traffic control communication protocols. Section 3 presents the related work on fingerprinting, while Section 4 explains our approach to the fingerprinting of aircraft. Section 5 describes the data collection using our research sensor network OpenSky. Section 6 evaluates our work and Section 7 discusses some of the insights we have gained. Finally, future work is contemplated in Section 8 and Section 9 concludes this paper.

CPS-SPC'15, October 16, 2015, Denver, Colorado, USA.
 ISBN 978-1-4503-3827-1/15/10 ...$15.00.
DOI: http://dx.doi.org/10.1145/2808705.2808712.

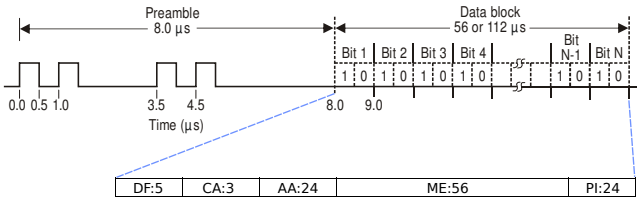

Figure 1: 1090ES data link format [16]. The fields are message format (DF), transponder capabilities (CA), 24-bit aircraft identifier (AA), message content (ME), and CRC (PI).

2. MODERN AIR TRAFFIC CONTROL

This section gives a short introduction to modern air traffic control communication in general and ADS-B in particular, as we use it for our fingerprinting process.

Overview of the ADS-B Protocol

ADS-B is considered the satellite-based successor of radar surveillance by Eurocontrol and the FAA. Until today, ATC relies on interrogation-based surveillance to retrieve an aircraft's identity and altitude. ADS-B's introduction shifts this traditional ATC paradigm towards *cooperative* and *dependent* surveillance. An aircraft retrieves its position and velocity using an onboard satellite receiver. This information is broadcasted twice per second by the transmitting subsystem ADS-B Out. The messages are received by ground stations and by nearby aircraft, if equipped with ADS-B In, where they are processed further (e.g., by collision avoidance systems such as TCAS). ADS-B offers many further fields such as ID, intent, urgency code, and navigation accuracy/uncertainty level.

Two ADS-B data link standards are currently in use, Universal Access Transceiver (UAT) and 1090 MHz Extended Squitter (1090ES). UAT has been created specifically for the use with aviation services such as ADS-B. It uses the 978MHz frequency and offers a bandwidth of 1Mbps. Since UAT requires fitting new hardware, as opposed to 1090ES, it is currently only used for general aviation in Eurocontrol and FAA-mandated airspaces, a fact that will not change in the foreseeable future. Commercial aircraft, on the other hand, employ 1090ES, a combination of ADS-B and traditional secondary surveillance radar with the same bandwidth. This means that the ADS-B function can be integrated into the legacy radar system.

In this work, we focus on the 1090ES data link for our fingerprinting of commercial aircraft transponders, the format of which is shown in Fig. 1). Fig. 2 provides a graphical illustration of the ADS-B system architecture and the protocol hierarchy.[1] Estimates from [7, 21] and our own (European) data from the OpenSky network suggest that about 80% of all commercial aircraft are now equipped with ADS-B Out.

While the 1090ES data link provides a 24 bit CRC to detect and correct possible transmission errors, the ADS-B system does not offer any authentication or integrity checks to detect malicious interference. As such, security threats need to be handled using alternative means [18].

[1]The specification [13, 14] provides the full technical details of ADS-B.

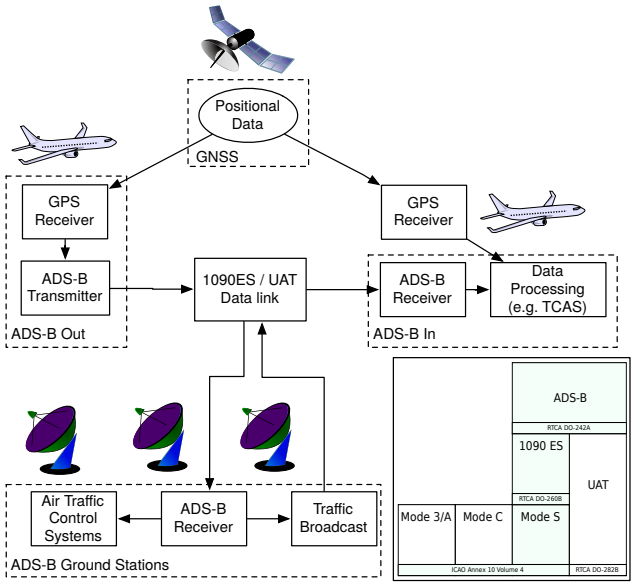

Figure 2: Overview of the ADS-B system [20]. Using a GNSS and other instruments, aircraft fetch their own position and velocity and broadcast these data alongside the aircraft identifier through the ADS-B Out system. Ground stations and other aircraft (via ADS-B In) receive these messages over the two possible data links, 1090ES or UAT.

3. RELATED WORK

Fingerprinting is a popular research area in wireless networks of any application *or use case*. With sufficient entropy in information on chip sets, firmware, drivers and other to tell apart different wireless devices, fingerprinting can for example be used to ensure the continuity of a wireless user over time. While to the best of our knowledge, there have been no previous attempts at fingerprinting aircraft transponders in any way, many works exist that apply a number of different techniques to other areas of wireless communication. These techniques can broadly by sorted into three different categories as defined by Zeng et al. [23]: software-based fingerprinting, hardware-based fingerprinting and channel/location-based fingerprinting.

3.1 Software-Based Fingerprinting

Software-based fingerprinting exploits variation in behavioral patterns of software deployed on wireless devices. Typically, even widely utilized wireless protocols are not specified into the last possible detail, either on purpose or because of non-specificity during the design phase. This leaves a lot of tolerance for device manufacturers and driver developers for their own software implementations, leading inevitably to variations that can be exploited for fingerprinting features. Our work on fingerprinting is loosely based on [5], where the authors develop a passive fingerprinting technique that identifies the wireless device driver of clients running IEEE 802.11 by exploring differences in the probing behavior of the clients. Similar works are also [2, 3], where the authors use passive spectral analysis to identify WLAN cards by exploiting the periodicity caused by distinct implementations of rate switching and active scanning algorithms.

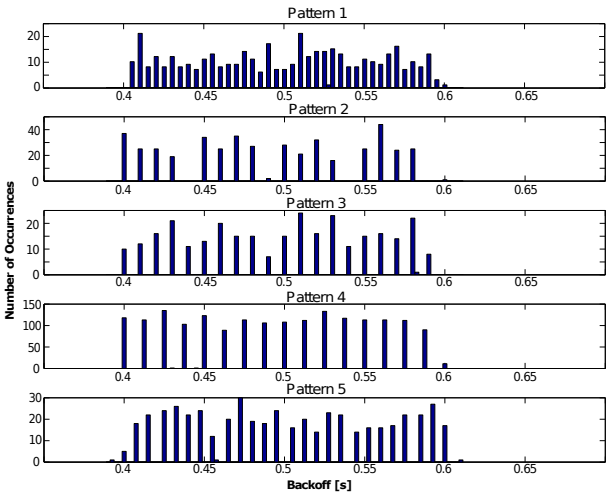

Figure 3: A representative illustration of five different transponder types. The graph shows the histograms of five time series of collected ADS-B position messages.

Compared to the large and often non-transparent ecosystem of wireless LAN cards and drivers, it is likely that large fleets of airline operators are fitted with very similar or even the same hardware, making them harder or even impossible to differentiate and on the other hand easier to study and copy as we do in this work.

3.2 Hardware-Based Fingerprinting

There are several techniques to identify hardware differences in wireless transmitters, which can be exploited to build signatures to fingerprint these devices and their users.

Such radiometric fingerprinting can for example be based on differences in the turn-on/off transient (see, e.g., [6]) or the modulation of radio signals. Both features have been shown to work in shorter-distance, non-mobile cases but are more difficult to apply in the highly mobile ADS-B setting with its long distances.

Clock skew is another popular fingerprinting feature in wireless devices. It can be measured using timestamps in transmitted messages and exploits the fact that no two clocks run precisely the same over time (see [8] for the primary work on clock skew fingerprinting).

Recent research examines the use of so-called physically unclonable functions (PUFs) for hardware-based fingerprinting, which essentially exploit specifically implemented circuits to create unique and secure signatures. For a good overview on PUFs, see [10].

3.3 Channel/Location-Based Fingerprinting

Wireless physical layer characteristics, based for example on received signal strength (RSS, e.g. [11]), channel impulse response (CIR, e.g. [24]) or the carrier phase (e.g. [22]) are being used to implement information-theoretically secure key exchange schemes.

Similarly, such radio frequency signals characteristics can be used for indoor and outdoor localization. Liu et al. [9] give an overview of the techniques used in wireless indoor positioning including the different algorithms (k-Nearest Neighbor, lateration, least squares and Bayesian among others) and primitives such as RSS and angle of arrival (AoA).

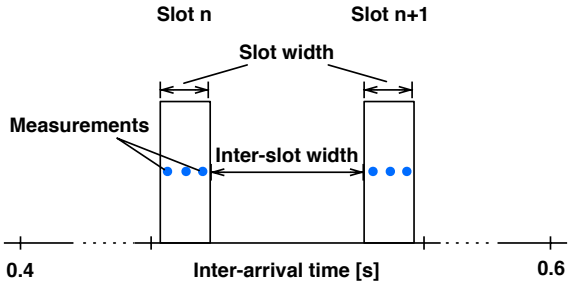

Figure 4: Schematic showing two slots as used by the transponder implementations, determined by measured inter-arrival times.

4. AIRCRAFT FINGERPRINTING

In this chapter, we analyse patterns of aircraft messages to identify distinct differences between ADS-B transponder types and their implementations used in the commercial aviation market. We engineer several fingerprinting features based on transmission behavior deduced from randomly chosen message inter-arrival times.

As is the case in many wireless networking ecosystems (see Section 3), these transponders exhibit some different behaviors on the data link level as well as the physical layer which can be utilized to distinguish incoming messages. In the following, we identify and describe such differences on the data link layer using manual and automatic features selection and classification.

Feature Engineering

The only information needed for the features described in this section is a message's arrival time in the form of an absolute time stamp t_i. From this, we can calculate the inter-arrival time Δt between two subsequent messages from the same aircraft (as indicated by its transponder identification) by subtracting t_i from t_{i+1}. Indeed, while ADS-B is not encrypted, exploiting such timing and inter-arrival information between various message types is naturally possible even with fully encrypted messages when the same transmission patterns are followed.

A standard implementation of the ADS-B protocol broadcasts three types of messages in a regular manner:

- **Position messages:** The aircraft broadcasts a message with its own position on average every 0.5 seconds. A transmission mechanism is used to send the next message after a time interval randomly drawn from [0.4; 0.6] seconds.
- **Velocity messages:** The aircraft broadcasts a message with its current velocity on average every 0.5 seconds. Similar to the position messages, the random message transmission interval is specified to be between 0.4 and 0.6 seconds.
- **Identification messages:** The aircraft broadcasts a message with its own ICAO (International Civil Aviation Organization) 24-bit identifier on average every 5 seconds. Their transmission interval is randomly drawn between [4.8; 5.2] seconds.

Table 1: Statistics about the utilized OpenSky dataset collected by a single sensor between November 9 and November 18 of 2014.

Flights	44,692
Unique ICAOs	4,997
# messages	30,772,643
Time frame	10 days

Through our explorative research, we discovered a number of variations in the transmission periodicity across the aircraft data we analyzed. The key insight here is that all major implementations do not use a truly random interval but instead use a number of possible slots placed more or less evenly throughout the specified interval. Over time, this leads to very different-looking distributions of the inter-arrival times of a given message type (see Fig. 3 for an illustration of some representative transponder behavior), based on which we develop some distinguishing features as explained in the following:

- **Slot number:** The most obvious feature is the number of slots in the given interval of 0.2s for position and velocity messages and 0.4s for identification messages.
- **Slot width:** The second feature is the width of a slot. The time interval which constitutes a slot is defined by the minimum and maximum measured inter-arrival times of messages in this slot (rounded to what we believe is the actually programmed time).
- **Inter-slot width:** Analogous to the previous feature, there are intervals between slots which are not used for sending a message (see Fig. 4).
- **Missing slots:** Some implementations consistently do not use every fifth slot (i.e., those at 0.44, 0.49, 0.54 and 0.59 seconds for position and velocity messages). A subset of these uses the 0.59s slot but only very sparingly.
- **No width slots:** Some implementations' first and last slots do not have a width. All messages are sent exactly at 0.4 / 0.6 seconds respectively if these slots are chosen.
- **First slot:** Regardless of the slot pattern, transponders differ in the timing of the first slot that is being used, or in other words the actual minimum time interval Δt_{min} between two consecutive messages of the same type.
- **Last slot:** Analogous to the last point, transponders also differ in the timing of the last slot that is being used, or in other words the actual maximum time interval Δt_{max} between two consecutive messages of the same type.

5. EXPERIMENTAL SETUP

In this section, we describe our experimental setup, including the data collection process.

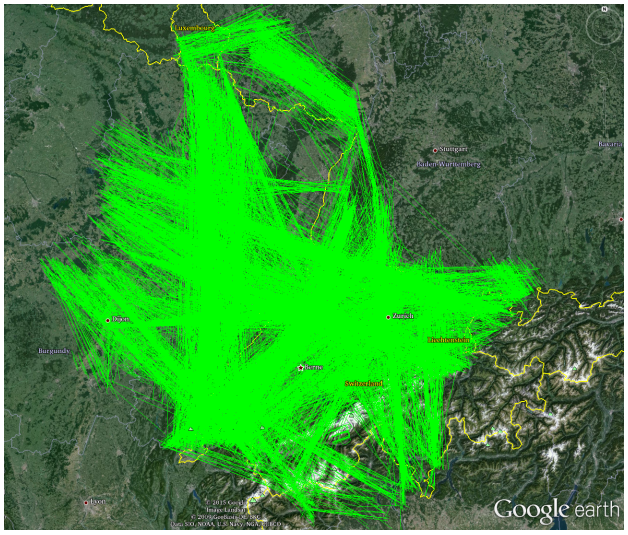

Figure 5: Exemplary visualization of 2910 of the flight trajectories used for our data analysis spanning roughly one day.

Data Collection and Hardware

As ADS-B has been in the roll-out phase for years, we can use data from actual aircraft collected in real-world wireless environments. For our evaluation, we rely on data obtained from the OpenSky project [17]. OpenSky is a participatory sensor network that collects ADS-B messages in a centralized database. In its current deployment, it receives data from 26 sensors, capturing more than 30 % of the commercial air traffic over central Europe. The data is made freely available to researchers. For the present analysis (see also Table 1), we use a dataset that spans the period between November 9 and November 18, 2014. This dataset contains 30,772,643 ADS-B messages received from SBS-3 sensors manufactured by Kinetic Avionics. Besides the message content, they provide a timestamp of the message reception. The timestamps have a clock resolution of 50 ns. All sensors have omnidirectional antennas and can receive signals from a distance of up to 400 km. We stripped down the dataset to only use flights for our evaluation which had at least 200 received messages. The final data sample consisting of 2910 flights is visualized in Fig. 5.

6. EVALUATION

We first analyze our data by hand, sorting the flights according to different clusters according to their slot numbers and missing slot behavior. Based on all feature combinations, we discovered six main types of transponder behavior in our dataset. We further encountered numerous special cases with unique feature combinations at least in our data set, making these aircraft more identifiable and traceable, even when their correct ID is not broadcasted.

Table 2 shows the values of the features inherent to the 6 main types we have identified. We chose to name the first two types 1a and 1b since they are very similar to each other in comparison with the other types, and differ only in additional slots at the beginning and the end. It is interesting to note, that some of these implementation violate the original ADS-B specification of an inter-arrival time between 0.4

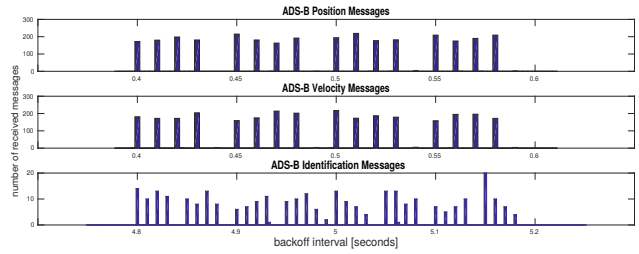

Figure 6: A representative illustration of the different message types. The graph shows the histograms of three time series of collected ADS-B position, velocity and identification messages from the same flight. The pattern characteristics are invariant across all types.

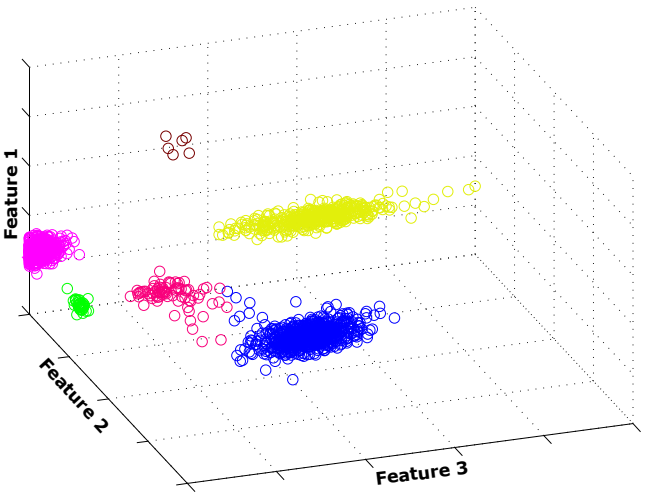

Figure 7: The graph illustrates the clustering of transponders along three dimensions.

and 0.6 seconds. Some are in a clear violation such as type 5 which has its last slot at 0.61s, while others have their slots centered exactly at 0.4s (or 0.6s), causing one half of the slot to be outside the specified interval. This is presumably also the explanation for the "no width slots" feature found in type 1b and 4, which means the edge slots are both at exactly the edges of the defined interval.

We further found that the transponder software typically exhibits the same patterns within every one of three regular message types as shown in Fig. 6. More concretely, for the identification messages that are broadcasted every 5s the described behaviors stay the same and are only spread out over an interval of 0.4s instead of 0.2s. On the other hand, we could not find any additional noticeable patterns in the inter-arrival times between different message types (e.g., between positional and velocity messages).

6.1 Comparison with k-Means Clustering

After hand-crafting clusters by exploring our features through observation as described in the last section, we compare our results with an unsupervised clustering approach. Using the k-Means clustering algorithm, we found the best results for six clusters. Fig. 7 illustrates an example of these clusters in three-dimensional space of complex features. We can see that there are 5 very distinct and large clusters on these dimensions, with a sixth smaller cluster. There are some flights that lie in between clusters, causing occasional unstable assignments. Apart from this, both approaches match with good accuracy (see Table 3 for the comparison).

Table 3: Distribution of different transponder types in our dataset, supervised approach vs. clustering.

Type	Supervised	Clustering
Type 1a	6.2%	6.1%
Type 1b	28.3%	32.6%
Type 2	41.0%	34.6%
Type 3	18.3%	21%
Type 4	6.1%	8.4%
Type 5	0.1%	0.1%

6.2 Time-Stability of Results

To verify the stability of our results over time, we trained all flights collected in our original dataset and looked for flights with the same ICAO identifier over the following week. With 1287 returning flights, we found that the estimation of the transponder type stayed the same with 99.8% likelihood (see Table 4). We found that the mis-classifications were all caused by transponders shifting on the spectrum between the very similar cluster types 1a and 1b, as the first and last slot features' accuracy was not sufficient . The last slot feature was the least stable while the missing slot feature's presence did not change at all in our test.

6.3 Mapping against Open Source Aircraft Data

To verify our findings and conduct further research into the matter of differences in ADS-B transponders, we required some type of ground truth on aircraft and their equipment. ADS-B transponders form part of the avionics the plane was manufactured with or later upgraded by the fleet operator. There is a wide variety in transponders manufactured and installed around the world, depending on business and regulatory reasons. For new aircraft where the transponder came with the installed avionics at delivery, the purchaser selects a whole avionics suite from the available options given by the manufacturer of the aircraft. When the transponder is retrofitted later, the options are much broader and a suitable transponder can be chosen from any that are certified for a) the operator's home nation and b) for the airframe in question. Since such data is not available directly from aircraft vendors and airlines, we conducted our mapping with open source data freely accessible on the internet. Using the database available in the Planeplotter software[2], we could map the ICAO number received in the ADS-B messages of any given flight to its aircraft type as saved in the database. The ICAO number also provides the current airline of the corresponding aircraft, giving another important classification feature. We used a version of the SQLite database file database.sqb downloaded in November 2014, containing 120,149 rows of aircraft data.

[2]http://www.coaa.co.uk/planeplotter.htm

Table 2: Feature combinations of different transponder implementations. Number of slots, first slot, and last slot features are given for position and velocity messages.

Feature	# Slots	Slot width	Inter-slot width	Missing slots	No width slots	First slot	Last slot
Type 1a	39	±0.00025s	0.005s	No	No	0.405s	0.595s
Type 1b	41	±0.00025s	0.005s	No	Yes	0.40s	0.60s
Type 2	16	±0.001s	0.01s	Yes	No	0.40s	0.59s
Type 3	20	±0.0005s	0.01s	No	No	0.40s	0.59s
Type 4	16	±0.0015s	0.125s	No	Yes	0.40s	0.60s
Type 5	26	+0.00016s	0.008s	No	No	0.40s	0.61s

We further conducted a Google research exercise to find out which of the aircraft fleet are equipped with which kind of transponder. This type of data is not necessarily easily available but can eventually be inferred from cross-referencing many articles and data sheets on avionics equipment of different fleets around the web.[3] Some of the required information can also be contained in existing scientific articles such as [1]. Using these sources, we found concrete information on some of the fleets we observed in our data set and used them as exemplary representatives of the whole cluster. Interestingly, the different implementations are not exclusive to a single manufacturer as seen in Table 5. While we do not see a direct negative impact by our work on the security or privacy of the transponder manufacturers or users, we do not not publish the mappings between aircraft fleet and transponder behavior before obtaining feedback by the affected parties.

We could not establish a link between different versions of the implementation of the ADS-B standard (DO-260, DO-260A or DO-260B), which can add to the variety of the installed landscape, as fleets which already have ADS-B installed get eventually upgraded to newer versions. As the behavior of the transmission periodicity can easily be changed with a software upgrade, this can also confound the results.

7. DISCUSSION

In this section we further analyze our findings by suggesting some potential applications and discussing a number of insights we learned during our work.

7.1 Potential Applications

We suggest some potential applications of fingerprinting ADS-B transponders and/or aircraft in general.

7.1.1 Intrusion detection

Our work on fingerprinting can lay the groundwork for an anomaly detection system to identify all manner of inconsistencies in the operation of the protocol, most notably detect potential intrusions. ADS-B - and air traffic communication in general - has a number of well-known security problems as described, e.g., in [18, 16]. The completely unauthenticated nature of the protocol enables anyone with cheap off-the-shelf software-defined radios and software available on the internet to listen and send ADS-B messages with little knowledge. A typical threat model against which an intrusion detection system (IDS) could be used successfully, is the injection of so-called ghost aircraft into the 1090MHz channel. Concretely, we can assume that an attacker creates correctly formatted ADS-B messages, covering the expected types (position, velocity, identification) in valid sequential orders and spacings according to the standard specification. If we also assume the attacker uses a legitimate ICAO address and reasonable flight parameters (e.g., believable altitude and speed), such an injected aircraft cannot be distinguished from a real one using standard ATC procedures.

ADS-B has been developed over twenty years ago, illustrating the decade-long protocol cycles found in aviation and the low probability of a new protocol or upgrade addressing the security problems in ADS-B in the near future. Due to the slow-moving nature of the aircraft industry caused by legacy requirements, security approaches that do not require any modifications to the deployed ADS-B systems and protocols are severely needed. Such countermeasures can function alongside the current system without disrupting it and still provide an immediate, significant improvement in terms of security [19]. IDS can provide such transparent countermeasures by detecting anomalies in received flight data and alerting the responsible authorities. IDS use a multitude of learned features to tell apart normal from suspicious behavior. Fingerprints of any kind can provide such features which an attacker has to adequately mimic when inserting false data onto the wireless channel. It has to be noted, that such an approach cannot provide guaranteed security. As with all types of fingerprints and anomaly detection systems, an attacker can learn the features of the system and adapt the injected messages to match the patterns expected by the IDS. This is no different with the data link features discussed in this work. However, we maintain their usefulness not only against naive attacker models. The more features we track, the more degrees of freedom we take away for the attacker, and consequently the more difficult it becomes to inject ghost aircraft without being noticed by the system.

7.1.2 Privacy implications

Flight privacy is an aircraft's ability to prevent unauthorized parties from tracking its current or past location. It helps preserve aircraft operators/owners interests, in terms of safety or sensitive business information which could be compromised if it were possible to for example track the movements of large companies' CEOs [15]. The current standard for flight privacy in the US is the so-called Block Aircraft Registration Request (BARR) mechanism. Upon the request of a private aircraft owner or operator, the FAA ceases to make public the information about the private aircraft's flight, also excluding them from web trackers such as Flightradar24, which adhere to these policies.

[3]See for example http://goo.gl/VCGr4x.

Table 4: Time stability of the analyzed features over different days when collecting 100 messages.

Feature	Stability
Slot number	99.3%
Missing slots	100%
First slot	96.5%
Last slot	94.4%
Overall classification	99.8%

Naturally, the possibility of transponder fingerprinting has some implications on this type of flight privacy. While the ability to fingerprint specific aircraft or types of aircraft is not usually considered a problem for scheduled airliners, this could be different for private or business aircraft. The 1090ES version of the ADS-B protocol was developed to be open by design without concern for privacy mechanisms. It offers anyone with a receiver the opportunity to track the identity and movements of aircraft in range, regardless of their BARR status.

Because of these possibilities, there have been many concerns within the general aviation (GA) community. The UAT data link of ADS-B used by GA offers such a privacy mechanism. More concretely, an aircraft can generate a non-conflicting, random, temporary ID to avoid consistent tracking over time by third-party services. However, this generated ID can only be used under visual flight rules while not receiving ATC services, severely limiting its usefulness. Besides this, it has been shown that the DO-282B privacy solution has serious weaknesses, as the real ID of the aircraft and its random ID are correlated [15]. Yet, even when this could be fixed very easily, it would not close the fingerprinting-based privacy issue discussed in this work. While we did not explicitly analyze UAT in this work, we have no reason to believe that it exhibits no fingerprintable patterns

7.1.3 Business intelligence

The dataset can provide an interesting picture of the current ADS-B transponder market. As mentioned above, this data is not necessarily easily available and prove interesting for competitors or market researchers.[4] The data can for example easily be broken down into segments, showing the proliferation of certain transponder types or manufacturers in different countries or regions; alternatively, it would be possible to analyze trends over time.

7.1.4 Adherence to standards

The most straight-forward way to apply the presented fingerprinting analysis is to check transponder implementations for their adherence to the DO-260/A/B standards. As has been mentioned above, most of the implementations are more or less clearly outside the specified transmission intervals (with the exception of Type 1a) specified in the RTCA documents. While this might not be a major problem in the discussed cases, it gives rise to the question about other standard violations by current commercial ADS-B transponders, potentially in areas where the cause for concern is greater. The fact that slots or intervals are used in the first place is not specified in these standards (we can only speculate that there might be legacy reasons for this design choice); a truly random transmission periodicity would also have different implications for collision avoidance on the ADS-B channel.

[4]Although there are paid options offering some of this data, e.g. the Aviation Week Intelligence Network http://awin.aviationweek.com

Table 5: Manufacturers of the various transponder behavior classes.

Type	Manufacturers	Examples
Type 1a	Rockwell Collins	TPR 901
Type 1b	Honeywell	TRA-67A
Type 2	Honeywell	TRA-100
Type 3	Rockwell Collins, ACSS	GLU-920/925, XS-950
Type 4	Honeywell	Embraer SBAS, A380
Type 5	Garmin	G3000, G5000

7.2 Further Insights

While we conducted our experiments, we learned a number of things that might not be surprising to aviation industry insiders but shows the type of conclusions that can be inferred through scrutiny of the data using techniques described in Section 4:

- Newly developed aircraft (e.g. Airbus 380-800, Boeing 787-800) have the same transponders across airlines. This stems the fact that these aircraft types have ADS-B fitted in from their development stage and are delivered to all airlines with the same configuration in terms of air traffic communication hardware. This so-called supplier furnished equipment is delivered by Rockwell Collins in case of the 747-800 and the 787-800.

- In contrast to this, older aircraft types are retrofitted and their ADS-B transponders typically vary across airlines. For example, the Boeing 737, 767, 777 aircraft can be equipped with so-called buyer furnished equipment from Honeywell, ACSS or Rockwell Collins.

- In our dataset, with more than 99% likelihood a given airline fleet uses the same transponder (e.g., all 737-800 operated by Ryanair are the same). This seems in line with expectations and standard industry processes about purchase and retrofitting of transponders.

7.3 Mitigation

If the presented approach is to be considered a challenge to privacy, there is little in terms of quick solutions that could be done to mitigate this problem currently. Although the task is daunting, a strategy to solve the privacy challenges is possible and should be multi-pronged. Companies would need to provide software updates to all their transponders which would need to be applied by airlines and private pilots. To make such updates effective, however, the different supplies are required to agree on a common implementation of their ADS-B message system. Defining the standard DO-282B [14] more rigorously by the RTCA would help, although changing standards is generally a lengthy process in many technical areas. It is not clear if any single implementation of randomly chosen message intervals offers a better performance from a networking perspective in the given scenario, as the interval slots chosen by aircraft are

independent of each other. Yet, performance is something which should be thoroughly analyzed before making a decision as the 1090 MHz channel is notoriously overloaded with message loss rates of up to 90% in crowded airspaces [20].

8. FUTURE WORK

In future work, we plan to extend this fingerprinting approach in several ways and include it in a larger intrusion detection system. For an attack to be successful, the attacker must prove sufficient knowledge of both the ADS-B protocol and customs in air traffic control. This includes the use of matching values for fields in the different message types but also the transmission of all of the same message types the aircraft-specific transponder is broadcasting and doing so with the correct temporal spacing. Many currently used ADS-B transponders exhibit very different, often not standard-compliant, behavior on the application layer.[5] A system that tracks an aircraft's historical fingerprint can flag discontinuities when an attacker introduces forged messages without accurately copying the appropriate characteristics.

By using established methods from wireless fingerprinting in WiFi or sensor networks, it could be possible to fingerprint not only types of transponders based on their software implementations but exploit variations in the transponder hardware to gather even more distinguishing features. On the data link layer, clock skew fingerprinting could be a possible extension of this work as could be an analysis of possible physical layer features of the received message signals (we employed such PHY-layer features for an anomaly detection approach in [19]). If it is indeed possible to collect more fine-grained information from transponders, it could be feasible to fingerprint not only aircraft types or airline fleets but get to the level of individual aircraft. Naturally, this would have much stronger implications concerning both privacy and security applications discussed previously.

Furthermore, there are other air traffic communication protocols that might be vulnerable to similar fingerprinting approaches. Even though protocols such as Mode S do not use regular broadcast messages but are bursty and based on interrogation, one can imagine to find patterns of some sort in their specific implementations.

9. CONCLUSION

In this paper, we showed that it is possible to exploit implementation differences in aircraft ADS-B transponders for passive fingerprinting. Using simple means, we created a number of different features that enabled us to distinguish different transponder classes. Through mapping our classes with available open source databases, we can establish the aircraft types and airline fleets that use the same transponders. This enables us to get an overview of the currently installed transponder base. We suggested and discussed some applications for this method, covering intrusion detection, privacy implications, business intelligence, and checking the adherence to standards. We believe this work is a first step towards facilitating more research into the implications of fingerprinting aircraft transponders, which is particularly important considering the security and privacy problems of many wireless air traffic protocols.

[5]Honeywell offers an active tracker of standard conformance by observed ADS-B transponders under http://www.dissrr.com/1090GS/

10. REFERENCES

[1] Busyairah Syd Ali, Arnab Majumdar, Washington Y Ochieng, and Wolfgang Schuster. Ads-b: The case for london terminal manoeuvring area (ltma). In *Tenth USA\ Europe Air Traffic Management Research and De-velopment Seminar (ATM2013)*, 2013.

[2] Cherita L Corbett, Raheem A Beyah, and John A Copeland. Passive classification of wireless nics during active scanning. *International Journal of Information Security*, 7(5):335–348, 2008.

[3] Cherita L Corbett, Raheem A Beyah, and John A Copeland. Passive classification of wireless nics during rate switching. *EURASIP Journal on Wireless Communications and Networking*, 2008:28, 2008.

[4] Andrei Costin and Aurélien Francillon. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *Black Hat USA*, 2012.

[5] Jason Franklin, Damon Mccoy, Parisa Tabriz, and Vicentiu Neagoe. Passive data link layer 802.11 wireless device driver fingerprinting. In *In Proc. USENIX Security Symposium*, 2006.

[6] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis. Radio frequency fingerprinting for intrusion detection in wireless networks. *IEEE Transactions on Defendable and Secure Computing*, 2005.

[7] ICAO. Status of ADS-B Avionics Equipage Along ATS Routes L642/M771 For Harmonized ADS-B Implementation. In *ADS-B Seminar and 11th Meeting of ADS-B Study and Implementation Task Force*, Apr. 2012.

[8] Tadayoshi Kohno, Andre Broido, and Kimberly C Claffy. Remote physical device fingerprinting. *Dependable and Secure Computing, IEEE Transactions on*, 2(2):93–108, 2005.

[9] Hui Liu, Houshang Darabi, Pat Banerjee, and Jing Liu. Survey of wireless indoor positioning techniques and systems. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 37(6):1067–1080, 2007.

[10] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security*, pages 3–37. Springer, 2010.

[11] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 128—-139, 2008.

[12] Donald McCallie, Jonathan Butts, and Robert Mills. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*, 4(2):78–87, August 2011.

[13] RTCA Inc. Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B). DO-260B with Corrig. 1, 2011.

[14] RTCA Inc. Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast. DO-282B with Corrigendum 1, December 2011.

[15] Krishna Sampigethaya, S Taylor, and Radha Poovendran. Flight privacy in the nextgen: Challenges and opportunities. In *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013*, pages 1–15. IEEE, 2013.

[16] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Experimental analysis of attacks on next generation air traffic communication. In *Applied Cryptography and Network Security*, pages 253–271. Springer, 2013.

[17] Matthias Schäfer, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, and Matthias Wilhelm. Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research. In *ACM/IEEE International Conf. on Information Processing in Sensor Networks*, 2014.

[18] M. Strohmeier, V. Lenders, and I. Martinovic. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. *Communications Surveys & Tutorials, IEEE*, 17(2):1066–1087, 2015.

[19] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. Intrusion Detection for Airborne Communication using PHY-Layer Information. In *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*. Springer International Publishing, July 2015.

[20] Martin Strohmeier, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B. *Communications Magazine, IEEE*, 52(5), May 2014.

[21] Laurent Vidal. ADS-B Out and In - Airbus Status. ADS-B Taskforce - KOLKATA, Apr. 2013.

[22] Qian Wang, Hai Su, Kui Ren, and Kwangjo Kim. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *2011 Proceedings IEEE INFOCOM*, pages 1422–1430. IEEE, April 2011.

[23] Kai Zeng, Kannan Govindan, and Prasant Mohapatra. Non-Cryptographic Authentication and Identification in Wireless Networks. *IEEE Wireless Communications*, pages 1–8, 2010.

[24] Junxing Zhang, Sneha K. Kasera, and Neal Patwari. Mobility Assisted Secret Key Generation Using Wireless Link Signatures. In *2010 Proceedings IEEE INFOCOM*, pages 1–5. IEEE, March 2010.