BALANCING OPERATOR PRIVACY AND FUTURE AIRSPACE SURVEILLANCE

Krishna Sampigethaya*, Radha Poovendran, Capt. Stephen Taylor*****
***Information Science & Analytics Team, Boeing Research & Technology, Bellevue, WA**
****Network Security Lab, University of Washington, Seattle, WA**
*****Boeing Business Jets (BBJ), Seattle, WA**
{radhakrishna.sampigethaya, stephen.taylor2}@boeing.com; rp3@uw.edu

Abstract

Future general and business aviation aircraft are envisioned to depend on air-to-air and air-to-ground data communications for air traffic management. However, ease of access to wireless communications as well as the personal, political or proprietary nature of air travel raises privacy concerns for some aircraft users. A major concern is exploitation of aircraft's communications for deriving identity and position trajectories of that aircraft, resulting in potential privacy violations such as by helping to infer travel intent and profile places of interest. Privacy enhancement is however challenging to achieve due to a delicate balance with airspace security. This paper identifies location privacy threats and proposes anonymity solutions that can enhance privacy level of aircraft operators and passengers without compromising airspace security.

1 Introduction

Current air traffic management (ATM) systems are at their life's end, with infrastructures not having growth capacity to meet the projected traffic demand. New innovations including Automatic Dependent Surveillance Broadcast (ADS-B) and Aeronautical Telecommunications Network (ATN) are modernizing ATM, allowing civil aircraft to engage in distributed air traffic control and share data with ground systems as well as with each other [1,2].

Using ADS-B an aircraft can periodically broadcast a traffic beacon containing its identifier, 3-D position, velocity, intent and other spatial data [1]. All one-hop neighbors with ADS-B transponders can use these broadcasts to accurately locate and monitor the aircraft. The resulting high accuracy and performance of air traffic surveillance enhances situation awareness and safety of mobile aircraft in airspace. ADS-B is a key enabler for making each aircraft independently maneuver and choose flight paths, i.e., the Free Flight concept [3].

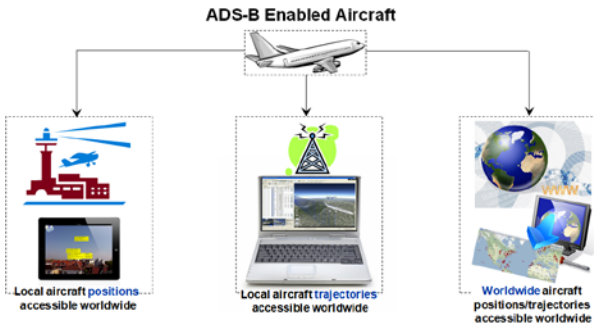

Figure 1. ADS-B based aircraft tracking tools.

Another latest advance in ATM is the consideration of an airborne IP-based ATN as a globally feasible technology for enabling beneficial transition from voice to data-based air traffic services and aeronautical operational control [2]. This paradigm shift promises to enable decentralization of air traffic management, reducing cognitive load on the ground control and aircraft human operators. Today, airborne IP networking capability is tested in some commercial aircraft for providing Internet access to onboard passengers [4].

This paper identifies that ADS-B has potential privacy concerns for general and business aviation aircraft. ADS-B data

communications can make aircraft become identifiable, locatable and traceable nodes on a geographic map and potentially on the Internet (see Fig. 1). The paper's finding is further substantiated by recent privacy concerns raised against ADS-B equipage by general aviation aircraft operators [8].

Privacy issues must be resolved to create public trust in future air transport and accelerate beneficial deployment of ADS-B, a major challenge in the modernization of ATM. The paper streamlines this effort by identifying, evaluating, and mitigating potential privacy threats related to ADS-B enabled general and business aviation aircraft applications in a future airspace.

1.1 Problem Statement

This paper studies the problem of making a mobile aircraft capable of protecting privacy of its operator and/or passengers. The focus is on *ATM broadcasts from aircraft*, i.e., ADS-B data and IP ATN communications, which can be potentially misused to invade *location privacy*, i.e., the ability to prevent other parties from learning one's current and past location [9]. Location privacy can be preserved by making communications to be *anonymous*, i.e., not traceable from a receiver to the sender [10]. A major challenge with adopting this solution approach in future ATM, however, is maintaining integrity and timely availability of aircraft data for air traffic surveillance and airspace security.

The paper considers location privacy to be a concern only for business jets, chartered or personally owned aircraft. These aircraft are hereon referred as **private aircraft**. *Commercial airliners are not expected to be vulnerable to location privacy threats*, since they are operated on published routes and regulated to use permanent identifiers which can allow easy aircraft identification. Furthermore, application layer specific privacy issues in airborne IP network, such as potential exploitation of ATN data, ACARS messages, or onboard Internet user data, are beyond the scope of this investigation which focuses on IP network and physical layers.

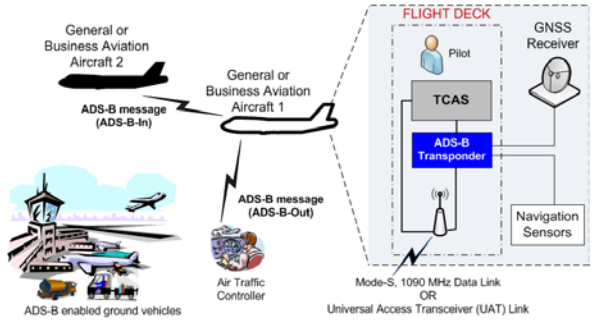

Figure 2. System model considered.

1.2 Contributions of this Paper

- Identifies general and business aviation aircraft privacy requirements and challenges in future ATM.
- Proposes privacy enhancing technologies to provide identity and location anonymity for general and business aviation aircraft broadcasts.
- Presents a preliminary assessment of the level of location privacy achievable in airspace.

1.3 Paper Outline

The next section describes the system model considered, and the section following the next presents the location privacy threats. The subsequent four sections present the proposed security requirements, privacy solutions, and performance evaluation approach. The last three sections offer open problems, related work and conclusions.

2 System Model Considered

Figure 2 illustrates the system model consisting of aircraft and ground-based ADS-B stations. Each aircraft is equipped with advanced positioning units, e.g., GPS, to compute accurate spatial information, i.e., position, time, velocity, heading, etc., ADS-B transponder to broadcast traffic beacons. Additionally, future aircraft may participate in airborne IP network systems for ATN and Internet applications (not shown in the figure). Aircraft move in airspace, sharing information as well as communicating with air traffic control

centers and third-party service providers connected to the ADS-B stations and Internet access points, respectively. Furthermore, unauthorized receivers may passively listen to transmissions in the airspace (again not shown in the figure).

2.1 Applications Considered

In ADS-B, each aircraft periodically broadcasts traffic beacons, once or twice per second, using the ADS-B Out capability. Ground controllers and aircraft one communication hop away use the ADS-B In capability for ground surveillance and airborne navigation/surveillance, respectively. ADS-B datalink standards include 1090 MHz Extended Squitters and Universal Access Transceiver, both with a transmission range of 100 miles or more [11].

Furthermore, airborne IP networking enables multi-hop communications and end-to-end applications between aircraft and between aircraft and ground systems of air traffic control centers, airline operation centers, or Internet service providers. The growing number of airborne IP network applications includes ATN services, i.e., safety-critical air traffic services and business-critical aeronautical operational control, and non-critical passenger services such as Internet. A potential IP wireless datalink is the L-band Digital Aeronautical Communication System with a typical range of 135 miles or more [2].

2.2 System Assumptions

Each aircraft possesses a globally coordinated permanent unique digital identifier, such as the 24-bit International Civil Aviation Organization (ICAO) address, tail number or flight number [11]. For security and liability in controlled airspaces, this permanent identifier is assumed in all traffic communications from aircraft. However, in an uncontrolled airspace, it is assumed that each private aircraft can use a temporary identifier in communications, and move freely in Visual Flight Rules (VFR) or Instrument Flight Rules (IFR) modes [12]. For example, in class G airspace at altitudes less than 14,500 feet above the continent with a typical maximum allowable speed of 460 km/hr, and class A airspace greater than 18,000 feet over the ocean with a typical average en route speed of 900 km/hr. The use of ADS-B broadcasts and ATN communications in uncontrolled airspaces is assumed to be for situational awareness enhancement and not for safety-critical applications, e.g., separation assurance.

Further, each aircraft logical network domain is assumed to employ a different IP identifier for applications. Furthermore, it is assumed that all aircraft participate in ADS-B application, i.e., at least use the ADS-B Out capability, as well as the IP ATN applications, but optionally use Internet access.

2.3 Adversary Model

This paper considers an adversary to be an entity external to the system. The adversary is capable of passive eavesdropping and recording all broadcasts from a target aircraft in the system, i.e., ADS-B data and IP radio broadcasts of the target, in a region of interest or from departure to destination point. The adversarial objective is to misuse the overheard broadcasts and derive information for personal, political or business advantage. Since the major focus of this paper is privacy threats from unauthorized access and misuse of ATM broadcasts, active adversarial threats are not considered such as spoofing false target aircraft or corruption of traffic data. Furthermore, communication jamming threats are not considered to threaten privacy.

3 Location Privacy Threat to ADS-B Users

Based on adversarial attack and the vulnerable aircraft communications, location privacy threats are classified as follows.

3.1 Unauthorized Tracking of ADS-B

In ADS-B, periodic (once or twice per second) traffic beacons from an equipped private aircraft will contain an authentic digital

identity as well as a highly accurate position and spatial information, e.g., velocity, intent, etc. of that aircraft. Therefore these broadcasts can serve to perform traffic control tasks while ensuring liability in the shared networked airspace. However, the periodic beacons containing position and identity may be recorded and used by the adversary, up to 100 miles or more from source of ADS-B broadcasts, to obtain unique identifiers of communicating aircraft as well as record position trajectories of these uniquely identifiable aircraft.

3.2 Impact of Tracking on Location Privacy

Private aircraft are often used or owned by entities to visit places of political, business or personal interest, hence unauthorized location tracking can invade aircraft user's or owner's privacy in unanticipated ways. Location trajectories of a private aircraft, when correlated with other information databases such as geographic maps and business/political developments, can help in the identification of places visited by the aircraft as well as inference of travel intent of the user. Furthermore, location history of an aircraft over time can lead to profiling of the user's personal preferences and interests.

The privacy of general and business aviation aircraft operators is usually protected using a process driven by the aviation regulators. For example, a private aircraft operator may request the aviation administration that flight tracking data of the private aircraft (e.g., radar tracking data of the aircraft) be not disclosed to third-parties. However, ADS-B tracking by third parties cannot be prevented by this process since anyone can passively track ADS-B transmissions of aircraft (see Figure 3).

4 Proposed Privacy Related Requirements

Privacy-enhancing technologies which provide confidentiality, such as cryptographic encryption, can mitigate privacy risks by controlling access to sensitive or personal data in the IP ATN and Internet communications.

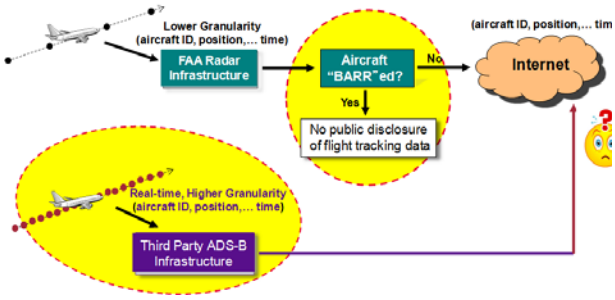

Figure 3. Illustration of a privacy protection process for general and business aviation, and its potential relevance to ADS-B.

However, these solutions are not useful for ADS-B traffic beacons and IP network physical layer transmissions, since these (inherently broadcast) communications must remain openly accessible. Therefore, different security properties are required for location privacy enhancement of these ATM broadcast communications from aircraft.

- *Communication Anonymity*. Broadcasts from an aircraft must not be linkable to the aircraft's digital identifier by unauthorized entities.
- *Location Untraceability*. Two consecutive broadcasts from an aircraft cannot be linked together by unauthorized entities.
- Airspace security. The integrity and timely availability of ATM broadcasts from aircraft must be guaranteed.
- *Liability*. ATM broadcasts from an aircraft must be irrevocably linkable to that aircraft by authorized entities.

5 Using Pseudonym as Aircraft Identifier

In order to protect the privacy of aircraft operators a solution approach is to assign each aircraft with two types of digital identifiers: (*i*) A long-term identifier as the real aircraft identity which can be used for unique identification of the aircraft at ground controllers, similar to an Electronic License Plate for future networked automobiles. (*ii*) A set of short-term identifiers, such as pseudonyms. A pseudonym will be unique to an aircraft, but it does not reveal the real identity of the vehicle except to a trusted authorized entity

such as the air traffic control center. Hence, use of a pseudonym in aircraft broadcasts provides communication anonymity while satisfying airspace security and liability, since only the trusted authority can derive the aircraft's real identity from the aircraft's observed broadcasts. Overall, this solution makes the mobile aircraft a traceable node for ADS-B transponders in the airspace, while preventing any identification from access to aircraft's ICAO address.

For designing a fully decentralized solution, i.e., with no trusted authority requirement, an aircraft's pseudonym can be a self-chosen temporary identifier known to only the aircraft. Such a solution however presents several challenges, since additional mechanisms are required for ensuring airspace security and liability. For example, the need to verify integrity of received ADS-B broadcasts (e.g., use of multilateration of traffic beacons received on the ground [14]) and the ability to verify real-identity of aircraft in the event of an emergency or accident (e.g., authorized access to aircraft transponders). This problem will hence be considered in a future work.

5.1 Applicability to ADS-B

For ADS-B, the default identifier is assumed to be the permanent 24-bit ICAO address. An aircraft in an uncontrolled airspace, operating under VFR or IFR and not accessing any air traffic service, can use a pseudonym as identifier. This is evident from the "privacy mode" option available for the ADS-B Universal Access Transceiver datalink which can allow aircraft to operate anonymously when operating under VFR mode in airspace [11,18].

To generate a 24-bit pseudonym for aircraft, one approach is to make the airplane compute a random identifier as a pseudonym. A practical solution is outlined in RTCA DO-282A standard [11], using which the aircraft computes the pseudonym as a function of a random quantity, e.g., the location and/or time of use of pseudonym, and the ICAO identifier. Because air traffic controllers know the ICAO address of the aircraft as well as can record and verify ADS-B broadcasts from the aircraft, they can maintain liability in airspace when emergency events or accidents occur. Another promising approach is to allow aircraft to share an encryption key with air traffic control center [15], and using this key to secretly communicate the random quantity used in the pseudonym generation.

5.2 Vulnerability: Predictable Mobility

The use of pseudonyms cannot provide location untraceability if there is spatial and temporal correlation between aircraft locations. For instance, the attacker may overhear a target's ADS-B broadcast containing the ICAO address at a prior time during flight when the aircraft used air traffic service. At a subsequent time instance when the aircraft stops use of air traffic service and places a pseudonym in its ADS-B broadcast, the adversary may link the pseudonym and ICAO address based on temporal/spatial correlation between consecutive locations of aircraft. Hence, an attacker can link an aircraft's pseudonym to the aircraft. Further, even if the aircraft began its flight with a pseudonym and never used air traffic services, the attacker may correlate the pseudonym with the aircraft by physically identifying the aircraft during flight, e.g., when the aircraft traverses a visually monitored airspace. Furthermore, if the pseudonym is generated with location and/or time of first use as the randomizer, location traceability can allow adversary to compute and correlate pseudonym to the aircraft.

A solution approach is to update the pseudonym between two broadcasts [9]. Such an approach however is still weak in the presence of the underlying predictable mobility of nodes and short inter-message periods [16]. The adversary can potentially link the new and old pseudonym using the spatial and/or temporal correlation between consecutive locations of aircraft observed at the short inter-message period, e.g., 500 milliseconds to 1 second for ADS-B broadcasts.

Therefore, the next section proposes distributed solutions that can potentially allow a target aircraft to enhance its location privacy level at each pseudonym update by involving neighbor aircraft.

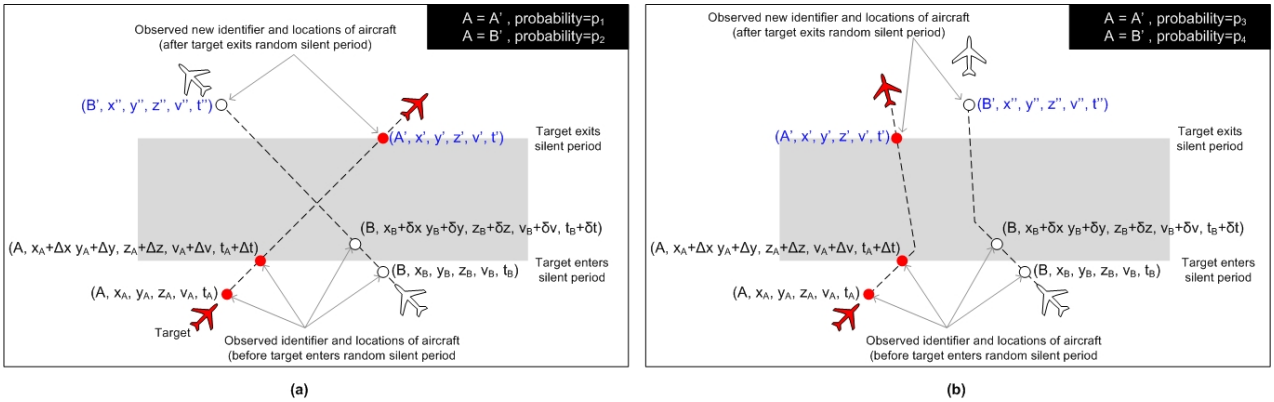

Figure 4. Illustration of random silent period solution for privacy enhancement of a target.

5 Mitigating Aircraft Location Tracking

An aircraft's 3-D position at any given time depends on factors such as the atmospheric conditions, the flight levels of other aircraft in the area, flight distance, the stage of the flight the aircraft is in (ascent, cruise, or descent) and the aircraft's optimal flight level. The paper proposes privacy to be an additional factor in choosing aircraft position. Based on privacy level desired by a target aircraft user in a particular region (in uncontrolled airspace) during a specific period, and other factors listed above, the target is free to choose a 3-D position trajectory. The target can use one of the proposed solutions described below to mitigate unauthorized determination of the trajectory.

The basic idea of our proposed solutions is to increase the uncertainty for the adversary attempting to link a pseudonym with a permanent aircraft identifier by introducing in the pseudonym update (*i*) spatial uncertainty or (*ii*) both spatial and temporal uncertainty.

5.1 MIX-Airspaces

Based on the concept in [9], this paper proposes a solution called MIX-airspace. Certain bounded regions in an uncontrolled airspace can be designated as MIX-airspaces, where aircraft do not transmit but update their identifier. As a result, for a target aircraft navigating through a MIX-airspace, the entry point may not be linkable to the exit point provided there are two or more aircraft simultaneously in the same airspace.

However, this solution has some major challenges. First, the solution may not work well when there is a strong temporal and spatial correlation between aircraft locations, since each aircraft would exit the bounded region at a predictable time and 3-D exit point. Moreover, assigning an adequate number of MIX-airspaces in a class G or class A airspace to assure a location privacy level to aircraft operators is a challenging problem which must be considered separately.

5.2 Random Silent Period

A promising solution for mitigating location tracking is to use a random silent period in the pseudonym updates [13], [16]. Figure 4 illustrates the approach based on the proposed random silent period solution (for the sake of clarity, rectangular regions are used). As seen, a target aircraft broadcasts with a pseudonym A in the presence of neighboring aircraft broadcasting with a pseudonym B. The target then updates pseudonym and does not transmit for a random duration, followed by broadcasts with a new pseudonym A'. Since the aircraft with pseudonym B is near the target and updates to B' with the target, the adversary can probably mistake B' instead of A' as the target's updated pseudonym. Therefore, overlapping random silent periods between a target and neighbors can mitigate tracking of target.

However, as discussed later, random silent period solution enlarges the ADS-B broadcast period, i.e., reduces the timely availability of aircraft traffic beacons, which in turn potentially

degrades airspace security. The next solution addresses this tradeoff.

5.3 Privacy Enhancing Groups

In order to achieve a random time period for pseudonym update without trading airspace security, one approach is to leverage group navigation property of aircraft. Geographically proximate aircraft with same average velocity and similar direction can navigate as a fully-connected group over a period of time. The group of aircraft can continue to broadcast traffic beacons with pseudonyms, while coordinating to be represented by a common valid group identifier for most purposes as well as establishing secrets on-the-fly for group-based operations. Each aircraft reduces its transmission range to reach only the group members (such as 3 – 5 nm). Each group has a leader with a large transmission range that is sufficient to reach airborne and ground transponders (such as 100 nm). A candidate for the group leader is a commercial airliner that does not require location privacy.

In such a solution, the adversary can at best know only the group's identifier and the group leader's location [16]. Given that the group identifier is only traceable to a navigating group of aircraft and that members can self update their pseudonyms while participating in the group, each member can potentially achieve an extended random time period for pseudonym update. This random period is equal to the time duration for which the member remains in the group. The ground controllers can still identify and accurately trace valid nodes in the sky, while unauthorized eavesdroppers can at best randomly guess the trajectories of the airborne nodes.

5.4 Applicability of Random Silent Period

Since the random silent period solution enlarges the ADS-B broadcast period, the resulting location privacy level is potentially obtained at the cost of surveillance accuracy because of the reduced availability of traffic beacons.

However, currently none of the proposed solutions apply to aircraft navigating in a controlled airspace where update of ADS-B identifier is not allowed because of regulatory constraints. Nevertheless, there may be some scenarios in controlled airspaces where private aircraft can perform identifier updates without compromising airspace security and liability. This problem will be investigated in a future work.

6 Location Privacy Evaluation

This section presents an approach to measure the level of location privacy offered to a target aircraft by location tracking mitigation solutions.

6.1 Privacy Metrics

The level of location privacy provided to a target aircraft by each identifier update can be measured using an *anonymity set* that includes the target and other nodes with identifiers indistinguishable from that of the target [10]. Assuming that all nodes in the anonymity set are equally likely to be the target, the level of location privacy is equal to the size of the anonymity set. This paper uses *entropy*, a well-known metric for measuring uncertainty, to quantify the location privacy level of the anonymity set.

Let the target anonymity set be denoted by S, and the size of anonymity set be denoted as $|S|$. Let the probability that an element i of S is the target T be $p_i=\Pr(T=i)$, $\forall i \in S$ with $\sum_{i=1}^{|S|} p_i = 1$. Then, the entropy of S is given as:

$$H(p) = -\sum_{i=1}^{|S|} p_i \log_2 p_i$$

6.2 Location Tracking Method Considered

Figure 5 shows a target that is being tracked and is updating its identifier at location l_0 and time t_0. The target anonymity set S is computed as follows. The *reachable area* of the target is defined to be the bounded region where the target is expected to reappear after the identifier update. For example, in Figure 5, if the target enters a random silent period during the update, the reachable area is then determined by the allowable movement directions, the horizontal and vertical minimum separation, about the anonymity set, each element of the anonymity set is equally likely to be the potential candidate for the target. The adversary can hence randomly choose an element as the target.

6.3 Privacy from Random Silent Period

The location privacy provided by the proposed random silent period solution, under the location tracking method described above,

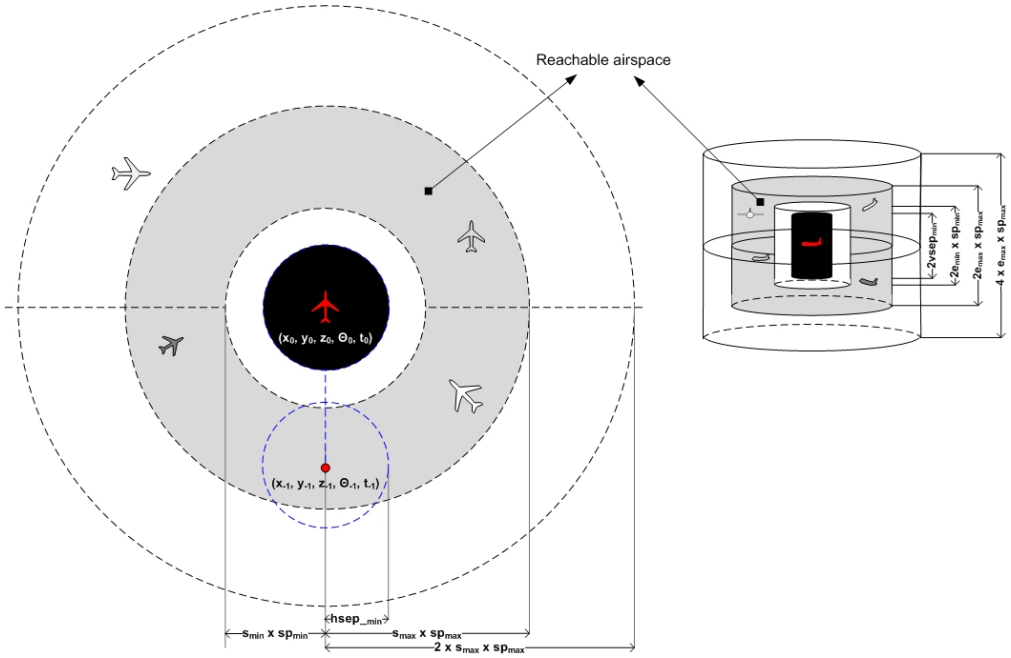

Figure 5. Illustration of airspace used to derive a target aircraft's (red) anonymity set.

$hsep_{min}$, $vsep_{min}$, respectively, the known achievable speed range [s_{min}, s_{max}], elevation range [e_{min}, e_{max}], and the update period which is between a minimum and maximum silent period [sp_{min}, sp_{max},]; the reachable area in Figure 5 is for random node mobility in horizontal as well as vertical directions. The target anonymity set includes nodes that update their identifiers with the target and appear in the reachable area of the target. As shown in Figure 3 if all nodes update their identifiers with the target and appear in the reachable area after a random silent period, S will contain all the five nodes, including the target itself.

Upon computing the target's anonymity set, for tracking a target aircraft the adversary must choose a potential candidate from the anonymity set to be the target. Assuming that the adversary has no additional knowledge can be upper bounded for a given node density in airspace. From Figure 5 it is seen that the target anonymity set can at most include all the nodes that are within the cylindrical region from the location where the target enters a random silent period. For simplification of analysis, this paper considers only the horizontal area (on the left of Figure 5). Assuming that nodes are uniformly distributed in airspace with a density ρ, number of nodes in this area distributes as a spatial Poisson process and bounds for the average (expected value) anonymity set size at each update is [16]:

$$1 \le E\{|S|\} \le \frac{\rho\pi R}{1-e^{-\rho\pi R}},\ R = (2s_{\max} sp_{\max})^2 - hsep_{\min}^2$$

.

Hence, the bounds for entropy are:

$$0 \le H(p) \le \log_2\left(\frac{\rho\pi R}{1-e^{-\rho\pi R}}\right).$$

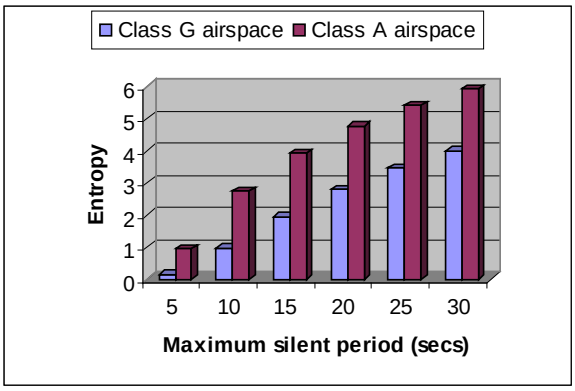

Figure 6. Theoretical estimates of max. location privacy for target (node density = 30 per 10^4 nm).

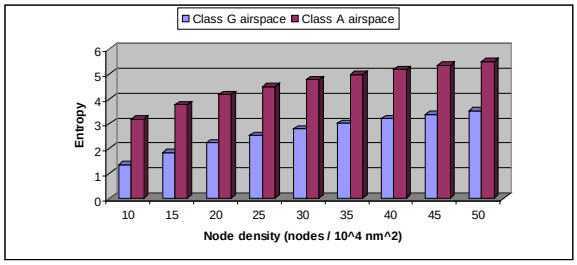

Figure 7. Theoretical estimates of max. location privacy for target (sp_{max} = 20 secs).

Using the derived upper bound, the theoretical maximum for the location privacy level achievable at each pseudonym update by the target can be determined. Figure 6 and Figure 7 show the theoretical maximum location privacy level for different random silent period values and different airspace densities, respectively. The entropy increases with increase in silent period duration as well as node density. For a given node density, class A airspace offers a higher entropy because of the higher speeds achievable by aircraft (i.e., average of 900 km/hr), when compared to class G airspace (maximum speed of 460 km/hr).

7 Discussion and Open Problems

7.1 Maximizing Privacy Level per Update

Not all neighbors of the target aircraft may update their pseudonym and contribute to target anonymity set. Hence, target's location privacy level is not maximized for a given node density in airspace, i.e., achievable privacy is less than in Figure 6 and Figure 7. In [17], a scheme called Swap is proposed for a target to maximize achievable location privacy level at each pseudonym update. The idea is to enable the target and a neighboring aircraft to engage in a protocol for exchange of pseudonyms before entering a random silent period. The adversary can make only a random guess of the neighbor involved in pseudonym exchange and if an exchange occurred. This allows nodes which did not update their identifier to be in the anonymity set, hence potentially maximizing location privacy. Applicability of this solution to ATM remains to be investigated.

7.2 Advanced Location Tracking Methods

A sophisticated adversary can employ advanced computation algorithms to track an aircraft. One example is *correlation tracking* which leverages predictable mobility of nodes [13], [16], [17]. Assuming mobility parameters of the target aircraft remain unchanged during the random silent period the adversary can estimate a location trajectory for the target, thereby assigning non-uniform probabilities for the target anonymity set to reduce uncertainty. The performance of the proposed solutions under correlation tracking is an open problem that must be investigated in the future.

7.3 Adequate Levels of Location Privacy

The future airspace will have different stakeholders with ephemeral relationships, with different levels of desired privacy. An open problem is to determine the minimum and maximum levels of privacy and the different contexts under which privacy becomes important for each stakeholder.

8 Conclusions and Future Work

This paper address privacy needs of ADS-B enabled general and business aviation aircraft in the next-generation air transportation. The

paper proposes solutions for ADS-B anonymity, hence increase the level of privacy for the aircraft operator and/or passengers. The proposed privacy enhancement technologies are applicable to mitigate location tracking of a target aircraft's ADS-B message broadcasts containing aircraft identifier and accurate positions. Preliminary analysis shows that with the increased air traffic density projected for future airspaces, the proposed solutions can potentially perform well.

Future work includes a detailed evaluation of the proposed solutions, using (*i*) advanced location tracking methods, and (*ii*) air traffic data for continental class G and oceanic class A airspaces where Free Flight is possible. Furthermore, opportune flight scenarios (e.g., aircraft maneuvers and flight phases) that can guarantee high levels of privacy while not violating aircraft safety margins and airspace security remain to be identified for other airspace classes. Incentive schemes to enable active participation, i.e., update of aircraft identifier and movement, of non-cooperative aircraft in the anonymity set must also be investigated.

References

[1] RTCA DO-242A, (2002), Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B).

[2] Bauer, C., Ayaz, S., 2008, A thorough investigation of mobile IPv6 for the aeronautical environment, IEEE Vehicular Technology Conference-Fall, Calgary, BC, pp. 1-5.

[3] RTCA, (1995), Final Report of RTCA Task Force 3 Free Flight Implementation.

[4] Bhadouria, A., (2007), Airborne Internet : market & opportunity, MIT Thesis. http://dspace.mit.edu/handle/1721.1/42349

[5] Poovendran, R. et al.., (2009), A community report of the 2008 high confidence transportation cyber-physical systems workshop, http://www.ee.washington.edu/research/nsl/aar-cps

[6] Scovel, C., (2009), Federal Aviation Administration: Actions Needed To Achieve Mid-Term NextGen Goals, http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/WEB_FILE_NextGen_Statement.pdf

[7] ICAO ACP, (2009), Manual for the ATN using IPS Standards and Protocols (Doc 9896), http://www.icao.int/anb/Panels/ACP/

[8] AOPA, Re: Docket Number FAA-2007-29305 Notice of Proposed Rulemaking; Automatic Dependent Surveillance -Broadcast (ADS-B) Out Performance Requirements to support air traffic control (ATC) service, http://www.aopa.org/advocacy/articles/2008/080304ads-b-comments.pdf

[9] Beresford, A.R., Stajano, F., 2003, Location privacy in pervasive computing, IEEE Pervasive Computing, vol.2, no.1, pp. 46-55.

[10] Chaum, D. L., (1981), Untraceable electronic mail, return addresses, and digital pseudonyms, Communications of the ACM 24:2, pp. 84-90.

[11] RTCA DO-282A, (2004), Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast (ADS-B), Vol. 1.

[12] FAA, (2008), Pilot's handbook of aeronautical knowledge, Chapter 14, http://www.faa.gov/Library/manuals/aviation/pilot_handbook/

[13] Huang, L., Matsuura, K.; Yamane, H.; Sezaki, K., (2005), Enhancing wireless location privacy using silent period," IEEE Wireless Communications and Networking Conference, pp. 1187-1192.

[14] Krozel, J. and Andrisani, I., (2005), Independent ADS-B Verification and Validation," AIAA Aviation, Technology, Integration, and Operations Conference (ATIO), pp. 1–11.

[15] Valovage, E., (2007), Enhanced ADS-B Research, IEEE Aerospace and Electronic Systems Magazine, vol.22, no.5, pp.35-38.

[16] Sampigethaya, K.; Li, M; Huang, L; Poovendran, R., (2007), AMOEBA: Robust Location Privacy Scheme for VANET, IEEE Journal on Selected Areas in Communications, vol.25, no.8, pp.1569-1589.

[17] Li, M., Sampigethaya, K., Huang, L., and Poovendran, R., (2006), Swing & swap: user-centric approaches towards maximizing location privacy. In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society (WPES '06), pp. 19-28.

[18] Capezzuto, V., ADS-B Status Briefing: ASAS TN2.5, http://www.asas-tn.org/towards-asas-gn/session-1/6_ADS_B_vinny.ppt

Copyright Statement