Location Privacy of ADS-B for General Aviation

Honggu Lin[a], Haomiao Yang[b]
School of Computer Science & Engineering
University of Electronic Science and Technology of China
Chengdu, China
ahonggulin@hotmail.com, bhaomyang@uestc.edu.cn

Jing Zeng
The Second Research Institute
Civil Aviation Administration of China
Chengdu, China
zcaac@yahoo.com.cn

Abstract—Automatic Dependent Surveillance Broadcast (ADS-B) is a satellite-based system that makes an aircraft equipped with it periodically generates ADS-B broadcasts including the aircraft's identifier, position, velocity, etc. Since the broadcasts can enhance navigation capability remarkably, it has replaced radar and becomes the backbone of the air traffic management (ATM) of next generation. However, the leak of identity and location privacy allows adversaries to track flights easily. Especially in general aviation, people's travel destination may be related to personal privacy, commercial secrets and other important information that need to be protected. In this paper, the author studies a well-known location privacy protection scheme named random silent period which enhances the uncertainty by mix the target plane with other planes in the anonymity set and entropy is used to evaluate the uncertainty. Furthermore, we proposes a new correlation tracking method to improve the uncertainty. The evaluation of location privacy demonstrates that the method is more practical and accurate than the simple tracking method.

Keywords— ADS-B; location privacy; random silent period; entropy; tracking

I. INTRODUCTION

All aircraft, including commercial, business, general, and military aviation, must possess necessary communications and networking infrastructures [1]. Air Traffic Management (ATM) systems worldwide are refreshing their decades-old ground and space infrastructures to ADS-B which will allow each aircraft to engage in distributed air traffic control concepts/procedures and share data with ground systems as well as with each other [2,3].General aviation covers a wide range of aircraft, from personally-owned aircraft to law enforcement and emergency services aircraft to business jets [1]. Note that this paper considers privacy to be a concern only for general aviation aircraft users. Commercial airliners and cargo aircraft are not expected to be vulnerable to location privacy threats, since they are operated on published routes and regulated to use permanent identifiers for easy aircraft identification.

ADS-B system is a crucial component of the federal aviation administration (FAA)'s next generation upgrade, and it provides a safer and more efficient way for the aviation management than the ground radar system [3, 4, 5]. This is because ADS-B system is on the aircraft and it broadcasts aircraft position and other data updated every second to nearby ground stations, aircraft and surface vehicles, while the ground radar system is on the ground dependent on human participation and positions are updated every twelve seconds [6, 7, 8, 9].

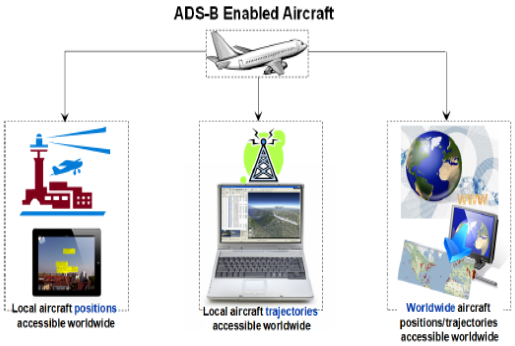

Figure 1. ADS-B Based Aircraft Tracking Tools [1]

Although ADS-B have so many advantages such as convenience and efficiency, it also suffers from the location privacy problems that may be concerned with people's travel destination, commercial secretes, etc. For example, the application named "Plane Finder AR" allows precise tracking of air crafts using ADS-B transmissions. Therefore, it is necessary to find a way out to protect the our location privacy. In 2012, Krishna ET al. [1] proposed first a location privacy protection scheme of the general aviation named random silent period which introduces the spatial and temporal uncertainty through updating the identifiers of air crafts but no transmitting them in a small period of time named maximum silent period so as to confuse the target aircraft with other air crafts. In other words, the random silent period enhances the identity uncertainty of air crafts by mixing the target plane with other planes in the anonymity. Furthermore, the scheme achieves the location privacy by using the simple tracking method where the adversary assumes that each element of the anonymity set is equally likely to be the potential candidate for the target.

However, the simple tracking method can be only applied in a very ideal environment. In practice, an

adversary can employ some advanced computation algorithms to track a target aircraft. For example, the adversary can predict a trajectory for the target in advance, and thus estimate different probabilities for the air crafts in the anonymity set to reduce the uncertainty.

. In this paper, the author proposes a new correlation tracking method in which the adversary can assign a non-uniform probability distribution to the target anonymity set. As a result, the method is more practical and accurate than the simple tracking method.

II. ORGANIZATION OF THE PAPER

The next section describes the system model considered which is same as the model used in [1]. We demonstrate our proposed scheme in section four. In this section, we illustrate the simple tracking method and proposed a new tracking method named correlation tracking. Section five is the location privacy evaluation of the two tracking methods. We use entropy to evaluate the uncertainty and compare changes in the results of different variables in these two tracking methods. The last section offer open problems and conclusions.

III. SYSTEM MODEL CONSIDERED

The system model used in this paper the same as the model proposed by Krishna et al. [1] in 2012.

Figure 2 illustrates the system model consisting of aircraft and ground-based ADS-B stations. Each aircraft in the model first determines its position via GPS ,to generate accurate spatial information, i.e., position, time, velocity, heading, etc. then use ADS-B transponder on the aircraft to broadcast traffic beacons. ADS-B ground stations within range receive the broadcast and relay the information via a networked backbone to air traffic control. Properly equipped aircraft within range also receive the broadcast.

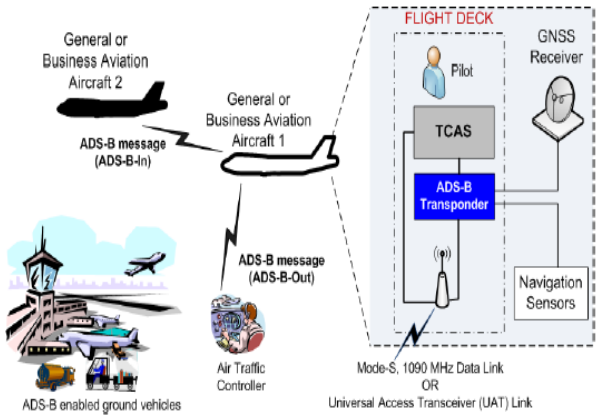

Figure 2. System Model Considered [1]

IV. PROPOSED SCHEME

A. Privacy Metric: Anonymity Set and Entropy

To measure the uncertainty, we use entropy 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, $\forall i \in S$ with $\sum_{i=1}^{|S|} P_i = 1$. Then, the entropy of S is given as:

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

The reachable area of the target is defined to be the bounded region where the target is expected to reappear after the update of the identifier [1]. For example, in Fig .1, if the target updates its identifier during the random silent period, there are several factors that are related to the determination of the reachable area, including the allowable movement directions, the horizontal and vertical minimum separation, $hsep_{min}$, $vsep_{min}$, respectively, the known achievable speed range $[S_{min}, S_{max}]$, and the update period which is between a minimum and maximum silent period $[SP_{min}, SP_{max}]$.

The target anonymity set contains nodes that update their identifiers with the target and appear in the reachable area of the target [10]. We assume that all nodes update their identifiers with the target after a random silent period, and thus S will contain all the nodes in the reachable area, including the target itself.

B. Simple Tracking

In this method, the adversary assumes that each element of the anonymity set is equally likely to be the potential candidate for the target, and hence, randomly chooses an element as the target [11]. So, we have

$$P_i = \frac{1}{E\{|S|\}} \qquad (2)$$

$$\sum_{i=1}^{|S|} P_i = 1 \qquad (3)$$

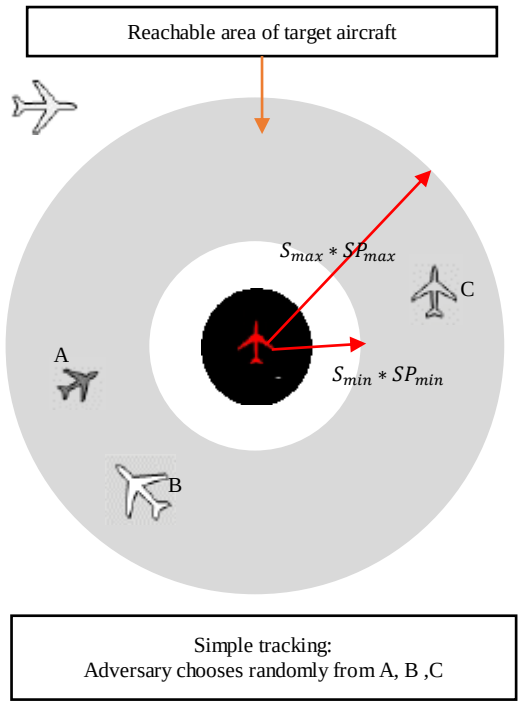

Figure 3. Simple Tracking

For simplification of analysis, this paper only considers the horizontal area. From Fig. 3 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. 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 [11].

$$1 \leq \mathrm{E}\{|S|\} \leq \frac{\rho A_r}{1-e^{-\rho A_r}} \tag{4}$$

$$A_r = \pi(2S_{max}SP_{max})^2 - hsep_{min}{}^2 \tag{5}$$

Using the derived upper bound, the theoretical maximum for the location privacy level achievable at each pseudonym update by the target can be determined.

Hence, the entropy of simple tracking is:

$$\begin{aligned} \mathrm{H}(p) &= -\sum_{i=1}^{|S|} P_i log_2 P_i \\ &= -\sum_{i=1}^{|S|} \frac{1}{\mathrm{E}\{|S_{A_r}|\}} log_2 \frac{1}{\mathrm{E}\{|S_{A_r}|\}} \\ &= log_2 \mathrm{E}\{|S_{A_r}|\} \end{aligned} \tag{6}$$

The expected size of the anonymity set of a target is:

$$\begin{aligned} \mathrm{E}\{|S_{A_p}|\} &= \mathrm{E}\{\upsilon(A_r)|\upsilon(A_r) \geq 1\} \\ &= \frac{E\{\nu(A_r)\}}{1-\Pr\{\nu(A_r)=0\}} \\ &= \frac{\rho A_r}{1-e^{-\rho A_r}} \end{aligned} \tag{7}$$

C. *Correlation Tracking*

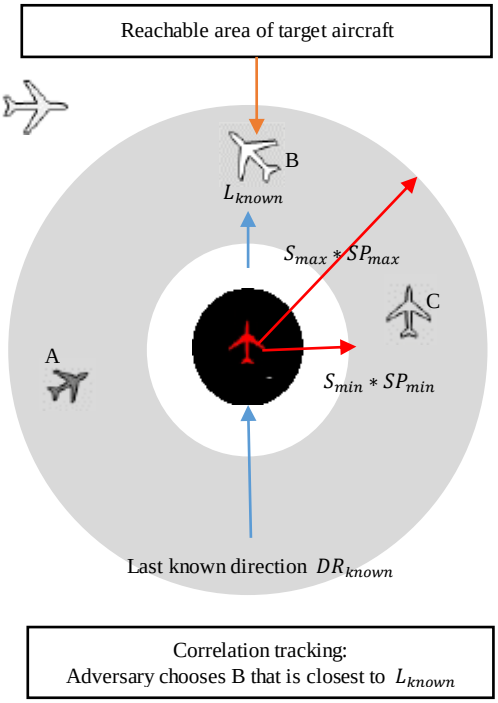

Figure 4. Correlation Tracking

Under correlation tracking, the adversary can assign a non-uniform probability distribution to the target anonymity set. And there are the following four steps to calculate $P_i, \forall i \in S$.

- *Step-1:*
  To confirm the target anonymity set S using the same method as the simple tracking.
- *Step-2:*
  As illustrated in Fig. 4, after determining A_r, based on target's last known location L_{known}, last known speed SP_{known}, and last known direction DR_{known} at time t, assumed that the velocity and the direction of the target aircraft have not changed during the random silent period the adversary can estimate target's location L_{known1} in A_r at a future time $speriod_{min} + bperiod$ where $speriod_{min}$ is the minimum silent period and $bperiod$ is each broadcast period.
  So $t_i = speriod_{min} + (i-1)bperiod$, where $t_i \leq speriod_{max}$, hence the adversary can obtains up to n estimated target position $\{L_{knowni}\}_{i=1}^{n}$ at time $\{t + t_i\}_{i=1}^{n}$.
- *Step-3:*
  The adversary chooses the aircraft that appears closest to L_{knowni} after update. Correlation tracking is repeated in A_r after each broadcast period until the maximum silent period $speriod_{max}$ is reached.
- *Step-4:*
  An element i that is chosen as a candidate at m of n estimated target positions in A_r is assigned a probability of $P_i = \frac{m}{n}$.

Hence, the entropy of correlation tracking is:

$$\begin{aligned} \mathrm{H}(p) &= -\sum_{i=1}^{|S|} P_i log_2 P_i \\ &= -\sum_{i=1}^{|S|} \frac{m_i}{n} log_2 \frac{m_i}{n} \\ &= log_2 n - \tfrac{1}{n}\textstyle\sum_{i=1}^{|S|} m_i log_2 m_i \end{aligned} \quad (8)$$

Assume that m_i is a normal distribution with $\mu = \frac{n}{2}$ and $\sigma = \frac{n}{6}$, we have

$$m_i = \left| \frac{1}{\sqrt{2\pi}\frac{n}{6}} \exp\left[-\frac{1}{2}\left(\frac{x-\frac{n}{2}}{\frac{n}{6}} \right)^2 \right] \right| \quad (9)$$

Note that the random normal distribution number between 0 and *N* is produced by MATLAB. And then we round the decimal into integer and regard it as the distribution of m_i.

V. EVALUATION OF LOCATION PRIVACY

A. Simple Tracking Analysis

Fig. 5 and Fig. 6 show the maximum location privacy level for different random silent period values and different airspace densities respectively in simple tracking method. As shown, the entropy increases with silent period duration as well as node density. Especially in this paper we only consider class A airspace (i.e. average of 900 km/h). Thus,the $hsep_{min}$ is 6km [12].

B. Correlation Tracking Analysis

Fig. 7 and Fig .8 show the maximum location privacy level for different estimated times *N* and different size of anonymity set |*S*| respectively in correlation tracking method. As shown in Fig. 7, the entropy increases with *N* at the beginning but remains steady later. In Fig. 8, the entropy increases with |*S*| which increases with maxium silent period and node density according to (4)(5).

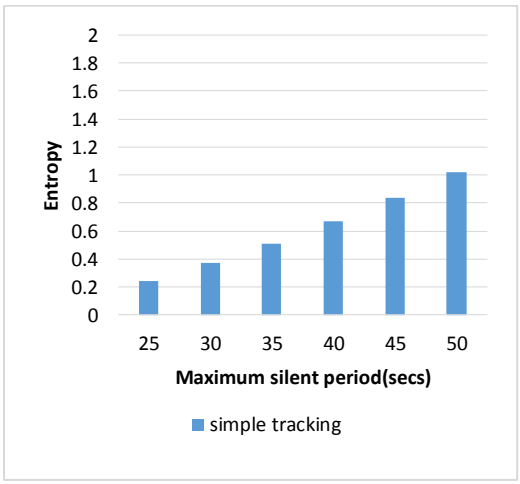

Figure 5. Theoretical Estimates of Max Location Privacy for Target (Node Density = 30 per 10^4 nm^2)

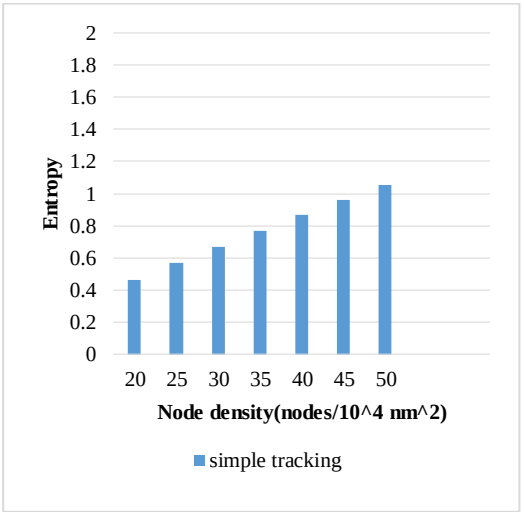

Figure 6. Theoretical Estimates of Max Location Privacy for Target (SP_{max} = 40 secs)

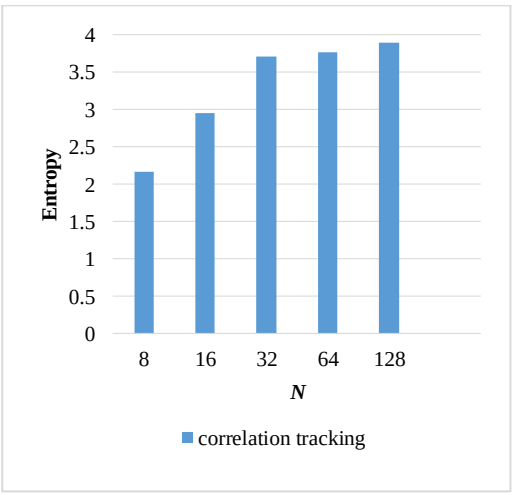

Figure 7. Theoretical Estimates of Max Location Privacy for Target (|*S*|=16)

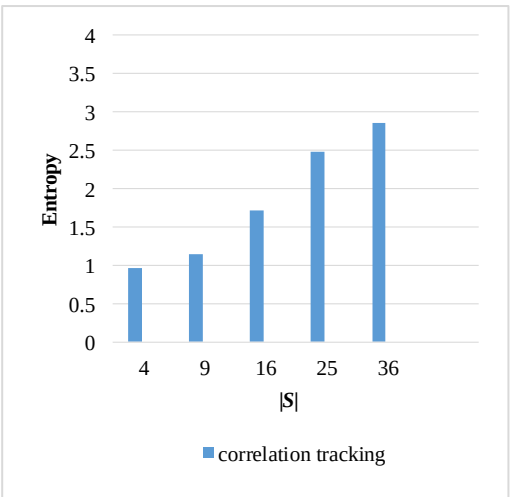

Figure 8. Theoretical Estimates of Max Location Privacy for Target (*N*=32)

IV. CONCLUSIONS

In this paper we focuse on the location privacy risks of ADS-B.A common underlying idea of these solutions is to introduce spatial and temporal uncertainty to reduce the correlation between two consecutively used identifiers of an aircraft.[1]We present a solution that can enable aircraft to independently maximize privacy level through update of aircraft pseudorandom identifiers during a random silent period.We analyze an evaluation method named simple tracking that Krishna et al. [1] proposed in 2012 and we propose a more pratical and accurate correlation tracking method.The evaluation of location privacy in these two tracking methods shows that the uncertainty increases with the size of anonymity set which further increases with air traffic density and the length of random silent period.In correlation tracking, when N increases,the entropy will increase at the beginning and remain steady later,so it is very necessary to find a proper N to evaluate the entropy in correlation tracking method.

In the future work, we will consider open problems such as a aircraft will update its pseudonym with probability $P_\mu \leq 1$ at each broadcast, enableing aircraft to safely and securely participate anonymously in IFR mode as well as enabling maximum privacy guarantees at the aircraft.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grants U1233108 and U1333127, the International Science and Technology Cooperation and Exchange Program of Sichuan Province, China under Grant 2015HH0040, and China Postdoctoral Science Foundation funded project under Grant 2014M562309.

REFERENCES

[1] Krishna Sampigethaya, Boeing Research & Technology (BR&T), Bellevue, WA Radha Poovendran, Network Security Lab (NSL), University of Washington, Seattle, WA Capt. Stephen Taylor, Boeing Business Jets, Seattle, WA, PRIVACY OF GENERAL AVIATION AIRCRAFT IN THE NEXTGEN

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

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

[4] Donald McCallie, Jonathan Butts∗, Robert Mills, Security analysis of the ADS-B implementation in the next generation air transportation system, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA, July7 2011

[5] Federal Aviation Administration, FAA's NextGen Implementation Plan, Washington, DC, 2011

[6] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wirelesslocation privacy using silent period," in Proc. of the IEEE Wireless Communications and Networking Conference (WCNC), March 2005, pp. 1187–1192.

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

[8] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," Journal of Cryptology, vol. 1, pp. 65–75,1988.

[9] 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/2008/080304 ads-b-comments.pdf

[10] ITT,ADSBExplained,Herndon,Virginia,2009,www.itt.com/adsb/adsb-explained.html

[11] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran, AMOEBA: Robust Location Privacy Scheme for VANET, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 25, NO. 8, OCTOBER 2007

[12] Civil Aviation Administration of China (2009-11-13) http://www.caac.gov.cn/D1/60ZNQD/ssmh /200911/t20091113_28887.html