Short-Term and Long-Term Solutions for Secure Verification of Aircraft-Reported ADS-B Location in Air Traffic Networks

Nikki Manuel and Depeng Li
Department of Information and Computer Sciences
University of Hawai'i at Manoa
{ndmanuel, depengli}@hawaii.edu

Abstract

Automatic dependent surveillance-broadcast (ADS-B) is the foundation of next generation air traffic management systems. The precision granted by ADS-B will allow for the network to support the huge growth in air traffic in the coming decades and assist both air traffic controllers and pilots in improving safety in flight. However, the ADS-B protocol has serious security vulnerabilities. Coupled with the importance of ADS-B in the air transportation system, these security issues make ADS-B an appealing target for attack by adversaries. This paper dismisses the need for encryption and focuses security strategies on location verification. Multilateration is combined with data fusion and location tracking for effective and undemanding short-term and long-term location verification. By taking input from air traffic controllers, a secondary location tracking systems allows for a backup record of controlled aircraft that can easily be referred to in emergencies.

1. Introduction

The U.S. Federal Aviation Administration has introduced the Next Generation (NextGen) upgrade to modernize the U.S. air traffic control system. NextGen will be expected to handle the growth of air traffic by manned and unmanned aircraft and to improve the safety of all passengers. This upgraded system is dependent on Automatic Dependent Surveillance-Broadcast (ADS-B), which wirelessly generates and broadcasts digital messages that contain the GPS coordinates of aircraft. Unlike traditional radar systems, ADS-B is intended to provide enhanced situational awareness by allowing aircraft to provide their identity, location, and intent.

The importance of ADS-B makes it an appealing target for attack by adversaries looking to negatively affect air traffic systems. ADS-B is made even more appealing because it has no built-in security countermeasures to prevent adversarial attacks. The inherent lack of security measures in the ADS-B protocol makes it susceptible to eavesdropping, jamming, message injection, message deletion, and message modification. [8]

The majority of proposed security solutions for ADS-B center on authentication of messages through methods such as public key infrastructure and fingerprinting. This paper argues that such message authentication techniques are not efficient for use in air traffic management and location authentication measures should instead be implemented to secure the ADS-B data link. Implementation of the location authentication strategies of multilateration, data fusion, and location tracking would be an alternate method of verifying the existence of aircraft in ADS-B data.

The remainder of this paper will proceed as follows: in Section II, problems with ADS-B and previously proposed solutions will be covered; in Section III, the inefficiency of broadcast authentication will be discussed and certain location authentication strategies will be dismissed; in Section IV, this paper will propose multilateration in combination with data fusion and location prediction as short-term and long-term strategies for verification of ADS-B location; finally, Section V concludes this paper with discussion of the solution and prospects for future research.

2. Background and Related Works

This section defines the problems related to security in ADS-B more thoroughly. First, a short overview of the currently used ADS-B protocol is provided. Building on this, the existing vulnerabilities

URI: http://hdl.handle.net/10125/50587
ISBN: 978-0-9981331-1-9

are outlined. Finally, the solutions proposed by previous research studies are identified.

2.1. ADS-B Overview

ADS-B forms the foundation for the future of air traffic management systems, allowing the shift from ground radar and navigational aids to precise tracking via satellite signals. These broadcasts contain the aircraft's position, velocity, identification, and other air traffic management-related information. It allows for cost-effective surveillance, cockpit advisory services to improve pilots' situational awareness, and cockpit critical services to safely improve air traffic capacity.

In the ADS-B system architecture, each aircraft computes its position and velocity with the help of on-board GPS then broadcasts this information to ground sensor stations and other aircraft at a rate of 1-2 times per second. ADS-B is supported by two different data links: 1090 MHz Extended Squitter (1090ES) and Universal Access Tranceiver (UAT). 1090ES is the major data link for scheduled air transportation. For purposes of air traffic management, ground sensor stations receive an aircraft's messages and forward them to air traffic control facilities. Surrounding aircraft with the proper equipment can receive these same messages, either forwarded by the ground sensor station or directly received from the transmitting aircraft.

2.2. Problems with ADS-B

The current version of ADS-B's data link has serious security concerns. These vulnerabilities are inherent to the nature of broadcasting over radio frequencies. Strohmeier et al. [8] define the possible attacks that ADS-B is susceptible to:

Eavesdropping: This passive attack consists of listening in on unsecured broadcast transmissions. This is the easiest attack to carry out and has long been acknowledged due to the inherent nature of ADS-B broadcasting unsecured messages over radio frequencies.

Jamming: Jamming is a problem common to all wireless communication. However, the effect of a jamming attack on ground station or aircraft receivers is particularly serious, considering the importance and criticality of the transmitted data. The inability of air traffic control to track aircraft would create severe problems in the transportation network.

Message Injection: Message injection consists of adding fake transmissions to the air traffic communication system. As demonstrated by researchers at Black Hat 2012 [2], injecting imposter messages is simple and cheap. This attack can be scaled formidably to flood the air traffic communication system with "ghost" aircraft transmitting false information.

Message Deletion: Legitimate messages sent by aircraft or ground stations can be "deleted" by transmitting the inverse of the signal (destructive interference) or causing a large enough number of bit errors for the receiver to classify the message as corrupt and drop it (constructive interference). Message deletion can make it look like an aircraft has disappeared.

Message Modification: The most complex attack to pursue, message modification can be carried out by sending a high-powered signal to replace part or all of a legitimate message, or switching any number of bits in the signal from 1 to 0 or 0 to 1. This injects false data into the legitimate message without the knowledge of the transmitting party and receiving party, resulting in an aircraft possibly reporting false position, identification, and trajectory.

2.3. Proposed Solutions for ADS-B Security

The security vulnerabilities of ADS-B have been well-known for a long time and the number of research studies focusing on it have been increasing steadily as the 2020 deadline for its full implementation draws closer. Sampigethaya et al. [6] analyze the security and privacy issues of aircraft communication systems, including ADS-B. The authors mention different methods of protecting ADS-B communication, from multilateration to cryptography.

The variety of security issues make cryptography an appealing solution. While Sampigethaya et al. mention symmetric key encryption as an efficient approach, the need to pre-share keys makes the implementation completely inefficient. With symmetric key encryption ruled out by most researchers, other studies have looked into public key encryption as an alternative encryption solution. Wesson et al. [9] have noted asymmetric, elliptic curve cryptography as the most practical and effective cryptographic approach. However, cryptography as a whole - whether symmetric or asymmetric - remains impractical due to the burden of key management and the limited capacity of ADS-B transmissions.

While cryptography is an appealing solution due to its ability to offer some level of protection for all possible attacks, even disregarding its implementation issues it is an inefficient solution due to the low threat of certain attacks. For example, eavesdropping is not necessarily an adversarial attack. On the contrary, the ability to track aircraft is a welcome one, as conveyed by the usefulness of online flight tracking websites such as Flight Radar 24 and Flight Aware. While eavesdropping can form the basis for the more sophisticated types of attacks, research should accept eavesdropping as a possibility and focus efforts on

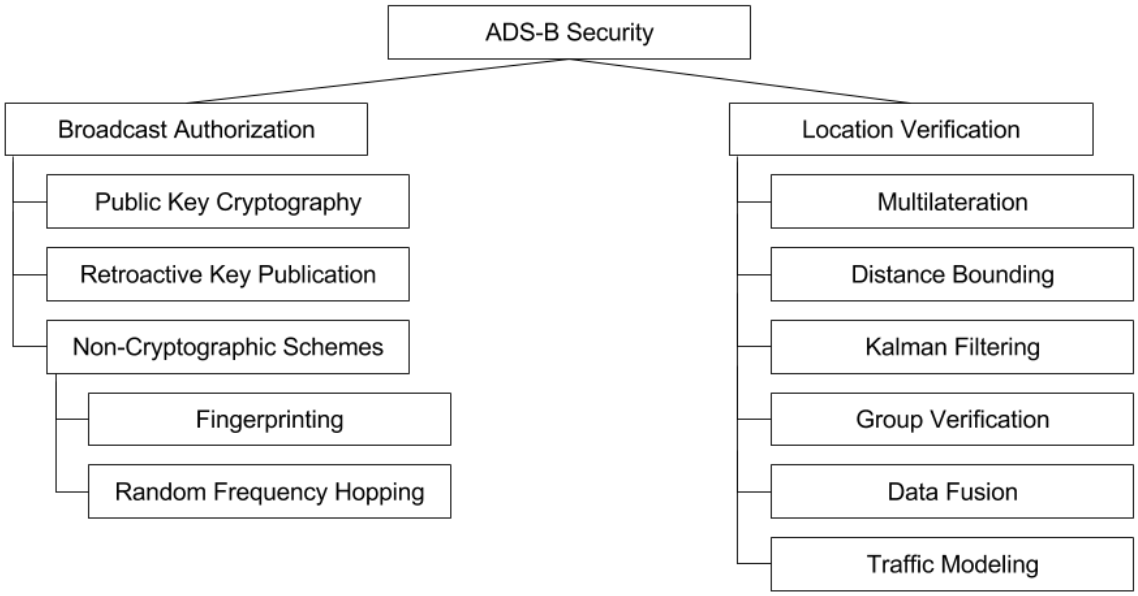

Figure 1. Taxonomy of ADS-B Security, by Strohmeier et al. [8]

preventing other attacks due to the difficulty to preventing eavesdropping without applying full encryption.

With eavesdropping allowed and the inefficiency of encryption acknowledged, it is important to look into other methods of verifying messages in the air traffic communications network. Strohmeier et al. [8] separate the approaches towards ADS-B security into Secure Broadcast Authentication and Secure Location Verification, as shown in Figure 1. Secure location verification focuses on verifying location claims made by ADS-B participants. Location verification techniques are separated into the following groups: multilateration [4, 5], distance bounding, Kalman filtering [4], group verification, data fusion[4], and traffic modeling.

3. Problem Description

Despite the number of possible solutions for ADS-B vulnerability, most proposals are limited, whether in ability or in implementation efficiency. The taxonomy of ADS-B security proposed by Strohmeier et al. [8] is used in this paper to categorize authentication solutions. This section discusses the problems of broadcast authentication to dismiss the need for encryption and to focus research on location authentication over data link authentication. However, not all location authentication techniques are sufficient enough to address ADS-B vulnerabilities and the remainder of this section will review issues found in location authentication strategies.

3.1. Inefficiencies of Broadcast Authentication

In accordance to the taxonomy proposed by Strohmeier et al., broadcast authentication consists of three branches: non-cryptographic schemes, public key cryptography, and retroactive key publication. Non-cryptographic schemes consist of fingerprinting and random frequency hopping. Fingerprinting consists of using hardware, software, and/or wireless channel imperfections and characteristics to identify and authenticate legitimate users and devices. Random frequency hopping consists of changing frequencies to avoid jamming and eavesdropping. These two non-cryptographic schemes are inapplicable to ADS-B security because fingerprinting has not been proven as a reliable way to identify between real and false traffic, while randomized frequency hopping requires pre-shared secret codes, which is not scalable for widespread use within the air traffic transportation network.

A public key infrastructure is similarly difficult to scale for such widespread use. Key distribution and key management pose significant challenges, with the requirement of a certificate authority and the possibility of producing an overwhelming amount of data link traffic due to certificate verification transactions. The possibility of retroactive key publication is also suggested as a variation on asymmetric cryptography. This strategy consists of senders retroactively publishing their keys and receivers authenticating the messages. However, this

strategy is not feasible due to the possibility of packet loss and the delay of key release producing a further delay in authentication.

3.2. Insufficiencies of Location Authentication

In consideration of the inefficiency of the broadcast authentication strategies, it is worthwhile to focus on authenticating ADS-B location data. Strohmeier et al. list the following strategies for location authentication: multilateration, distance bounding, Kalman filtering, group verification, data fusion, and traffic modeling. This paper suggests a combination of these strategies for short-term secure location authentication, but the drawbacks of each individual technique is examined.

Multilateration depends on two to four known locations cooperating with each other to determine the origin of an ADS-B signal by comparing the time the signal arrives at the different antennas. This technique is already being used in areas within the United States and Europe. However, because of the dependency on other verified sources, multilateration is not possible in open spaces, such as over oceans, which contradicts the intention of ADS-B.

Distance bounding is a method that calculates the location of an aircraft based on the time it takes for the verifying body to challenge the supposed aircraft and the supposed aircraft to respond. This works particularly well when there is more than one verifying body, but it also results in multilateration's problem of needing verified sources that may not be available in vast open spaces. In addition, attacks on distance bounding exist and the process takes too long to practically integrate in consideration of the high speed of air traffic. Finally, similar to the challenges of implementing certain cryptographic schemes, distance bounding requires the aircraft to be able to respond to the verifying body's challenge. This means ADS-B equipment needs to be altered to support this technique. In the face of these disadvantages, this paper dismisses distance bounding as a practical strategy for location authentication.

Kalman filtering is a technique that tests whether an aircraft's motions are in line with its ADS-B intent. However, it is susceptible to attack [1, 4] and requires more storage and processing. This paper dismisses Kalman filtering as a practical strategy for location authentication due to its vulnerabilities. It can still be implemented in combination with other strategies - and in fact works very well to support multilateration precision - but will not be covered due to its low relative usefulness in contrast with other strategies.

Group verification is a method of multilateration conducted by a group of aircraft in flight that verify other aircraft. This technique is supported by a study by Kovell et al. [4] that demonstrated that 91% of aircraft at a given time could be in a group large enough to take part in group verification. However, like distance bounding and cryptography schemes, the verification and trust process requires many additional messages, not to mention an overhaul of ADS-B's inherent broadcast protocol. This invalidates group verification as a feasible security technique.

Data fusion is a strategy that aggregates data from outside systems to check positional data from aircraft ADS-B. This works well with multilateration and is already being used. However, just like multilateration, data fusion contradicts the intention of ADS-B. While ADS-B is meant to be the foundation of NextGen, data fusion would require reliance on redundant systems such as the traditional primary radar system (PRS). ADS-B is intended to eventually phase out the PRS, and therefore data fusion is not a viable solution for long-term security.

The final listed location authorization strategy of traffic modeling relies on past air traffic data and machine learning in order to create a traffic model for each ground station. This allows the detection of abnormal air traffic. However, due to the lack of research supporting the viability of using machine learning for traffic modeling, particularly as air traffic greatly increases, this paper dismisses the strategy in favor of a proposed location tracking and prediction strategy.

4. Proposed Solution

From the review of the location authentication strategies, we can see the advantages and limitations of multilateration and data fusion. This paper suggests the combination of multilateration with data fusion as a short-term solution for location authorization. However, because of data fusion's reliance on redundant systems that are intended to be phased out as part of the next generation air traffic system, a location confirmation and tracking system is proposed for long-term implementation. The proposed long-term solution consists of an interface that takes advantage of an air traffic controller's ability to verify information while accepting control of aircraft and speaking directly with pilots. A secondary system keeps track of aircraft and the instructions they have been given, allowing for a backup record of controlled aircraft that a controller can quickly refer to in the case of a large influx of "ghost" aircraft or the sudden disappearance of aircraft.

4.1. Multilateration as Short-Term Solution

Multilateration uses verification sources on the ground in order to verify the location claims that aircraft makes. The main advantage of multilateration is that it is compliant with the ADS-B infrastructure that is already in place. It does not interfere with any

existing equipment. That is, it can be implemented on top of existing systems and will not obstruct the way they work.

It must be noted however that multilateration would require redundant systems. It may not make sense to pay for redundant systems that do what ADS-B should be able to do on its own, but in view of ADS-B lacking any security features and the ease of implementing multilateration systems on top of existing infrastructure, the cost is reasonable for the sake of security. In addition, it's important to remember that many flight and air traffic procedures already have redundant features in place to

Multilateration systems do not process any sensitive data, but it would still be a good idea to implement security features. For example, communication between the antennas should be properly encrypted and authenticated. Unlike ADS-B, multilateration would allow for this, so it should be taken advantage of. This will protect invalidated data from being injected and deleted in the network between multilateration antennas and central processing units. It would also be helpful to have systems that detect attempts to tamper with data and detect fraudulent identity claims.

4.2. Data Fusion as Short-Term Solution

Data fusion is one of the most important techniques for secure location verification. It involves the union of data from different sources, such as from radar systems and flight plans. Data fusion is valuable because it allows falsified data to be detected. The more sources of sensor data available, the harder it is for adversaries to implement attacks.

For this technique, the legitimacy of various data sources is the most important aspect. For example, ADS-B data could be used for location verification but if the data is falsified, it could lead to even more interruptions due to multiple sources reporting different information. In this case, ADS-B is not being used as a source of data. An ideal source of data for data fusion in the short-term is primary radar systems. Primary radar systems are already established, so no further costs are needed to create new data sources. In addition, data from the radar systems is relatively trustworthy due to less vulnerabilities inherent to the system. Along with radar system data, flight plan data also needs to be verified. However, this data comes directly from pilots and airline companies. As long as steps are taken to ensure that flight plan data is not tampered with, it is a trustworthy source for data fusion.

4.3. Combining Multilateration and Data Fusion for Short-Term Location Authorization

Multilateration involves ground-to-air verification for location claims. Data fusion combines data from flight plans and the primary radar system to determine the validity of an aircraft's path. These two techniques for location verification complement each other well, with multilateration verifying that an aircraft is where it claims to be and data fusion verifying that an aircraft is where it should be. Data fusion can depend on multilateration to ensure that the data it is processing is correct.

The problem with multilateration and data fusion is that they are not viable solutions for long-term security. In addition, one of the goals of the aviation industry's introduction of ADS-B is that it would eventually do away with the primary and secondary radar systems. Multilateration is not available over wide open spaces, especially over oceans, so it only offers a partial solution. On the other hand, ADS-B is capable of providing the information originally supported by primary and secondary radar systems, even over wide open spaces. While multilateration and data fusion work well for the present time, it would be valuable to consider long-term solutions that could aid in the secure verification of reported aircraft location.

4.4. Location Tracking for Long-Term Implementation

This paper proposes a location tracking and prediction system for long-term implementation as a solution to ADS-B security. This system would not require any changes in the systems already in place and would simply work as additional software on top of what is already in place for air traffic management systems. No extra equipment nor change in equipment would need to be implemented in aircraft systems.

The proposed tracking system would rely on data from flight plans and ADS-B. In this sense, this is a method of data fusion. However, it would also be reliant on air traffic controller data. As aircraft fly between different airspace designations, they are transferred between air traffic facilities. As aircraft are handed off between facilities, air traffic controllers manually accept control of the aircraft. By seeing aircraft on their digital scope and communicating with the respective pilots, air traffic controllers create an authorization system themselves. The proposed tracking system would keep track of these aircraft as the air traffic controllers authenticate their location and identity.

While a lone ghost aircraft does not pose a large problem to air traffic controllers, it can be imagined that a very large number of ghost aircraft suddenly appearing on a controller's scope can cause extreme loss of situation awareness. With the location tracking

system in place, air traffic controllers will instead be able to view only the traffic that has been confirmed. In this sense, it is like a backup image of a system that the controllers can refer back to. Controllers can refer to the location tracking system, which will only show verified aircraft. This sort of system will be especially important if an attacker were to populate a scope with so many ghost aircraft that the screen is completely covered with them. In this case, the tracking system will provide a clear image of aircraft that have been confirmed by at least one air traffic controller to be in the airspace. This can also work to defend from the possibility of an attacker suddenly blocking ADS-B signals to create a disappearance of aircraft from the scope. Using data that has been previously verified by air traffic controllers, the tracking system would be able to show a picture of aircraft to show controllers where their last reported location is. This would additionally allow controllers to have an idea of where their aircraft are, decreasing the possible loss of situational awareness.

This leads to another feature of the location verification system: location prediction. As air traffic controllers speak with aircraft, they verify information with the aircraft, such as aircraft type, speed, and intended path to an intended destination. This information is written down on strips of paper as controllers speak with aircraft. As this information is verified, the location verification system also takes in this information. This can be done through voice recognition, which is already implemented at air traffic control training centers. In addition, the information recorded via voice recognition could show up as a way for controllers to verify that it was correctly input into the location verification system. The verified information can be used by the system as a way to predict aircraft location in the case of a controller's loss of situational awareness - such as if an attacker were to make all aircraft disappear from a controller's scope or if information was falsified to make it look as if an aircraft was suddenly flying towards an object at very high speeds. The location verification system would simply keep track of intended path, intended destination, and controller instructions for aircraft direction and speed. Thus, a predicted path could be drawn from an aircraft to its destination, with the system showing a dot for the predicted location of an aircraft. Ideally, this dot would be in the same place as the aircraft. If an attacker were to make aircraft disappear from a scope or to falsify location or speed data, the controller would be able to refer to the last verified pathway in order to make an assessment about the true location of the aircraft.

4.5. Solution Analysis

The location authorization strategies previously mentioned were tested in a simulated environment based on live flight data. Local aircraft were tracked by processing ADS-B signals using MATLAB with RTL-SDR radio hardware. Figure 2 displays an example of data that was retrieved for the simulation. This includes aircraft identification, position information, speed, heading, and flight plan.

Several well-known Bayesian algorithms are often used as filtering algorithms to track objects whose dynamical behavior changes over time. The particle filter algorithm was chosen to track aircraft due to its suitability for nonlinear estimation and its use in signal processing. The algorithm consists of three parts: prediction of the state probability density function (PDF) using the system model, update via latest ADS-

Timestamp	ID	Type	Latitude	Longitude	Altitude	Speed	Direction	Flight Plan
1503952918	HAL255	B712	21.254704	-158.031891	1500	190	347	MAUI5 OGG LNY JULLE5
1503952918	UPS58	B744	21.007426	-158.433708	14700	436	258	KEOLA2 KATHS CRESP 2500N/17000W 2700N/18000E 2900N/17000E 2936N/16500E 3000N/16000E 3000N/15000E 2800N/14000E CANAI V75 NHC V91 MJC G581 IGURU Q13 PICHU HCN G581 ELATO V522 ABBEY
1503952918	HAL119	B712	21.001163	-157.703461	8900	290	299	V20 HOKLA JULLE5
1503952918	AAR232	A333	21.325161	-158.061264	1975	188	89	EGOBA1L EGOBA Y697 AGSUS Y697 LANAT Y51 KAGIS OTR13 SEALS 3400N/15000E 3000N/16000E 2800N/17000E 2500N/18000E 2200N/17000W SYVAD BOOKE BOOKE8
1503952918	MKU420	DH8D	21.200018	-157.816704	6300	230	137	PALAY2 LNY CAMPS3
1503952918	KAL53	B748	21.522812	-158.956284	14600	380	97	SEL Y697 LANAT Y51 KAGIS OTR13 SEALS 3400N/15000E 3000N/16000E 2800N/17000E 2500N/18000E 2200N/17000W SYVAD BOOKE BOOKE8

Figure 2. Sample data taken from live ADS-B tracking, August 28, 2017.

B data to modify the predicted PDF, and resampling to refine predictions.

The prediction is made according to the following evolution equation:

$$P_r = (P_t G_t G_r \lambda^2 \sigma) / ((4\pi)^3 R^4) \quad (1)$$

for which P_r is the received power, P_t is the transmitted power, G_r is the receiving antenna gain, G_t is the transmitting antenna gain, λ is the signal wavelength, σ is the target's radar cross-section, and R is the range to the target. This equation allows for the target locations to be estimated.

Huang et al. [3] additionally recommend the state equation:

$$x_t = f(x_{t-1}) + v_{t-1} \quad (2)$$

for the temporal evolution of the state vector x_t, where f is the state transition function and v_t is the process noise with zero mean. For the ADS-B system, the components of the state vector will be target locations for which an observation y_t will be represented as:

$$y_t = h(x_t) + n_t\,, \quad (3)$$

where h is the measurement function and n_t is the measurement noise, with n_t not correlated with v_t. With this, the particle filter algorithm is implemented in the following steps:

1. Particle generation: create N particles and associated weights $(x^n_{t-1},\ w(x^n_{t-1}))_{n=1,\ldots,N}$ according to the uniform distribution.
2. Prediction: particle propagation according to evolution equation (1).
3. Update: use ADS-B data to compute the likelihood of each particle and update the weights of all the particles.

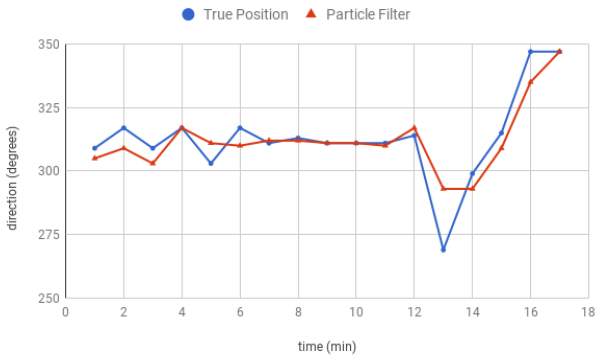

Figure 3. ADS-B Reported Location vs. Predicted Location For One Aircraft

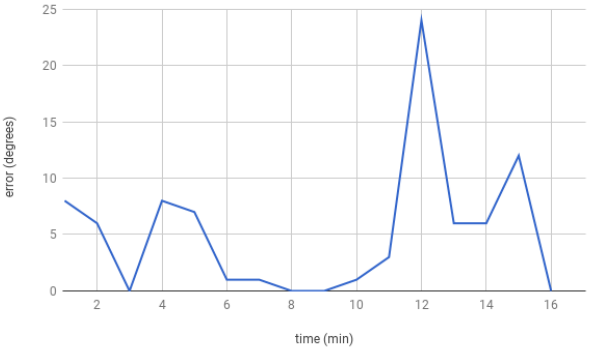

Figure 4. Particle Filter Error in Predicting Aircraft Location For One Aircraft

4. Resample: after a predetermined number of iterations, take N samples based on the updated data in the previous step
5. Reiterate: for $t = t + 1$, repeat these steps until the desired estimation error is received.

Through these methods, a performance evaluation was conducted using MATLAB to verify the ability to track and predict aircraft location using the particle filter error coupled with verified input to simulate air

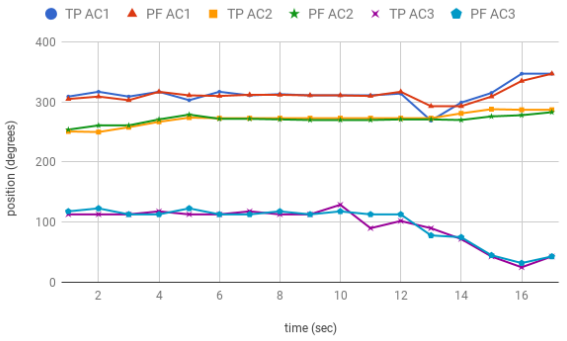

Figure 5. ADS-B Reported Location vs. Predicted Location For Three Aircraft

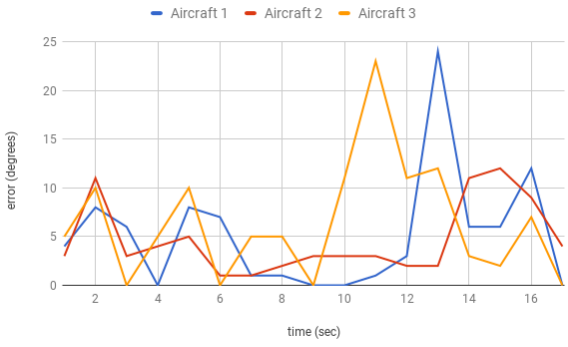

Figure 6. Particle Filter Error in Predicting Aircraft Location For Three Aircraft

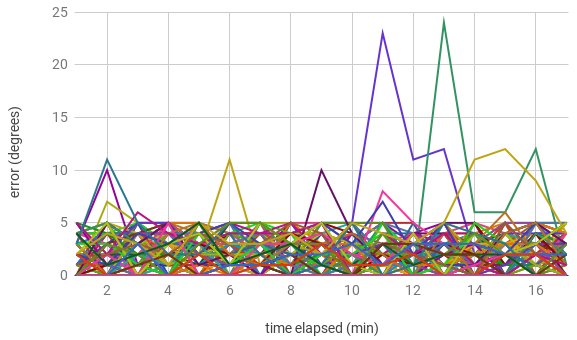

Figure 7. Particle Filter Error in Predicting Aircraft Location For 100 Aircraft

traffic control direction. This is in comparison to the real data obtained by the live ADS-B stream. Figure 3 shows an example of one case of comparison. The true position indicated by ADS-B for one aircraft was compared with its predicted position through the particle filter algorithm and verified position through simulated air traffic controller confirmation. Figure 4 shows the error rate made by the particle filter algorithm and simulated input in attempting to track and predict the aircraft's location. Aside from one instance of notable error, the algorithm did fairly well and was within eight degrees of the aircraft's true position. Figures 5 and 6 display the evaluation of three aircraft. Similar to the simulation for one aircraft, the algorithm and controller input do well in predicting the position of the aircraft.

As Figures 3 to 6 show, there are occasional errors in the combined ability of the particle filter algorithm and air traffic controller simulation to predict aircraft position. However, these errors often do not greatly deviate by more than ten degrees. Figure 7 demonstrates the particle filter algorithm errors for a set of one hundred aircraft. The overall degree of error remains small, with the majority of deviances below 5 degrees and the instances of high error degree occurring at a lower rate as the number of aircraft sample size increases.

The performance evaluation for location tracking and prediction via particle filter shows a lot of promise. Future research would include refinement of the algorithm for all dimensions of aircraft movement. In addition, implementation of real air traffic controller direction would likely increase dependability of the tracking and prediction algorithm in instances of adversarial attack.

5. Conclusion

ADS-B has been faulted for having no inherent security features. While this leaves the system vulnerable to various attacks, it is important to consider the viability of implementation for possible solutions. Suggestions for encryption or changes to aircraft systems are not realistic and lead to industry dismissal of security research. A location verification system would allow for a lightweight implementation that can provide air traffic controllers with a background reference they can refer to in case of attack.

6. References

[1] E. Chan-Tin, V. Heorhiadi, N. Hopper, and Y.D. Kim, "The Frog-Boiling Attack: Limitations of Secure Network Coordinate Systems", ACM Transactions on Information and System Security (TISSEC) 14.3 (November 2011).

[2] A. Costin and A. Francillon, "Ghost in the Air (Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices", Black Hat USA 2012, Las Vegas. Web. 15 Feb. 2017.

[3] M.S. Huang, R.M. Narayanan, Y. Zhang, and A. Feinberg, "Tracking of Noncooperative Airborne Targets Using ADS-B Signal and Radar Sensing," International Journal of Aerospace Engineering, vol. 2013, Article ID 521630, 12 pages, 2013.

[4] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, "Comparative Analysis of ADS-B Verification Techniques", The University of Colorado, Boulder 4 (2012).

[5] B. Nuseibeh, C.B. Haley, C. Foster, "Securing the Skies: In Requirements We Trust", Computer, IEEE Journals & Magazines, Sept. 2009.

[6] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty. "Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond", Proceedings of the IEEE 99.11 (November 2011): 2040-055.

[7] M. Schäfer, V. Lenders, and I. Martinovic. "Experimental Analysis of Attacks on Next Generation Air Traffic Communication", Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS) (2013): 253-71.

[8] M. Strohmeier, V. Lenders, and I. Martinovic. "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol", IEEE Communications Surveys & Tutorials 17.2 (2014): 1066-087.

[9] K.D. Wesson, T.E. Humphreys, and B.L. Evans. "Can Cryptography Secure Next Generation Air Traffic Surveillance?", IEEE Security & Privacy. Draft. (2014). Web. 15 Feb. 2017.