Department of Computer Science

Security of ADS-B: State of the Art and Beyond

Martin Strohmeier[*], Vincent Lenders[+], Ivan Martinovic[*]
[*]University of Oxford, United Kingdom
[+]armasuisse, Switzerland

CS-RR-13-10

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD

Security of ADS-B: State of the Art and Beyond

Martin Strohmeier*, Vincent Lenders+, Ivan Martinovic*
*University of Oxford, United Kingdom
+armasuisse, Switzerland

***Abstract*—Automatic dependent surveillance-broadcast (ADS-B) is the communications protocol currently being rolled out as part of next generation air transportation systems. As the heart of modern air traffic control, it will play an essential role in the protection of two billion passengers per year, besides being crucial to many other interest groups in aviation. The inherent lack of security measures in the ADS-B protocol has long been a topic in both aviation circles as well as the academic community. Due to recently published proof-of-concept attacks, the topic is becoming ever more pressing, especially with the deadline for mandatory implementation in most airspaces fast approaching.**

This survey first summarizes the attacks and problems that have been reported in relation to ADS-B security. Thereafter, we survey both the theoretical and practical efforts which have been conducted previously concerning these issues, including possible countermeasures proposed in the literature. In addition, the survey seeks to go beyond the current state of the art and gives a detailed assessment of security measures which have been developed more generally for related wireless networks such as sensor networks and vehicular ad hoc networks, including a taxonomy of all considered approaches.

***Index Terms*—ADS-B; aviation; security; wireless; privacy; broadcast**

I. Introduction

The world of air traffic control (ATC) is moving from uncooperative and independent (primary surveillance radar, PSR) to cooperative and dependent air traffic surveillance (secondary surveillance radar, SSR). This paradigm shift holds the promise of reducing the total costs deployment and improving the accuracy. However, it is well known in the aviation community that the ATC system, which is currently being rolled out, called *automatic dependent surveillance-broadcast* (ADS-B), has not been developed with security in mind and is susceptible to a number of different radio frequency (RF) attacks. The problem has recently been widely reported in the press and at hacker conventions. Academic researchers, too, proved the ease of exploiting ADS-B with current off-the-shelf hard- and software [1], [2]. The broad news exposure led the International Civil Aviation Organization (ICAO) to put the security of civil aviation on their agenda of the 12th air navigation conference, identifying "cyber security as a high-level impediment to implementation that should be considered as part of the roadmap development process" [3] and creating a task force to help with the future coordination of the efforts of involved stakeholders.

This shows that there is a widespread concern about the topic, created by the fact that ADS-B will be mandatory for all new aircraft in the European airspace by 2015[1] and has already been embraced by many airlines worldwide. EUROCONTROL approximates that already more than 50 percent of the aircraft worldwide are already equipped with ADS-B transponders. Countries such as Australia have already deployed full continental coverage, with ADS-B sensors being the single means of ATC in low population parts of the country [4].

This paper gives an overview about the research that has been done on the security of ADS-B and describes the potential vulnerabilities identified by the community. Since much relevant security research has been conducted in related fields such as wireless sensor networks or general ad hoc networks, we analyze proposed countermeasures from any of these areas that could be adapted for use in ADS-B or whether they are not applicable for reasons inherent to the system. Furthermore, the present work provides a threat catalogue, analysis and vulnerability categorization of the mainly used data link *Mode S*. We focus primarily on the security of ADS-B and not on other air traffic control (sub-) systems, such as GPS. Among other questions, we seek to answer why existing ideas for securing (wireless) networks such as traditional cryptography cannot simply be transferred and used in the protection of systems such as ADS-B.

While there were a number of reasons behind the switch to a modern air traffic management system, cost has consistently been mentioned as one of the most important ones throughout the process; existing radar infrastructures are simply much more expensive to deploy and maintain [5]. ADS-B, on the other hand, provides significant operational enhancements for both airlines and air traffic managers. The increased accuracy and precision improves safety and decreases the likelihood for incidents by a large margin, unless the system's weak security is exploited by malicious in- and outsiders.

The remainder of the survey is organized as follows: Section 2 gives a detailed overview over the security problems concerning ADS-B and a model of the networking environment. Section 3 broadly outlines solutions proposed in previous works on this topic and looks at the sister protocols ADS-C and military versions of ADS-B. Section IV surveys secure broadcast authentication methods to address the problem while Section V reviews approaches to establish secure location verification with ADS-B. Section 6 summarizes and Section 7 concludes the survey.

II. Problem Statement

This chapter defines the problems related to security in ADS-B more thoroughly. First, we give a short overview over the currently used ADS-B protocol and its existing

[1]Older aircraft need to be retrofit by 2017. The FAA mandates ADS-B in the US airspace by 2020.

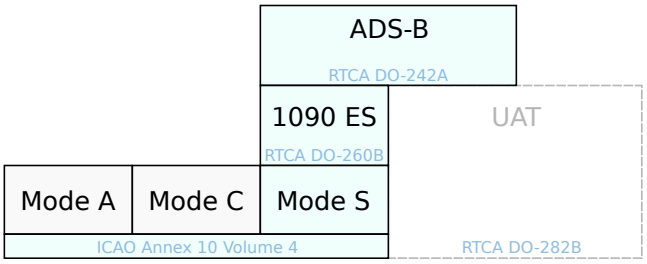

Figure 1. ADS-B hierarchy [1]

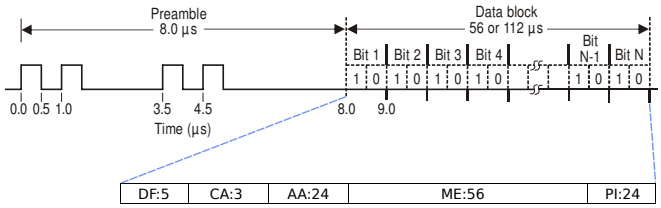

Figure 2. 1090 ES Data Link [1]

vulnerabilities. Building on this, a model of the ADS-B environment is outlined and the required attributes of possible solutions are identified.

A. ADS-B Protocol Overview

The American Federal Aviation Administration (FAA) as well as its European pendant EUROCONTROL named ADS-B as the satellite-based successor of radar. At its introduction, ADS-B has been a completely new paradigm for air-traffic control. Every participant retrieves their own position and velocity by using an onboard GPS receiver. The position is then periodically broadcasted in a message (typically twice per second) by the transmitting subsystem called ADS-B OUT. The messages then are received and processed by ATC stations on the ground as well as nearby aircraft, if equipped with the receiving subsystem ADS-B IN. Messages can integrate further fields such as ID, intent, urgency code, and uncertainty level.

There are two competing ADS-B data link standards that have been proposed: 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, utilizing the 978MHz frequency with 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. Commercial aircraft, on the other hand, employ SSR Mode S with Extended Squitter, a combination of ADS-B and traditional Mode S known as 1090ES (see Fig. 1). In other words, the ADS-B function can be integrated into traditional Mode S transponders. From here on, we focus on the commercially used 1090ES data link. The complete overview over the ADS-B protocol can be found in the specification documents [6], [7], [8], various other works give succinct, higher level descriptions of the protocol (e.g. [9], [2], [1]).

The 1090ES Data Link: As the name suggests, the 1090ES data link predominantly uses the 1090MHz frequency for communication sent out by aircraft, to both other aircraft and ground stations (Mode S also uses ground to air communication at 1030MHz for interrogations and information services). Figure 2 provides a graphical view of a 1090ES transmission, which starts off with a preamble of two synchronization pulses. The data block is then transmitted by utilizing pulse position modulation (PPM). With every time slot being 1µs long, a bit is indicated by either sending a 0.5µs pulse in the first half of the slot (1-bit) or in the second half (0-bit). It is important to note that PPM is very sensitive to reflected signals and multipath dispersion as this can play a major role in security and protocol considerations.[2]

There are two different possible message lengths specified in Mode S, 56 bit and 112 bit [6], whereas ADS-B solely uses the longer format. The downlink format field DF (alternatively UF for uplink messages) assigns the type of the message. 1090ES uses a multipurpose format as shown in Fig. 2. When set to 17, it indicates that the message is an extended squitter, enabling the transmission of 56 arbitrary bits in the ME field. The CA field indicates information about the capabilities of the employed transponder, while the 24 bit AA field carries the unique ICAO aircraft address which enables aircraft identification. Finally, the PI-field provides a 24 bit CRC to detect and correct possible transmission errors. It is possible for recipients to correct up to 5 bit errors in 1090ES messages using a fixed generator polynomial of degree 24.

This quick overview shows that only the 56 bit ME field can be used to transmit arbitrary data, i.e. utilized for a secure ADS-B solution. However, not only is it very limited in size but also typically occupied by positional and other data. Thus, the format as currently in practical use is intuitively very limiting to most types of security solutions as we will explain in more detail in this work.

B. Data Link Vulnerabilities

In this section, we discuss the vulnerabilities inherently stemming from the broadcast nature of RF communication when used without additional security measures. Contrary to wired networks, there are no practical obstacles for an attacker trying to access a wireless network such as buildings or security guards, making access control mechanisms very challenging. In [9], McCallie et al. defined a taxonomy for various possible attacks, even though their difficulty estimations have become somewhat dated with the widespread availability of cheap software-defined radios as recently illustrated in [1]. Despite this, the described attacks are ordered in increasing order of difficulty here, providing a comprehensive attacker model.

Eavesdropping: The most straightforward form among the many security vulnerabilities present in ADS-B is the act of listening in to the unsecured broadcast transmissions. This passive attack is called *Aircraft Reconnaissance* in [9]. As ADS-B is using unsecured messages over an inherently

[2]See [10] for more information on PPM and multipath.

broadcast medium, the possibility to eavesdrop is not surprising and has been mentioned since the early stages of development. Many non-adversarial services use this obvious privacy concern, e.g., to visualize air-traffic on the Internet,[3] yet eavesdropping also forms the basis for a number of more sophisticated active attacks. Furthermore, it is not only difficult to stop without full encryption but also is practically impossible to detect. A small number of countries (such as the United Kingdom) have long-standing, very general laws against listening in on unencrypted broadcast traffic which is not intended for the recipient[4] even though the technical realities render such legal approaches all but obsolete.

Jamming: Almost equally simple is the jamming attack, where a single node (both ground stations or aircraft) or an area with multiple participants is effectively disabled from sending/receiving messages by an adversary sending with sufficiently high power on the 1090MHz frequency of Mode S. It has generally also been proven feasible to do reactive jamming in real time, targeting only packets which are already in the air as assessed in [11]. While jamming is a problem common to all wireless communication, the impact is severe in aviation due to the system's inherent wide open spaces which are impossible to control as well as the importance and criticality of the transmitted data.

Message Injection: On the next higher level of difficulty, it is also possible to inject non-legitimate messages into the air-traffic communication system. Since no authentication measures are implemented at the data link layer, there is no hurdle at all for an attacker to build a transmitter that is able to produce correctly modulated and formatted ADS-B messages. See [1] for more details on how to conduct an attack with limited knowledge and very cheap and simple technological means which have been easily and widely available for some time. As another direct consequence of missing authentication schemes, a node can deny having broadcasted any (false) data and/or claim having received conflicting data, making any kind of liability impossible. Concrete attack instances that use message injection include [9]:

- Ground Station Flood Denial
- Aircraft Flood Denial
- Ground Station Target Ghost Inject
- Aircraft Target Ghost Inject

Message Modification: Modifying messages during transmission is typically done via two different approaches, overshadowing and bit-flipping. Overshadowing means that the attacker sends a high-powered signal to replace part or all of the target message. Bit-flipping on the other hand has the attacker superimposing the signal converting any number of bits from 1 to 0 (or the other way around). In both cases arbitrary data can be injected without the knowledge of any of the participants. Message modification can be regarded as even more sinister than the injection of a completely new message, since the manipulated message was originally legitimate. The feasibility of such message manipulation has recently been shown in [12] and [13]. Concrete attack examples are [9]:

- Virtual Aircraft Hijacking
- Virtual Trajectory Modification

Message Deletion: Legitimate messages can be physically "deleted" from the wireless medium by utilizing destructive or constructive interference. Destructive interference means transmitting the inverse of the signal broadcast by a legitimate sender. Due to superposition, the resulting signal should be erased or at least highly attenuated but in practice this approach has very precise and complex timing requirements, making it extremely challenging.

Constructive interference on the other hand does not require synchronization but simply causes a large enough number of bit errors. Since Mode S extended squitters' CRC can correct a maximum of 5 bit errors per message, if a message exceeds this threshold, the receiver will drop it as corrupted. While effectively destroyed, the receiver might at least be able to verify that a message has been sent, depending on the implementation and the circumstances. In any case, it is more subtle than complete jamming of the 1090MHz frequency. Message deletion is key to the following attacks [9]:

- Aircraft Disappearance
- Aircraft Spoofing

C. Identification of System Requirements

There are a number of demands on a security approach for ADS-B, stemming from the way it is needed to work in practical real-world aviation settings and the characteristics of the broadcast approach. We first codify the model and then follow up with an analysis of what we need to have as security primitives in air traffic control systems.

Network Properties:

- The assumed network model consists purely of unidirectional broadcasts. Although there is a growing body of research on Aeronautical Ad hoc Networks (AANETs) that provide multi-hop communication [14], the present real-world implementation is based on **single-hop unidirectional broadcast links**. Aircraft broadcast their position, velocity and direction in plain-text periodically every few hundred milliseconds, a concept called beaconing. Thus, in the following we concentrate mainly on the so-called beacon-based security.
- We **do not consider any type of energy constraints** in association with ADS-B devices.

[3]Prominent examples are flightradar24.com and radarvirtuel.com among many others.

[4]Section 48 of the Wireless Telegraphy Act of 2006 states that (1) "A person commits an offence if, otherwise than under the authority of a designated person— (a) he uses wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of a message (whether sent by means of wireless telegraphy or not) of which neither he nor a person on whose behalf he is acting is an intended recipient, or (b) he discloses information as to the contents, sender or addressee of such a message."

- Furthermore, there are **no significant computational constraints** with neither ground stations nor ADS-B units employed in aircraft.
- **Reliability has not been a major concern** yet, as some lost packets do not normally cause a problem. Indeed, the protocol does have no means to prevent collisions, the sender will not retransmit any packets and no guarantees are given. Loss is dealt with on higher layers. This is also reflected in [1], which shows that the packet error rate tends to hover around a mean of 33 %, independent of the channel. This means that there is some substantial packet loss on the physical layer that is likely to increase when the channel utilization rises over the next decades due to the mandatory ADS-B roll-out. This will be reinforced by the ever-increasing flight traffic,[5] especially in high-density airspaces.
- **The network is ad hoc and highly mobile.** Many nodes are moving at a velocity of up to 1,000 km/h or more. It is therefore extremely dynamic and communication between two nodes may last only a few seconds. Aircraft trajectories are principally not physically restricted, although there are often common routes and also air spaces restricted due to policies do exist.
- **The network is long range**, typically ADS-B is considered to be feasible at distances of 100 NM and more.[6]
- In contrast to other, independently deployed wireless (sensor) networks the **undetected physical capture of legitimate nodes is not the most important concern.** Legally having access to a legitimate ADS-B node, however, is not considered very difficult, at least when taking general aviation into account.

Security Attributes: Perrig and Tygar [16] identify two large themes around which secure broadcast revolves: First, make sure that receivers know that any received information comes from the appropriate sender, and second that senders can freely limit the recipients of broadcasted information. In light of the recently exploited inherent vulnerabilities of the ADS-B system with cheap off-the-shelf hardware [2], [1], this is quickly becoming the most important topic in ADS-B research. Based on the model defined above, any security scheme for ADS-B would have to satisfy the following properties:

- *Data integrity*: Ensures that the data is the same as has been provided by the sender and has not been modified by any third party.
- *Source integrity:* Ensures that a message originates from the participant that claims to have sent it.
- *Data origin authentication*: Ensures that a message originates from the location claimed in a message.
- *Low impact on current operations:* A scheme should be compatible with the current ADS-B installations and not overly affect both hard- and software standards.
- Sufficiently *quick and correct detection* of incidents.

[5]Growth rate forecasts from market analysts suggest a 5.1% increase per year between 2010 and 2030. Cargo traffic is expected to grow even more at 5.6% per year in the same time frame [15].

[6]Aviation typically uses the nautical mile, also abbreviated as nmi, as a distance measure which is 1,852m.

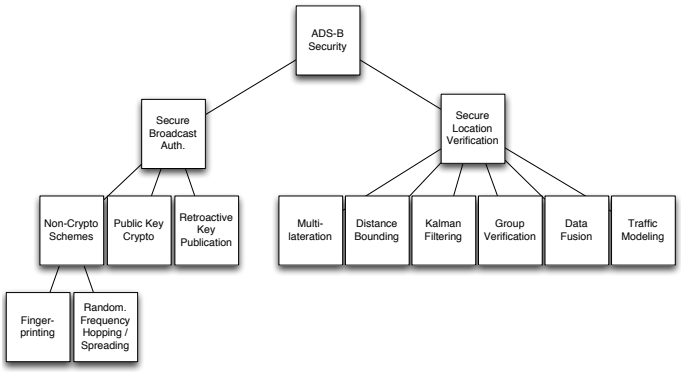

Figure 3. Taxonomy of ADS-B Security

- Needs to be *secure against DoS-attacks* against computing power.
- Any approach *needs to be easily scalable*. This is in respect to both a locally rising aircraft density and globally increasing aircraft traffic. The strain on the heavily used 1030 MHz channel should not measurably increase (e.g. due to an increased number and/or larger packets).
- *Robustness to packet loss.* A jammed wireless channel should decrease neither security nor reliability of the scheme.
- Achieving *non-repudiation* is seen as nice to have but not very high on the priority list for immediate air traffic security and is more of a legal topic.

III. Outlining Solutions

Substantial work has already been done on ADS-B security over the last decade and several approaches have been proposed in the literature to enhance ADS-B security in particular. Furthermore, a large amount of research has been done in related fields such as vehicular ad hoc networks (VANETs) or wireless sensor networks where broadcast authentication and security also play an important role. While some ideas may not be directly applicable to the aforementioned model and requirements of ADS-B, it might be possible to adapt them to the changed use case at hand. If not, besides the advantages and disadvantages of every approach we also list the major obstacles.

The remainder of this section first presents overview works in the community concerned with the security of ADS-B as a whole. We then consider ADS-B's sister protocols ADS-C and military versions of ADS-B in our context before analyzing all collected ideas in detail in the following sections.

As shown in the taxonomy in Fig. 3, we identified two distinct approaches to securing ADS-B: **Secure Broadcast Authentication** and **Secure Location Verification**. Consequently, Section IV examines the various schemes that apply asymmetric properties (cryptographic and non-cryptographic) to directly authenticate broadcast communication while Section V reviews several different methods that seek to verify the authenticity of location claims made by aircraft and other ADS-B participants.

A. Previous Works on ADS-B Security

Securing ADS-B communication was not a very high priority when it was specified to be the new standard in civilian secondary surveillance. Neither the RTCA standards [6], [7], [8] nor other requirements documents [17], [18] mention security in this context. However, security problems in ADS-B have been well-known for a long time, mostly because they are relatively obvious to the interested researcher.[7] For instance, weak ADS-B security has recently got very broad reporting in the mainstream press[8] due to two talks at the DEFCON and Black Hat security conferences.[9]

Sampigethaya and Poovendran [19], [20] first analyse the security and privacy of ADS-B and other related and unrelated communication systems which are part of the so-called "e-enabled aircraft". McCallie et al. [9] provide a current security analysis, focused on the nature of possible attacks and their difficulty. They give a systematic high-level overview and propose general recommendations for addressing ADS-B's problems. Costin and Francillon [2] as well as Schaefer et al. [1] analysed ADS-B security, too, focusing on the ease of exploiting ADS-B with current hard- and software and offering some possible countermeasures.

Kovell et al. [21] mention data fusion with other systems, multilateration and various cryptographic schemes as state of the art research on ADS-B security. They further conduct a more thorough analysis on Kalman filtering and group validation concepts and proposed mitigation methods. Nuseibeh et al. conduct an example of a formal security requirements analysis of ADS-B [22], proposing multilateration to deal with possible attack scenarios. Burbank et al. [23] present general concepts for communications networking to meet the requirements of future airspace systems, i.e. a vision of a mobile ad hoc and wireless networking concept for use in both the terminal area and in the en-route airspace. Li and Kamal [24] analysed the security of the whole FAA's Next Generation Air Transportation System (NextGen) of which ADS-B is a core component.[10] They develop a high-level defense-in-depth framework for analyzing NextGen and mention general secure communication approaches such as encryption, authentication and spread spectrum as part of the ADS-B security layer.

B. ADS-C

A theoretical, currently already available, way to deal with suspicious ADS-B participants would be to ask them to switch to the connection-oriented ADS-C (ADS-Contract, also known as ADS-Addressed). However, ADS-C also has a number of very severe inherent shortcomings, some of which are described by the ICAO: [26]

- It requires the installation of additional avionics (for data communications): FANS 1/A or ATN.
- Performance may be determined by the limitations of the communications media.
- A cost may be associated with the transmission of each report since the data is carried by a data link service provider:
- It does not support ASA because the messages are not directly available to other aircraft.

Overall, the current implementation of ADS-C over the outdated ACARS network[11] considerably limits its usefulness. It is also violating the basic assumptions of ADS-B, being a system that sends on demand instead of periodically broadcasting without being requested, which is why it is not considered any further.

C. Communication in Military Avionics

There is undoubtedly a much stronger need and motivation to implement stringent security in a military communications context. Though it is not the primary focus of this work, anything in practical use by military forces could naturally be of interest for civil security solutions as well. There are various standards currently in use by the US and NATO military, among them the cryptographically secured Mode 4 and Mode 5 as defined in the STANAG 4193 specification. Mode 4, which employs a 3-pulse reply to a challenge, has been in use for decades and according to the forecasts of the NATO Minimum Military Requirements is to be superseded by Mode 5 in 2015 (initial operational capability) and 2020 (full operational capability), respectively [27].

While the legacy Mode 4 indeed only allows airplanes to respond to challenges, Mode 5 adopts the ADS-B broadcast capability, so participants can announce their presence without a prior query, very useful in identification, friend or foe (IFF) [28]. On the security side, Mode 5 uses proprietary hardware and encryption algorithms with a black key concept;[12] it furthermore offers time-of-day authentication, automatic switchovers and a longer period [29]. The signal modulation is done via spread spectrum and operation requires a platform identification number (PIN). Mode 5 hardware is equipped with a unique identifier that informs about national origin and the platform number. Mode 5 has two different levels: Level 1 is the interrogation response mode, providing time, position and identification based on both GPS and traditional means. Level 2 is the broadcast mode and entirely based on GPS. There are currently no further available details on the security mechanisms, including the applied cryptography, of Mode 4 and 5 since this information is classified.

The ADS-B specification itself also mentions the message types/downlink formats Military Extended Squitter (DF19) as well as Military Use Only (DF22) without detailing them further, although it is known for example that DF19 makes ample use of bursts instead of regular beacon messages only [30].

[7] Especially on the Internet broad warnings have been floating around as early as 1999, e.g. http://www.airsport-corp.com/adsb2.htm, http://www.dicksmithflyer.com.au/cat_index_36.php

[8] E.g. http://www.forbes.com/sites/andygreenberg/2012/07/25/next-gen-air-traffic-control-vulnerable-to-hackers-spoofing-planes-out-of-thin-air/

[9] http://www.blackhat.com/usa/bh-us-12-briefings.html#Costin

[10] Although certainly not the only safety-critical wireless module. See e.g. [25] for concerns about the impact of GPS integrity on aviation safety.

[11] The Aircraft Communications Addressing and Reporting System (ACARS) will be superseded by the Aeronautical Telecommunications Network (ATN) and IP communication over the next decade.

[12] Black keys are safe to transmit since they are encrypted with a key encryption key. Red keys on the other hand are unencrypted and classified as highly sensitive.

Format #	DF					Military Extended Squitter
19	1 0011	AF : 3	Military Application : 104			

Figure 4. DF19 data format [30]

IV. Secure Broadcast Authentication

Secure Broadcast Authentication is one possible means to prevent and/or detect attacks in a unidirectional broadcast network such as ADS-B. This section will describe the various methods that have been proposed in the literature, typically for wireless sensor networks or VANETs and analyse their applicability to ADS-B.

Authentication of messages on a broadcast medium is hard, compared to point-to-point communication. A symmetric property is only useful in point-to-point authentication where both parties trust each other. Thus, an asymmetric mechanism is inherently required so that receivers can *verify* messages but are not able to *generate* authentic messages themselves [31]. For a good overview over secure broadcast communication in general, the reader is referred to [16].

The goal is to keep the open nature of ADS-B intact while offering a potential authentication mechanism. This could be done either globally or only selectively in cases where suspicious behaviour has been detected. Such reactive authentication could lessen the strain on the network by only requiring additional security (and thus computational and communicational overhead) at times when incidents seem more likely.

Furthermore, there is a distinction between broadcast schemes that are user-based vs. those that are node-based, or possibly both. Node-based (also known as host-based) schemes ensure the authenticity of a given node, i.e. the hardware. User-based schemes on the other hand look to authenticate a human user, regardless of the underlying hardware [32]. This work focuses mainly on node-based schemes.

A. Non-Cryptographic Schemes on the Physical Layer

Non-cryptographic schemes such as fingerprinting comprise various methods for wireless user authentication and device identification techniques, either based on hardware or software imperfections or characteristics of the wireless channel which are hard to replicate. The goal is to identify suspicious activity in a network. Finding a signature for legitimate beacons in a network, possibly being able to tell apart ground stations from aircraft, identifying the type of aircraft or even individual machines provides data useful for the development of an intrusion detection system [33]. If there are tangible differences between legitimate and non-legitimate packets on the physical layer, then machine learning techniques could be employed to develop a model for predictions of normal behaviour and also statistical thresholds beyond which an activity is considered suspicious. Even if it is only feasible to identify classes of devices instead of singular participants, this could prove to be valuable information in detecting intruders. Yet, fingerprinting does not provide surefire security in any way, and various attacks and concerns have been brought forward [34].

Currently, there have been no attempts at applying any kind of non-cryptographic schemes to boost the security of ADS-B. A common counter-argument has been the fact that contrary to e.g. the 802.11 markets the commercial airplane market is divided into two big players (Boeing and Airbus) which in the long run makes significant differences at least between ADS-B vendors unlikely. Still, fingerprinting has also been successfully employed to tell apart the exact same models from the same vendor. For a good overview of the state of the art in physical-layer identification of wireless devices, see [33].

Zeng et al. [35] broadly identified three different techniques that can be employed to enhance or even replace traditional cryptographic measures: Software, hardware and channel-based fingerprinting.

a) Software-Based Fingerprinting: This type of fingerprinting techniques tries to exploit distinctly different patterns or behaviour of software operating on wireless equipment. Depending on the specification of a protocol, there is a lot of leeway for manufacturers and developers when implementing software on a given device. If there is enough entropy in information about the combination of chip sets, firmware, drivers to tell apart different wireless users, this approach can be used to verify their continuity up to a certain degree. As a downside, it seems likely that large fleets of airline operators are fitted with very similar or same hardware, making them harder or even impossible to differentiate and on the other hand easier to study and copy for a potential attacker.

b) Hardware-Based Fingerprinting: A number of techniques have been proposed to identify devices based on unique hardware differences. Some of these differences can be used for *radiometric fingerprinting*, exploiting differences in the turn-on/off transient or the modulation of a radio signal to build unique signatures. While this works well for non-mobile cases and attackers with standard, off-the-shelf hardware, it can break down against more powerful adversaries employing software defined radios and be subjected to signal/feature replay attacks [33]. Furthermore, the existing research captured signals very closely to the fingerprinting antenna (15m or less) and in non-mobile settings, making it very improbable to work in the highly-dynamic, large-distance ADS-B setting.

Another unique hardware feature amongst wireless devices is *clock skew*. As no two clocks run precisely the same, this can be used to create signatures and enable identification. Unfortunately, to exploit this, we would require timestamps included in ADS-B messages. Also, it is possible for an attacker to eavesdrop on the communication and mimic the appropriate clock skew [36].

Recently reviewed options for future systems include the use of so-called physically unclonable functions (PUFs), which essentially exploit specifically implemented circuits to create unique and secure signatures, thus abandoning the scope of non-cryptographic solutions.[13] Furthermore, besides

[13]For a good overview on PUFs, see [37]

requiring new hardware, this approach also necessitates an overhauled messaging protocol, including a challenge and response model [38], making it a difficult fit for the requirements of the ADS-B protocol.

c) Channel/Location-Based Fingerprinting: Exploiting natural characteristics of the physical layer has been a hot research topic in relation with security in wireless networks. Various approaches have shown that this can be a viable alternative to more traditional authentication and verification measures, typically based on received signal strength (RSS, e.g. [39]), channel impulse response (CIR, e.g. [40]) or the carrier phase (e.g. [41]). They are comparably easy to implement in wireless systems and can offer reasonable security without requiring much overhead.

Any such concept requires bidirectional communication, however. One practical example is the retroactive authentication of data packets via an RSS list as proposed by Zeng et al. in [35]. As this temporal RSS variation authentication (TRVA) requires an ACK packet in a given coherence time, it is not compatible with current ADS-B protocols. Furthermore, it is doubtful if this could work with reasonable efficiency in a highly dynamic environment such as airborne MANETs. The coherence time T_C in which the channel stays stable in a wireless network where only one sender moves at 800km/h is roughly 0.6188ms. At a 1090ES bandwidth of 1 symbol/μs it is obvious that such protocols are impossible to deploy. This physical property also effectively denies the application of many other more sophisticated physical-layer schemes such as SecureAngle [42], which aims at securing wireless networks by using multiple antennas capturing the angle of arrival information of nodes to built signatures and detect anomalies. Similarly, practical indoor location-based geo-tags, built with surrounding radio frequency signals such as done in [43] are not applicable.[14]

Laurendeau and Barbeau [44], [45] exploit RSS similar to time difference of arrival concepts (see V-A) to localize malicious insiders in a vehicular ad hoc network with the help of various receivers. Taking into account that an attacker will not be inclined to cooperate and can even actively fake the signal strength he utilizes, their proposition enables the receivers of a message to at least identify a given area where it must have originated from.

d) Randomized/Uncoordinated Frequency Hopping / Spreading: A physical-layer scheme different from fingerprinting, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are both used in wireless systems to improve protection against malicious narrow band and pulse jamming as well as eavesdropping. In their usual form they both require a pre-shared spreading code or hopping pattern between sender and receiver which makes it hard to follow or hinder the communication for anyone without access to the code/pattern. This is also exploited in military communications (see Section III-C) but is not a viable option for world-wide civil and commercial ATC where such secret codes would presumably not stay secret for long.

[14]Although one advantage is that many legacy Mode S systems use several directional rotating antennas to pick up ADS-B signals. The extracted information about the angle-of-arrival could conceivably be used to raise red flags, as described in Section V-F.

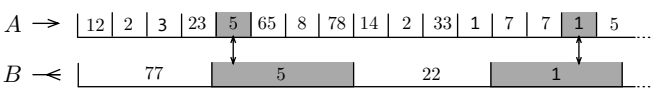

Figure 5. Uncoordinated Frequency Hopping after [46]. Both A and B regularly change their communication frequencies without having pre-established a common pattern. By statistical chance they will communicate on the same channel every so often.

The need for a pre-established code can be relinquished by employing random, uncoordinated versions of FHSS and DSSS. Strasser et al. [46] propose such a physical layer approach to counteract jamming in wireless broadcast scenarios. Uncoordinated Frequency Hopping (UFH) provides a viable way to broadcast initial messages without an attacker being able to jam the transmission in an efficient way. The key insight to these approaches is that, contrary to normal frequency hopping mechanisms, sender and receiver(s) rely on the statistical chance to be on the same channel at the same time. The obvious downside of UFH is its low bandwidth due to the fact that many times receivers will not listen on the correct channel. More concretely, the probability with UFH that a packet will be received at a node without an attacker being involved is $p_m \geq 1 - (1 - \frac{c_s}{c})^{c_r}$ (c being the number of possible channels, c_s and c_r the number of channels a sender/receiver is using simultaneously).

Based on the same principle are Uncoordinated Direct-Sequence Spread Spectrum (UDSSS) [47] and Randomized Differential DSSS [48]. Both these techniques rely on the statistical chance that spread codes randomly chosen by sender and receiver(s) will happen to be the same every so often.

While the proposed methods can effectively defeat jamming and modification attacks, the inherently lower performance and a prolonged transmission time make them difficult to use in a large-scale system such as ADS-B. Furthermore, authentication and security against replay attacks is only achieved by adding a private/public key infrastructure and timestamps, respectively.

B. Public Key Cryptography

Cryptographic measures have been a tried and tested means to secure communication in wireless networks and must subsequently also be considered in the ADS-B setting. One question to examine is if the current implementation of ADS-B can be encrypted. The first possibility would be to distribute the same encryption keys to all ADS-B participants worldwide, or at least to aircraft and ground stations in a given area. Such a vast group encryption scheme, including even general aviation, would be considered extremely insecure to both inside and outside attacks. This inherent weakness is non-fixable even with very frequent key updates (which also would again increase the complexity of the encryption deployment). In short, such a scheme would fulfill none of the required

criteria listed in Section II-C. Finke et al. [49] examine various encryption schemes, including the possibility to do the key management for symmetric encryption out of band, for example through the controller-pilot data link communication (CPDLC) which they consider worth exploring further. The authors also give an analysis of the security and practicability of asymmetric, symmetric and format preserving encryption. In their conclusion, they support a symmetric cipher using the FFX algorithm which can encrypt non-standard block sizes (i.e. ADS-B's 112 bit messages) with sufficient entropy. However, the difficulties concerning key management and distribution are widely acknowledged.

As mentioned before, if broadcast authentication is needed, one requires an asymmetric property, a characteristic fulfilled by public key cryptography. Samuelson and Valovage [50] report on an implementation of authentication and encryption in UAT using a public key infrastructure (PKI). Their method uses a hash to create a message authentication code (MAC) that can be used to authenticate the message and can be extended to full encryption but no further details are publicly available. There are related patents filed under the names "Secure ADS-B Authentication System and Method" [51] and "Automatic Dependent Surveillance System Secure ADS-S" [52] by Sensis Corporation.[15] The general idea is to use a challenge/response format with an authenticator ground station, who authenticates every participant in its reach and notifies a higher authority and/or all other participants of any failed authentication. This concept requires the station to have access to a worldwide database of secure keys that is both hard to maintain globally as well as subject to possible security breaches. if this is the case, the system can be used to not only identify ADS-B participants but also pilots and various other people/systems taking part in the flight process. Furthermore, ADS-S includes a changed modulation and complete overhaul of the messaging system, making it incompatible with ADS-B and as such very costly and extremely doubtful to be deployed widely in the future.

Costin et al. [2] suggest a "lightweight" PKI solution which essentially amounts to a retroactive part publication of the key as discussed in Section IV-C: Aircraft A transmits the signature distributed over a number N of ADS-B messages, so that after every N messages the surrounding participants have received A's signature. The recipients keep the messages until the full signature has been transmitted, at which point they can authenticate the buffered messages. The authors suggest that the PKI key distribution necessary for this scheme could be done during an aircraft's regular check-ups.

Ziliang et al. [53] present a concrete PKI solution for data authentication in ADS-B/UAT based on Elliptic Curve Cipher and X.509 certificates. The authors try to tackle a number of problems involved with cryptography such as key size length and keeping the broadcast nature of ADS-B. UAT offers much longer messages than 1090ES, with payloads of 16 or 32 bytes when transmitted from aircraft and even 464 bytes in ground message bursts [54]. Yet, their conclusion is that the data block format needs to be changed, no matter which type of cryptography is used. Consequently, they propose and implement their authentication scheme with a slightly changed UAT message type. In 1090ES, this scheme would require not only using the DF24 Extended Length Messages available in the Mode S standard but still need 5 messages to divide and accommodate the signature data and timestamps, a solution that hardly looks scalable in an already crowded frequency. On top of this, the description leaves very much open the question of an efficient certificate distribution scheme.

[15]Now owned by defense contractor Saab AB.

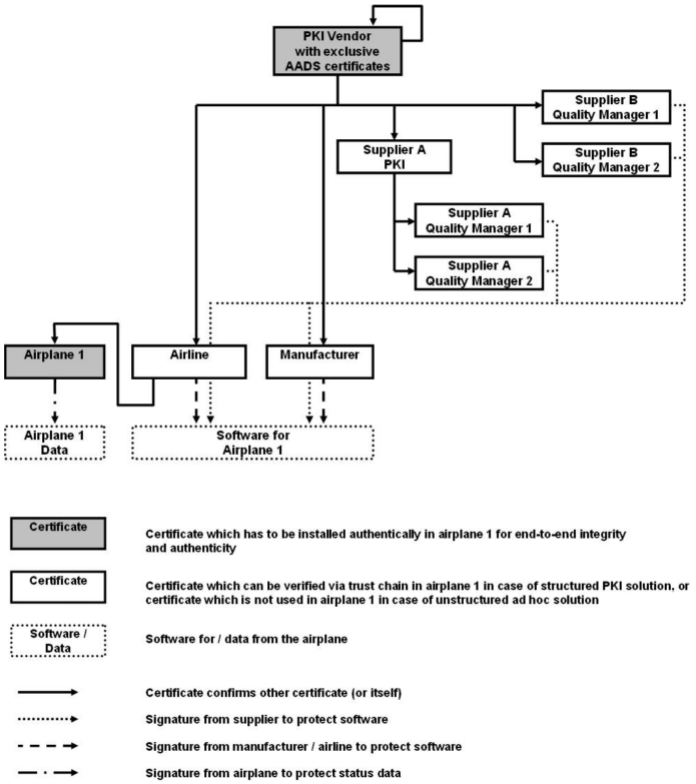

Figure 6. Outline of a public key infrastructure from [57]. A PKI vendor supplies airlines, manufacturers and external suppliers with the required certificates.

Raya and Hubaux [55], [56] discuss using Public Key Cryptography in VANETs. In short-range scenarios with beacons sent every 100-300ms and up to 120 mobile nodes in a 300m communication range, they calculated with message sizes from 294 to 791 bytes (depending on the system) and found the performance to be acceptable in simulations.

Robinson et al. [57] analyse various different solutions to create PKI infrastructures for a general airplane assets distribution system (AADS). Although, the work is not discussing the ADS-B protocol but instead focusing on the distribution of software and data on the ground, the authors identify the airline industry's needs and requirements from a PKI infrastructure, and it seems plausible that the same system could be used to secure air traffic control data. According to their analysis, an ad hoc approach employing pre-loaded trust certificates and without a central authority could be used as a short-term solution until a more structured, long-term public key infrastructure has been developed (see Fig. 6 for an outline of their proposal).

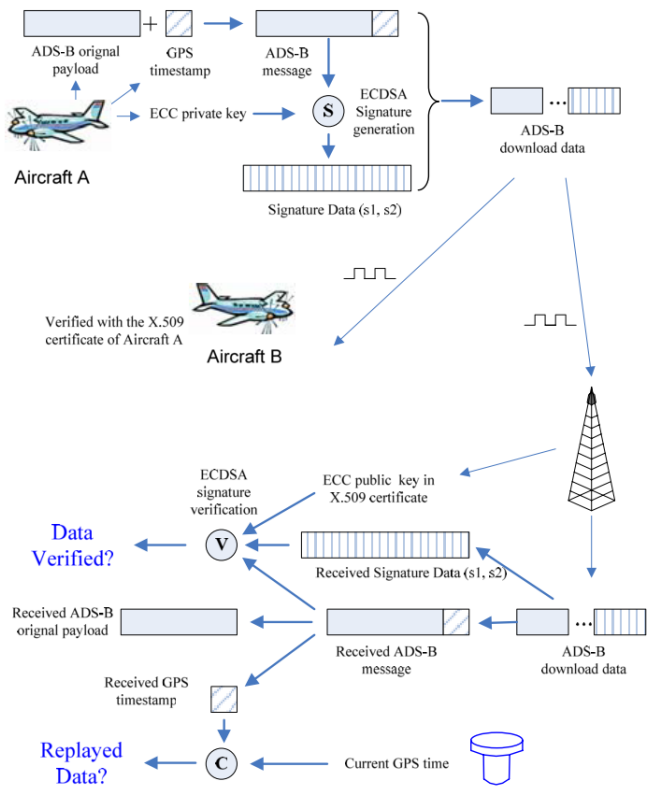

Figure 7. Example of a typical encryption scheme adapted for ADS-B from [53]. It employs elliptic curve cryptography to generate signatures which can be verified with the responding certificate by other aircraft and ground stations. An additional GPS timestamp prevents replay attacks.

The obvious idea for a centralised key distribution would be to have aviation authorities such as the FAA act as a certificate authority (CA). But assuming the role of a CA is no easy task, even many specialized institutions had to report numerous security breaches over the last decades. Furthermore, if this problem is sufficiently solved, there remains the question of how aircraft from airspaces mandated by different authorities can securely communicate with each other. These challenges are somewhat analog to the same approach in vehicular networks as discussed in [58] but arguable even worse due to the large internationalization of the ADS-B network.

There are certain natural disadvantages to using an encryption solution that cannot be overcome (or only with great difficulty) as mentioned in [59]:

- Despite the encryption of data frames, management and control frames are not protected.
- It immediately and unmitigatably breaks compatibility with the installed base.
- Key exchange is notoriously difficult in ad hoc networks, which are by definition without a centralized institution. They are often too dynamic, requiring constant adaptation. This would result in too much overhead in both the number as well as the size of messages.
- The open nature of ADS-B is widely seen as a feature. A cryptographic system implemented in a way comparable to ADS-S does not offer public broadcast communication.
- One-time signatures even using advanced techniques such as Merkle-Winternitz prove infeasible due to their overhead of 80 bytes and more, simply to sign 60 bits [31].

To conclude this section, it is generally difficult to build any kind of encryption scheme with the currently accepted 1090ES data link. Approaches have been shown to be theoretically possible with the higher bandwidth UAT, although practical proof of scalability and practicability have not been given yet. Furthermore, at this point in time it does not seem likely that UAT will play a role apart from general aviation in the FAA-mandated airspace. So, while UAT offers more technical possibilities not only for security and encryption, and even combined UAT/1090ES transmitters are neither a technical nor a regulatory problem,[16] traditional cryptography in conjunction with the current installment of ADS-B does not seem like a worthwhile route for further research at the present.

C. Retroactive Key Publication

A variation on traditional asymmetric cryptography is the technique of having senders retroactively publishing their keys which are then used by receivers to authenticate the broadcast messages. This approach that has been proposed for use in various fields [60], [16]. The key concept is simple: Any broadcasting entity produces an encrypted message authentication code (MAC) which is then sent along with every message. After a set amount of time or messages, the key to decrypt this MAC is published. All listening receivers, who have buffered the previous messages, can now decrypt the messages and ensure the continuity of the sender over time.

The TESLA (Timed Efficient Stream Loss-Tolerant Authentication) protocol [61], standardized in RFC 4082,[17] can provide efficient broadcast authentication on a large scale, while being able to cope with packet loss and real-time applications. The µTESLA broadcast authentication protocol is the adaptation of TESLA for wireless sensor networks [62].

Both TESLA and µTESLA use one-way key chains as shown in Fig. 8: The broadcaster chooses a random key K_n and applies a public pseudo-random function F as often as required to acquire the keys: $K_i = F(K_{i+1})$, $0 \leq i \leq n-1$. Subsequently, every secret $K_i, i > 0$ is used for sending in the i-th interval and disclosed to the public after a number of time intervals d. As every previous key K_i with $i < j$ can be recovered by the receiver(s) by applying the one-way function F, the receiver needs to do two things to authenticate a message: [48]

1) Authenticate the key K_i against previously received keys to ensure they are from the same key chain.

[16] "There is nothing in the regulations and there are no technical hurdles that would prevent a manufacturer from building a combination UAT/1090ES box, one that would eliminate the different-technology blind spots while allowing high-flying aircraft the ability to get FIS-B through UAT." http://www.flyingmag.com/technique/proficiency/ins-and-outs-ads-b

[17] "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", http://www.ietf.org/rfc/rfc4082.txt

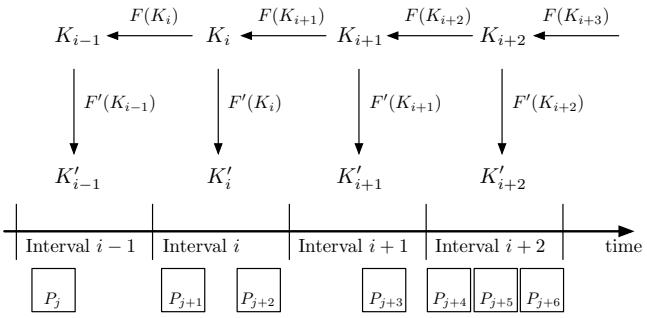

Figure 8. The figure illustrates TESLA's utilization of one-way chains after [61]. The first one-way function F generates the chain, following that the second one-way function F' derives the MAC keys. Time is divided into separate intervals i, all having the same length. The packets P_j are each sent during one specific interval. For every such packet, the sender computes a MAC with the key that is in accordance with that interval. E.g. P_{j+2}'s MAC is calculated based on its data and key K'_i. Disclosing the keys of previous intervals can be done either by attaching the key to sent packets or in separate messages.

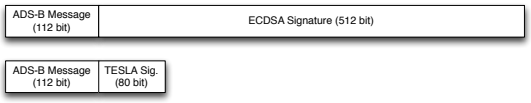

Figure 9. TESLA signatures vs. ECDSA signatures. Tesla signatures cost significantly less overhead compared to many other cryptographic solutions.

2) Ensure that the message with key K_i could only have been sent before the key has been published (requiring loose time synchronization), i.e. before interval $i + d$.

The fact that µTESLA uses symmetric cryptography in connection with time as its asymmetric property makes it an interesting idea for adaptation to ADS-B since sufficiently good time synchronization could be provided via GPS (this would require sending the GPS timestamps in a new protocol field since this is not currently the case). The advantages of µTESLA are obvious: ADS-B keeps its open and broadcast nature and a complex PKI infrastructure is not required to ensure a sender's continuity, although it could be added if identification and source integrity are required (e.g. solely for well-connected ground stations). Nonetheless, it enables a participant to protect itself against impersonation attacks. In areas well-served by ground stations any break in continuity detected by any single one of them would immediately set off red flags.

Another advantage of µTESLA is that lost packets on the notoriously jammed 1090 MHz frequency (there is no medium access control in place) are not an integral problem for authentication. Furthermore, the overhead for communication as well as required modifications to the ADS-B protocol are significantly less than with traditional asymmetric cryptographic methods.[18]

On the other hand, µTESLA also has some disadvantages when applying it to AANETs. There is a need to reinitialize it (if used for identification) and it can be susceptible to memory-based DoS (depending on the setup of the receiver). To counter this, Eldefrawy et al. [63] propose an approach that utilizes forward hashing using two different nested hashes and the Chinese Reminder Theorem, resulting in a system that does not need to be reinitialized.

Haas and Yu [64] compare TESLA and ECDSA-based authentication by simulating their performance in a real-world VANET scenario (although not including certificate distribution). Regarding channel congestion and MAC layer delay they found that the TESLA protocol with keys attached to a following broadcasts performed significantly better than ECDSA or a TESLA-scheme that publishes keys in separate packets.

Hu and Laberteaux [65] discuss a combination of a full-blown PKI infrastructure with CAs distributing 512 bit signatures to bootstrap 80 bit TESLA signatures for short-term authentication in VANETs. Such a system offers comparably lightweight integrity and possibly on-demand authentication, if needed and requested.

V. Secure Location Verification

Besides securing the communication - and thus the location data - of ADS-B, there are other approaches to ensure the integrity of air traffic management. The general idea of secure location verification is to double check the authenticity of location claims made by aircraft and other ADS-B participants. This is inherently different to the verification of the broadcast sources and messages. The baseline is to establish means to find the precise location of a sender, effectively offering some redundancy and thus the ability to double check any claims made. As an additional advantage any such approach creates more location data, which can be merged with ADS-B and radar and offer a back-up system in case of failure of these primary navigation systems or GPS.

A. Multilateration

Multilateration, or hyperbolic positioning, is a popular form of *Co-operative Independent Surveillance* and has been successfully employed for decades in military and civil applications. If the precise distance between four or more known locations and an unidentified location can be established, it is a purely geometric task to find the unknown point. We can, for example, use the received ADS-B signals which travel at the speed of light to estimate the distance. Since we do not know the absolute time a message needed to travel from an airplane to a receiver, we have to employ the time difference of arrival (TDOA).[19]

Thus, multilateration requires a number of antennas in different locations that receive the same signal at different times. From the TDOA, hyperboloids can be calculated on which the aircraft's position must lie. With four or more receivers, a 3D position can be estimated by finding the intersection of the hyperbolas as shown in Fig. 10.

[18]The original µTESLA requires a 6 byte MAC.

[19]For a full explanation of the multilateration process in aviation see e.g. [66] or [67].

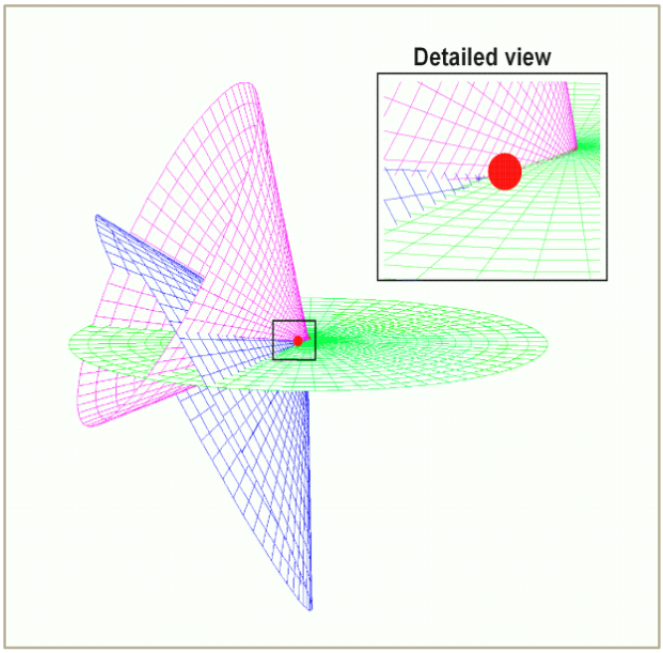

Figure 10. Intersection of three hyperboloids from [68]. With four receivers in a 3D setting, one can specify the origin of the message as the red point where the computed hyperboloids intersect.

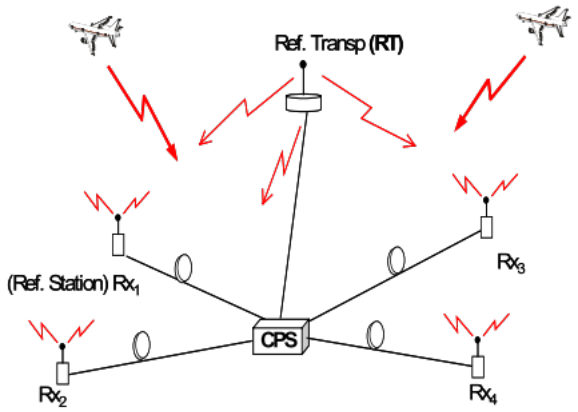

Figure 11. Basic multilateration architecture from [69]. Four (or more) receiver stations (Rx) measure the time at which they receive the same message from an aircraft. They send this data to the central planning station which can calculate the aircraft's position from the time difference of arrival between the receiver stations.

Performing multilateration by utilizing TDOA is currently the preferred solution for location verification on the ground. It is used in the field (e.g. by the ASDE-X system [70]) at various US airports[20] and also being rolled out in Europe in connection with the CASCADE project.[21] One major advantage of multilateration is the fact that it can utilize aircraft communication that is already in place. Thus, there are no changes required to the currently existing infrastructure in aircraft, while on the ground receiver stations and central processing stations have to be deployed (see Fig. 11).

While currently used mainly in comparably short distances (taxiway and runway on airports, up to about 60 m height), Wide Area Multilateration (WAMLAT) has also been a popular research topic. Compared to primary radar systems, WAMLAT is relatively easy and cost-effective to install and use on the ground but can also be successfully employed in an airborne MANET.[22] Using an estimated distance of a target between four or more receivers, it is possible to tell the 3D position of a sender with roughly 30 m accuracy (at 90 NM distance) compared to 20 m for ADS-B [71]. However, in comparison to ADS-B the accuracy of multilateration in practice deteriorates over long distances (see Fig. 12).

There have been various practical studies of multilateration using ADS-B signals. For example, [5] examines it as a method to provide a means to backup and validate ADS-B communication. Johnson et al. [72] describe their proof of concept work in a war-zone in Afghanistan. Kaune et al. [73] built a proprietary low cost test bed to do multilateration with ADS-B signals. Thomas [74] presents findings from two controlled helicopter flights in the North Sea.

Daskalakis and Martone [75] give a technical assessment of the possibility of using ADS-B and WAMLAT in the Gulf of Mexico, testing a single controlled flight with good accuracy.

A recent work at MITRE Corporation [76] analyzes the attempt to build an alternative navigation system with WAMLAT in the FAA-mandated US airspace. The authors discuss the potential use of already deployed sensors for multilateration around three airports with flat terrain, also noting that the challenge is greater in more mountainous areas. Further, they provide some sensor placement discussion, determining the optimal choice and number from a given database concerning requirements such as accuracy and low dilution of precision.

Despite its successful use in the field, multilateration leaves a number of open problems in terms of secure location verification, for example the estimation of aircraft altitudes with ground-based receivers is known to be very difficult. Galati et al. [77] discuss the theoretical application secondary surveillance radar as basis for multilateration in airport surveillance. They analyze a case study of Marco Polo airport in Venice and look at technical details such as dilution of precision and multilateration algorithms and conduct simulations with five sensors in a 25 km radius around the airport. They propose angle-of-arrival measurements to improve the unsatisfying height estimates provided by wide area multilateration.

The International Civil Aviation Organization also names a few of the known limitations of multilateration: [26]

1) Aircraft have to be equipped with a functioning transponder.
2) It is susceptible to multi-path.
3) The transmitted signal has to be correctly detected at multiple receiving stations.
4) Communication links are needed between remote receiver/transmitter sites and the master processing station.

Essentially, some of the limitations stem from cost and logistic reasons as it can be difficult and expensive to deploy enough sensors and stations in very remote and inaccessible areas.

[20] See the manufacturer's description: http://www.saabsensis.com/docs/128/

[21] http://www.cascade-eu.org

[22] Although vast open spaces such as found in e.g. Australia or over oceans can prove infeasible for the use of multilateration and have been one of the very reasons driving the development and deployment of ADS-B.

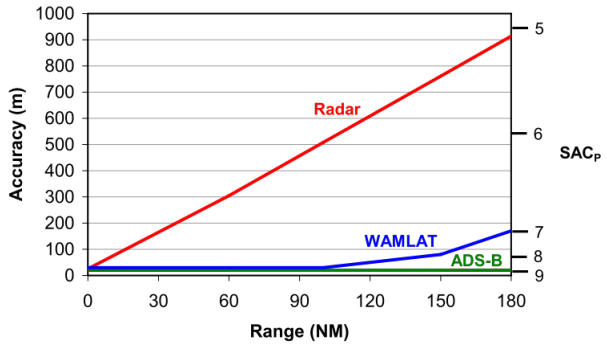

Figure 12. Comparison of location estimation accuracies when utilizing primary radar, wide area multilateration and ADS-B [5]. SAC_p denotes the Surveillance Accuracy Category for Position as defined in [5].

Furthermore, [52] mentions an attack vector for an adversary trying to fool a receiver system utilizing multilateration for location verification. An attacker would need to purchase and modify four traffic-collision avoidance system (TCAS) receivers and use a GPS/WAAS time transfer unit between the units to ensure relative timing accuracy. Furthermore, he needs to engineer an algorithm similar to the one the TCAS uses to determine aircraft's tracks. As this involves both a certain cost and non-zero engineering knowledge the difficulty of exploiting this threat is relatively high, certainly when compared with the simplicity of spoofing ADS-B messages.

In principle, there always remains the question of how to secure the communication needed to perform multilateration and relay the localisation information to the other participants. If it is not properly secured, Sybil attacks, where a number of dishonest nodes deceive their environment, are entirely possible [78].

B. Distance Bounding

Distance bounding is another method that has been employed in wireless networks to partly localize other participants and ensure secure transaction e.g. for RFID communication. First presented by Brands and Chaum in 1993 [79], the idea behind distance bounding is to establish a cryptographic protocol with the goal to have a prover P show to a verifier V that P is within a certain physical distance (see Fig. 14 for the concrete protocol). The universally valid fact that electromagnetic waves travel roughly at the speed of light c, but never faster, builds the foundation of all distance bounding protocols.[23] This enables the computation of a distance based on the time of flight between the verifier's challenge and the corresponding response by the prover. The determined distance serves as an upper-bound, an additional piece of information that can subsequently be used as a means to verify and authenticate a node by checking the truth of its claims. When distance-bounding is performed by various trusted entities (such as ground stations) these can collaborate and find the

[23]This is in contrast to e.g. distance estimation via received signal strength, which can be influenced and faked by a malicious node.

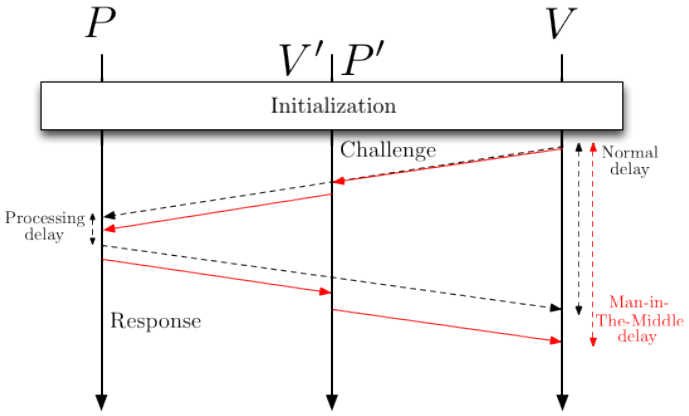

Figure 13. Principle of distance bounding protocols. The verifier V sends a challenge to the prover P who then, after processing, sends his response (black dashed arrows). A man in the middle (V'/P') can only increase the distance by adding further processing delays, but not decrease it (red arrows).

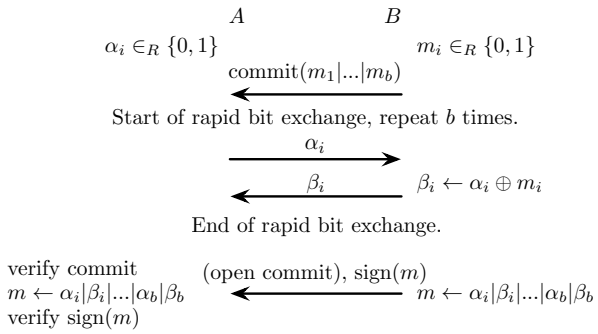

Figure 14. Original untrusting distance bounding protocol by Chaum and Brands [79]. A is the verifier, B the prover. After the protocol exchange A can verify that B is within a given distance.

actual location of the prover via trilateration.[24] There are various practical attacks on distance bounding schemes given in the literature, among them a number of relay attacks such as the so-called distance fraud, mafia fraud and terrorist fraud [80] as well as the newer distance hijacking attack [81].

Consequently, an abundance of protocols have been suggested to deal with these various deficiencies. Song et al. [82] give an example of a secure distance bounding mechanism for VANETs, comprising three steps:

1) Traditional distance bounding is used to find the lower bound of the distance between V and P. P can only increase the time to respond to V's challenge and as such only appear further away than it really is.
2) The verifier then checks the claimed location of P for plausibility (also see Section V-F):
   a) Transmission range-based verification: There are limits on the maximum distance of wireless transmission in practice. Test runs can help to find practical upper bounds for ADS-B users in a certain location/path. If the prover claims to be further

[24]Triangulation is not to be confused with the previously described multilateration. The former uses the absolute measurements of three or more distance circles to determine positions, while the latter uses the *difference* in distance between the measurements.

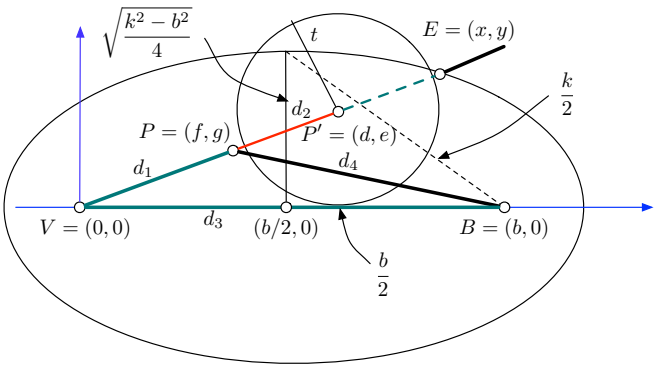

Figure 15. Network topology for a minimum distance guarantee after [82]. V is the verifier, P the prover, P' its claimed location. B is a common neighbour of both V and P who gives an estimate E of P's position. Considering the ellipse and a certain error distance, B can detect the distance enlargment of P.

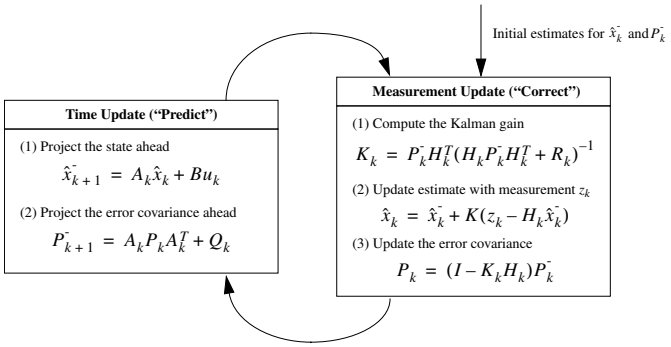

Figure 16. Basic concept of Kalman filtering from [86]. The time update step projects the measured variables and the error covariances. The measurement update step computes the Kalman gain and updates the estimates and error covariances with the actual measurements.

away, it can be considered malicious.

b) Speed-based verification: Considering the fact that the typical speed of a given airplane in differing flight stages is known (certainly the physically possible minimum and maximum velocity), consecutive position claims have to be in a given window.

3) To further improve the security, after all plausibility checks have been passed, the verifier chooses a common neighbour B. That neighbour of both P and V then gives its location estimation E for P as shown in Fig. 15. Whenever the estimate lies outside the error margin, B knows that P enlarged its distance.

While in the literature distance bounding has been used mostly for close-up, indoor communication, it has been modeled for use in VANETs up to a distance of 225 m between prover and verifier [82], [83]. Tippenhauer and Capkun [84] also considered the impact of moving targets on distance bounding protocols and verifiable multilateration. In their original implementation, it takes about 600ms to perform a full localization, which, at a speed of only 500 km/h means that a target already moves 75 m during the process. The authors propose Kalman filters (see Section V-C) to smoothly keep track of the prover's location and detect any malicious tampering by outsiders.

Besides its current unsuitability for the long distances and high velocities present in air-traffic control, another main disadvantage of distance bounding is the fact that it inherently requires a response by the prover to the verifier's challenge and thus from an ADS-B point of view enforces an entirely new protocol paradigm. As an additional, on-demand feature it could still provide crucial information about the legitimacy of nodes in areas where PSR is not present (or is phased out due to cost reasons) .

C. Kalman Filtering and Intent Verification

Kalman filters (also known under the technical term linear quadratic estimation) [85] have already seen extensive use in broader ATC applications, e.g. to filter and smoothen GPS position data in messages. It is used to observe noisy time series of measurements and tries to statistically optimally predict future states of the measured variables of the underlying system.

A high level overview of the Kalman filtering algorithm comprises two distinct steps, a prediction step and an update step (see Fig. 16). As the procedure is recursive it can easily be used and updated in real time, without having to save more than the last state.

- Prediction step: In the first step, the current state variables are predicted as well as the connected uncertainties.
- Update step: For every following step, the previously obtained estimates are then updated with a weighted average. During this process, the estimates with higher certainty are assigned higher weight.

The theory behind Kalman filtering requires the observed system to be linear and the underlying measuring variables and errors to follow a normal distribution, although there have been developments to adapt the approach to non-linear systems, too.

Kalman filtering plays a crucial role in the multilateration approach, sorting out noisy signals and smooth over missing data (Fig. 17). It is also a useful tool in general to predict the future values of a feature based on collected historical data. More concretely, it is used in ground systems to filter and verify the state vectors and trajectory changes reported by ADS-B aircraft and conduct plausibility checks on these data [87]. Krozel et al. [88] then go on further to verify the intent of the aircraft by first defining local and global correlation functions to evaluate the correlation between aircraft motions and the ADS-B intent (Fig. 16). Then the authors compute geometric conformance, i.e. if the aircraft is in given horizontal and vertical limits and intent conformance, i.e. analyzing the aircraft motion and comparing it to a plausible intent model in several dimensions (in this case horizontal, vertical and velocity).

Kovell et al. [21] note that since Kalman filtering is used in a number of ADS-B related systems, it is essential to distinguish between Kalman filters dealing with an aircraft's GPS position, with received signal strength of packets and the angle of arrival at a recipient's antenna and their proposed use for real time

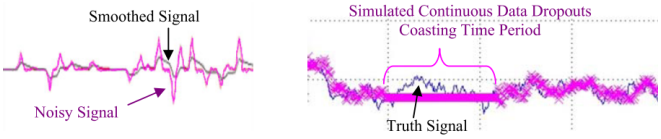

Figure 17. Example of Kalman filtering from [88]. Noisy signals are being smoothed (left), dropped data being coasted over below a given cutoff point (right).

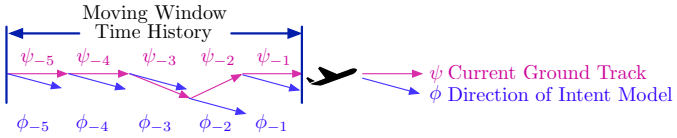

Figure 18. Practical application of intent verification in ADS-B from [88]. The example analyzes the horizontal aircraft motion with a global correlation function as a moving window over local correlation functions.

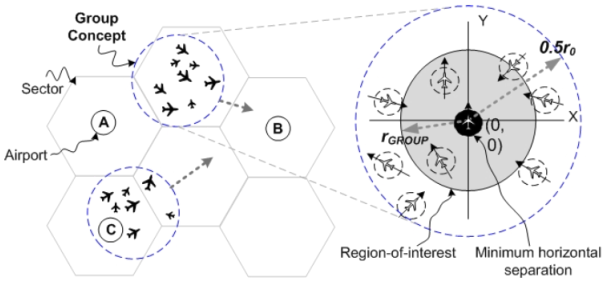

Figure 19. Illustration of the group concept from [19]. Four or more aircraft V are in any group G. Each group then can internally use multilateration to verify each other's location claims as well as those of outsiders in range. r_0 is the wireless communication range, $0.5r_0$ considered geographically proximate and thus acceptable for group establishment, given sufficient communication quality. To lower group overhead, the region of interest for a group can be restricted to r_{group}.

positional claim verifications of an aircraft onboard of other aircraft. Kalman filtering of positional claims is slightly more difficult in aircraft-to-aircraft systems but there are no inherent impossible obstacles to it.

From an attacker's point of view, Kalman filters can be tricked by a so-called frog boiling attack [89]: The adversary is jamming the correct signal, while continuously transmitting an ever-so-slightly modified position. If this is done slowly enough, the Kalman filter will see the injected data as a valid trajectory change. This exposes a general weakness of Kalman filtering as the approach is based on comparatively little historical data. But it is still of great use since obviously bogus manoeuvres, speeds, features can be detected (see also Section V-F) and the complexity of any attack is greatly increased. Another general downside is that it opens up more DoS-possibilities due to the largely increased computational complexity at every receiver, although this is not a major problem with comparably powerful installations in ground stations and airplanes. A possible threshold time after which sufficient trust has been established between two participants based on data validated by Kalman filtering is still open research [21].

D. Group Verification

Group verification is another concept proposed to mitigate security and privacy concerns over the use of ADS-B [19]. It aims at securing the airborne ADS-B IN communication by employing multilateration done by a group to verify location claims of non-group members in-flight. A given authenticated group with 4 or more aircraft having established trust can communicate with each other to utilize multilateration (based on TDOA or RSS) just as ground stations can (see Section V-A). If a forged position report is detected, the sensible reaction would be to increase the circle of avoidance around nearby airplanes since their position cannot anymore be regarded as precisely known and thus safe.

Kovell et al. [21] conducted a study about the applicability of the group concept in commercial aviation in the United States airspace. Examining the vast differences in traffic density over the US, they found that around 91% of aircraft at a given time could be part of a sufficiently large group of 4 aircraft or more.

Group verification has a number of downsides. First of all, it requires many additional messages to implement the verification and trust process. As ADS-B is purely unidirectional broadcast, a new protocol is needed to support the group concept. Concerning the question of which protocol to use, the authors mention the L-Band Digital Aeronautical Communication System (L-DACS) as one possibility. L-DACS is being developed by EUROCONTROL as a future IP technology for air-to-air communication but unfortunately there is no specification in sight in the medium term.[25] If such a protocol can be successfully implemented, there remains the central problem of how to manage the secure authentication of members that are to be accepted into the group in the first place. It is very complicated to establish trust in new groups of MANETs and to reliably avoid malicious aircraft. Furthermore, the performance of the system in reaction to intelligent intentional jamming of some or all communication would have to be considered.

On the other hand, even without a perfectly secure solution, the group concept would raise the difficulty and engineering effort of certain attacks on airborne aircraft by orders of magnitude.

E. Data Fusion and Trust Management

Data fusion is quickly becoming a cornerstone of modern intelligent transport systems (ITS). The concept can be used at various stages of data processing, Baud et al. [90] e.g. describe the fusion of radar and ADS-B data and show that this approach can improve the quality of tracking in practice. Concerning ADS-B security, the literature proposes to

[25]"In addition to the air/ground capability, some of the assessed technologies could also support additional features such as air/air (point to point and/or broadcast) communications and digital voice. However the support of these capabilities needs further investigation." http://www.eurocontrol.int/communications/public/standard_page/LDACS.html

check positional data obtained from within the system against data coming in from other, independent sources. Adequate data can e.g. stem from multilateration (see Section V-A), traditional primary radar systems or even flight plan data. Such verification can provide a way of knowing if some of the involved systems work outside normal parameters, be it from a malicious source or not. Subsequently, automated technical or non-technical procedures can be carried out, identifying the problem and reacting accordingly. This process comprises an analysis of the trust-worthiness of the data, if it has been vulnerable to tampering depending on the system and the precision/measurement uncertainty of the respective technologies (as given e.g. in [5]). The trust-worthiness can then be calculated by looking at the correlations and further features deduced through machine learning processes which aim to expose anomalies in received information and thus to enable more automated detection of attacks.

An example of this is given in [91]. The authors use the cosine similarity between claimed and estimated positions to judge the trustworthiness of a participant's claims and maintain historical beacon trust information :

$$Sim_{Cos}(\vec{E},\vec{O}) = \frac{\vec{E}\cdot\vec{O}}{|\vec{E}|\cdot|\vec{O}|} = \frac{x_E \times x_O + y_E \times + v_E \times v_O}{\sqrt{x_E^2+y_O^2+v_E^2}\times\sqrt{x_O^2+y_O^2+v_O^2}} \quad (1)$$

x_O, y_O are the coordinates, v_O the velocity as claimed in the last received message. x_E, y_E are the estimated coordinates of the claimant, based on the previously received message. As a further step they calculate the time-based weighted trustworthiness of a beacon message, taking into account the cosine similarity of the last I beacon messages and their respective estimates:

$$T_{beacon} = \frac{\sum_{i=1}^{I} Sim_{Cos}(\vec{E},\vec{O})(w_i)^n}{\sum_{i=1}^{I}(w_i)^n} \quad (2)$$

It is easy to make a case for data fusion, since many of the required components are already available and a two-out-of-three (2oo3) approach is widely accepted best practice in many industries dealing with processes that are crucial to safety and security. It has even been suggested to equip the average car with primary surveillance radar, to secure vehicular ad hoc networks [92].

There are already a number of integrated systems being deployed (such as ASDE-X) that are inherently fusing the data of various sub-systems (ADS-B, multilateration, flight plan information, radar data) to increase both security and accuracy in airport proximity. The clear advantage of data fusion is the compatibility with legacy systems, including the fact that the ADS-B protocol does not need to be amended to provide these additional features. The downsides include increased cost for additional systems to provide the necessary redundancy.

F. Traffic Modeling and Plausibility Checks

Traffic modeling could provide a mechanism to detect deviations from normal ADS-B behaviour. By utilizing historical data as well as machine learning methods it is possible to create a model of a map for each ground station, providing a means to verify location claims made by aircraft via ADS-B. Figure 20 shows how a typical heat map based on RSS values looks from the point of view of a ground station. Such models can provide hints about non-matching location claims of a message send by an aircraft. Other potential considerations include checking for a certain number of consecutive packets of the same - or different - aircraft with the same RSS/angle-of-arrival, or otherwise suspicious absolute values which could indicate a stationary, ground-based attacker (e.g. RSS/AoA values outside typically observed thresholds).

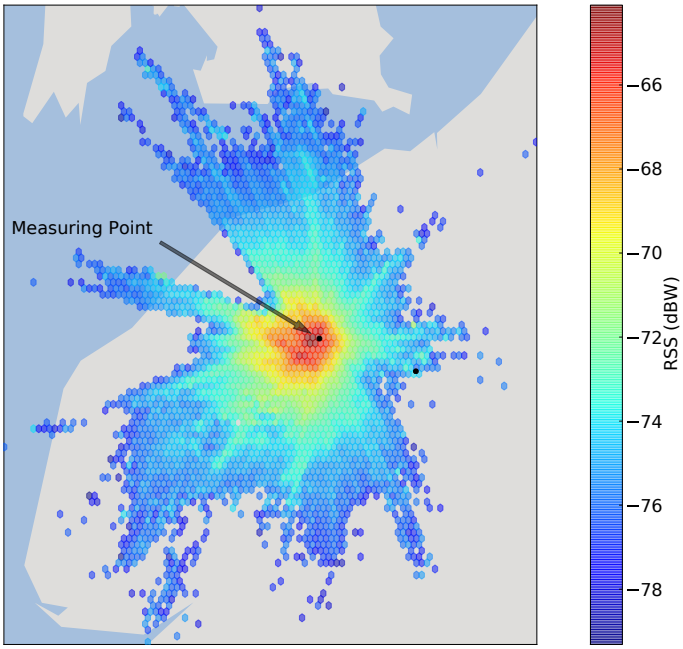

Figure 20. Example of an RSS heat map used for traffic modeling from [1]. The colors indicate the received signal strength at a single measuring point which correlates strongly with the distance. Though it is relatively easy for an attacker to manipulate the RSS, it becomes increasingly difficult the more measuring points have to be deceived.

Xiao et al. [93] used a similar statistical approach for the detection of Sybil nodes in VANETs. They propose an algorithm that could be performed by any node that has received enough measurements of e.g. signal strength from nearby witnesses. While a single estimated position of a node may not be an accurate representation of the real location, a larger sample of estimated positions would have to be very similar to the node's position claims over a given period of time.

More formally, if in a period Δt_o there are n sequential positions $l_1, ..., l_n$ claimed by an airplane and the corresponding estimated positions $l_1^{'}, ..., l_n^{'}$, then the difference between the two can be treated as a random error. That means that a large enough sample of differences is distributed normally with a mean μ_d and a variance σ_0^2. Under these assumptions, it is sufficient to test against the hypotheses:

$$H_0 : \mu_d = 0 \;\; H_1 : \mu_d \neq 0$$

$$H_0^{'} : \sigma^2 \leq \sigma_0^2 \;\; H_1^{'} : \sigma^2 > \sigma_0^2$$

If both H_0 as well as $H_0^{'}$ are true than it can be assumed that the claimant has given valid positional reports within the chosen level of significance (see [93] for further explanations and simulation results in VANETs). As this method is only really practical for fixed receivers, the goal is to use ground stations to detection of unusual behaviour. They are also more likely to be able to collect enough samples to make the verification process as sound as possible.

On top of this, there are numerous comparably simple rules that can be utilized as potential red flags by an intrusion detection system without resorting to more complex measures. Neither of these rules are necessary nor sufficient by themselves to detect an ongoing attack. But depending on the scenario and the attacker's savvy, they can indicate unusual behaviour that should be further investigated either by a human or handled through additional technical means. For example, it is very plausible to outright drop a number of packets where either the data or the meta data is technically or physically impossible. Doing so can significantly reduce the strain on the ADS-B system and even prevent both spoofing and DoS attacks which are not crafted carefully enough. If a large number of potential red flags are checked for an intrusion detection system, not only the risk for an attacker to cause an alert increases significantly, but also the cost and complexity of an attack rise. While this does not constitute theoretical perfect security, plausibility checks can be very useful in practice.

Mitigating factors exist across various layers, from the physical to the application layer. Some are available to ground stations/air traffic control only, others also to aircraft-to-aircraft (A2A) ADS-B IN communication. Such cases include but are not limited to:

- Investigating **airplanes which suddenly appear** well within the maximum communication range of a receiver.
- Dropping **aircraft which are violating a given acceptance range threshold**, producing impossible locations [94].
- **Aircraft violating a given mobility grade threshold**, producing impossible minimum or maximum velocities [94].
- **Maximum Density Threshold**: If too many aircraft are in a given area, ATC software will typically alarm the user [94].
- **Map-based Verification**: Aircraft in unusual places such as no-fly areas or outside typical airways (this might possibly be better handled at the ATC software layer) [94].
- **Flight plan-based Verification**: Flooded/attacked ground stations are able to check ADS-B messages against the existing flight plan.
- Obvious **discontinuities in one of the 9 ADS-B state vector data fields** (also see the related Section V-C) .

As explained before, such potential red flags need to be handled with utmost care and can typically not be automated but require much additional scrutiny before any action is taken (e.g., the packet/flight is considered an attack and dropped from ATC monitors). Yet, they also enable the opportunity to follow up and activate further means to secure the airspace. For example, when using such centralized detection at the ground stations, these same stations could then destroy messages sent by the detected offenders as outlined in [95], [96].

VI. Summary and Further Discussion

Tables I-III provide a compact overview over the effectiveness of all examined solutions in combating the various proposed attacks as well as offering advantages and disadvantages concerning the feasibility to implement each approach in the real world. As has been laid out, there is no single optimal or even good solution when considering means that have no or little impact on the currently employed ADS-B software and hardware. Table I shows the attacks the discussed approaches can counteract. We see that most security schemes focus on attacks of the message injection/modification class. This has two main reasons that have been mentioned throughout this work: First of all, the open nature of ADS-B has been considered a desirable feature in most scenarios. So unless there is a major paradigm shift in the way air traffic communication and control is handled currently, there is no interest in protecting against passive listeners, despite this being the first stepping stone for more sophisticated and problematic attacks. Second, passive attacks such as eavesdropping are simply much more difficult to protect against without having a full cryptographic solution. Similarly, attacks on the physical layer, such as continuously jamming the well-known frequency or the more surgical message deletion are hard to defend against, with measures on the same layer (e.g. uncoordinated spread spectrum) providing some of the only approaches to this general wireless security problem. All discussed approaches do however address message insertion and tampering, either by protecting outright against it through verification (cryptographic methods) or by detecting anomalies in the data (e.g. Kalman filtering, multilateration).

	Injection / Modification	Eavesdropping	Jamming / Deletion
Physical Layer Authentication	+	-	-
Uncoordinated Spread Spectrum	-	+	+
(Lightweight) PKI	+	+	-
µTESLA	+	-	-
Wide Area Multilateration	+	-	-
Distance Bounding	+	-	-
Kalman Filtering	+	-	-
Group Verification	+	-	-
Data Fusion	+	-	-
Traffic Modeling	+	-	-

Table I
Overview of capabilities of various security approaches against feasible attacks on ADS-B.

	Data Integrity	Source Integrity	Location Integrity	DoS
Physical Layer Authentication	No	Yes	Possibly	Partly
Uncoordinated Spread Spectrum	No	No	No	Yes
(Lightweight) PKI	Yes	Yes	Yes	Partly
µTESLA	No	Yes	No	No
Wide Area Multilateration	No	No	Yes	No
Distance Bounding	No	No	Partly	No
Kalman Filtering	No	Partly	Partly	No
Group Verification	No	Possibly	Yes	No
Data Fusion	No	Partly	Yes	Backup
Traffic Modeling	No	No	Yes	No

Table II
OVERVIEW OF SECURITY FEATURES OF VARIOUS APPROACHES FOR USE WITH ADS-B.

	Difficulty	Cost	Scalability	Compatibility
Physical Layer Authentication	Variable	Variable	Variable	Requires additional hard-/software. No modifications to the ADS-B protocol.
Uncoordinated Spread Spectrum	Medium	Medium	Medium	Requires new hardware. No modifications to the ADS-B protocol.
(Lightweight) PKI	High	High	Medium	Distribution infrastructure and changes in protocol and message handling needed.
µTESLA	Medium	Medium	High	New message type required for key publishing, MAC added.
Wide Area Multi-lateration	Low	Medium	Medium	No change to ADS-B required. Separate hardware system.
Distance Bounding	High	Medium	Low	New messages and protocol needed.
Kalman Filtering	Low	Low	High	No additional messages needed. Separate software system.
Group Verification	High	Medium	Low	New messages and protocol needed.
Data Fusion	Low	Medium - High	Medium	No change in ADS-B required. Separate system.
Traffic Modeling	Medium	Low	High	Additional, separate entities for ground stations needed.

Table III
OVERVIEW OF FEASIBILITY ATTRIBUTES OF VARIOUS APPROACHES FOR USE WITH ADS-B.

Table II takes a look at the security features the discussed schemes can provide. As discussed before, only a full cryptographic public key infrastructure can guarantee the integrity of received data. All other approaches either aim to secure the integrity of the source (e.g. µTESLA, many of the discussed physical layer schemes) or seek to verify the provided location data independently. Additional protection against flood denial of service attacks against ATC systems can be directly provided by spread spectrum approaches and cryptography, while other methods rely on higher layers to sort out false aircraft claims.

Table III provides an overview over the feasibility of the different approaches in practical settings, especially considering the current state of air traffic control in the aviation industry. As is to be expected, the difficulty and cost columns are mostly correlated. The difficulty to overcome technical challenges is particularly high for distance bounding, which is yet in its beginnings and a full-blown public key infrastructure. In contrast, we see wide-area multilateration, Kalman filters and data fusion techniques already in use in the field. This naturally translates to the cost factor which plays an important role in industry decisions. One can choose between a completely new protocol which addresses the security question better than the current installment of ADS-B does, slight modifications such as new message types, or a transparent, parallel system which requires new software and/or new hardware in different scales. This touches also on the question of scalability. For example, the fusion of various ATC systems and their data (PSR, SSR, ADS-C, WAMLAT, FANS) is an obvious and necessary idea. Yet, it is common knowledge in the aviation community that a "major part of the business case for Automatic Dependent Surveillance - Broadcast (ADS-B) is attributed to the savings generated by decommissioning or reducing reliance on conventional radar systems" [5]. Thus, it seems inefficient and unlikely to have legacy and/or new backup systems around on a broad scale, simply to fix the inadequateness of ADS-B related to security.

Considering the fact that the invention, certification and large-scale deployment of air-traffic systems takes decades, as currently seen in the example of ADS-B, it seems equally non-sensible to present a completely overhauled ATC-system at this point in time. In practice this means that incremental changes with backwards compatibility as a main factor kept in mind are more likely to be successful than a completely new proposal. On the other hand, cost and complexity of deployment cannot be the only factors taking into consideration - not having security is famously even much more expensive.[26] As mentioned throughout this work, it can be a useful dichotomy to distinguish between attack detection, attack prevention and dealing with suspected attacks. In this paper, we focused mainly on attack detection and prevention, leaving attack reaction for future research.

VII. CONCLUSION

This survey sought to review the available research on the topic of securing the ADS-B protocol in particular and air traffic control communication in general. We provided an in-depth overview of the existing work, both specific to ADS-B as well as ideas brought in from related fields such as VANETs. After reviewing the literature, it seems that the solutions currently under consideration (and in use in practice such as multilateration) can only be a fill-in, providing a quick

[26]"If you think safety is expensive, try an accident", an insight by easyJet owner Stelios Haji-Ioannou that came after facing manslaughter charges for the deaths of employees in a shipping disaster at a former company.

improvement to the security of the current system. For all-encompassing security (and possibly privacy), new message types and/or completely new protocols would need to be defined. Taking this into account for the creation of a long-term security solution in dependent air traffic surveillance, it makes sense to consider the impact of both secure broadcast authentication approaches as well as secure location verification. This should include a thorough breakdown of future traffic density, including upper bounds on wireless communication not only on current navigation channels, as well as the possible impact of communication and message overhead of a new protocol to not run into hard challenges again in the foreseeable future.

REFERENCES

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

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

[3] ICAO, "Cyber Security for Civil Aviation", in *Twelfth Air Navigation Conference*, 2012, pp. 1–4.

[4] EUROCONTROL, "Cascade news 9 - update on developments", October 2010.

[5] A Smith, R Cassell, T Breen, R Hulstrom, and C Evers, "Methods to Provide System-wide ADS-B Back-Up, Validation and Security", in *25th Digital Avionics Systems Conference*, 2006, pp. 1–7.

[6] RTCA Inc., "Minimum aviation system performance standards for automatic dependent surveillance broadcast (ads-b)", DO-242A (including Change 1), December 2006.

[7] 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 Corrigendum 1, December 2011.

[8] RTCA Inc., "Minimum operational performance standards for universal access transceiver (uat) automatic dependent surveillance – broadcast", DO-282B with Corrigendum 1, December 2011.

[9] 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*, vol. 4, no. 2, pp. 78–87, August 2011.

[10] John R. Barry, *Wireless Infrared Communications*, Kluwer Academic, Boston, 1994.

[11] Matthias Wilhelm and Ivan Martinovic, "Short paper: reactive jamming in wireless networks: how realistic is the threat?", *Proceedings of the fourth ACM conference on Wireless network security*, pp. 47–52, 2011.

[12] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Čapkun, "Investigation of signal and message manipulations on the wireless channel", in *ESORICS'11 Proceedings of the 16th European Conference on Research in Computer Security*, 2011.

[13] Matthias Wilhelm, Jens B Schmitt, and Vincent Lenders, "Practical message manipulation attacks in IEEE 802.15.4 wireless networks", in *MMB & DFT 2012 Workshop Proceedings*, 2012.

[14] Hua Li, Bo Yang, Cailian Chen, and Xinping Guan, "Connectivity of Aeronautical Ad hoc Networks", in *2010 IEEE Globecom Workshops*. December 2010, pp. 1788–1792, Ieee.

[15] Boeing Commercial Airplanes Market Analysis, "Boeing current market outlook 2011-2030", 2011.

[16] Adrian Perrig and Doug Tygar, *Secure Broadcast Communication in Wired and Wireless Networks*, Springer, 2003.

[17] Patrick J Martone and George E Tucker, "Candidate requirements for multilateration and ADS-B systems to serve as alternatives to secondary radar", in *Digital Avionics Systems, 2001. DASC. 20th Conference*, 2001, pp. 1–12.

[18] Christos Rekkas and Melvyn Rees, "Towards ADS-B implementation in Europe", *2008 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles*, pp. 1–4, September 2008.

[19] Krishna Sampigethaya and Radha Poovendran, "Security and privacy of future aircraft wireless communications with offboard systems", *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, pp. 1–6, January 2011.

[20] Krishna Sampigethaya and Linda Bushnell, "A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance", in *AIAA Proceedings*, 2009, pp. 1–10.

[21] Brandon Kovell, Benjamin Mellish, Thomas Newman, and Olusola Kajopaiye, "Comparative Analysis of ADS-B Verification Techniques", 2012.

[22] Bashar Nuseibeh, Charles B Haley, and Craig Foster, "Securing the Skies: In Requirements We Trust", *Computer*, vol. 42, no. 9, pp. 64–72, 2009.

[23] Jack Burbank, Robert Nichols, Sunita Munjal, Robert Pattay, and William Kasch, "Advanced communications networking concepts for the National Airspace System", in *2005 IEEE Aerospace Conference*. 2005, pp. 1905–1923, IEEE.

[24] Winston Wenhua Li and Pan Kamal, "Integrated Aviation Security for Defense-in-Depth of Next Generation Air Transportation System", in *IEEE Conference on Technologies for Homeland Security*, 2011, pp. 136–142.

[25] Washington Y. Ochieng, Knut Sauer, David Walsh, Gary Brodin, Steve Griffin, and Mark Denney, "GPS Integrity and Potential Impact on Aviation Safety", *Journal of Navigation*, vol. 56, no. 1, pp. 51–65, January 2003.

[26] Julio C. Siu, "ICAO Concepts and References Regarding ADS-B, Multilateration and Other Surveillance Techniques", in *ICAO/FAA Workshop on ADS-B and Multilateration Implementation*, 2011, number September.

[27] Richard Wagner, "IFF, Combat ID and the Information Domino Effect", Tech. Rep., Canadian Department of National Defence, 2009.

[28] Office of Technology Assessment U.S. Congress, *Who Goes There: Friend or Foe?*, U.S. Government Printing Office, Washington, DC, 1993.

[29] Larry Kenney, Joe Dietrich, and Jerry Woodall, "Secure ATC surveillance for military applications", *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pp. 1–6, November 2008.

[30] RTCA Inc., "Proposed change to do-181d and ed-73c for higher squitter rates at lower power", Special Committee 209 ATCRBS / Mode S Transponder MOPS Maintenance, April 2007.

[31] Mark Luk, Adrian Perrig, and Bram Whillock, "Seven cardinal properties of sensor network broadcast authentication", *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks - SASN '06*, p. 147, 2006.

[32] Thomas YC Woo and Simon S Lam, "Authentication for Distributed Systems", *Computer*, vol. 25, no. 1, pp. 39–52, 1992.

[33] Boris Danev, Davide Zanetti, and Srdjan Capkun, "On physical-layer identification of wireless devices", *ACM Computing Surveys*, vol. 45, no. 1, pp. 1–29, November 2012.

[34] Boris Danev, Heinrich Luecken, Srdjan Capkun, and Karim El Defrawy, "Attacks on physical-layer identification", in *Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 89–98.

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

[36] Suman Jana and Sneha Kumar Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews", *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, March 2010.

[37] Roel Maes and Ingrid Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions", *Towards Hardware-Intrinsic Security*, , no. 71369, pp. 3–27, 2010.

[38] Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications", *2008 IEEE International Conference on RFID*, pp. 58–64, April 2008.

[39] 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*, 2008, pp. 128—-139.

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

[41] Qian Wang, Hai Su, Kui Ren, and Kwangjo Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless

networks", *2011 Proceedings IEEE INFOCOM*, pp. 1422–1430, April 2011.

[42] Jie Xiong and Kyle Jamieson, "SecureAngle: Improving Wireless Security Using Angle-of-Arrival Information", in *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, p. 11.

[43] Di Qiu, Dave De Lorenzo, Sherman Lo, Dan Boneh, and Per Enge, "Physical Pseudo Random Function in Radio Frequency Sources for Security", in *Proceeding of ION ITM*, 2009, pp. 26–28.

[44] Christine Laurendeau and Michel Barbeau, "Insider attack attribution using signal strength-based hyperbolic location estimation", *Security and Communication Networks*, vol. 1, no. July, pp. 337–349, 2008.

[45] Christine Laurendeau and Michel Barbeau, "Probabilistic Localization and Tracking of Malicious Insiders Using Hyperbolic Position Bounding in Vehicular Networks", *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 128679, 2009.

[46] Mario Strasser, Christina Pöpper, Srdjan Capkun, and Mario Cagalj, "Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping", *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 64–78, May 2008.

[47] Christina Pöpper, Mario Strasser, and Srdjan Capkun, "Jamming-resistant Broadcast Communication without Shared Keys", in *Proceedings of the USENIX Security Symposium*, 2009, pp. 231–247.

[48] Donggang Liu, Peng Ning, Sencun Zhu, and Sushil Jajodia, "A Tree-Based μTESLA Broadcast Authentication for Sensor Networks".

[49] Cindy Finke, Jonathan Butts, Robert Mills, and Michael Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system", *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3–11, March 2013.

[50] Ken Samuelson, Ed Valovage, and Dana Hall, "Enhanced ADS-B Research", *2006 IEEE Aerospace Conference*, pp. 1–7, 2006.

[51] Marc Viggiano, Edward Valovage, Ken Samuelson, Dana Hall, et al., "Secure ads-b authentication system and method", 2010, US Patent 7,730,307.

[52] Leonard Schuchman, "Automatic dependent surveillance system secure ads-s", 2011, US Patent 7,876,259.

[53] Feng Ziliang, P A N Weijun, and Wang Yang, "A Data Authentication Solution Of ADS-B System Based On X .509 Certificate", in *27th International Congress of the Aeronautical Sciences*, 2010.

[54] Chris Moody, "System Description for the Universal Access Transceiver", Tech. Rep. November, FAA, 2000.

[55] Maxim Raya and Jean-Pierre Hubaux, "The security of vehicular ad hoc networks", *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks - SASN '05*, p. 11, 2005.

[56] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[57] Richard V Robinson, Mingyan Li, Scott A Lintelman, Krishna Sampigethaya, Radha Poovendran, David Von Oheimb, and Jens-Uwe Bußer, "Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes", in *AIAA Aviation Technology Integration, and Operations (ATIO) Conference*, 2007.

[58] Bryan Parno and Adrian Perrig, "Challenges in Securing Vehicular Networks", in *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005, pp. 1–6.

[59] Junqi Zhang and Vijay Varadharajan, "Wireless sensor network key management survey and taxonomy", *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, March 2010.

[60] Adrian Perrig, Ran Canetti, J. D. Tygar, and Dawn Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels", in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 56–73.

[61] Adrian Perrig, Dawn Song, and Ran Canetti, "The TESLA Broadcast Authentication Protocol", 2005.

[62] Adrian Perrig, Robert Szewczyk, J D Tygar, Victor Wen, and David E Culler, "SPINS : Security Protocols for Sensor Networks", *Wireless networks 8*, vol. 8, no. 5, pp. 521–534, 2002.

[63] Mohamed Hamdy Eldefrawy, Muhammad Khurram Khan, Khaled Alghathbar, and Eun-Suk Cho, "Broadcast authentication for wireless sensor networks using nested hashing and the Chinese remainder theorem.", *Sensors*, vol. 10, no. 9, pp. 8683–95, January 2010.

[64] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux, "Real-World VANET Security Protocol Performance", *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–7, November 2009.

[65] Yih-Chun Hu and Kenneth P Laberteaux, "Strong VANET Security on a Budget", in *Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, 2006, vol. 06, pp. 1–9.

[66] Andreas Savvides, Heemin Park, and Mani B. Srivastava, "The bits and flops of the n-hop multilateration primitive for node localization problems", *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications - WSNA '02*, p. 112, 2002.

[67] WHL Neven, TJ Quilter, R Weedon, and RA Hogendoorn, "Wide Area Multilateration Report on EATMP TRS 131/04 Version 1.1", Tech. Rep., 2005.

[68] Ning Xu, Rick Cassell, and Carl Evers, "Performance assessment of Multilateration Systems - A solution to nextgen surveillance", in *Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2010, pp. 2–9.

[69] Gaspare Galati and Mauro Leonardi, "Wide area surveillance using SSR mode S multilateration: advantages and limitations", in *European Radar Conference (EURAD)*, 2005, pp. 225–229.

[70] J.G. Herrero, J.A. Besada Portas, F.J.Jimenez Rodriguez, and J. R Casar Corredera, "ASDE and multilateration mode-S data fusion for location and identification on airport surface", in *Radar Conference, 1999. The Record of the 1999 IEEE*, 1999, number 34, pp. 315–320.

[71] Leon Purton, Hussein Abbass, and Sameer Alam, "Identification of ADS-B System Vulnerabilities and Threats", in *Australian Transport Research Forum, Canberra*, 2010, pp. 1–16.

[72] Jerry Johnson, Holger Neufeldt, and Jeff Beyer, "Wide area multilateration and ADS-B proves resilient in Afghanistan", in *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2012 IEEE*, 2012.

[73] Regina Kaune, Christian Steffes, Sven Rau, Wolfgang Konle, and Juergen Pagel, "Wide area multilateration using ADS-B transponder signals", in *Information Fusion (FUSION), 2012 15th International Conference on*, 2012, pp. 727–734.

[74] Paul Thomas, "North sea helicopter ADS-B/MLat pilot project findings", in *Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), 2011 Tyrrhenian International Workshop on*, 2011, pp. 53–58.

[75] Anastasios Daskalakis and Patrick Martone, "A technical assessment of ADS-B and multilateration technology in the Gulf of Mexico", in *Proceedings of the 2003 IEEE Radar Conference*. 2003, pp. 370–378, Ieee.

[76] Frederick A Niles, Robert S Conker, M Bakry El-Arini, Daniel G O'Laighlin, and Dmitri V Baraban, "Wide Area Multilateration for Alternate Position, Navigation, and Timing (APNT)", Tech. Rep. 1, 2012.

[77] Gaspare Galati, Mauro Leonardi, Pierfrancesco Magarò, and Valerio Paciucci, "Wide area surveillance using SSR mode S multilateration: advantages and limitations", in *Radar Conference, 2005. EURAD 2005. European*, 2005.

[78] John R. Douceur, "The sybil attack", *Peer-to-peer Systems*, pp. 251–260, 2002.

[79] Stefan Brands and David Chaum, "Distance-bounding protocols", *Advances in Cryptology - EUROCRYPT'93*, pp. 344–359, 1994.

[80] Jolyon Clulow, Gerhard P Hancke, Markus G Kuhn, and Tyler Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks", in *Security and Privacy in Ad-hoc and Sensor Networks*, 2006, pp. 83–97.

[81] Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, and Srdjan Capkun, "Distance Hijacking Attacks on Distance Bounding Protocols", *2012 IEEE Symposium on Security and Privacy*, pp. 113–127, May 2012.

[82] Joo-Han Song, Vincent W. S. Wong, and Victor C. M. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks", *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, pp. 1–5, 2008.

[83] Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Škorić, Dave Singel, and Srdjan Čapkun, "Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System", in *Computer Security–ESORICS 2012*, 2012, pp. 415—-432.

[84] Nils Ole Tippenhauer and Srdjan Čapkun, "ID-Based Secure Distance Bounding and Localization", in *Computer Security–ESORICS 2009*, 2009, pp. 621–636.

[85] Rudolph Emil Kalman, "A new approach to linear filtering and prediction problems", *Journal of basic Engineering*, vol. 82, no. Series D, pp. 35–45, 1960.

[86] Greg Welch and Gary Bishop, "An introduction to the Kalman filter", pp. 1–16, 1995.

[87] Dieter Fox, Jeffrey Hightower, Lin Liao, and Dirk Schulz, "Bayesian Filters for Location Estimation", *Pervasive Computing*, vol. 2, no. 3, 2003.

[88] Jimmy Krozel, Dominick Andrisani, Mohammad A Ayoubi, Takayuki Hoshizaki, and Chris Schwalm, "Aircraft ADS-B Data Integrity Check", in *AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum*, 2004, pp. 1–11.

[89] Eric Chan-Tin, Victor Heorhiadi, Nicholas Hopper, and Yongdae Kim, "The Frog-Boiling Attack: Limitations of Secure Network Coordinate Systems", *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 3, pp. 27, 2011.

[90] O Baud, N Honore, and O Taupin, "Radar / ADS-B data fusion architecture for experimentation purpose", in *9th International Conference on Information Fusion*, 2006, pp. 1–6.

[91] Yu-chih Wei, Yi-ming Chen, and Hwai-ling Shan, "Beacon-based Trust Management for Location Privacy Enhancement VANETs", in *13th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2011.

[92] Gongjun Yan, Stephan Olariu, and Michele C. Weigle, "Providing VANET security through active position detection", *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, July 2008.

[93] Bin Xiao, Bo Yu, and Chuanshan Gao, "Detection and Localization of Sybil Nodes in VANETs", in *International Conference on Mobile Computing and Networking: Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006, pp. 1–8.

[94] Tim Leinmuller, Elmar Schoch, and Frank Kargl, "Position verification approaches for vehicular ad-hoc networks", *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, October 2006.

[95] Ivan Martinovic, Paul Pichota, and Jens B Schmitt, "Jamming for Good: A Fresh Approach to Authentic Communication in WSNs", in *WiSec '09: Proceedings of the second ACM conference on Wireless network security*, 2009, pp. 161–168.

[96] Matthias Wilhelm and Ivan Martinovic, "WiFire: A Firewall for Wireless Networks", *ACM SIGCOMM Computer Communication Review*, vol. 4, no. 4, pp. 456–457, 2011.