Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures

Daniel Moser
Dept. of Computer Science
ETH Zürich, Switzerland

Patrick Leu
Dept. of Computer Science
ETH Zürich, Switzerland

Vincent Lenders
armasuisse
Thun, Switzerland

Aanjhan Ranganathan
Dept. of Computer Science
ETH Zürich, Switzerland

Fabio Ricciato
Faculty of Computer and Information Science
University Ljubljana, Slovenia

Srdjan Capkun
Dept. of Computer Science
ETH Zürich, Switzerland

ABSTRACT

Multilateration techniques have been proposed to verify the integrity of unprotected location claims in wireless localization systems. A common assumption is that the adversary is equipped with only a single device from which it transmits location spoofing signals. In this paper, we consider a more advanced model where the attacker is equipped with multiple devices and performs a geographically distributed coordinated attack on the multilateration system. The feasibility of a distributed multi-device attack is demonstrated experimentally with a self-developed attack implementation based on multiple COTS software-defined radio (SDR) devices. We launch an attack against the OpenSky Network, an air traffic surveillance system that implements a time-difference-of-arrival (TDoA) multilateration method for aircraft localization based on ADS-B signals. Our experiments show that the timing errors for distributed spoofed signals are indistinguishable from the multilateration errors of legitimate aircraft signals, indicating that the threat of multi-device spoofing attacks is real in this and other similar systems. In the second part of this work, we investigate physical-layer features that could be used to detect multi-device attacks. We show that the frequency offset and transient phase noise of the attacker's radio devices can be exploited to discriminate between a received signal that has been transmitted by a single (legitimate) transponder or by multiple (malicious) spoofing sources. Based on that, we devise a multi-device spoofing detection system that achieves zero false positives and a false negative rate below 1%.

CCS Concepts

•Security and privacy → Spoofing attacks; Intrusion detection systems; •Networks → *Sensor networks;*

Keywords

Air traffic control; ADS-B; Multilateration; Spoofing; Physical-layer; Intrusion detection

MobiCom'16, October 03 - 07, 2016, New York City, NY, USA

ISBN 978-1-4503-4226-1/16/10...$15.00

DOI: http://dx.doi.org/10.1145/2973750.2973763

1. INTRODUCTION

Vehicle tracking is a key feature to enable safe navigation and collision avoidance for airborne, ground, and maritime traffic control systems. For example, in commercial air traffic control systems, the locations of all aircraft are continuously monitored to inform pilots and air traffic controllers on the ground about potential collisions. Similarly, collision avoidance systems in future autonomous car navigation systems will require car tracking to prevent collisions at road intersections [23].

A popular tracking approach is to let the vehicles determine their own positions and broadcast them to nearby nodes over the wireless channel. In the next-generation air transportation system, each aircraft determines its position with the aid of global navigation satellite systems such as GPS, and this information is periodically broadcasted over the Automatic Dependent Surveillance - Broadcast (ADS-B) system to surrounding aircraft and sensors on the ground [38]. This autonomous tracking paradigm based on position claims has several advantages, but it makes the system vulnerable to location spoofing attacks [4, 32]. For instance, an attacker can inject false position messages in order to emulate the presence of a "ghost" aircraft into the air traffic surveillance systems, or it can spoof the location of a real aircraft by sending false position claims. It has been shown that these attacks are easy to launch on real systems [32]. The ability to verify the location claims in such systems is therefore of high importance [28].

To counteract spoofing attacks on ADS-B and similar systems, various multilateration-based verification techniques have been previously proposed in the literature [25, 9, 34, 10, 11]. These schemes generally differ in the adopted ranging techniques – time-difference-of-arrival (TDoA), time-of-flight (ToF), or mobility-differentiated time-of-arrival (MDToA) – however they all share the same underlying mathematical principle of lateration. While these solutions are effective at preventing single-device attacks, where the adversary sends spoofing signals from a single radio location, they were not designed to be secure against multi-device attacks, where the adversary controls a set of geographically distributed spoofing devices. In this scenario, the attacker places a separate spoofing device in the proximity of each receiver and therefore sends appropriately delayed copies of the same signal to different sensors. In this way the attacker can spoof an arbitrary position without being detected by the multilateration verification scheme.

In this work, we move beyond the single device attacker model and evaluate the feasibility of multi-device attacks. We show that multi-device location spoofing attacks are practical to implement

and can successfully compromise existing multilateration systems. To this end, we perform controlled attack-experiments against the OpenSky Network [35], an air traffic surveillance system that implements the time-difference-of-arrival (TDoA) multilateration method for localization of aircraft with ADS-B signals. The OpenSky Network is a crowdsourced large-scale ADS-B sensor network which captures 60 percent of all aircraft flying over Europe.

In the analyzed air traffic control system, as in most other systems, the ground receivers are at publicly known locations and placed far apart (usually several km) meaning that the attacker can easily prevent its spoofed signals from reaching multiple receivers. Closer placement of receivers would still not prevent attacks if an attacker deploys directional antennas and reduces its transmission power.

The main challenge for the attacker is to precisely synchronize its devices in order to tightly control the arrival times of spoofed messages at the receivers. Our setup consists of distributed commercial off-the-shelf (COTS) software-defined radio devices on top of which we implement our spoofing system. Our results show that by relying on standard synchronization techniques (e.g. GPS), we can successfully spoof locations within the OpenSky Network with sufficient accuracy. This result naturally extends to other multilateration systems and therefore fully supports the use of multi-device attacker models in the analysis of all location verification solutions.

In order to detect multi-device location spoofing attacks, we propose to leverage two physical-layer features, namely, transmitter tuning frequency precision and transient phase noise. Relying on these features, we develop a detection method for multi-device spoofing attacks and evaluate its performances with real-world ADS-B data. Our results show that our method achieves zero false positives and a false negative rate below 1%, with a detection delay in the order of few seconds.

The contributions of this paper are the following:

- We investigate the feasibility of launching multi-device attacks on wireless localization systems. To the best of our knowledge, this work is the first to experimentally validate such an attacker model.
- We propose two new physical-layer features to detect multi-device attacks.
- We demonstrate that our features are able to distinguish spoofing and legitimate signals in less than ten seconds with less than eight receivers in the context of air traffic control.

2. BACKGROUND ON ADS-B SECURITY

2.1 System and Threat Model

The system model we consider in this work is motivated by air traffic monitoring (ATM) systems. In the next generation air transportation system, aircraft determine their own position from satellite navigation systems and broadcast it periodically to the surrounding ground stations. These position reports, called “squitters" in avionics jargon, represent the location claims of the aircraft along a track. In future, these location claims will be transferred over the ADS-B system. ADS-B does not define its own data transmission protocol but relies on a legacy wireless data link from secondary surveillance radar called Mode S [30]. Neither ADS-B nor Mode S provide any security guarantees such as authenticity or data encryption. ATM localization is therefore vulnerable to two kinds of spoofing attacks [32]:

Threat 1: An aircraft may broadcast periodic position updates which do not correspond to its real track. This attack is conceivable e.g., when a malicious pilot fakes the trajectory of an hijacked aircraft.

Threat 2: A third-party attacker on the ground injects fake position updates which do not correspond to any aircraft but look authentic to the ADS-B reception system. This produces one or more “ghost" aircraft in the air traffic monitoring system. This attack could be used by a malicious party to create confusion for pilots or air traffic controllers on the ground who have to deal with the fake information in their flight procedures and collision avoidance processes.

2.2 Limitations of Existing Countermeasures

The ADS-B system has not been designed for security, and it cannot prevent or detect the attacks described above. Interviews conducted in the aviation community [37] suggest that ADS-B signal spoofing is an open problem in deployed air traffic monitoring systems. However, given that the ADS-B signals are typically received by multiple receivers on the ground, it is possible to verify the location claims using *multilateration*. Several techniques have been proposed in the literature. For example, the authors of [25] propose to use the time-difference-of-arrival (TDoA) between difference receivers in combination with hyperbolic localization to verify the position claims in ADS-B messages. Capkun and Hubaux [9] build on the time-of-flight (ToF) derived from a secure distance bounding protocol between a prover and several verifiers to devise a verifiable multilateration system that is secure against adversaries. Schäfer et al. [34] have suggested a mobility-differentiated time-of-arrival (MDToA) method to verify signals between distributed receiver sites without the need for tight time synchronization among the multilateration sites. Chen et al. [10] perform statistical hypothesis testing on the residuals after the multilateration to detect location spoofing attacks.

While these techniques differ in the ways the location verification is performed, they all share the common assumption that the attacker is using a single device and therefore transmits spoofing signals from a single location. This assumption may hold true for Threat 1 when the aircraft aims at hiding its actual location by sending out fake position updates from its transponder. However, in both threat models, an attacker could rely on multiple spatially distributed devices to control individually the time of arrival at each receiver by sending delayed copies of the same signal at different locations.

Alternative approaches to secure ranging and localization systems are through the deployment of covert base stations (CBS) [8], or by using multiple or directional antennas [45] at the receiver locations. CBS provide a secret input to the system due to the fact that they are either hidden, meaning the attacker does not know their position during attack time, or they are in random movement, to which the attacker would need to adapt constantly. CBS help securing a wide variety of localization systems, but they are not applicable in ATM systems. ATM’s ground systems are large and often statically deployed at sites of existing publicly known legacy sensors and radar sites due to the readily available infrastructure.

By using multiple or directional antennas, it is to some extent possible to check the angle of arrival of the signal and thus verify the bearing of the transmitter. However, antenna systems that are capable of determining the bearing of the signal are costly, and the purpose of ADS-B is to reduce deployment costs by having simpler omnidirectional antenna structures as opposed to the directional antennas used currently for secondary radar [7]. Securing the system with angle information is therefore also not well suited to secure future ATM scenarios as these antennas will not be available in ADS-B deployments.

Sampigethaya et al. [31] proposed using aircraft to act as verifiers of position claims through exchanging information with other aircraft in the same airspace over an IP network. Current aircraft systems fail to provide this functionality in multiple ways. Not all aircraft are equipped with GPS technology, thus providing only coarse-grained position and time information. If an aircraft was to participate in a location verification scheme, high accuracy position as well as time is mandatory. While aircraft receive the ADS-B squitters from other aircraft and process them to give the pilots a sense of their surrounding airspace, these signals are not recorded with high-precision time information but rather forwarded from the ADS-B transponder to the pilot's cockpit display unit. Finally, only the newest aircraft are beginning to be equipped with network technologies to transmit data between aircraft and ground. Implementing a spoofing detection scheme on aircraft not equipped with general purpose network technology would require transmitting position and time information over conventional channels like Mode S. These channels are already at their capacity limits with standard in-flight transmissions and therefore will only add more congestion to the network.

3. MULTI-DEVICE ATTACK ON TDOA MULTILATERATION

In this section, we describe our multi-device attack setup and show how it can be used to effectively spoof the TDoA multilateration system used in the OpenSky network. Our main goal is to determine the timing precision required at the attacker's devices in order to accurately spoof ADS-B location claims that are verified by the multilateration system. We first describe the multilateration system and the experimental multi-device attack setup used for our analysis. Then, we present the results of the spoofing accuracy compared to the localization accuracy of ADS-B signals from legitimate aircraft.

3.1 Multilateration System

In our study, we use the multilateration system provided by the OpenSky Network [35]. The OpenSky Network is a crowdsourced ADS-B sensor network that collects among other things the periodic position messages sent by the aircraft. As of today, the sensor network comprises more than 50 sensors operated by volunteers which are deployed across ten European countries. The sensor coverage allows capturing around 60% of all flights that fly over Europe. The received ADS-B messages are collected at a central location for archival and real-time multilateration purposes. The OpenSky Network has different types of sensors, but the multilateration results are based on the Radarcapes from Jetvision [1]. The Radarcapes offer nanosecond-precision timestamps that the sensors assign to each ADS-B message after being received. The clocks of the Radarcapes that are used for the timestamps are all synchronized over GPS.

The multilateration technique employed by the OpenSky Network is based on hyperbolic localization, the same method that has been proposed for the secure verification of ADS-B position messages in [25]. Our results are however not specific to a particular multilateration technique and the timing precision requirements for the attack as well as the effects translate to other multilateration-based verification techniques as well such as [9, 34, 10].

In hyperbolic localization, the multilateration is performed through a ranging and a lateration step. The range R is the wave speed v (close to the speed of light in air) times the wave propagation time T. The multilateration system estimates the ranges based on the time-difference-of-arrival $\Delta_{i,j}$ of a signal at sensors i and j as

$$\Delta_{i,j} = T_i - T_j = \frac{R_i - R_j}{v}.$$

The second step is lateration. From the above equations for the ranges and the known positions of the sensors (x_i, y_i, z_i), the position (x, y, z) of the node to be localized can be estimated by calculating $(\hat{x}, \hat{y}, \hat{z})$ such that

$$(\hat{x}, \hat{y}, \hat{z}) = \underset{x,y,z}{\operatorname{argmin}} \sum_{i=1}^{n} [|\vec{x}_i - \vec{x}| - R_i]^2,$$

with

$$|\vec{x}_i - \vec{x}| = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}$$

where n corresponds to the number of sensors. To solve these equations, at least four sensors are needed. The resulting set of equations is not linear and can not be solved analytically. Several methods exist to numerically solve the above problem which mainly depend on the complexity and accuracy. For solving the equations, the OpenSky Network relies on a computationally lightweight linear approach [36]. This approach yields one of the most accurate linear least square solutions for multilateration [19].

3.2 Attacker Implementation

The adversary's goal is to spoof consecutive locations $(\hat{x}, \hat{y})$ of an aircraft over time such that the spoofed aircraft appears to be flying along a legitimate path[1]. In order to remain undetected by the multilateration-based verification system, the attacker must fulfill the following requirements:

1. The ADS-B messages should look like legitimate signals. The attacker must therefore make sure the ADS-B protocol semantics are correct and that the pretended trajectory is plausible (for example with a plausible speed, heading and altitude).

2. The time difference of arrival $\Delta_{i,j}$ between all sensors must be such as if the signal was transmitted from the spoofed location.

3. Each sensor should only receive the signals from the intended attacker device. If a sensor receives signals that are intended for other sensors, it can raise an alarm by detecting delayed copies of the same location claim.

To fulfill these requirements, we implemented a programmable ADS-B transponder in C++ using software-defined radios. The transponder consists of a regular PC and a USRP from Ettus Research [2] as the radio front-end as shown in Figure 1. The main design challenge was to achieve very tight time synchronization at different transponders in order to precisely control the spoofed signal's time difference of arrival at the receivers. Since radio signals travel close to the speed of light in free space, a timing offset of 1 μs already translates to 300 meters ranging error. Therefore, nanosecond-level precision is required between the transponders of the attacker in order to spoof locations with meter-level accuracy.

This time synchronization accuracy is particularly difficult to achieve on software-defined radios. Since the ADS-B signals are

[1]Note that we restrain ourselves in this work to spoofing of 2-dimensional positions because wide-area multilateration systems are not able to accurately determine the altitude of the aircraft due to a bad dilution of precision (DOP) when all sensors are on the ground. The attack setup we present can however be used to spoof 3-dimensional positions as well.

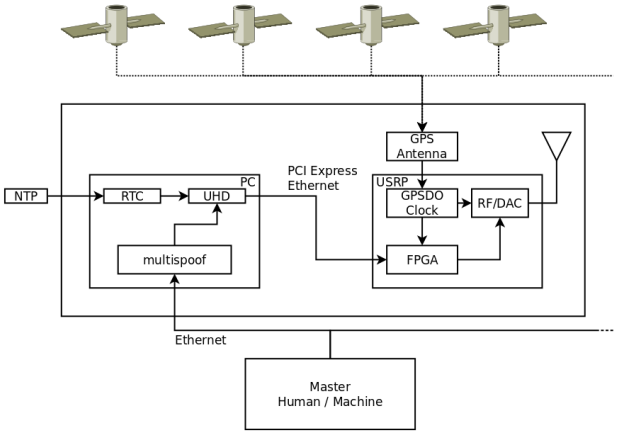

Figure 1: Software-defined radio architecture of the transponders for the attack. Time sychronization of the software-defined radios (USRP) is achieved using GPS disciplined oscillators.

generated in software on the CPU of the PC running with an operating system, it is hard to control the exact time of a particular operation on the CPU given the natural random jitter of the operating system and the interface to the USRP. To address this problem, we devised a software-defined architecture in which the PC only precomputes the messages and the required timing constraints for the attack, while the FPGA on the USRP is doing the actual scheduling of the transmissions over the radio front-end.

The transmitter pipeline works as follows. The code on the PC (referred to as *multispoof*), takes as input from a master PC an arbitrary trajectory to be spoofed and generates the sequence of all ADS-B messages that a transponder should transmit according to the standard [30] when flying this trajectory. Important are the position messages which are sent twice per second including the spoofed locations. These messages are then transformed to a stream of digital IQ samples on the PC according to the pulse position modulation (PPM) of the Mode S data link. These computed IQ samples are then transferred to the USRP through the USRP Hardware Driver (UHD). However, the ADS-B signals are not immediately transferred over the radio front-end but first buffered in the internal memory of the USRPs. The transmission times of these buffered samples are different for each radio and carefully selected in order to mimic the time difference of arrivals between the multilateration sensors for the claimed locations. The FPGAs on the USRPs then independently trigger the transmission of the samples of each ADS-B message based on the times specified in the buffers.

The last challenge to solve is the time synchronization among the USRPs. Classical software-defined radios such as the USRPs do not provide enough clock stability for the intended purpose because the clock used to trigger the FPGA is derived from a local oscillator which significantly drifts apart for different radios. Our approach to solving this problem was to replace the local oscillator of the USRPs with a GPS-disciplined oscillator (GPSDO). A GPSDO is an oscillator which is controlled by a tracking loop locked to the GPS signal. The GPS satellites are equipped with atomic clocks with very high time stability and therefore provide an excellent signal source for time synchronization. By locking the oscillators of the USRP to the GPS timing source, the USRP are now synchronized with very high accuracy and can trigger the transmissions at the correct times. The detailed schematics of the attacker setup is shown in Figure 1.

3.3 Experimental Results

Equipped with the attacker setup described above, we demonstrate in the following the feasibility to perform multi-device location spoofing attacks in the OpenSky Network. In addition to demonstrating the feasibility of these attacks, we further aim at understanding the limiting factors for the attacker and therefore perform additional benchmarks which serve to quantify the impact of different factors on the spoofing accuracy.

Performing an experimental over-the-air attack on a system like the OpenSky Network has some legal and safety implications, and we, therefore, have to be careful when designing the experiment. First, the 1090 MHz channel used to transmit ADS-B signals is licensed, and as such, only certified transponders are allowed to transmit in this frequency band. Second, the spoofed messages may be misinterpreted as legitimate signals by listening aircraft and ground controllers in the neighborhood leading to safety issues for the regular air traffic. To avoid legal and safety complications, we decided to minimize the risk of emitting spoofed messages to the outside world as much as possible and perform the experiments by transmitting the signals from the attacker to the receivers over shielded RF cables whenever possible. Only to study the impact of the channel conditions on the spoofing accuracy, we perform controlled over-the-air experiments with an antenna. Furthermore all the over-the-air experiments were conducted inside a large 7-floor concrete building with shielded windows to avoid any leakage to the outside world. We confirmed the same by measuring whether spoofed messages were received from the outside of the building.

3.3.1 Controlling the TDoA between Individual Receiver Pairs

In the first series of experiments, we quantify the ability of the attacker to control the exact TDoA for messages that are received by individual receiver pairs. The ability to control the TDoA at two receivers is the key to the success of the spoofing attack. The TDoA is affected by various factors including (i) the time synchronization error between the attacker devices, (ii) the measurement accuracy of the receivers to determine the time-of-arrival, (iii) the synchronization accuracy of the receivers themselves, (iv) and the channel quality between the attacker devices and the receivers (multipath reflections may add different delays to the propagation paths between sender and receivers). To discern the effect of these various factors, we evaluate the TDoA between two OpenSky receivers in three separate experiments:

Over-the-air: In this setup, we use two spoofing devices. Each spoofing device transmits its signals over an omnidirectional antenna to the receivers. The distances between the spoofing devices and the target receivers are 20 and 35 meters, respectively. Both transmitters and receivers are placed within the above-mentioned building. The wireless links between transmitters and receivers are line-of-sight, however since the devices are placed indoors, their channels will be affected by multipath reflections. Hence, we consider this experimental setup unfavourable for the attacker, since in reality, ADS-B receivers are placed outdoors on elevated spots and an outdoor channel is much less affected by multipath reflections than indoors. Nevertheless, we consider this experiment as useful to understand the accuracy of the attack when the channel is highly affected by multipath (i.e., worst case for the attacker).

Cable: In this setup, we directly connect the transmitters to the receivers with a shielded RF cable. Over cable, the channel is in very much in favor of the attacker since it is not affected by

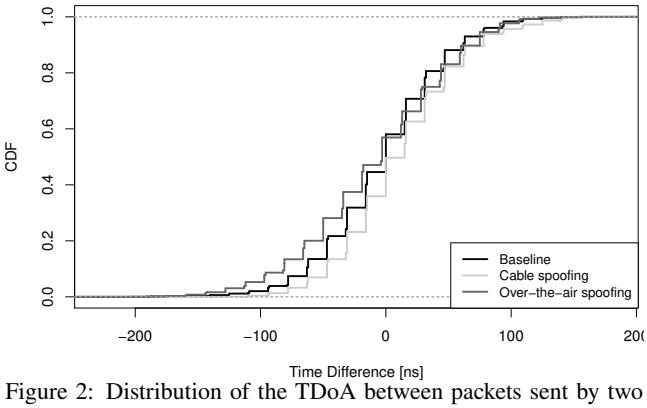

Figure 2: Distribution of the TDoA between packets sent by two spoofing devices. Over-the-air and cable experiments are close to the baseline.

multipath reflections. Therefore, this setup is useful at quantifying the noise caused by the synchronization error between the transmitters of the attacker setup since channel effects are ideal.

Baseline: This experiment is performed as a baseline to quantify the inherent noise of the receivers in measuring the TDoA of a signal that arrives exactly at the same time at the two receivers. To make sure that the signal arrives at the same time at both receivers, we use a single transmitter that is connected directly to both receivers over a T-connector and shielded RF cables of equal lengths.

Figure 2 shows the distribution of the TDoA for our three experimental setups when the spoofers are configured to produce a TDoA of zero at the two receivers. Several interesting conclusions can be made from the resulting distributions. First, the distribution for all three experiments shows a comparable standard deviation. While both cable-based measurements are distributed with standard deviation σ of about $50ns$, the measurements over the air yielded a standard deviation of approximately $60ns$. This indicates that the primary source of noise is not related to the synchronization error of the spoofer setup or the wireless channel but from the noise of the receivers themselves. The distribution of the mean TDoA values are also quite similar. The over-the-air experiments hold a mean deviation of $-7.5ns$, the spoofers over cable a mean of $11.4ns$, while the baseline only differs $-1.8ns$ from the expected mean of $0ns$. While both, the cable and over-the-air experiments do not perfectly match the signals of our baseline experiment, they do not add much additional error compared to the large uncertainty resulting from the high standard deviation of the TDoA measurements. These results confirm that an attacker can precisely time the TDoA at two receivers while using two separate spoofing devices.

3.3.2 Spoofing Accuracy

To evaluate the location spoofing attack performance, we use five spoofing devices that transmit signals to five OpenSky sensors as depicted in Figure 3. Each sensor is assigned with the location of a different airport in Switzerland. The distance between these locations measures between 30 and $130km$. When spoofing, a ghost aircraft is flown at a steady altitude of $10,000m$ between the two towns Thun and Solothurn corresponding to a distance of around $35km$. During this time, we transmitted a total of 494 position squitters per spoofing pipeline of which just over 250 messages were received on average per sensor. Around one-fourth of all transmitted messages were received by all five sensors, enabling the multilateration of the

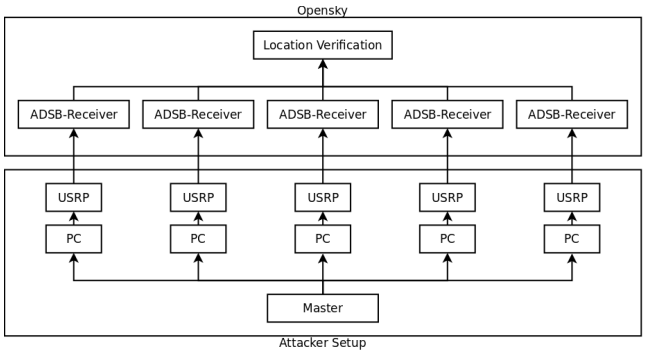

Figure 3: Overview of the multilateration attack setup. A master node connected to five attacking devices (PC and USRP) controls the exact time at which the five OpenSky receivers receive the ADS-B messages for multilateration.

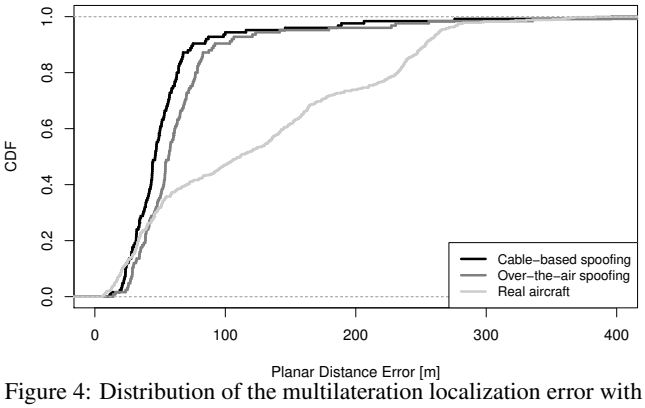

Figure 4: Distribution of the multilateration localization error with multi-device spoofing and messages from real aircraft measurements.

aircraft's position from these timestamps. The reception rates represent typical message losses in the real world [35].

As before, we conducted these experiments over cables. To estimate the location error in an over-the-air attack, we also spread the cable-based TDoA distributions by approximately 25%. This factor accounts for the wider TDoA distribution when the signals are transmitted over-the-air. We additionally extracted signals from legitimate aircraft recorded by OpenSky on September 11th, 2015 and identified a subset of 623 position messages that were received by the same set of five sensors. These sensors observed 66 different airplanes during the course of the day which we multilaterate in order to compare the estimated position with the actual postion reported in the ADS-B messages.

Figure 4 shows the ECDF of the multilaterated planar distance error for over-the-air spoofing estimation, cable spoofing and real-world aircraft. We can see that for a small number of multilaterated real aicraft messages, the planar localization error is smaller than for the spoofed messages. However, for more than 70 percent of the posititions of the real aircraft, the error is larger than spoofed aircraft. The spoofing accuracy is slightly better over cable than over-the-air but the difference is not that significant compared to the difference with the real aircraft messages. Over-the-air, only 90% of the multilaterated results lie within an error radius of 100 m from the actual spoofed positions, whereas the cable-based measurements produced 95% of multilaterated positions within the same error radius. This shows that an attacker can use multiple devices to accurately spoof arbitrary positions in a TDoA multilat-

eration system and that the error introduced is not larger than the typical error of multilaterated real aircraft.

4. SPOOFING DETECTION BASED ON PHYSICAL-LAYER FEATURES

In the previous section, we successfully demonstrated the feasibility of a multi-device location spoofing attack. In this section, we investigate the use of physical-layer features to distinguish if a signal originated from a single or multiple transmitters and hence, detect the multi-device attack in ATC scenarios. Physical-layer features are low-level signal characteristics of the received waveform prior being demodulated.

4.1 Requirements for an ATC IDS

Our intrusion detection system (IDS) is intended to work with the system constraints of the existing ATC technologies and procedures. This leads us to the following desired core properties of such an IDS concerning the data link layer, receiver locations and its acquisition methods:

No changes to the data link layer: The 1090ES (Mode S) [30] data-link layer protocol used by ADS-B cannot be modified easily. Any change to the data link would require the development and a deployment of new standards to all aircraft in the world which could easily take 10-20 years in order to complete. Therefore, the design of an IDS should integrate with existing message formats and communication protocols and must not require additional information exchanges. Introducing cryptographic mechanisms [44, 21] or distance bounding protocols [9, 11] for attack detection is, therefore, out of scope in the context of ATC systems.

Known receiver locations: The acquisition hardware for the IDS is to be collocated with existing multilateration receivers. These are typically at publicly known locations. Therefore, a hardness assumption can not be extracted from hidden receivers and associated properties of attacker channels such as proposed by previous work [8].

Decentralized acquisition: Acquisition devices are spatially separated. Therefore, recorded signals need to be sufficiently reduced in dimensionality before the extracted information can be combined into a centralized entity for intrusion detection.

4.2 Feature Selection

Our idea of using physical-layer features is inspired by radio fingerprinting techniques. However, our application of physical-layer features in this work differs from classical device fingerprinting approaches such as proposed in the literature [14, 16, 47, 22, 17, 27, 24, 6]. While the goal of classical device fingerprinting is to identify a specific device from a set of known devices at a single verification site, we use physical-layer features quite differently. In our context, physical-layer features are used to compare the signal of a seemingly single and unknown transmitter received at multiple receivers.

We have identified two challenges that are unique to this scenario. First, receivers introduce their own device-specific noise into the measurements of the physical-layer features. Since features collected by multiple receivers must be compared, it is necessary to identify features which are least affected by the receiver noise. Secondly, classical wireless device fingerprinting systems operate on optimal channels with the devices located in a somewhat close proximity to the signal's source and do not move as fast as to introduce a significant amount of Doppler shift. In contrast, our system has to deal with far-away, high-speed transmitter nodes. These properties render the channel far from optimal and distort the signal before it arrives at the receivers. We will experience interference, multipath propagation and Doppler effects, challenging the extraction of transmitter-specific features.

From the multitude of possible features, we have selected and evaluated two physical-layer features: a *frequency-based* feature of the modulated signal and a *phase-based* feature of the signal transient. We wanted the properties of our features to be universal, such that all tested devices exhibit the feature and unique, enabling all tested devices to be distinguished. Furthermore, the features should be extracted locally without the need for any external data and should be resilient to disturbances in the channel. Finally, an attacker should not be able to emulate the feature easily.

4.3 Frequency-based Feature

The idea behind the frequency feature is to take advantage of the imperfections in the transmitter's synchronization. In radio devices, the carrier frequency of the transmitted signal is derived from a local oscillator. In practice, it is impossible to perfectly synchronize the local oscillators of different devices that are separated over large distance. The clocks need to be synchronized with methods such as e.g. GPS-disciplined oscillators, which rely on wireless GPS signals for clock synchronization. Thus, the relative frequency offsets between different transmitters allow to discriminate whether the signals at different receivers originated from a single source or from multiple devices. We extract the *harmonic* peak frequency from a received discrete-time signal u through applying a discrete Fourier transform and maximizing the respective spectrum. The *harmonic* peak frequency is extracted as

$$f_p^{\mathrm{u}} = \operatorname*{argmax}_f |\mathcal{F}\{\mathrm{u}\}(f)|.$$

While normally applied to a stationary spectrum, this means of calculating the frequency offset yields the average of spectral contributions at different times for our signals with underlying frequency drifts. We obtain the harmonic frequency offset of two presumably identical signals u and v as follows:

$$\Delta f^{(\mathrm{u},\mathrm{v})} = f_p^{\mathrm{u}} - f_p^{\mathrm{v}}$$

Our distance metric between two signals captured at a receiver pair $\{i, j\}$ for the frequency offset is defined as

$$d^{(i,j)} \triangleq |\Delta f^{(i,j)} - \Delta f_{Rx}^{(i,j)} - \Delta f_D^{(i,j)}|.$$

This metric accounts for the receiver frequency offset $\Delta f_{Rx}^{(i,j)}$ as well as the expected Doppler shift $\Delta f_D^{(i,j)}$. The Doppler shift is calculated from protocol information where we process the aircraft's indicated speed vector and use

$$f_D = \left(\frac{v_r}{c} - 1\right) f_0$$

to calculate the signal's Doppler shift, with v_r being the radial velocity of the aircraft relative to the fixed receiver and f_0 being the nominal transmission frequency.

For illustration purposes, Figure 5 shows the distributions of the medians of the frequency offsets in our datasets with multi-device spoofing signals and legitimate aircraft (see Section 5.1 for the details of the experimental setup). Since real aircraft are moving, the received signals at the sensors experience a Doppler shift which we compensate by extracting the speed of the aircraft from the ADS-B messages. As we can see, the signals from real aircraft are located nearer to an offset of zero, the spoofer's signal offsets lie further from zero and experience a much flatter slope. This separation, especially between the Doppler compensated and the spoofer's curve

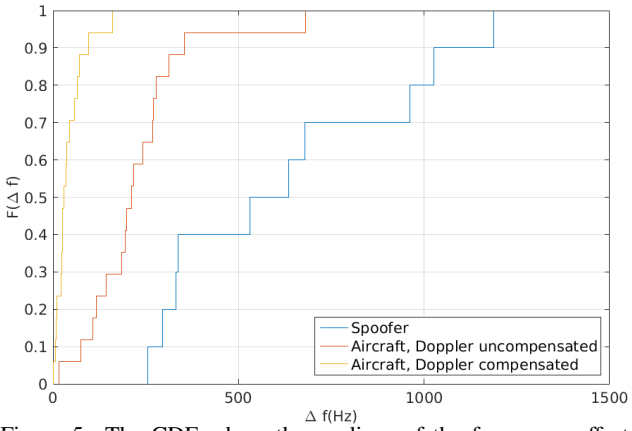

Figure 5: The CDFs show the medians of the frequency offsets of different spoofer and aircraft datasets. To the left we have the Doppler compensated and uncompensated aircraft signals; to the right the spoofer's frequency offsets.

highlight the applicability of this feature to discern spoofed signals originating from different attack devices.

However, we recognize that an attacker might be able to counteract his device's frequency offset by measuring the offsets himself and correct them in software prior to transmitting the spoofing signals. Additionally, the attacker may try to improve the stability and accuracy of the synchronization method and thus reduce his transmitter's frequency offsets. Nevertheless, a non-zero frequency offset is likely to remain given the imperfections in the hardware components used in the attacker's radio transmitters.

4.4 Phase-based Feature

Our second feature is based on the signal phase information. The radio front-end hardware introduces random, short time span phase variations called signal phase noise that cannot be emulated or compensated in the software during the signal generation. The phase noise is independent of the synchronization accuracy between transmitters and therefore remains discriminative even when the frequency offset between two signals is zero.

Before we can work with phase related properties, it is necessary to extract a phase vector. The extraction process is shown in Figure 6. We start by extracting the phase from the baseband signal vector u as

$$\tilde{\varphi} = \tan^{-1}\left(\frac{\mathrm{Im(u)}}{\mathrm{Re(u)}}\right).$$

To prevent distortion, we interpolate the phase vector to hold only one value for each pulse position. The resulting instantaneous phase vector φ can be decomposed as:

$$\varphi = \theta + \phi + \hat{\phi},$$

where θ denotes the initial phase, ϕ represents the frequency errors and $\hat{\phi}$ is the phase noise of the system. After unwrapping the phase, we calculate a regression curve over the extracted instantaneous phase. Using this approach, we are able to circumvent the need to measure the absolute value for the initial phase and the frequency errors as they are accounted for in the regression. Finally, the regression residual $\hat{\phi}$ is taken to represent the phase noise.

We have found in our experiments that the phase noise in the signal transient is most discriminative with regards to discerning different transmitters and decided to use the phase noise value of the first message pulse as the feature. Our observed behavior is consistent with prior studies [41, 42] that the PLLs exhibit transient

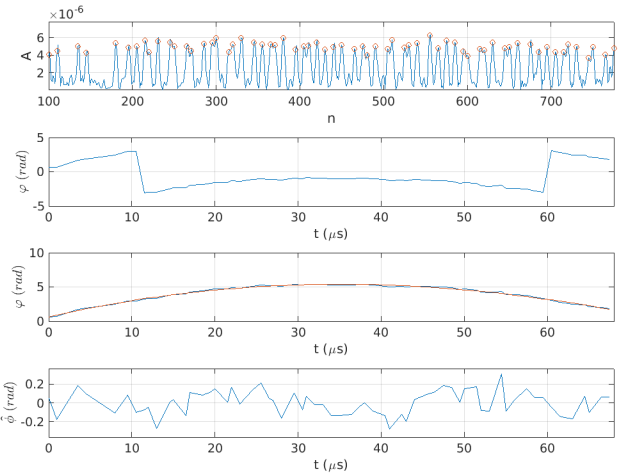

Figure 6: Phase extraction process for a sample message. The top plot reports the signal amplitude, followed by the instantaneous phase ϕ. The third plot shows the instantaneous phase after unwrapping (blue line) and the corresponding regression (orange). The difference between the two represents the phase noise and is displayed in the bottom plot.

behavioural characteristics during the tuning process to the carrier frequency. Therefore, observing additional pulses of the recorded signal will not improve our detection of a multi-device spoofing attack. The signals were captured using one sample per pulse. The phase noise for the first pulse is the first value in the phase noise vector $\hat{\phi}^{\mathrm{u}}$. This phase noise is extracted from a discrete-time signal u.

Figure 7 shows the different distributions of the phase transient for different transmitter/receiver pairs (see Section 5.1 for details about the experimental setup). While many pairs exhibit clearly distinguishable distributions, for some pairs the curves are very similar. We noticed that the transmitters with similar phase transient distributions have consecutive serial numbers, supporting our assumption that this feature is related to the hardware components.

While this feature's variance is similar across transmitters, the median of these distributions vary significantly (Figure 7). This effect leads us to use the median as the basis for our distance metric. For any given transmitter pair $\{i, j\}$, we define the distance metric as

$$d^{(i,j)} = |\hat{\phi}^i[1] - \hat{\phi}^j[1]|.$$

As shown in Figure 8, even though both distributions for the spoofer and the aircraft's signals are well separated, they still exhibit an overlapping area. We therefore aggregate this feature's data at more than two receivers to extract meaningful results and for the final distinction between legitimate and spoofing signals.

4.5 Decision Policy

Classification of the received signals is achieved through hypothesis testing. We define two hypotheses:

$$\mathcal{H}_0 : d^{(i,j)} = 0$$
$$\mathcal{H}_1 : d^{(i,j)} > 0,$$

where $\mathcal{H}_0$ denotes the null hypothesis, i.e. signals are legitimate, while $\mathcal{H}_1$ indicates that an attack is being launched against the system. The decision parameter $d^{(i,j)}$ represents the distance metrics for the frequency and the phase feature, respectively. We conduct

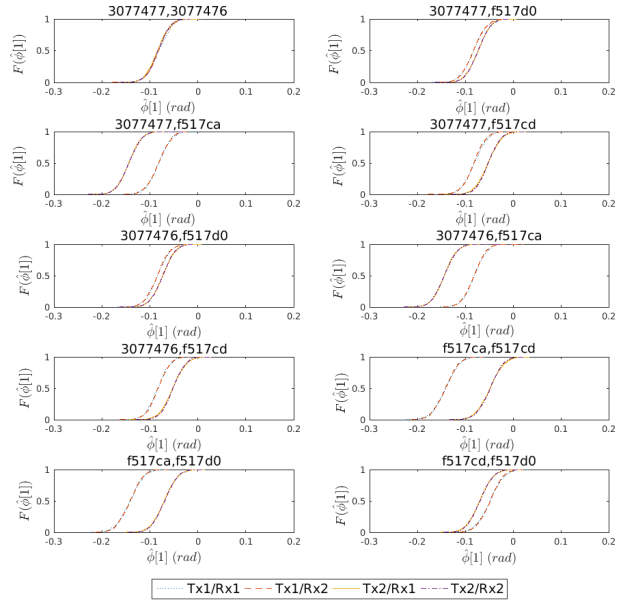

Figure 7: These CDFs show the distribution of the phase transient feature for different transmitter, receiver pairs.

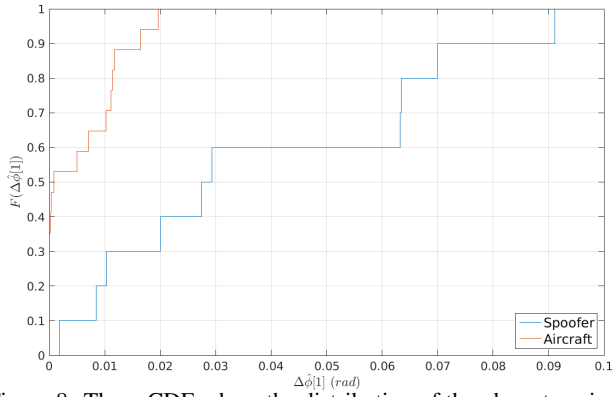

Figure 8: These CDFs show the distribution of the phase transient feature for real and spoofed signals.

the binary hypothesis testing for each sensor pair individually, yielding a 0 for normal operations and a 1 for an attack situation. The system then performs an OR operation on the results of all receiver pairs and determines its current state from this result. Therefore, it is sufficient for our system to raise an alarm if only one receiver pair detects an ongoing attack.

5. EVALUATION

The first part of this section introduces the experimental setup for the spoofing detection evaluation. In the second part, we describe the performance of our intrusion detection scheme.

5.1 Experimental Setup

To evaluate the performance of the frequency- and phase-based features for attack detection, we rely on an experimental setup with USRPs as the attacker devices and signal acquisition devices to derive the features. We rely on the experimental spoofing platform presented in Section 3. The spoofing dataset consists of 12 subsets, for all possible receiver combinations, with 2,000 received ADS-B squitters on average. To acquire real-world signals, we placed two receiving USRPs equipped with antennas for ADS-B reception with a separation of $25km$ between them. These sensors recorded a total of 17 datasets of ADS-B messages from 17 legitimate aircraft on June 9th, 2015. Each dataset holds between 71 and 263 messages. The attacker devices and receivers were in both cases synchronized using the internal GPS-disciplined oscillators. The signals were sampled at $10Msps$.

On the software side, we used a modified version of the `gr-air-modes` [26] ADS-B receiver for software-defined radio platforms. We modified the original program to pass the IQ signal samples through the whole processing chain. After successful detection and decoding of an ADS-B squitter, the receiver stores the IQ samples and the corresponding reception time to disk. For post-processing, we filtered all signals using a 4 MHz raised cosine band-pass filter with a roll-off factor of 0.1. Further, we discarded all transponder signals not adhering to the RTCA spectrum specification detailed in DO-260B [29].

5.2 Methodology

Our evaluation of the previously described features is conducted on the collected data, which includes real-world and spoofed transponder signals. The performance of intrusion detection of the frequency and the phase feature are evaluated separately. We designed our intrusion detection system in such a way that it requires little prior information to classify the received signals. For the example of the phase-based feature, no additional information is required. However, for the frequency based feature, it is necessary to know the average of all frequency offsets of a specific receiver pair and the velocity of the transponder from ADS-B protocol data a priori for estimating the Doppler shift.

5.3 Metrics

We evaluate the performance of our IDS according to three main metrics (i) false positive rate, (ii) false negative rate and (iii) decision latency. The false positive rate describes the set of signals, which originated from a real transponder but were wrongly classified as being spoofed. We want to keep the false positive rate as close to zero as possible, as ATC personnel should not be bothered too much by false alarms. A high false positive rate could have the effect of indifference towards alerts from the ATC personnel. If an adversary spoofs aircraft's signals with the alerts being ignored, our countermeasure would lose its sense. On the other hand, the false negative rate describes the set of spoofing signals, that were not detected by our system. Again, this value should be as close to zero as possible for our IDS to be effective and secure.

The third metric we use to evaluate the performance of our system is the *decision latency*. As it is not practical to base a decision only on the first message our system requires a number of received signals at multiple receivers. The ADS-B message rate, the number of received signals and the number of receivers required contribute to the decision latency.

5.4 Attack Detection Performance

Figure 9 shows the results for different configurations of the frequency and phase feature. Using the frequency offset, our IDS detects 96% of attacks with zero false positives using the average 30 messages, making use of four receivers. With the same parameters, the phase feature accomplishes an attack detection rate of 92% with again zero false positives. Using the average over 10 messages already skews our results as we encounter false positive classifications immediately from the beginning. If our IDS only uses one message for decision making, the false positive rate starts to dominate the classification results.

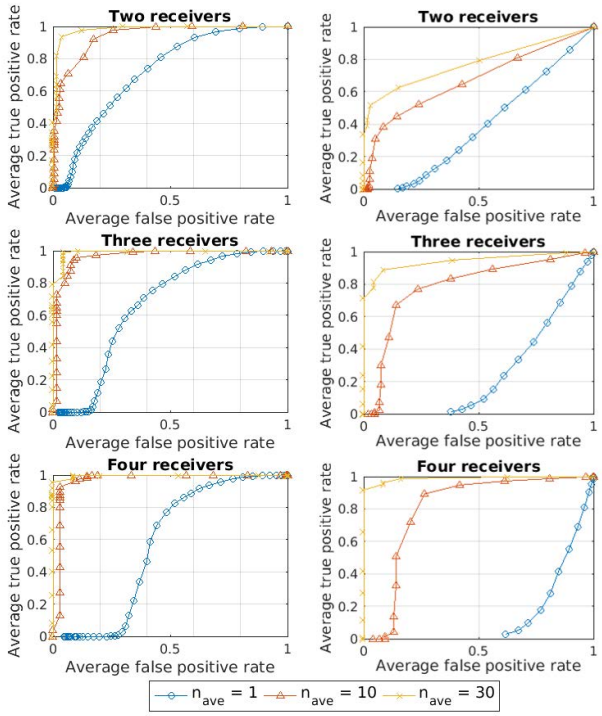

Figure 9: ROC curves for an IDS based on the frequency offset feature (left column) and on the phase feature (right column).

We observe that increasing the number of receivers is not optimal in every scenario. Furthermore, the number of receivers does not have the same effect for both the features. It is the phase feature that gains most from using multiple receivers. Generally, it can be stated that a higher receiver number will lower the false negative rate. This is an effect of our aforementioned decision policy (see Section 4.5) which is based around the fact that we raise an alarm if at least one pair of receivers detect an attack. On the other hand, using more receivers increases the false positive rate. Additionally, increasing the number of messages accounted for in the decision will lower the false positive rate. The aforementioned effects are detailed in Figure 10 where on the left hand side we take a fixed number of messages ($n = 30$) and a fixed number of receivers ($n_{rx} = 3$ for frequency and $n_{rx} = 4$ for phase) on the right hand side. The figure also shows the average error rate we calculated as the mean value between false positive and false negative rates.

For ideal IDS performance, we extended the parameter ranges to find the combinations which detected at least 99% of attacks with zero false positives. We vary the numbers of messages between 1 and 70 and the number of receivers between 2 and 10. As shown in Figure 9 and Figure 11, the system could not compensate a low number of messages with a higher number of receivers. We also observe that the gain from increasing the number of receivers from 3 to 4 has a negligible impact for the frequency feature while the impact is significant for the phase feature.

5.5 Channel Influence on the Phase Feature

While our attacker model enables the attacker to acquire an arbitrarily good channel, he might choose to opt for a non-ideal channel to distort his transmitter's hardware effects on the signal. Such a non-ideal channel might lead to multipath effects, thus distorting the signal's phase due to multiple copies arriving at the sensor at slightly different times. To better understand the channel's effect

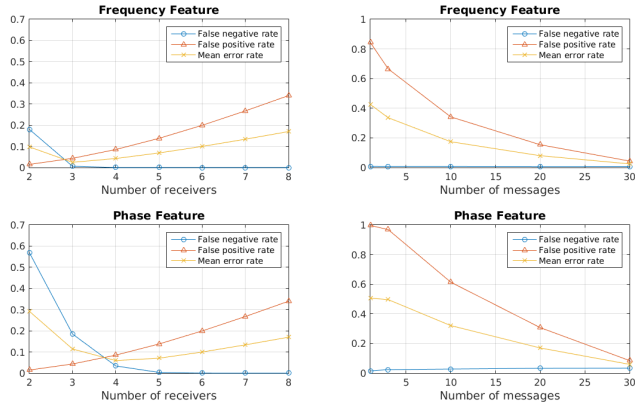

Figure 10: IDS performance for both the frequency offset and phase transient feature. The left column holds IDS performances for a fixed number of messages and variable number of receivers, while the right column shows the effect of varying the number of messages with a constant number of receivers.

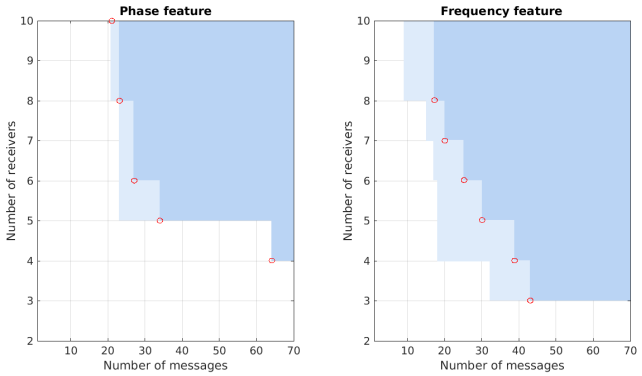

Figure 11: Ideal parameter combinations for both features. Ideal performance thereby refers to zero false positives and a false negative rate under 1%. Parameter regions consistently yielding ideal performance are highlighted in dark blue. Regions that contain some ideal parameter combinations are marked light blue. Marked red are the minimum parameter combinations for consistent ideal performance, i.e. Pareto-optimal parameter combinations.

on the phase feature, we have conducted an additional experiment with one transmitter pair. During these experiments, the channel was chosen both line-of-sight as well as non-line-of-sight (NLoS). Figure 12 shows our evaluations regarding the signal's phase transient in various channel conditions. Apparently, having a multipath environment increases the variance of our feature compared to an ideal channel. The medians are, however, still distinguishable enough to detect multiple transmitters. For the NLoS channel, the feature is significantly distorted to defeat the attack detection. While we acknowledge the possibility of an attacker distorting the phase transient through transmitting over a suboptimal NLoS channel, we deem the possibility of success very low. It is unlikely for an attacker to control in which way his signal is distorted over an NLoS channel, as he would need highly detailed knowledge about the channel. Additionally, sending over a bad channel works against the attacker's primary goal, which is to tightly control the time-of-arrival of his signal at the receiver.

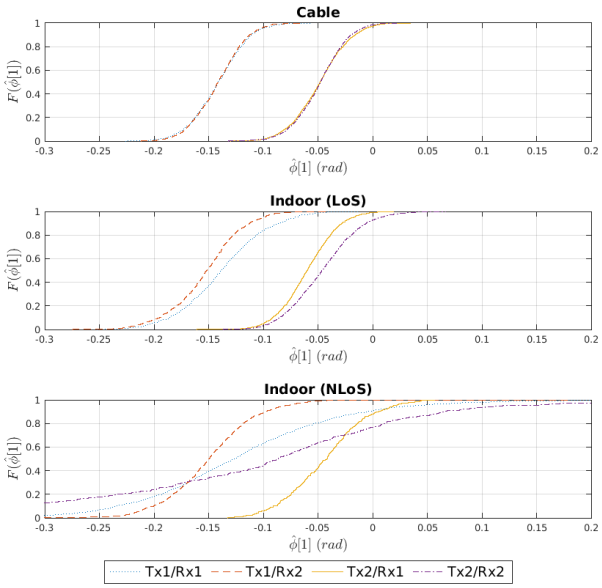

Figure 12: Effects of different channel conditions on the phase feature for the same USRP transmitter pair. The top plot shows the results for an ideal/cable based channel. The others depict the effect of the channel both line-of-sight and non-line-of-sight on our phase feature.

6. DISCUSSION

As shown in Figure 11, there are multiple possible combinations of the number of receivers and messages that yield optimal IDS performance. Our goal is to find the combination yielding the lowest decision latency. To determine a decision latency, we need to further define the message rate and the message loss factor. According to [30], an aircraft broadcasts 2 position and velocity messages per second and 1 identity message every 5 seconds. Taking into account further messages like priority status, TCAS and eventual emergency messages, we estimate an average message rate of 5.4 messages per second. The message loss at each receiver is estimated to be 10%. Using these parameters, we can conclude that for the frequency feature, using either 8 receivers and 17 messages or 7 receivers and 20 messages, will result in a minimal decision latency of 7.7 seconds. With the phase feature, we obtain a latency of 9.4 seconds with 27 messages received at 6 receivers.

For our IDS's operation, it is not necessary to always perform ideally in the first place, allowing us to reduce the number of messages for attack decision and thus reducing decision latency. An aircraft's trajectory has such a high message count that we can consider making decisions based on tens of messages. This assumption of course only holds as long, as our system's false positive decisions are not temporally clustered but evenly distributed. Therefore, we analyzed the intervals between two false positive decisions. Our IDS performs very promisingly for the phase feature, never yielding two consecutive false positive when deciding on a set of 10 messages. The frequency feature, on the other hand, does not perform as well as the phase feature. Using more messages for a decision does not lower the false positive rate that significantly.

While we only presented each feature individually in this paper, it is of course also possible to combine both features for decision making. However, we would need to establish a valid reference for the frequency feature based on known valid aircraft's signals. This could be established trough periodically employing the phase feature to build and refresh this reference set of signals. However, as we have shown some device's to exhibit the same phase transient behaviour, a sophisticated attacker with big enough budget might theoretically acquire multiple similar devices. Using a large set of sensors coupled with an attack detection policy, where an alarm will be issued for the case that only a subset of sensors determine an attack state, might defeat the attack through the added complexity for the attacker when deploying a large number of spoofing devices. In such a scenario, the attacker would also need to expose himself more, as his time spent in the proximity of the sensors rises, risking early exposure by the authorities.

The limitations of our intrusion detection system are that the frequency feature can be influenced by the attacker through measuring his device's frequency offsets and correcting them in the signal generation chain. He might also use a more precise synchronization method than GPS that will result in smaller frequency offsets between his transmitters. The phase transient feature can, however, not be influenced that easily because it is affected by the inherent noise of the hardware. The attacker has still the possibility to overstock on software-defined radios and measure their phase transient properties, selecting a subset of his stock for the attack. While an attacker might act according to this approach, financial factors might limit him on acquiring a large enough set of transmitters. The financial factor is also the reason why we deem attempts to reduce the noise by using high-end RF equipment such as low-noise arbitrary waveform generators (AWG) or special-purpose hardware a challenge for the attacker. Danev et al. [13] have shown that AWGs are able to replay recorded signals to an extent where fingerprinting systems can not distinguish between the legitimate transmitter and an AWG. While high-end AWGs might be able to produce highly accurate signals with little noise in the transient phase, they are by a factor of 20 to 100 times more expensive than today's SDR platforms and would require a prohibitively high budget on the attacker's side since a distributed attack requires at least a couple of such devices.

7. RELATED WORK

Costin [12] and Schäfer [33] take an experimental approach to assess possible attacks against ADS-B based on protocol semantics of ADS-B message content. Our work instead focuses on timing attacks on ADS-B multilateration, a threat model they did not consider. Previous work [20, 3, 28, 38, 9, 21] suggest to use multilateration systems to verify the location data in ADS-B and other attack scenarios. However, they do not look at distributed attack models as we do in this work.

Several efforts have been devoted by the research community on securing multilateration systems. Chen et al. [10] and Du et al. [15] proposed methods for attack detection based on statistical hypothesis testing, either before [10] or after [15] the localization phase. However, this approach is based on the assumption that spoofed TDoA patterns yield statistically significant differences from a single (non-spoofed) transmitter, an assumption that is clearly invalidated by our experimental results.

Performance evaluations of multilateration in adversarial setups were conducted in previous work [5, 43]. Therein, the adversary leverages beamforming to falsify the signal strength at the receivers. They consider RSS-based localization and study the problem from a theoretical perspective. In contrast, our work focuses on time-based multilateration and provides an experimental assessment. The problem of detecting multiple attackers masquerading as a single legitimate node and injecting spoofed traffic into a wireless network was also proposed [46], again in the framework of RSS-based, not time-based localisation.

Using the angle-of-arrival (AoA) to detect spoofers with multi-

ple or directional antennas [45] is opposite to the goals of the introduction of ADS-B, which is to abolish secondary radar and subsequently directional antennas. It would however be possible, to use the directional antennas of the secondary radar for an AoA system during the transition period towards fully deployed ADS-B. While AoA will detect most attackers, it will still fall victim to the most determined and prepared. Combined with our approach from this paper, such a system would detect even very determined attackers that can evade the detection from AoA through adding a second hurdle.

Tippenhauer et al. [40] have analyzed the requirements to spoof GPS signals. Although GPS and ADS-B multilateration are both based on the TDoA principle, these two systems are fundamentally different: in GPS a single receiver collects TDoA measurements from multiple transmitters, while the situation is reversed in ADS-B, where a set of receivers measure the arrival times of signal from a single transmitter. Therefore, the attack requirements are markedly different for the two systems.

Transmitter-specific hardware features have been used for device identification and authentication [14, 16, 47, 22, 17]. Brik et al. [6] identify wireless devices according to their specific frequency offset. Others have looked at frequency-domain correlations [39] as well as signal phase [18, 42, 41] to identify a transmitting device. Differently from such previous work, where physical-layer features were employed for transmitter identification and authentication, here, we rely on physical-layer features to reveal whether the signal was transmitted from a single source or instead by multiple (coordinated) devices. Moreover, while previous work has assumed ideal channels, we have designed features that can be robustly acquired across the non-ideal channel between a moving aircraft and ground stations.

8. CONCLUSIONS

This work has shown that a distributed multi-device attacker model is a realistic threat scenario to TDoA multilateration systems. We have shown that using COTS software-defined radios with GPS synchronization, it is possible to generate spoofing signals with a sufficient synchronization over large areas such that the localization error of the multilateration becomes indistinguishable from the error of legitimate signals.

Given this result, we have analyzed the usage of physical-layer features to detect multi-device attacks against wireless multilateration systems. We identified and evaluated a frequency-based and a phase-based feature which can be used to detect distributed attackers. These features are well suited to detect distributed spoofing attacks in air traffic surveillance scenarios because the attack detection is (i) purely passive, (ii) does not require any changes to the legacy data communication protocols, (iii) requires only limited exchange of information between the sensors, and (iv) works even when the multilateration sensor locations are known by the attacker.

9. ACKNOWLEDGEMENT

This work was partially supported by the Zurich Information Security and Privacy Center. It represents the views of the authors.

10. REFERENCES

[1] Radarcape. http://shop.jetvision.de/Radarcape. [Online; accessed 11/13/2015].

[2] X300 Product Page. http://www.ettus.com/product/details/X300-KIT. [Online; accessed 12/07/2014].

[3] Wide Area Multilateration, Report on EATMP TRS 131/04, Version 1.1. https://www.eurocontrol.int/sites/default/files/publication/files/surveilllance-report-wide-area-multilateration-200508.pdf, 2005. [Online; accessed 02/16/2015].

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

[5] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker. The directional attack on wireless localization -or- how to spoof your location with a tin can. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, Nov 2009.

[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, pages 116–127, New York, NY, USA, 2008. ACM.

[7] S. R. Bussolari and D. J. Bernays. Mode s data link applications for general aviation. In *Digital Avionics Systems Conference, 1995., 14th DASC*, pages 199–206. IEEE, 1995.

[8] S. Capkun, K. Bonne Rasmussen, M. Cagalj, and M. Srivastava. Secure location verification with hidden and mobile base stations. *Mobile Computing, IEEE Transactions on*, 7(4):470–483, April 2008.

[9] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1917–1928 vol. 3, March 2005.

[10] Y. Chen, W. Trappe, and R. Martin. Attack Detection in Wireless Localization. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1964–1972, May 2007.

[11] J. T. Chiang, J. J. Haas, J. Choi, and Y.-C. Hu. Secure Location Verification Using Simultaneous Multilateration. *IEEE Transactions on Wireless Communications*, 11(2), feb. 2012.

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

[13] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy. Attacks on physical-layer identification. In *Proceedings of the Third ACM Conference on Wireless Network Security*, WiSec '10, pages 89–98, New York, NY, USA, 2010. ACM.

[14] B. Danev, D. Zanetti, and S. Capkun. On physical-layer identification of wireless devices. *ACM Comput. Surv.*, 45(1):6:1–6:29, Dec. 2012.

[15] W. Du, L. Fang, and P. Ning. Lad: Localization anomaly detection for wireless sensor networks. In *International Parallel and Distributed Processing Symposium - IPDPS*, page 874, 2005.

[16] K. J. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. *Radio Science*, 36(4):585–597, 2001.

[17] J. Hall. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *In Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT*, pages 201–206. Kranakis, 2004.

[18] J. Hall, M. Barbeau, and E. Kranakis. Detection of transient

in radio frequency fingerprinting using signal phase. *Wireless and Optical Communications*, pages 13–18, 2003.

[19] IA Mantilla Gaviria. *New strategies to improve multilateration systems in the air traffic control*. PhD thesis, Universitat Politècnica de València, 2013.

[20] ICAO. Guidance Material: Security issues associated with ADS-B. Technical report, 2014.

[21] T. Kacem, D. Wijesekera, , and P. Costa. Integrity and authenticity of ads-b broadcasts. In *IEEE Aerospace Conference*, 2005.

[22] D. Knox and T. Kunz. Secure authentication in wireless sensor networks using rf fingerprints. In *Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on*, volume 1, pages 230–237, Dec 2008.

[23] T. Leinmuller, E. Schoch, and F. Kargl. Position verification approaches for vehicular ad hoc networks. *IEEE Wireless Communications Magazine*, 13(5):16–21, 2006.

[24] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of the 5th ACM Workshop on Wireless Security*, WiSe '06, pages 33–42, New York, NY, USA, 2006. ACM.

[25] M. Monteiro. Detecting malicious ads-b broadcasts using wide area multilateration. In *Proceedings of the 34th Digital Avionics Systems Conference (DASC)*, September 2015.

[26] Nick Foster. gr-air-modes. https://github.com/bistromath/gr-air-modes. [Online; accessed 12/07/2014].

[27] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*, MobiCom '07, pages 111–122, New York, NY, USA, 2007. ACM.

[28] K. Pourvoyeur and R. Heidger. Secure ADS-B Usage in ATC Tracking. In *Digital Communications - Enhanced Surveillance of Aircraft and Vehicles*, TIWDC/ESAV, 2014.

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

[30] RTCA, Inc. Minimum operational performance standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance - Broadcast (ADS-B) and Traffic Information Services - Broadcast (TIS-B). *Report DO-260B (with Corrigendum 1)*, Dec 2011.

[31] K. Sampigethaya and R. Poovendran. Visualization & assessment of ADS-B security for green ATM. In *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th*, pages 3.A.3–1 – 3.A.3–16, October 2010.

[32] M. Schäfer, V. Lenders, and I. Martinovic. Experimental analysis of attacks on next generation air traffic communication. In *Applied Cryptography and Network Security (ACNS)*. Springer, June 2013.

[33] M. Schäfer, V. Lenders, and I. Martinovic. Experimental analysis of attacks on next generation air traffic communication. In M. Jacobson, M. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *Applied Cryptography and Network Security*, volume 7954 of *Lecture Notes in Computer Science*, pages 253–271. Springer Berlin Heidelberg, 2013.

[34] M. Schäfer, V. Lenders, and J. Schmitt. Secure track verification. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 199–213, May 2015.

[35] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm. Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research. In *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, IPSN '14, pages 83–94, Piscataway, NJ, USA, 2014. IEEE Press.

[36] R. Schmidt. A New Approach to Geometry of Range Difference Location. *Aerospace and Electronic Systems, IEEE Transactions on*, AES-8(6):821–835, Nov 1972.

[37] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic. On Perception and Reality in Wireless Air Traffic Communications Security. *ArXiv e-prints*, Feb. 2016. http://arxiv.org/pdf/1602.08777v2.

[38] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic. Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B. *IEEE Communications Magazine*, 52(5):111–118, May 2014.

[39] W. Suski, M. A. Temple, M. J. Mendenhall, and R. Mills. Using spectral fingerprints to improve wireless network security. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, Nov 2008.

[40] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 75–86, New York, NY, USA, 2011. ACM.

[41] J. Toonstra and W. Kinsner. Transient analysis and genetic algorithms for classification. In *WESCANEX 95. Communications, Power, and Computing. Conference Proceedings., IEEE*, volume 2, pages 432–437 vol.2, May 1995.

[42] J. Toonstra and W. Kinsner. A radio transmitter fingerprinting system odo-1. In *Electrical and Computer Engineering, 1996. Canadian Conference on*, volume 1, pages 60–63 vol.1, May 1996.

[43] T. Wang and Y. Yang. Analysis on perfect location spoofing attacks using beamforming. In *INFOCOM, 2013 Proceedings IEEE*, pages 2778–2786, April 2013.

[44] K. D. Wesson, T. E. Humphreys, and B. L. Evans. Can cryptography secure next generation air traffic surveillance. *IEEE Security and Privacy Magazine*, 2014.

[45] J. Xiong and K. Jamieson. Secureangle: Improving wireless security using angle-of-arrival information. In *ACM SIGCOMM HotNets*, 2010.

[46] J. Yang, Y. Chen, W. Trappe, and J. Cheng. Detection and localization of multiple spoofing attackers in wireless networks. *Parallel and Distributed Systems, IEEE Transactions on*, 24(1):44–58, Jan 2013.

[47] P. Yu, G. Verma, and B. Sadler. Wireless physical layer authentication via fingerprint embedding. *Communications Magazine, IEEE*, 53(6):48–53, June 2015.