Orbit-based Authentication Using TDOA Signatures in Satellite Networks

Eric Jedermann
jedermann@cs.uni-kl.de
University of Kaiserslautern
Germany

Martin Strohmeier
Martin.Strohmeier@armasuisse.ch
Armasuisse
Switzerland

Matthias Schäfer
schaefer@cs.uni-kl.de
University of Kaiserslautern
Germany

Jens Schmitt
jschmitt@cs.uni-kl.de
University of Kaiserslautern
Germany

Vincent Lenders
vincent.lenders@armasuisse.ch
Armasuisse
Switzerland

ABSTRACT

Given the nature of satellites orbiting the Earth on a fixed trajectory, in principle, it is interesting to investigate how this invariant can be exploited for security purposes. In particular, satellite orbit information can be retrieved from public databases. Using time difference of arrival (TDOA) measurements from multiple receivers, we can check this orbit information against a corresponding TDOA-based signature of the satellite. In that sense, we propose an orbit-based authentication scheme for down-link satellite communications in this paper. To investigate the properties and fundamentals of our novel TDOA signature scheme we study two satellite systems at different altitudes: Iridium and Starlink.

Clearly, many challenging questions with respect to the feasibility and effectiveness of this authentication scheme arise; to name some: how many receivers are necessary, how should they be distributed, and how many consecutive measurements do we need for the TDOA signatures. We address these questions by a full factorial experimental design using a simulation framework, we developed for that purpose. Besides a deep understanding about the effects of the major factors on the authentication performance, we find that in adequate configurations, even under a versatile attacker, the orbit-based authentication scheme is able to achieve low false authentication rates well below 1% at false rejection rates of about 2%, for both, Iridium and Starlink satellites.

CCS CONCEPTS

• **Security and privacy** → *Systems security*; *Authentication.*

ACM Reference Format:
Eric Jedermann, Martin Strohmeier, Matthias Schäfer, Jens Schmitt, and Vincent Lenders. 2021. Orbit-based Authentication Using TDOA Signatures in Satellite Networks. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28–July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3448300.3469132

WiSec '21, June 28–July 2, 2021, Abu Dhabi, United Arab Emirates

ACM ISBN 978-1-4503-8349-3/21/06.
https://doi.org/10.1145/3448300.3469132

1 INTRODUCTION

Satellite communications systems such as GPS and parts of Iridium are known to have security issues, most prominently being vulnerable to spoofing attacks. Various analyses [23, 26] and some countermeasures [17, 18] to those attacks were introduced.

While newer constellations such as the Russian GLONASS or the European GALILEO address problems such as spoofing through cryptographic means, updating already deployed and widely used systems with additional cryptographic primitives is often unattractive. The requirement of backwards compatibility of field devices or the expensive exchange of equipment on sender and receiver side are two prominent reasons against subsequent systematic updates and are good arguments to design alternative countermeasures, often based on physical layer security mechanisms.

To that end, this paper introduces the concept and investigates the *feasibility* of authenticating satellite communication based on sequences of time difference of signal arrival measurements, called *TDOA signatures*. The proposed TDOA signature method shows promise as a lightweight security upgrade for existing satellite systems without changes in their hardware or protocols. It builds on the fact that a satellite's identity – which we aim to authenticate – is tightly coupled with its orbital state vector and epoch (collectively "orbit"). Each satellite has its own unique orbit and its signals therefore create unique TDOA patterns (signatures) as it passes by a set of terrestrial receivers. If the orbit is known and the observed TDOA signature matches the expected signature, the satellite's signals are successfully authenticated. Hence, in analogy to the concept of location-based authentication that was first introduced by Denning and MacDoran in 1996 [7], we authenticate satellite communication signals by applying a light-weight TDOA orbit verification.

Our simulative evaluation of the fundamental properties of this approach shows that it is very effective. Compared to existing authentication schemes based on signal fingerprinting (e.g., [17]), hardware requirements for measuring TDOAs are low and knowledge of satellite orbits is abundant and easily accessible through extensive public databases. In contrast, fingerprinting-based authentication involves learning its signal fingerprint, which is "specifically difficult for Low-Earth Orbit (LEO) satellites" [17]. Since most satellites in orbit are LEO satellites (78%), and as they experience a huge growth in recent times this work focus on LEOs; note, however, that our approach should also be well applicable for satellites at higher altitudes.

Contributions. This paper provides two main contributions. First, we introduce the concept of combining the known satellite orbit with observable TDOA-based signatures to authenticate satellite communications. We have performed extensive simulations based on real-world satellite databases to obtain realistic false rates. Second, we conducted an analysis of variance (ANOVA) to study the effects of different factors on the feasibility and accuracy of this approach. This analysis provides insights on which factors influence the performance of the authentication scheme the most.

2 BACKGROUND

The principle of location-based authentication was introduced in 1996 by Denning and MacDoran [7]. Later, it was adopted by Singelee and Preneel [24] for distance bounding-based authentication. Both utilized it as an alternative to traditional authentication via knowledge (secrets) or ownership (chip cards). This principle has also been proposed in the form of multiple receiving antennas for the verification of satellite signals. This approach has emerged as one main alternative to traditional signal-processing based anti-spoofing techniques (see [21] for a detailed overview of attack and defense options using the example of GNSS). Going one step further, Jansen [11] and Tippenhauer [26] analyse the feasibility and required accuracy for a successful GNSS-spoofing attack, and discuss possible countermeasures under a scenario with multiple spoofers.

Oligeri et al. [17] suggest an alternative authentication approach by using software-defined radios to collect I/Q samples of Iridium signals in combination with convolutional neural networks to create physical-layer fingerprints. With their system an accuracy between 80% and 100% was possible, depending on the underlying assumptions. In another recent work of Oligeri et al. [18], the authors used unencrypted Iridium Ring Alert messages to verify their own position. Based on this independent verification, the detection of GNSS spoofing was possible. Also they briefly analyzed the feasibility of spoofing Iridium signals for their approach and point out some hurdles that increase the effort for an attacker compared to spoofing GPS signals.

Beyond authentication, satellite security has recently become a hot research topic. Lohani and Joshi [15] provide an introduction to satellite networks and their security challenges. Pavur et al. [19] reveal the feasibility of eavesdropping on unencrypted Internet traffic via satellites with publicly available consumer equipment.

The literature covers several main TDOA-based location determination algorithms. Chan and Ho [4] proposed a two-staged least squares approach, which was improved by Chan et al. [3] using a closed-form approximate maximum likelihood algorithms. Ho and Xu [10] developed a weighted least squares minimization for TDOA and FDOA measurements to estimate the location and velocity of the target. Liu et al. [14] developed a maximum likelihood estimator for decentralized scenarios. In a satellite scenario, however, these approaches suffer from either a low accuracy or demanding system requirements arising from an inconvenient dilution of precision (DOP). The DOP is a geometric metric for the relative distribution of the receivers and senders in a setup. As the receivers come relatively closer together and the sender departs from the receivers, the DOP becomes ever worse. Worthy and Holzinger [29] investigate the influence of the DOP on orbit determinations.

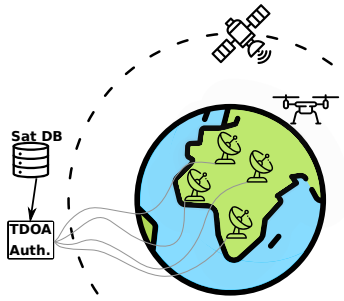


Figure 1: Orbit-based authentication using TDOA signatures.

2.1 Time Difference of Arrival

In our proposed authentication scheme, we focus on TDOA as it can be measured with simple hardware and is well understood.

A sender transmits a signal at time t_0. Depending on the distance d and signal velocity c, the time of flight (TOF) is $TOF = \frac{d}{c}$. The receiver a with the distance d_a to the sender receives the signal at an individual time of arrival (TOA) $TOA_a = t_0 + TOF_a = t_0 + \frac{d_a}{c}$. The same holds for a second receiver b: $TOA_b = t_0 + \frac{d_b}{c}$.

Hence, for receivers a and b their time difference of arrival is: $TDOA_{ab} = TOA_b - TOA_a = TOF_b - TOF_a = \frac{d_b - d_a}{c}$. Below the $TDOA_{ab}$ is referred to as $TDOA_b$, since all TDOAs are in reference to the same receiver (here a).

The TDOA metric does not require any synchronization between the receivers and the sender, but among the receivers. Therefore, the synchronization accuracy is one of the factors discussed in Section 5. With multiple TDOA measurements and the knowledge of the receiver positions, it is possible to draw conclusions about the position of the sender.

2.2 LEO Satellite Constellations

To investigate the influence of factors such as the amount of receivers or the number of messages (more in chapter 5) the data of two different satellite systems are used. The first one is the Iridium satellite system, which consists of 75 LEO satellites with an altitude of 780 km. The second system is the Starlink system, which currently consists of 887 satellites at an average altitude of 530 km. More details about the processing and the source of the satellite data is provided in chapter 3.3.

3 ORBIT-BASED AUTHENTICATION

3.1 Concept

This work investigates a system for authenticating received satellite signals based on TDOA signatures. A TDOA signature is defined by the resulting time difference of arrivals due to the $n \cdot m$ positions of $n + 1$ receivers relative to m orbit positions of the sending satellite. Here m represents the number of TDOA measurements, coinciding with downlink messages from the satellite.

The concept of the authentication scheme is illustrated in Fig. 1: A sender is emitting a signal, which is received by multiple receivers. The sender can be a satellite (or a drone, in case of an attacker), as visualized in the upper right corner of Fig. 1. Satellites are orbiting

the earth at a known orbit, while drones are assumed to fly in the atmosphere. Multiple receivers that notice the message *cooperate* to assess whether the transmission comes from an expected satellite. Each receiver i from the $n+1$ receivers (in the middle of the figure) observes the j-th message at an individual time of arrival TOA_{ij}. The TOAs of multiple receivers are collected and are combined to time difference of arrival $TDOA_{ij}$ measurements (on the left side of the figure). Overall, we obtain the TDOA signature of the sender as the matrix $\mathcal{T} = (TDOA_{ij})_{i=1,\ldots,n,j=1,\ldots,m}$. As illustrated, we assume a server-based centralized computation of the TDOA signature; a completely distributed computation would also be possible, yet may become expensive in the required meshed communication between the receivers.

For authenticating the TDOA signature, the orbit data of all satellites is required, which is available from public databases. For each satellite in the database the expected TDOA signature is compared to the received TDOA signature to determine the source of the signal. Due to the knowledge of the orbits of the satellites and the fact that every satellite can be identified by its orbit, this can be used to authenticate a received message and in case of rejection the respective receiver under attack can be alerted. The communication between receivers and the TDOA signature server could either be itself based on the satellite communication system or use an out-of-band terrestrial channel.

With this concept, it is possible to realize a continuous authentication, where a single message or small bursts of messages can be authenticated independent from previous communication.

3.2 The TDOA Signature Mechanism

We now describe the TDOA signature mechanism in some more detail. First, the observed TDOA signature $\mathcal{T}^o$ is compared with the expected signature $\mathcal{T}^s$ of each satellite s. The root mean squared error (RMSE) is then calculated as

$$E_s(\mathcal{T}^o, \mathcal{T}^s) = \sqrt{\frac{1}{nm} \sum_{j=1}^{m} \sum_{i=1}^{n} (\mathcal{T}_{ij}^o - \mathcal{T}_{ij}^s)^2}$$

between both signatures.

Satellites that are below the horizon of receivers are not visible and are assumed not to send a receivable signal. The satellite with minimum error is selected as temporal signal source. This is conceptually similar to a nearest neighbour match in the TDOA/time domain.

In a second step, it is evaluated whether the signal is coming from the satellites region or from another signal source inside the atmosphere, e.g. a drone, in the same direction. Therefore, a 3-dimensional grid of points is arranged between the receivers and the satellite. The RMSE of each grid point's signature is evaluated. If a grid point below 100 km in altitude has a significant (40%) lower RMSE, it is assumed to be an attacker from inside the atmosphere, like a drone or a plane.

This proposed algorithm was tested together with variants of least-squares and probability-density based algorithms and has turned out to be the most reliable.

3.3 Simulation Model Assumptions and Real-World Satellite Data

The status of a satellite orbit is publicly available in a so-called Two-Line-Element (TLE). Each TLE contains information about the satellite like the current epoch, the inclination and eccentricity, to name a few. They are used to describe the position and velocity of the satellite in the True Equator Mean Equinox (TEME) coordinate system. This coordinate system is an inertial coordinate system that is not rotating with the earth (it is fixed w.r.t. the stars). The given TLE orbit deviates from the real position of the satellite over time, therefore, an equal distributed position error is introduced for sending satellites. This TLE accuracy will be discussed in more detail in Section 5.

For the simulation a TLE dataset from the 13th January 2021 from NORAD [5] is used. It contains the data of nearly 3.4k satellites, including 2.7k LEO satellites. The python-library 'sgp4' [1] is used to calculate their orbital positions and to convert positions between the TEME and the international terrestrial reference system (ITRS). The ITRS is an earth fixed system (rotating w.r.t. the starts) , used by the 'astropy' [6] library to manage the positions of the earth fixed receivers. The receivers positions are converted into TEME to calculate the TOF to the satellites signal.

The receiver positions are newly generated in each replication of the simulation. Therefore, a center position is randomly chosen from a set of 21 hard-coded locations in cities of Europe. The newly generated receiver locations are uniformly arranged in a circle around this center position.

Two factors influence the geometry of newly generated receivers: the diameter of the circle and the number of receivers. For both factors a noise of 10 to 20% is added to randomize the positioning to make the results more reliable. During the simulation a normal distributed error is added to each TOA measurement, to cover synchronization and sampling inaccuracies of the receivers. All three factors (diameter of circle, number of receivers and receiver inaccuracies) are investigated in detail in Section 5.

4 ADVERSARY MODEL

To describe the adversary model, some assumptions about the attacker are made: at first we limit the attacker to use a single signal source. Stronger models such as a distributed attacker with multiple signal sources are discussed in Section 7.

Second, we assume that the attacker's signal is received by all receivers that are used for creating the TDOA signature. In case a signal is received by only one or two receivers we can discard this signal, since a signal from a legitimate satellite should be received by multiple receivers in the satellite's beam. The scenario of a degraded authentication, where fewer receivers are used and thereby a wider range of valid positions are enabled, is not considered here.

Besides this receiving property, the receivers cannot yet distinguish between a valid satellite signal and an attacker signal, for example, by analyzing the modulation or other properties.

In addition, the positions of all receivers are known to the attacker (as well as, of course, the position of the satellite to be spoofed). Therefore, it is able to place an attacking drone between a satellite and the receivers. Thereby the existence and the trajectory of the drone is unknown to the receivers.

Two attacker variants are introduced: First a satellite attacker, where the signal is coming from a malicious satellite. The attacking satellite is assumed to be commonly registered in public satellite databases. Thereby its orbit is available. The second attacker is drone-based, with the drone inside the atmosphere. To cover different types of drones, the altitude varies between 30 meters and 18 km above the receivers. Within the different altitudes a large variety of drone velocities is covered, from no velocity, as a hovering quadcopter, up to 468 km/h, the speed of the 'reaper drone'. Thereby it covers the range from cheap amateur drones to professional high flying pseudo satellites.

5 EXPERIMENTAL DESIGN

In this section, all factors that are relevant for the system performance are discussed. We start with the primary factors, for which different levels are varied over a wide range in the experiments, and continues with secondary factors, which are fixed to a system typical value as discussed below. The influence of the primary factors are subject to a subsequent analysis of variance (ANOVA).

5.1 Primary Factors

Number of receivers (n_r): One perfect TDOA value restricts the possible signal source locations to a hyperboloid. A second TDOA value reduces the possible positions to the interception of two hyperboloids, a circular line. With a third TDOA value (four receivers) only one remaining position is available, theoretically. So in the simulations, the starting level for the number of receivers is chosen at 4 receivers, to avoid a trivially poor performance of the authentication system. The number increases in multiples of 2, up to 20, which leads to 9 levels.

Distribution diameter (d_d): The diameter of the circle, on whose circumference the receivers are placed, starts with a diameter of 1km and increases in steps of 1 km up to 10 km. This is a rather dense distribution of the receivers relative to the distance from the satellite, but is chosen to challenge the authentication system.

Number of messages (n_m): The number of messages determines how many TDOA measurements are used for authentication. We start at the minimum of one message and increase in steps of 2 up to 11 messages. Then it increases from 15 in steps of 5 up to 30 messages. Clearly, the number of messages constitutes a trade-off between accuracy and reaction time of the system time to illegitimate signals. A smaller number of messages has a positive influence on the reaction time. Larger numbers of messages, on the other hand, have a positive effect on the accuracy of the system.

Altitude of the Satellites (a_s): The altitude of the satellites that should be authenticated. In our experiments, two levels of satellite altitudes are used: 780 km to simulate Iridium satellites and 530 km for Starlink satellites.

5.2 Secondary Factors

Interval between messages: The time interval between two messages is fixed to 0.1 seconds. This is done in order to enable independence of the TDOA measurements and take care of the satellites movement during this time.

Measurement errors: The measurement errors of the simulated system are assumed to come from two sources of inaccuracy: the limited sampling rate of the devices and imperfect synchronization between the receivers. For evaluating the synchronization error, the GPS system is assumed, where the synchronization accuracy is given between ≤ 40 ns [9] and 50 ns [2]. For evaluating the influence of the sampling rate, various software defined radios were considered. Their range of sampling rates reaches from 20 msps [8] up to 1 gsps [20] [25]. The time between two samples reaches from 50 ns to 1 ns. To cover these effects, the measurement error is conservatively modeled by a Normal distribution with zero mean and a standard deviation of 100 ns.

TLE accuracy: The deviation of the modeled satellites position in the TLEs to the real position is subject to multiple investigations. Many of them give an accuracy of about 1 to 4 km [12, 13, 27, 28], while the maximum was found on LEO cube-sats at 10 to 30 km [22]. To cover all investigations, the maximum value of 30 km is used in the simulations as an upper bound for the deviation of a sending satellite's position.

factor	DF	Sum Sq	Mean Sq	F value	Pr(>F)
a_s	1	0.417	0.41706	2614.1	$< 2.2 \cdot 10^{-16}$
n_m	9	0.417	0.04636	290.5	$< 2.2 \cdot 10^{-16}$
d_d	9	1.818	0.20206	1266.5	$< 2.2 \cdot 10^{-16}$
n_r	8	0.023	0.00293	18.4	$< 2.2 \cdot 10^{-16}$
$a_s n_m$	9	0.09	0.00996	62.4	$< 2.2 \cdot 10^{-16}$
$a_s d_d$	9	0.655	0.07283	456.5	$< 2.2 \cdot 10^{-16}$
$n_m d_d$	81	0.632	0.00780	48.9	$< 2.2 \cdot 10^{-16}$
$a_s n_r$	8	0.006	0.00077	4.8	$6.035 \cdot 10^{-6}$
$n_m n_r$	72	0.045	0.00063	3.9	$< 2.2 \cdot 10^{-16}$
$d_d n_r$	72	0.03	0.00042	2.6	$1.815 \cdot 10^{-12}$
$a_s n_m d_d$	81	0.117	0.00144	9	$< 2.2 \cdot 10^{-16}$
$a_s n_m n_r$	72	0.012	0.00016	1	0.45761
$a_s d_d n_r$	72	0.014	0.00020	1.2	0.08901
$n_m d_d n_r$	648	0.13	0.00020	1.3	$1.585 \cdot 10^{-5}$
$a_s n_m d_d n_r$	648	0.1	0.00015	0.97	0.69678
residuals	9000	1.436	0.00016		

Table 1: ANOVA table on the influence of the primary factors.

Response Variable. The output of the algorithm is a Boolean if the received signal is authenticated or not. This response can be classified as one of four cases: correctly authenticated (true positive), falsely authenticated (false positive), correctly rejected (true negative) and falsely rejected (false negative). The $\mathbf{F}_\beta$ score is used as response variable in the experimental design:

$$\mathbf{F}_\beta = \frac{(1+\beta^2) \cdot \text{true\_positive}}{(1+\beta^2) \cdot \text{true\_positive} + \beta^2 \cdot \text{false\_negative} + \text{false\_positive}},$$

with a β of 0.2, giving a higher weight to the falsely authenticated, and therefore successful, spoofing events over the false alarms.

Replication. Each configuration of the primary factors, is repeated totally 900 times, in 6 independent executions (chunks) of 150 repetitions each. The 150 repetitions are composed of 50 repetitions with a valid source satellite, 50 with an invalid source satellite and 50 invalid drone sources. Both invalid sources are assumed to be attackers, as described in chapter 4. In total, the full factorial design with $9 \cdot 10 \cdot 10 \cdot 2$ experiments and 900 repetitions is performed.

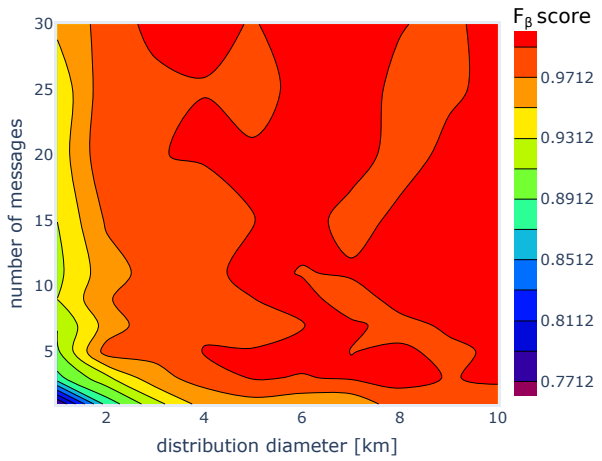


Figure 2: Influence of receiver numbers and distribution diameter at 6 receivers on F_β score (satellite altitude 530 km).

6 RESULTS

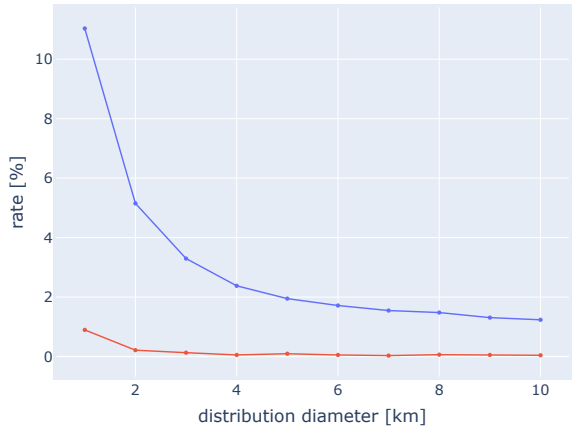
During the simulations, the authentication system's response is captured and classified. For each experiment, the responses of the 150 repetitions in one chunk are summed up to one data point. This leads to one data point for each experiment in one chunk. All chunks, with a total of 10800 data points are then subject to an ANOVA under a linear regression model of the factors for the response variable.

The ANOVA results of the F_β score in Table 1 score show a highly significant effect of the primary factors altitude of satellites (a_s), distribution diameter (d_d) and number of messages (n_m). Somewhat surprisingly, the effect of the number of receivers (n_r) is comparably small. Also the effects of the remaining higher order interactions are negligible.

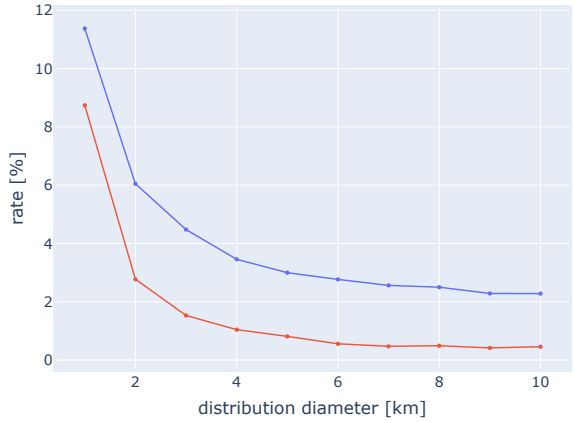
The effect of the distribution diameter is of major interest for designing such an authentication system, since it is the most important factor that can be influenced by a user of a satellites system.

In Fig. 2 this fact is visible again: The F_β score for Starlink satellites is represented by different colors. As the color changes from blue to red the F_β score increases from 0.77 in blue areas above 0.99 at red areas. The x-axis represents the distribution diameter, the y-axis shows the number of messages. The positive effect of an increased distribution diameter (along the x-axis) is much more visible than the positive effect for a higher number of messages (along the y-axis). This confirms the results of the ANOVA, that the distribution diameter is the more influencing factor. So if multiple receivers are available, those should be chosen appropriately to maximize the covered area.

In a second experiment, the accuracy with 6 receivers at 5 messages and varying distribution diameters are evaluated. To compare the accuracy on a more fine-grained level, the number of replications was increased to 30,000. The repetitions were again split up in 10,000 valid satellite sources, 10,000 invalid satellite sources and 10,000 invalid drone sources. This experiment was executed twice, once with Iridium satellites and once with Starlink satellites.



(a) FRR and FAR for Iridium satellites.



(b) FRR and FAR for Starlink satellites.

Figure 3: False rejection rates (blue) and false acceptance rates (red) at 6 receivers and 5 messages.

The results of this simulations are illustrated in Fig. 3. Here, the x-axis is the distribution diameter, while the y-axis shows the percentage of the falsely rejected rate (*FRR* in blue) and falsely authenticated rate (*FAR* in red). The rates can be calculated by

$$FRR = \frac{\text{false\_rejected}}{\text{false\_rejected} + \text{true\_rejected}},$$

$$FAR = \frac{\text{false\_accepted}}{\text{false\_accepted} + \text{true\_accepted}}$$

In Fig. 3a the rates of the Iridium satellites are presented. The *FRR* (blue line) drops from 11% at 1 km to 1.7% at 6 km, and even further to 1.2% for larger diameters. While the FAR (red line) falls from 0.9% at 1 km below 0.1% at 4 km and becomes even slightly smaller for higher distribution diameters.

Fig. 3b shows the rates for authenticating Starlink satellites. Here, the FRR (blue line) reaches 2.7% at 6 km diameter and drops further to 2.3%. The FAR (red line) hits 0.5% at 6 km diameter and remains under this value. These evaluations indicate again that low flying satellites are harder to authenticate.

7 DISCUSSION

We discuss two assumptions of our scheme in the following.

7.1 Multi-Device Attackers

First, we assume that the attacker is equipped with only a single sender. While stronger threat models considering multi-device attackers have been discussed in the literature (e.g,. [30]), the requirements in terms of resources and synchronization are significantly higher. This has been investigated in the related domain of aircraft verification by Moser et al. [16]. Their results show that it is, in principle, possible to achieve an attacker precision of 50 ns and to spoof positions of an airplane in 35 km distance. Besides the increased attack threshold, the geometric difference to satellites is an important factor, which we plan to investigate further.

7.2 Databases and Space Situational Awareness

A second basic requirement for our scheme is the sufficient accuracy and completeness of public available satellite databases. After one day, the accuracy is typically given within a few kilometers [12, 13, 22, 27, 28]. The completeness of the satellite database is similarly important, since our proposed approach is currently not able to detect undocumented signal sources. A possible way to increase the reliability is to combine data from different sources such as Space-Track, Union of Concerned Scientists, or NORAD.[1]

Turning the table, our TDOA scheme could be used to verify the content and completeness of these existing databases in order to improve space situational awareness (SSA). SSA – keeping track of objects in space – is crucial for controlling and mitigating threats to existing satellites and new launches. Accurate location data is required for space debris management and collision avoidance, however, the complexity to obtain this data is high and only accessible to a handful of major state actors. These actors use expensive measurement equipment to collect and publish catalogs such as the US Air Force's Space Surveillance Network (SSN), the equivalent by the European Space Agency, or the Russian catalog of space objects. If another actor does not want to trust these catalogs (cases of space deception have been increasing) they have little means to re-create them from scratch. In order to deal with this problem, we can conceive the much more feasible task to verify the published orbits of active communication satellites based on the TDOA of their signals.

8 CONCLUSION

In this work, we introduced a novel concept of authenticating satellite communications by combining the knowledge of satellite orbits with observable TDOA-based signatures. To evaluate the proposed approach, simulations[2] followed by an analysis of variance (ANOVA) were performed. The results of the ANOVA show a significant influence of three factors: the altitude of the satellites, the distribution diameter of the receivers and the number of messages used for authentication. Further evaluation showed that the false authentication and false rejection rates were at 0.1% and around 2%, respectively, which is promising with respect to the feasibility and accuracy of our concept.

[1] Sources at space-track.org, ucsusa.org and celestrak.com/NORAD, respectively.
[2] Code available on GitHub

REFERENCES

[1] Brandon Rhodes at pypi.org. sgp4: Track earth satellite TLE orbits using up-to-date 2020 version of SGP4. https://pypi.org/project/sgp4/. Accessed: 2021-03-26.
[2] Ken Behrendt and Ken Fodero. The perfect time: An examination of time- synchronization techniques. *Schweitzer Engineering Laboratories*, 01 2005.
[3] Yiu-Tong Chan, H Yau Chin Hang, and Pak-chung Ching. Exact and approximate maximum likelihood localization algorithms. *IEEE Transactions on Vehicular Technology*, 55(1):10–16, 2006.
[4] Yiu-Tong Chan and KC Ho. A simple and efficient estimator for hyperbolic location. *IEEE Transactions on signal processing*, 42(8):1905–1915, 1994.
[5] North American Aerospace Defense Command. Celestrac: Norad two-line element sets current data. https://www.celestrak.com/NORAD/elements/. Accessed: 2021-03-26.
[6] Astropy community. The astropy project. https://www.astropy.org/. Accessed: 2021-03-26.
[7] Dorothy E Denning and Peter F MacDoran. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security*, 1996(2):12–16, 1996.
[8] Great Scott Gadgets. Hackrf one. https://greatscottgadgets.com/hackrf/one/. Accessed: 2021-03-26.
[9] GPS.gov. Gps accuracy. https://www.gps.gov/systems/gps/performance/accuracy/. Accessed: 2021-03-26.
[10] KC Ho and Wenwei Xu. An accurate algebraic solution for moving source location using TDOA and FDOA measurements. *IEEE Transactions on Signal Processing*, 52(9):2453–2463, 2004.
[11] Kai Jansen, Nils Ole Tippenhauer, and Christina Pöpper. Multi-receiver gps spoofing detection: Error models and realization. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 237–250, 2016.
[12] TS Kelso et al. Validation of SGP4 and IS-GPS-200D against GPS precision ephemerides. *Technical White Paper*, 2007.
[13] Creon Levit and William Marshall. Improved orbit predictions using two-line elements. *Advances in Space Research*, 47(7):1107–1115, 2011.
[14] Zhixin Liu, Yongjun Zhao, Dexiu Hu, and Chengcheng Liu. A moving source localization method for distributed passive sensor using TDOA and FDOA measurements. *International journal of antennas and propagation*, 2016, 2016.
[15] Shivam Lohani and Rinki Joshi. Satellite network security. In *Int. Conf. on Emerging Trends in Communication, Control and Computing*. IEEE, 2020.
[16] Daniel Moser, Patrick Leu, Vincent Lenders, Aanjhan Ranganathan, Fabio Ricciato, and Srdjan Capkun. Investigation of multi-device location spoofing attacks on air traffic control and possible countermeasures. In *22nd Annual International Conference on Mobile Computing and Networking*, pages 375–386, 2016.
[17] Gabriele Oligeri, Simone Raponi, Savio Sciancalepore, and Roberto Di Pietro. Past-ai: Physical-layer authentication of satellite transmitters via deep learning. *arXiv preprint arXiv:2010.05470*, 2020.
[18] Gabriele Oligeri, Savio Sciancalepore, and Roberto Di Pietro. Gnss spoofing detection via opportunistic iridium signals. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 42–52, 2020.
[19] James Pavur, Daniel Moser, Vincent Lenders, and Ivan Martinovic. Secrets in the sky: on privacy and infrastructure security in dvb-s satellite broadband. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 277–284, 2019.
[20] Pervices. Cyan SDR. http://www.pervices.com/. Accessed: 2021-03-26.
[21] Mark L Psiaki and Todd E Humphreys. Gnss spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270, 2016.
[22] Kathleen Riesing. Two line element sets of cubesats in leo: Accuracy assessment and estimation techniques for improvement. *29th Annual AIAA/USU Conference on Small Satellites*, 2015.
[23] Ruben Santamarta. A wake-up call for satcom security. *Technical Paper*, 2014.
[24] Dave Singelee and Bart Preneel. Location verification using secure distance bounding protocols. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, pages 7–pp. IEEE, 2005.
[25] Solonet. XRAD-3200 SDR. http://www.solenet.com/products/xrad-3200.html. Accessed: 2021-03-26.
[26] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful gps spoofing attacks. In *18th ACM conference on Computer and Communications Security*, pages 75–86, 2011.
[27] David A Vallado and Paul J Cefola. Two-line element sets–practice and use. In *63rd International Astronautical Congress, Naples, Italy*, 2012.
[28] David A Vallado, B Bastida Virgili, and Tim Flohrer. Improved ssa through orbit determination of two-line element sets. In *ESA Space Debris Conference*, 2013.
[29] Johnny L Worthy III and Marcus J Holzinger. Uncued satellite initial orbit determination using signals of opportunity. In *AAS/AIAA Astrodynamics Specialist Conference*, 2015.
[30] Jie Yang, Yingying Chen, Wade Trappe, and Jay Cheng. Determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks. In *IEEE INFOCOM 2009*, pages 666–674. IEEE, 2009.