Towards Security-Optimized Placement of ADS-B Sensors

Ala' Darabseh
ala.darabseh@nyu.edu
New York University Abu Dhabi

Christina Pöpper
christina.poepper@nyu.edu
New York University Abu Dhabi

ABSTRACT

Automatic Dependent Surveillance–Broadcast (ADS-B) sensors deployed on the ground are central to observing aerial movements of aircraft. Their unsystematic placement, however, results in over-densification of sensor coverage in some areas and insufficient sensor coverage in other areas. ADS-B sensor coverage has so far been recognized and analyzed as an *availability* problem; it was tackled by sensor placement optimization techniques that aim for covering large enough areas. In this paper, we demonstrate that the unsystematic placement of ADS-B sensors leads to a *security* problem, since the realization and possible deployment of protective mechanisms is closely linked to aspects of redundancy in ADS-B sensor coverage. In particular, we model ADS-B sensor coverage as a multi-dimensional security problem. We then use multi-objective optimization techniques to tackle this problem and derive security-optimized near-optimal placement solutions. Our results show how the location of sensors play a significant role in reducing the success rate of attackers by providing a sufficient number of sensors within a specific geographical area to verify location claims and reducing the exposure to jamming attacks.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

ADS-B, Spoofing, Jamming, Sensor Placement, MLAT, GDOP

ACM Reference Format:

Ala' Darabseh and Christina Pöpper. 2022. Towards Security-Optimized Placement of ADS-B Sensors. In *15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16 - May 19 2022, San Antonio, Texas, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3395351.3399361

1 INTRODUCTION

Commercial aircraft use the ADS-B (Automatic Dependent Surveillance–Broadcast) system [2, 6] to broadcast messages that are received by on-ground sensors of air-traffic control (ATC) and observation networks (such as Flightradar24, FlightAware, & OpenSky Network). However, the open communication of ADS-B where messages are sent without encryption and integrity protection also suffers from the risk of spoofing and jamming attacks.

The placement of sensors is critical for the functioning of ADS-B. The current deployment of ADS-B sensors oftentimes places them arbitrarily on the ground (e. g., by volunteers contributing to the OpenSky Network [13]), which creates some overcrowded areas and others without coverage [3]. Optimal sensor placement has typically been investigated as an availability problem: How to place the receivers such that they provide the best coverage for a geographical area [7, 10, 18]? Placing them too close to each other leads to high and possibly unnecessary redundancy, whereas placing them too far apart may result in lost observation areas because the wireless channel is faulty and messages may get lost.

To counter this risk, attack detection and prevention techniques have been developed for the ADS-B context: (1) A common approach to detect tampering with ADS-B messages and the reported aircraft locations is the use of Multilateration (MLAT) [9], which allows to validate the reported locations in the messages with computed locations based on measurements from multiple sensors. MLAT requires the message to be received by four (or more) receivers on-ground in order to derive the aircraft's location. (2) Other approaches for validity checking rely on a smaller number of received messages: Strohmeier et al. [14] proposed a lightweight approach to validate the received aircraft location claim based on the K-Nearest Neighbors algorithm (K-NN), requiring only two sensors for location verification in two dimensions (2D). This approach leads to less accuracy than MLAT, but can be used in geographic areas covered by only two sensors. (3) To counter jamming attacks, finally, it is beneficial to place sensors in maximum distances to decrease the probability that all sensors in the reception range of a certain geographic area are impacted by a jamming attack.

The aim for an optimized placement of ADS-B sensors that does not only target coverage (i. e., availability of the ADS-B service), but supports the deployment of defense mechanisms (i. e., considers the security aspect of sensor deployment) creates the following challenge: *How can the different security requirements on the numbers and locations of ADS-B sensors best be fulfilled*? We note that MLAT does not only need messages from at least four sensors, but its accuracy also relies on the level of Geometric Dilution of Precision (GDOP) [19] which again depends on the locations and number of sensors. From a practicality aspect, we further need to consider that real-world deployments cannot easily be modified to reflect optimal sensor placements. This creates a second challenge: *Knowing what an optimal sensor placement from the security perspective would be, how can existing placements of ADS-B sensors best be enhanced by placing a certain number of additional sensors in a given area?*

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
WiSec '22, May 16 - May 19 2022, San Antonio, Texas, USA
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3399361

As a reaction to these questions, we tackle the problem of *Optimal Sensor Placement (OSP) for ADS-B from the security perspective*, incorporating the constraints imposed by attack detection techniques. In this paper, we extend our work in [4] from one security objective to multiple security-relevant dimensions. First, we consider MLAT for verifying aircraft locations claims in the received ADS-B messages. In this objective, we aim to provide a sensor placement solution where each broadcast message is to be received by at least four sensors and can accordingly be verified by an MLAT check. Second, since the cost of MLAT checks is rather high, and it requires at least four sensors, which is hard to guarantee, we introduce a second objective: Location verification checks at a lower cost level but with less accuracy compared to MLAT. Finally, in our third objective, we aim to provide a sensor setup that behaves favorably under jamming attacks. We discuss three directions that can potentially reduce the effect of jamming attacks, (a) maximize the distance between the sensors, (b) maximize the distance between the jammer and the sensors, (c) minimize the number of sensors within the range of the jammer. Our solution aims to optimize with respect to all of these dimensions.

We address two research questions: (1) **Optimal setting**: determine the minimum number of ADS-B sensors and their near-optimal locations that are required to cover a specific geographic area, (2) **Real-World Setting**: determine the minimum number of new sensors and their locations to be added to the existing sensors to reach a close-to-optimal sensor deployment. We treat each security dimension as an objective function to be optimized. Our target is to solve the OSP problem by providing solutions for sensor coverage that allow the aircraft to be tracked during their flight time while allowing the deployment of security checks that enable to verify ADS-B messages and place sensors in a way that mitigates the effect of jamming attacks. The main key of our approach is that all objective functions are optimized simultaneously, where each solution is non-dominated by another one. For this purpose, we adopt the Non-dominated Sorting Genetic Algorithm (NSGA-II) [17] algorithm. In short, our main contributions in this paper are:

- We model the problem of ADS-B sensor placement under security considerations as a Multi-Objective Optimal Sensor Placement Problem (OSP) with respect to three concrete security objectives—two for location verification (MLAT & leightweight verification) and one for jamming prevention.
- We specify and formally introduce the three security objectives and investigate their impact on ADS-B sensor locations. For the case of jamming attacks, our approach consists of a systematic way of including three security directions that impact the success of jamming attacks.
- We provide a set of non-dominated solutions for the proposed problem at a sample location in central Europe. Each solution provides a suitable compromise between all objectives without degrading any of them.

2 THREAT MODEL

We consider two types of attacks on ADS-B communication:

(1) **ADS-B Location Spoofing**: The attacker exploits the open nature of ADS-B communication to modify the content of transmitted ADS-B message that are within the attacker's range. He/she can insert own messages or modify the broadcast location of the aircraft which leads to receiving a modified location by the on-ground sensors. The success of the attack depends on whether the attacker is located in a geographical area that is only covered by few sensors, where location verification methods cannot be applied.
(2) **ADS-B Jamming**: The attacker tries to block the communication that is received by the on-ground sensors by causing interference on the wireless channel to prevent the reception of ADS-B messages. The attacker can use any software radios with amplifiers that are typically cheap and affordable.

3 OVERVIEW: OBJECTIVE FUNCTIONS (OFs)

We aim to solve the Optimal Sensor Placement (OSP) problem under the consideration of multi-objective functions (MOF) that provides defense mechanisms in addition to full coverage. A set of security objectives are considered to solve the OSP problem. We briefly describe them in this section while a detailed and self-contained description is available as a technical report [5].

3.1 OF 1: Multilateration (MLAT) under GDOP

Since MLAT requires 4 or more sensors to verify a location claim, by this first objective, we aim to identify the best sensor deployment solution such that each message can be received by at least 4 sensors.

Let us assume an airspace $\mathcal{A}$ that contains the expected ADS-B traffic. Then we take m sample locations $\mathbf{p_j}$ from airspace $\mathcal{A}$: $\mathcal{A} = \{g_j|\mathbf{p_j}\}_{j=1,\cdots,m}$, where, g_j represents the *required* GDOP value at $\mathbf{p_j}$. In addition, given a placement $\mathbf{S} = \{\mathbf{s_i}\}_{i=1,\cdots,n}$ of n ADS-B sensors, we write $\widehat{g_j} = gdop_{\mathbf{S}}(\mathbf{p_j})$ to denote the *achieved* GDOP value at the location $\mathbf{p_j}$ due to the particular geometry of $\mathbf{S}$. For readability, we omit the subscript and write $\widehat{g_j} = gdop(\mathbf{p_j})$.

In order to find the best deployment of ADS-B sensors and their corresponding locations from $\mathbf{S}$, to satisfy a per-location GDOP requirement for a given airspace $\mathcal{A}$, we assume δ to be the tolerance parameter on the GDOP at any location, where $\mathbf{S}$ can only be admitted if: $\forall\ \mathbf{p_j} \in \mathcal{A} :\ |\widehat{g_j} - g_j| < \delta$, which is equivalent to $\|\hat{g} - \mathbf{g}\|_\infty < \delta$, where $\|.\|_\infty$ represents the sup-norm defined by $\|\hat{g} - \mathbf{g}\|_\infty = \max_j |\widehat{g_j} - g_j|$.

The Mean Squared Deviation (MSD) between the achieved and the required GDOP in the entire airspace of our first objective is:

$$MSD(\mathbf{S}) = \frac{1}{m}\sum_{j=1}^{m}(g_j - \widehat{g_j})^2. \quad (1)$$

3.2 OF 2: Lightweight Location Check with Transmission Range Evaluation

Our second objective is designed based on Lightweight Location Estimation [14] to provide a security check with fewer sensors. However, the accuracy of this check is less than the MLAT-check (objective 1), but still, this lightweight method can provide fine results with small budget, and it can be used in areas where MLAT is not available either due to lack of a number of sensors or an attack that affects the area and disrupts some of the sensors.

To achieve the second objective, we use the transmission range or distance as an evaluation principle to deploy the sensors. In more details, given an airspace $\mathcal{A}$ with m uniform sample locations $\mathbf{p_j}$ from $\mathcal{A}$, the following spatial data matrix is defined: $\mathbf{A} = \{tr_{(j,s)}|\mathbf{p_j}\}_{j=1,\cdots,m}$ where, $tr_{(j,s)}$ represents the *best* minimal distance from $\mathbf{p_j}$ to sensor $\mathbf{s_i}$, the required one. In addition, given a placement $\mathbf{S} = \{\mathbf{s_i}\}_{i=1,\cdots,n}$ of n ADS-B sensors, we write $\widehat{tr_j} = tr_{\mathbf{S}}(\mathbf{p_j})$ to denote the *achieved* distance from the location $\mathbf{p_j}$ to $\mathbf{s_i}$ due to the particular geometry of $\mathbf{S}$. For readability, we omit the subscript and write $\widehat{tr_j} = tr(\mathbf{p_j})$.

Now, to find the minimal number of ADS-B sensors n_{min} and their corresponding deployment $\mathbf{S}$ to guarantee a per-defined transmission range requirement for a given airspace $\mathcal{A}$, let us assume tr_δ to be the tolerance parameter of tr at any location. A sensor placement $\mathbf{S}$ can only be accepted if:

$$\forall\ \mathbf{p_j} \in \mathcal{A},\quad \|\widehat{\mathbf{tr}} - \mathbf{tr}\|_\infty < tr_\delta. \tag{2}$$

3.3 OF 3: Low Sensor Density under Jamming

Tackling jamming attacks requires more sophisticated considerations to optimize the locations of sensors on ground. The aim of this objective is to reduce the effect of jamming by placing the sensors in a way that guarantees good coverage, while keeping the number of sensors affected by the jammer to a minimum. We incorporate three directions for the network topology of deployed sensors:

- **Direction 1:** Maximize the distance $dist(s_i, s_{\bar{i}})$ between sensors, where s_i and $s_{\bar{i}}$ are any two sensors in $\mathbf{S}$. The aim is to select the best candidates of sensors that are placed in locations far away from each other, in other words, the best low-sensor-density network. Sensor placement $\mathbf{S}$ can only be accepted if only the difference (MSD) between the required distance and computed distance is minimal.
- **Direction 2:** Maximize the distance $dist(jam_i, s_j)$ between jammer and sensors. This direction aims to reduce the Jamming-to-Signal (JSR) ratio [1].

$$JSR = \frac{P_j G_j {dist_{(t,s)}}^2}{P_T G_T {dist_{(jam,s)}}^2} \tag{3}$$

  where, P_j and G_j are the transmission power and antenna gain of the jammer, the P_T and G_T the transmission power and antenna gain of the transmitter, and $dist_{(t,s)}$, $dist_{(jam,s)}$ the distances from the transmitter (or jammer) to the sensor, respectively. As we can see from the Eq. 3, we can reduce the ratio either by changing the transmitter characteristics (the ADS-B out-device on all aircraft), or maximize the distance between jammer and receiver. Since it is hard to change the already deployed transmitters, we can work on the distance between the jammer and the receiver. Given list of k jamming attacks at different locations $\mathbf{J} = \{\mathbf{j_l}\}_{l=1,\cdots,k}$ within the airspace $\mathcal{A}$, let us assume $dist_{\bar{\delta}}$ to be the tolerance parameter of $dist$ between and jammer and any sensor. A sensor placement $\mathbf{S}$ can only be accepted if the distance between a jammer and any sensor under consideration is less than $dist_{\bar{\delta}}$ and get the minimal MSD.
- **Direction 3:** Minimize the number of sensors within the range of the jammer. As jammer tries to interfere with all the sensors that are within its range. We aim here to reduce the number of sensors that are within the range of the jammer, where at anytime the number of affected sensors is small as possible. A sensor placement $\mathbf{S}$ will only be accepted if the MSD between the achieved and required number of sensors within the LoS of the jammer is the minimal one.

We explain in the next section how these the optimization problems of the three directions are combined.

4 SYSTEM APPROACH AND METHODOLOGY

4.1 Fitness/Cost Function

The fitness function is designed according to MSD (Section 3). It computes the fitness of selected subsets of sensors from $\mathbf{S}$ that are chosen by the NSGA-II algorithm. It evaluates the placement of each subset of sensors by measuring the average of errors between the achieved and required value to get the final score. NSGA-II searches for the optimal Pareto frontier [11], and we consider all solutions with first Pareto front, non-dominated solutions.

As anti-jamming Objective Function 3 considers three optimization directions: two maximization problems and one minimization problem. We deal with them as one objective by using Weighted Sum Method [16]. Each direction can be assigned a weight, which reflects the importance of this direction against the other two, and then combined into one score: $OF = \sum_{i=1}^{3} FitnessScore_i * w_i$. where w_i is the weight for objective direction i, and $\sum_{i=1}^{3} w_i = 1$. We also define a cost or penalty function to increase the security. More details are provided in our technical report [5].

Finally, since we are working with a MOF problem and each objective implies different checks with different unit scales, we normalize all the obtained scores to simplify the evaluation.

4.2 OSP problems and Case Studies

We consider two scenarios:

(1) **Scenario 1: OSP from Scratch.** We consider the situation where the volume space $\mathcal{A}$ is not covered by any sensor. Thus, we can find the best minimal number of n ADS-B receivers and their locations to cover $\mathcal{A}$ without further restrictions. We note that this case is idealistic and hard to achieve in practice, but serves as a bound and optimal solution we can compare real-world setting to.
(2) **Scenario 2: Optimal Network Augmentation.** By this scenario, we wish to augment the current deployment by adding n^* additional receivers to the existing ones to provide a near-optimal solution. We look for the best number n^* of new sensors $\mathbf{S^{new}}$ that can be added to the deployed ones $\mathbf{S^{depl}}$ to provide the best near-optimal solution.

4.3 Procedure for Solving OSP Problems

To solve the OSP problems, we adopt the MSD to get the scores of all defined objectives (Section 3). First, we compute and derive the following structures to be used through our computations.

(1) Compute direction cosines for all points in $\mathcal{A}$ to all sensors in $\mathcal{S}$, and for all jammers in $\mathcal{J}$ to all sensors in $\mathcal{S}$.

(2) Compute the distance using the defined expression of Euclidean Distance, (1) from each point in $\mathcal{A}$ to all sensors in $\mathcal{S}$, (2) from each jammer in $\mathcal{J}$ to all sensors in $\mathcal{S}$, (3) compute the distance between all sensors in $\mathcal{S}$.

We then compute the objective functions. Each procedure is applied at every generation of NSGA-II.

(1) Find the set $\mathcal{S}^j_{LOS}$ of all ADS-B receivers for which Inequality of Line-of-Sight (LOS) [4] is valid.
(2) If $|\mathcal{S}^j_{LOS}| >= 4$, compute the GDOP at $\mathbf{p_j}$ for all 4-sized subsets of $\mathcal{S}^j_{LOS}$ using the closed-form expression proved in [19]. Then set $\widehat{g_j}$ (achieved GDOP) to the minimal value found.
(3) Otherwise, set $\widehat{g_j} = \infty$ (the GDOP cannot be evaluated), and check if $|\mathcal{S}^j_{LOS}| < 2$, set $\widehat{tr_j} = \infty$. (The lightweight location check can not be evaluated).
(4) Otherwise, get the minimal two values, which represent the closest two sensors, and assign it to the $\widehat{tr_j}$ (minimal transmission range).
(5) Get the best sub-set that has the maximum distance from all sensors (**Objective 3, Direction 1**).
(6) For each jammer l in $\mathcal{J}$, find the set $\mathcal{S}^l_{LOS}$ of all ADS-B receivers that are within the range l^{th} jammer. If $|\mathcal{S}^l_{LOS}| = 0$, set $\widehat{dist_{jam2s}} = \infty$ (**Direction 2**), and $\widehat{LOS_{jam}} = 0$ (**Direction 3**) (best solution).
(7) Otherwise, get the distance from each l for all sensors, and then get the minimum one, and repeat step 6 for all subsets of sensors to find the $min(|\mathcal{S}^l_{LOS}|)$.

5 EXPERIMENTAL EVALUATION

We consider a small geographical area around Frankfort Airport, between 47.4–51.4 latitudes and 5.71–9.71 longitudes decimal degrees for evaluation. We were able to get the location of 21 ADS-B receivers from OpenSky for this specified area; sensors that were placed arbitrarily. We evaluate this real-world deployment to check how far it is from the optimal solution. Table 1 shows the fitness values of all objective functions by this deployment. We consider these values as reference points.

First, we assume this area is not covered by any sensors and we want to place n new sensors considering the objective functions that we have. First, we use the basic GA [8] to get the fitness value of each objective alone and then the fitness value of all together across different number of sensors. Based on the experiments, we observed that at $n = 30$ the genetic algorithm stops improving the fitness value, so we consider it to be the best minimum number of sensors that are required to cover the whole area of study with respect to the three defined objectivesd. Thus, we use $n = 30$ as the number of sensors to cover the whole area from scratch for the rest of the experiments (more details about the fitness values by GA and generations can be found in [5]).

Table 1: Fitness Values of Objectives with Random Placement of 21 sensors from OpenSky

	OF1	OF2	OF3
Fitness Value	0.02203632	0.02732189	0.05420901

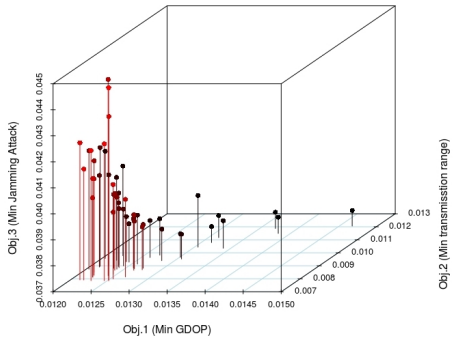


Figure 1: The fitness function values of all objectives for placing $n = 30$ new sensors. Each dot represents the solution of a set of locations of $n = 30$ ADS-B sensors.

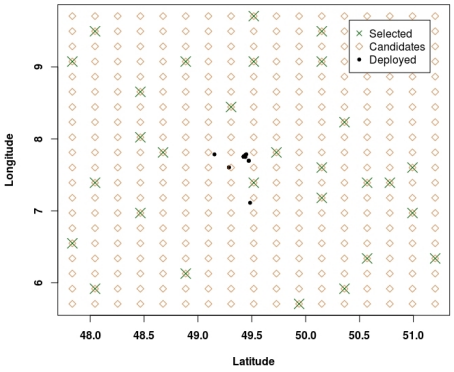


Figure 2: The geographical representation of the 21 deployed sensors, 30 new selected sensors, and 400 candidates locations that the NSGA-II algorithm have to choose from.

The obtained solution by GA considers all objectives together, where we are not able to select the best solution for each objective. Thus, we run the NSGA-II and we got a set of solutions where each solution is non-dominated by another. Figure 1 shows set of solutions to place $n = 30$ new sensors with their fitness function. We have to illustrate that each solution represents the locations of the $n = 30$ sensors that we are wishing to place. The solution with minimal fitness value are considered better than the ones with high values. As an example, from Figure 1, we can say the solutions that are located close to the bottom left corner are near-optimal solutions for the first and second objectives, while the solutions are considered near optimal based on the third objective where they are close to the ground surface of the cube.

To depict where these sensors are placed compared to the already deployed ones in real-world maps, Figure 2 shows the location of the already 21 deployed sensors, and the best 30 selected sensors out of 400 candidates sensors to cover the area under investigation. As we can see the deployed ones are concentrated close to each other, while the obtained solution from NSGA-II distributes the sensors over the whole area in a way to guarantee full coverage and at the same time satisfies the objective functions.

Moreover, we consider the scenario where we have to add n new sensors to the already deployed ones to get a near-optimal solution. We assume we have to add $n = 15$ new sensors and we need to check the set of solutions to place them with the 21 sensors from

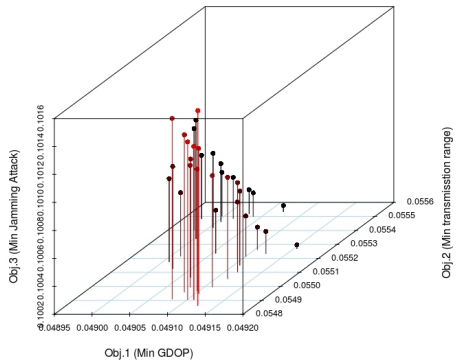


Figure 3: The fitness function values of all objectives for placing 15 new sensors in addition to 21 already deployed sensors $n = 15 + 21$.

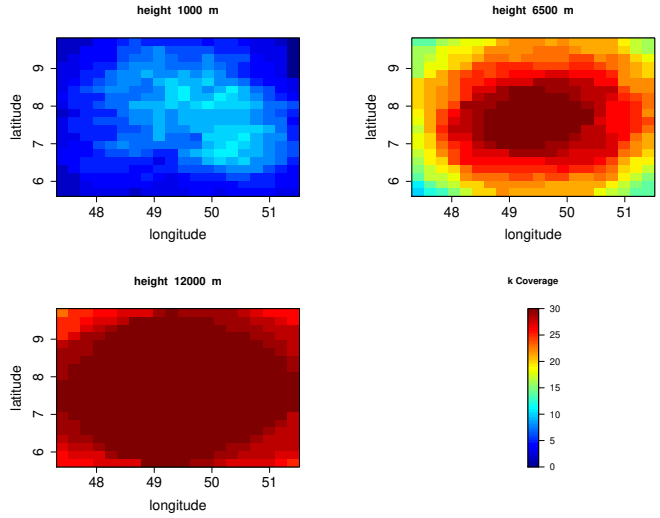


Figure 4: Simulated k-coverage heatmap for best placement solution of $n = 30$ ADS-B sensors.

OpenSky. Figure 3 presents the set of sensors with their fitness values. As shown, the set of solutions go slightly to the right-up. This means that we can still be close to the optimal scenario with $n = 15$ sensors and the solutions can be enhanced if we increase the number of sensors, but we restrict ourselves here to $n = 15$ to show how the sensor deployment with low budget can get benefit from our method by placing sensors with the already deployed ones.

As our first objective targets to have full coverage while minimizing the GDOP value, we test the k-coverage and GDOP distribution for one of the obtained solutions from NSGA-II. As we can see from Figure 4, the selected sensors can still achieve good coverage where MLAT or Lightweight checks can be used to verify the aircraft locations. At the same time, the GDOP value is reduced significantly as shown in Figure 5 compared to the GDOP value from the 21 deployed sensors.[1] For about 90% of the area under consideration the currently deployed sensors have high GDOP values above 60, whereas this can be reduced to only 24% of the area for the $n = 30$ newly deployed sensors.

[1]See [5] for more details on the k-coverage and GDOP values of the deployed sensors.

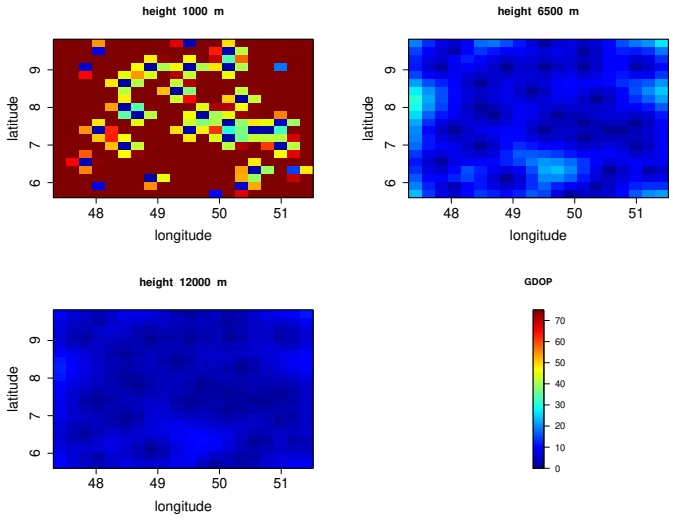


Figure 5: Simulated GDOP values for best placement solution of $n = 30$ new sensors.

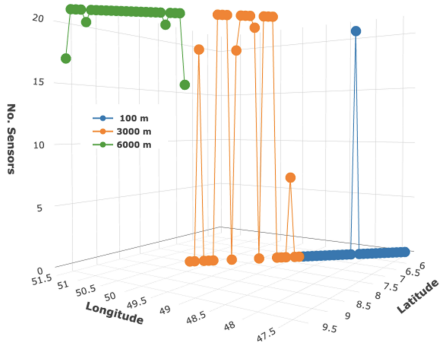


Figure 6: The number of sensors that are affected by the jamming attack setup (75 jammers at three height levels across the whole area) with the $n = 21$ already deployed sensors from OpenSky. Each dot in the figure represents the location of the jammer in 2D.

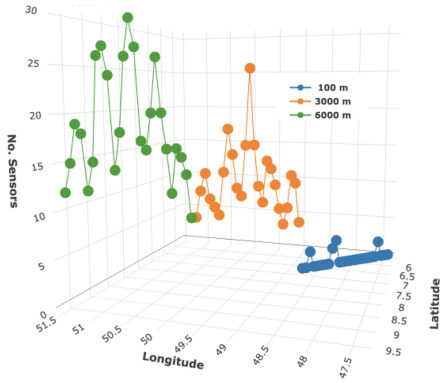


Figure 7: The number of sensors that are affected by the jamming attack setup with $n = 30$ newly selected sensors and 75 jammers.

Lastly, we evaluate the resistance of the current deployment against jamming attacks. We generated 75 jammers across the whole

area at different altitudes. We assume the attacks could be at different locations, like on high buildings or even on the aircraft. First, we check how many sensors out of 21 sensors are affected by such a setup. Figure 6 reflects how successfully the attackers at 3000 m and 6000 m height are able to jam almost all the deployed sensors since they are placed close to each other and they are within the range of the attackers. For test purposes, we assign similar weights for all three directions of our third objective (1/3 in each case), however, these values can be adjusted according to needs. Second, we test how the locations of the selected solution of $n = 30$ sensors are resistant to the jamming attack. As we can see from Figure 7, the number of sensors that are affected by jamming is reduced compared to the one of the deployed ones. We note that these numbers are across the whole area, while the ones that are shown in Figure 6 are all concentrated within the range of currently deployed sensors.

6 RELATED WORK

Multilateration (MLAT) [9] is used to verify the trustworthiness of location claims in received messages. However, the percentage of messages that can be veritably by MLAT with GDOP < 10 is only around 5.24% from the whole messages [15] because it requires at least four sensors. Another K-NN based approach [15] is proposed to verify the messages that are received by two sensors where 41.48% of received messages can be verified but in 2D dimensions. MAVPro [3] also proposed to verify the messages that are received by one sensor but with less accuracy.

All of these location checks depend on the number and the location of the receiving sensors. In an unstructured placement of ADS-B receivers, the location verification checks become inapplicable and the aircraft may not be tracked by the ATC. Recently, the OSP problem in an avionic context has been investigated [12]. The authors verify the messages in 2D based on the assumption that MLAT applied with coplanar receivers generally results in a poor vertical dilution of precision. We believe that, if the receivers are placed and spread carefully, then the coplanarity assumption can be broken due to the Earth curvature.

7 CONCLUSION

This paper proposed a multi-objective optimization problem (MOOP) addressing the placement of ADS-B sensors on-ground under security considerations. We tackled the Optimal Sensor Placement Problem with respect to three objective functions. The first and second objectives aim to provide an optimal solution that guarantees coverage where each ASD-B message must be received by at least one receiver and at the same time allows location checks of the aircraft to verify the trustworthiness of the received claim locations in the ADS-B message. In our third objective, we aim to reduce the effect of jamming attacks by placing sensors in a way that minimizes the number of sensors affected by the attackers. We use the Non-dominated Sorting Genetic (NSGA-II) algorithm to optimize and get our set of solutions. For our results the obtained solutions are optimized simultaneously and each solution is non-dominated by another, giving the sensor deployers flexibility in selecting an optimal solution based on budget and needs.

ACKNOWLEDGMENTS

This work is supported by the Center for Cyber Security at New York University Abu Dhabi (NYUAD). The authors gratefully acknowledge support of and interaction with armasuisse Science & Technology. We would like to thank the OpenSky Network for support, specifically Martin Strohmeier for his collaboration and feedback at the early stages of this work.

REFERENCES

[1] [n. d.]. *Manuals Combined: Electronic Warfare and Radar Systems Engineering Handbook: 2013, 2012, 1999, 1997 Plus Principles of Naval Weapons Systems, Satellites And Radar Fundamentals.* Jeffrey Frank Jones. https://books.google.com/books?id=noNHDwAAQBAJ

[2] W Blythe, H Anderson, and N King. 2011. ADS-B Implementation and Operations Guidance Document. *International Civil Aviation Organization. Asia and Pacific Ocean* (2011).

[3] Ala' Darabseh, Hoda AlKhzaimi, and Christina Pöpper. 2020. MAVPro: ADS-B Message Verification for Aviation Security with Minimal Numbers of on-Ground Sensors. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20).* Association for Computing Machinery, New York, NY, USA, 53–64. https://doi.org/10.1145/3395351.3399361

[4] Ala' Darabseh, Evangelos Bitsikas, Brice Tedongmo, and Christina Pöpper. 2020. On ADS-B Sensor Placement for Secure Wide-Area Multilateration. *(MDPI) Multidisciplinary Digital Publishing Institute* 59, 1 (2020). https://doi.org/10.3390/proceedings2020059003

[5] Ala' Darabseh and Christina Pöpper. 2022. Towards Security-Optimized Placement of ADS-B Sensors. arXiv:cs.NI/2204.01994

[6] William Dunlay and Jasenka Rakas. 2011. NextGen, the Next Generation Air Transportation System: Transforming Air Traffic Control from Ground-Based and Human-Centric to Satellite-Based and Airplane-Centric. (09 2011), pp. 7–13.

[7] Samaneh Hojjatoleslami, Vahe Aghazarian, and Ali Aliabadi. 2011. DE Based Node Placement Optimization for Wireless Sensor Networks. In *2011 3rd International Workshop on Intelligent Systems and Applications.* 1–4. https://doi.org/10.1109/ISA.2011.5873254

[8] Sourabh Katoch, Sumit Singh Chauhan, and Vijay Kumar. 2021. A review on genetic algorithm: past, present, and future. *Multimedia Tools and Applications* (2021), 1 – 36.

[9] Ivan A. Mantilla-Gaviria, Mauro Leonardi, Gaspare Galati, and Juan V. Balbastre-Tejedor. 2015. Localization algorithms for multilateration (MLAT) systems in airport surface surveillance. *Signal, Image and Video Processing* 9, 7 (01 Oct 2015), 1549–1558. https://doi.org/10.1007/s11760-013-0608-1

[10] Ivan A. Mantilla-Gaviria, Mauro Leonardi, Gaspare Galati, Juan V. Balbastre-Tejedor, and Elías de los Reyes Davó. 2012. An effective procedure to design the layout of standard and enhanced mode-S multilateration systems for airport surveillance. *International Journal of Microwave and Wireless Technologies* 4, 2 (2012), 199–207. https://doi.org/10.1017/S1759078712000219

[11] Kaisa Miettinen. 1998. Nonlinear multiobjective optimization. In *International series in operations research and management science.*

[12] Márcio Monteiro, Alexandre Barreto, Research Division, Thabet Kacem, Jeronymo Carvalho, Duminda Wijesekera, and Paulo Costa. 2015. Detecting malicious ADS-B broadcasts using wide area multilateration. In *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC).* 4A3–1–4A3–12. https://doi.org/10.1109/DASC.2015.7311413

[13] Matthias Schäfer, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, and Matthias Wilhelm. 2014. 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.* IEEE Press, 83–94.

[14] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2015. Lightweight Location Verification in Air Traffic Surveillance Networks. In *CPSS@ASIACSS.*

[15] Martin Strohmeier, Ivan Martinovic, and Vincent Lenders. 2018. A k-NN-based localization approach for crowdsourced air traffic communication networks. *IEEE Trans. Aerospace Electron. Systems* 54, 3 (2018), 1519–1529.

[16] Xin-She Yang. 2014. Chapter 14 - Multi-Objective Optimization. In *Nature-Inspired Optimization Algorithms*, Xin-She Yang (Ed.). Elsevier, Oxford, 197–211. https://doi.org/10.1016/B978-0-12-416743-8.00014-2

[17] Yusliza Yusoff, Mohd Salihin Ngadiman, and Azlan Mohd Zain. 2011. Overview of NSGA-II for Optimizing Machining Process Parameters. *Procedia Engineering* 15 (2011), 3978–3983. https://doi.org/10.1016/j.proeng.2011.08.745 CEIS 2011.

[18] Yijie Zhang and Mandan Liu. 2020. Adaptive Directed Evolved NSGA2 Based Node Placement Optimization for Wireless Sensor Networks. 26, 5 (jul 2020), 3539–3552. https://doi.org/10.1007/s11276-020-02279-2

[19] Jijie Zhu. 1992. Calculation of geometric dilution of precision. *IEEE Trans. Aerospace Electron. Systems* 28, 3 (1992), 893–895.