Dang, Yongchao; Benzaid, Chafika; Shen, Yulong; Taleb, Tarik

GPS Spoofing Detector with Adaptive Trustable Residence Area for Cellular based-UAVs

Published in:
2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings

DOI:
10.1109/GLOBECOM42002.2020.9348030

Published: 01/12/2020

Document Version
Peer reviewed version

GPS Spoofing Detector with Adaptive Trustable Residence Area for Cellular based-UAVs

Yongchao Dang *, Chafika Benzaïd *, Yulong Shen ‡, and Tarik Taleb* †
* Aalto University, Espoo, Finland, †University of Oulu, Oulu, Finland and ‡ Xidian University, Xi'an, China
* Email: firstname.lastname@aalto.fi and ‡ ylshen@mail.xidian.edu.cn

***Abstract*—The envisioned key role of Unmanned Aerial Vehicles (UAVs) in assisting the upcoming mobile networks calls for addressing the challenge of their secure and safe integration in the airspace. The GPS spoofing is a prominent security threat of UAVs. In this paper, we propose a 5G-assisted UAV position monitoring and anti-GPS spoofing system that allows live detection of GPS spoofing by leveraging Uplink received signal strength (RSS) measurements to cross-check the position validity. We introduce the Adaptive Trustable Residence Area (ATRA); a novel strategy to determine the trust area within which the UAV's GPS position should be located in order to be considered as non-spoofed. The performance evaluation shows that the proposed solution can successfully detect spoofed GPS positions with a rate of above 95%.**

***Index Terms*—UAV, GPS spoofing, RSS, Adaptive Trustable Residence Area (ATRA)**

I. Introduction

5G and beyond wireless networks are envisioned to foster the proliferation of massive Internet of Things (IoT). Improved coverage, connectivity and energy efficiency are essential requirements to make this vision a reality. Unmanned Aerial Vehicles (UAVs), or commonly known as drones, are recognized as a promising technology to assist upcoming wireless networks in meeting the massive IoT requirements, thanks to their deployment and movement flexibility and their capability of establishing line-of-sight (LOS) communication links. Indeed, UAVs have become an integral part of several critical applications, such as rescue management, first aid and even time-critical systems [1]. However, the anticipated growth in UAV usage calls for addressing the challenge of their secure and safe integration in the airspace.

As a response to this challenge, the development of Unmanned Aircraft Systems (UAS) Traffic Management (UTM) systems are considered mandatory to manage both visual and beyond-visual LOS drone operations in low-altitude airspace [2]. The services delivered by a UTM system encompass drone registration and identification, flight planning and authorization, real-time tracking, and geo-fencing. It is worth noting that UAV positioning information is instrumental for UTM systems to fulfill their mission. Such information can be provided by different positioning technologies and periodically reported to UTM leveraging the communication capabilities of 5G and beyond networks [3]. The global navigation satellite system (GNSS), specifically GPS, is the primary location technology used by UAVs due to its global coverage and accuracy. Nevertheless, the unencrypted civil GPS signals are inherently vulnerable to spoofing attacks. Indeed, an attacker can use low-cost software defined radio (SDR) tools, such as USRP, to generate fake signals with false navigational information in order to fool the UAV's GPS receiver into calculating false positions [4]. In another attack scenario, a malicious UAV may deliberately report false GPS data to UTM, leading to violation of no-fly zone regulation and/or collision risks. Thus, it is imperative to incorporate appropriate measures into UTM systems to validate the positioning information and consequently counteract GPS spoofing attacks.

Several solutions have been proposed for detection and mitigation of GPS spoofing attacks, which can be broadly classified into two categories, namely, GPS signal analysis methods (e.g., [5]–[8]) and GPS information analysis methods (e.g. [9]–[13]). For instance, the authors in [5] devised a multi-antenna anti-spoofing technique for mitigating the spoofing signals. Similarly, in [6] presented a spatial signal processing approach for GPS spoofing detection and mitigation. The spatial signal processing takes advantage of multi-antenna reception for spatially filtering out fake GPS signals beamforming or null steering. In fact, multiple received signals having the same or very similar direction of arrival (DoA) is an indicator of GPS spoofing. In [7] and [8], the cross-correlation between the military and civil GPS signals is used for detecting the spoofing of unencrypted GPS signals. The cross-correlation strategy requires a communication link between a secure receiver and the defended receiver to perform the spoofing detection. The authors in [9] proposed Crowd-GPS-Sec, a solution that leverages the position messages periodically broadcast by the aircraft/UAV and their time of arrival to detect and localize GPS spoofing attacks. To safeguard civil GPS receivers against spoofing attacks, Wesson *et al.* [10] proposed to authenticate GPS signals by combining signature-based authentication of GPS navigation messages with a statistical hypothesis test. Similarly, Wu *et al.* [11] used SM cryptographic algorithms, particularly SM2, SM3 and SM4, to authenticate the BeiDou-II navigation messages. In [12], a trusted hardware is leveraged to generate cryptographically-signed GPS messages in order to resist spoofing attacks. The UAV's camera view is used in [13] to cross-check if the UAV's GPS position is spoofed or not.

Although the proposed GPS spoofing detection methods are effective, their adoption imposes more antennas and computational load on the receiver. In fact, the estimation of phase delay and direction of arrival requires an inertial measurement

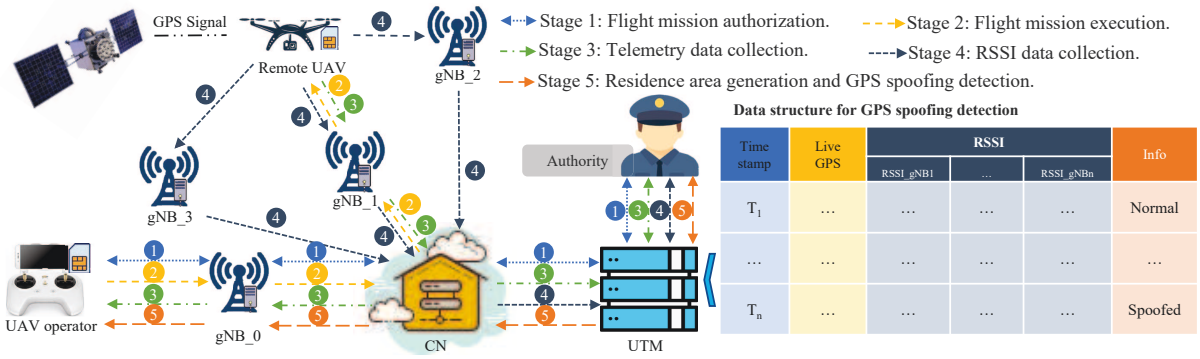


Fig. 1. High-level architecture of the remote 5G UVA's position and GPS spoofing detector.

unit (IMU) or multiple reception antennas, while the cross-correlation induces computation overhead. Those methods can hardly implement into drone due to limited battery capacity and the extra weight load on the drone. Furthermore, most existing solutions consider UAV as a victim receiving spoofed GPS signals. Nevertheless, the UAV may be malicious and deliberately reports fake GPS information to the UTM.

In this paper, we propose a novel cost-effective method to detect the spoofed GPS positions reported to UTM by an UAV. The proposed method leverages the Received Signal Strength (RSS) collected from multiple 5G base stations to infer the UAV's residence area, enabling UTM to cross-check the validity of positioning information provided by the UAV. Unlike the aforementioned solutions, the proposed approach requires no additional hardware or computation load at the UAV. Furthermore, it can be easily supported by 5G networks, thanks to the recent 3GPP's standardization work to expose network capabilities and information to UTM [14]. Followings are the major contributions of this paper:

- First, we propose a 5G-assisted UAV position monitoring and anti-GPS spoofing system (see Fig. 1) that allows live detection of GPS spoofing by leveraging Up-link received signal strength (RSS) measurements to cross-check the position validity. It is worth mentioning that the proposed system is compliant with the 3GPP specification for enabling UAV tracking services over mobile networks [15];
- To improve the positioning accuracy, we propose to subdivide the residence area calculated from the RSSI measurements into weighted trust areas, where the highest weight is assigned to the trust area with the highest likelihood of containing the UAV;
- To achieve higher GPS spoofing detection accuracy, we propose the Adaptive Trustable Residence Area (ATRA) algorithm which determines the trust areas within which the reported GPS position should be located in order to be considered as non-spoofed. The determination of ATRA depends on trust levels and the tolerable GPS margin error;
- Finally, the performance of the proposed ATRA-based GPS spoofing detector is evaluated in both free-space and urban area environments. The obtained results show the high effectiveness of the proposed solution in detecting spoofed GPS positions.

The remainder of this paper is organized as follows. Section II presents the proposed RSSI-assisted UAV position monitoring and anti-GPS spoofed system, providing details on the system high-level architecture and the devised ATRA-based GPS spoofing detector. The performance evaluation results of the ATRA-based GPS spoofing detector are discussed in Section III. Conclusion and future work are presented in Section IV.

II. 5G-ASSISTED UAV POSITION MONITORING AND ANTI-GPS SPOOFING SYSTEM

A. System High-Level Architecture

According to Federal Aviation Administration (FAA) regulation, UAVs need to report their location to UTM for safety and security purposes [16]. In the view of supporting this regulation, 3GPP defined the interfaces enabling UAV identification and tracking services over a mobile network [15]. Following the 3GPP specification [15], we propose a 5G-assisted UAV position monitoring and anti-GPS spoofing system that allows live detection of spoofed GPS position by leveraging Uplink RSS measurements to cross-check the position validity.

As depicted in Fig. 1, the proposed system proceeds in five (05) stages to continuously monitor the UAV location while detecting the spoofed GPS positions. The UAV operator, remotely controlling a UAV, first sends a flight mission request to the UTM, specifying the mission type and its starting and ending geolactions. Upon receiving the request, the UTM checks the request's compliance with regulatory requirements, in which case UTM issues the flight route and clearance to the UAV. In case of regulation violation, the UAV operator will be notified in order to change the flight mission plan. Once authorized to start its mission, the UAV needs to periodically broadcast its telemetry data, including GPS position, over the air for collision avoidance and airspace enforcement [14]. Collected by the nearby base stations, the position information is augmented with the uplink RSS measurements and reported to the UTM. The collected RSS measurements are used by the

UTM to infer the UAV's residence area, enabling to cross-check that the GPS position provided by the UAV is not spoofed. When a GPS spoofing is detected, a warning is sent by UTM to the UAV operator.

As shown in Fig.1, the UTM maintains for each UAV authorized to fly a list containing the live GPS positions reported by the UAV, the associated uplink RSSI information, and their collection timestamps. The decision on whether the reported GPS position is spoofed or not is stored in the "Info" field.

The details on the residence area estimation and the GPS spoofing detection are provided in the subsequent sections.

B. RSSI-based Positioning Approach

The 5G new radio (NR) technologies is envisaged to play an essential role in enhancing positioning accuracy, owing to the high frequency bands and dense deployments [17]. Indeed, the characteristics of the uplink or downlink radio signals are utilized to infer the location of a user equipment (e.g.,UAV). Potential radio signal-based localization approaches that will be supported by 5G NR include Time of Arrival(ToA), Angle of Arrival(AoA), and Received Signal Strength Indicator (RSSI) [18]. In the aforementioned approaches, the node(e.g., UAV) position is estimated based on the distances or angles to the anchors (e.g., 5G base station), calculated using ToA, RSSI and AoA signal measurements [19]. Compared to other signal-based localization techniques, RSSI measurements can easily be obtained from base stations without any extra hardware. Moreover, Mechanisms such as (Extended) Kalman Filter and Particle Filter can be used to reduce distance estimation error. For these reasons, an RSSI-based positioning scheme is adopted in this work to assist UTM in detecting GPS spoofing attacks. In what follows, the principle of RSSI-based technique is explained.

In RSSI-based localization techniques, the distance between the transmitter (e.g., UAV) and the receiver (e.g., gNB base station) is computed using an appropriate path loss model. A common path loss model is the log-normal shadowing model, which is able to model both LOS and NLOS communication links [20]. It can be expressed in dBm as:

$$\begin{cases} P_r(d) = \overline{P}_r(d) + \chi_\sigma \\ \overline{P}_r(d) = \overline{P}_r(d_0) + 10n\log(\dfrac{d}{d_0}) \\ \overline{P}_r(d_0) = \dfrac{P_t G_t G_r \lambda^2}{(4\pi)^2 d_0^2 L} \end{cases} \quad (1)$$

where $P_r(d)$ is the received power (in dBm) as a function of the distance d (in meter) separating the transmitter (e.g., UAV) from the receiver (e.g., gNB). $\overline{P}_r(d)$ is the corresponding average power (in dBm). χ_σ is a zero-mean Gaussian random distribution with standard deviation σ (in dBm); i.e., $\chi_\sigma \sim \mathcal{N}(0, \sigma)$. $\overline{P}_r(d_0)$ is the reference power (in dBm) received at close-in reference distance d_0. $\overline{P}_r(d_0)$ can be estimated by the Friis free-space equation. P_t is the transmitted power (in dBm), while G_t and G_r are, respectively, the transmitter and receiver antenna gains expressed in mW. λ represents the wavelength, and $L \geq 1$ is the total losses of the antenna's circuitry. n is the path loss exponent (PLE), which indicates the rate at which the path loss increases with distance.

The path loss model in (1) can be used for computing the RSSI-based distance, $\widehat{d}$ (in meters), between the transmitter and the receiver as follows:

$$\widehat{d} = d_0 10^{\frac{P_r(d_0) - \overline{P}_r(d)}{10n}} \quad (2)$$

From (2), the difference between the sent and received signal and the value of the PLE parameter have a significant impact on the accuracy of the estimated distance.

C. GPS Spoofing Detector

1) ***RSSI Estimation and Selection****:* We assume that the RSSI signal propagation follows the log-normal shadowing model presented in Eq. (1). It is worth mentioning that the distance separating the transmitter (i.e., UAV) from the receiver (i.e., gNB) has a significant impact on the signal power accuracy [21]. Indeed, the RSSI accuracy decreases greatly as the distance increases, which may lead to huge effect on the RSSI-based distance estimation error.

In this paper, a trilateration method is adopted for determining the UAV's position based on the distances calculated from the RSSI measurements of three base stations. To provide higher localization accuracy, the UTM performs the trilateration by selecting the three highest RSSI readings $RSSI_1$, $RSSI_2$, and $RSSI_3$, reported by base stations gNB_1, gNB_2, and gNB_3, respectively. In fact, a high RSSI value indicates that the UAV is closer to the base station, which results in reduced RSSI-based distance estimation error, and consequently improved localization accuracy.

2) ***Trust Level Computation****:* Let (X_1, Y_1), (X_2, Y_2) and (X_3, Y_3) denote the positions of the three selected base stations gNB_1, gNB_2, and gNB_3, respectively. Let R_1, R_2 and R_3 denote the estimated distances between the UAV and the base stations gNB_1, gNB_2, and gNB_3, respectively. If the distances are precisely measured, the trilateration approach determines the UAV's position by the intersection point between the circles centered at the base stations' positions with radii R_1, R_2 and R_3 as depicted in Fig. 2.(a). However, due to distance estimation error, the trilateration results in a residence area within which the UAV can be located as shown in Fig. 2.(b).

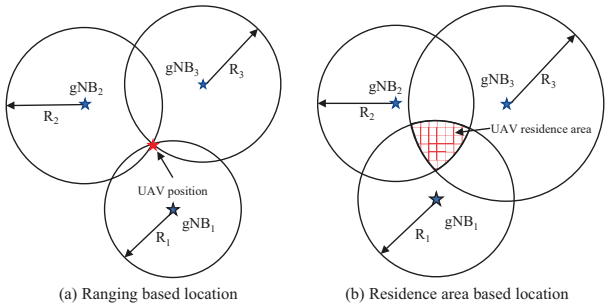


Fig. 2. Trust area and related trust level divisions.

To improve the positioning accuracy, we propose to subdivide the residence area into three trust areas with different trust levels $L1$, $L2$, and $L3$. The $L1$ trust area is mathematically defined by Eq. (3):

$$\begin{cases} d_1^2 = R_A^2 - [(x - X_A)^2 + (y - Y_A)^2] > 0 \\ d_2^2 = R_B^2 - [(x - X_B)^2 + (y - Y_B)^2] > 0 \\ d_3^2 = R_C^2 - [(x - X_C)^2 + (y - Y_C)^2] > 0 \\ d_1 \leqslant d_2 \ \wedge \ d_1 < d_3 \end{cases} \tag{3}$$

where (x, y) is a possible point inside the area. d_1, d_2 and d_3 are the distances between the point (x, y) and the borders included in the different trust level areas $L1$, $L2$ and $L3$, respectively. To obtain the $L2$ trust area, the fourth line in Eq. (3) should be replaced by:

$$d_2 \leqslant d_3 \ \wedge \ d_2 < d_1 \tag{4}$$

Similarly, the $L3$ trust area is obtained by replacing the fourth line in Eq. (3) by the following inequality:

$$d_3 \leqslant d_1 \ \wedge \ d_3 < d_2 \tag{5}$$

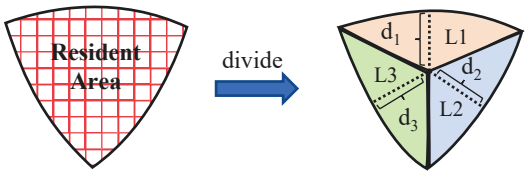


Fig. 3. The residence area divided into trust level areas.

Fig. 3 illustrates the obtained trust level areas. Each trust area of level L_i is assigned a weight ω_i, representing the likelihood that the UAV is located in this area. The assigned weight is function of the distances estimated from the RSSI measurements; i.e., R_1, R_2 and R_3. The trust area close to the border of the circle with the smallest radius is assigned the highest weight. This is, for instance, the case of the trust area with level L_1 in Fig. 3, which is close to the border of the circle with radius R_1. In fact, more the UAV is close to the base station, lower the distance estimation error will be. Thus, the UAV's real position is more likely to be near the border of the circle centered at the closest base station. Similarly, the area close to the border of the circle with the largest radius (e.g., trust area with level L_3 in Fig. 3) is assigned the lowest weight, indicating that the UAV is most improbable to be located in this area. The weight ω_i assigned to trust level L_i is computed as:

$$\boldsymbol{\omega_i} = \frac{R_{k1} R_{k2}}{\sum_{l=1}^{2} \sum_{k=l+1}^{3} R_l R_k}, k1 \neq k2 \neq i \ (k1, k2 = [1, 2, 3]) \tag{6}$$

The weights are normalized so that $\sum_{i=1}^{3} \boldsymbol{\omega_i} = 1$. Let us assume that the estimated distances R_1, R_2, and R_3 are $88m$, $136m$, and $170m$, respectively. Thus, the weights $\boldsymbol{\omega_1}$, $\boldsymbol{\omega_2}$, and $\boldsymbol{\omega_3}$ will be 0.46, 0.30, and 0.24, respectively.

The area outside the residence area is assigned a trust level $L0$. In what follows, we explain how the trust level is used by the UTM to detect the spoofed GPS positions reported by an UAV.

*3) **Adaptive Trustable Residence Area Determination**:* The adaptive trustable residence area (ATRA) is a sub-region of the residence area composed of the trust areas within which the reported GPS position should be located in order to be considered as non-spoofed. The determination of ATRA depends on trust levels and the tolerable GPS margin error. If no GPS spoofing happens, we assume that the UAV should be located within a circle of radius d_E centered at the planned position P_{gps} on the planned path, where d_E is the tolerable margin error in the GPS localization.

Let $\mathcal{T}$ denote the set of trust areas belonging to the ATRA, represented by their trust levels. The inclusion of a trust area of level L_i in the ATRA depends on the intersection area between the trust area and the GPS error tolerance area. A trust area is added to ATRA if one of the following conditions holds:

1) The whole trust area is inside the GPS error tolerance area (see Algorithm 1, lines 6–7). This is the case, for instance, of the trust area of level L_1 in Fig. 4. Thus, L_1 is added to $\mathcal{T}$;
2) The ratio of the non-overlapping trust area to the entire trust area is smaller than a threshold set to the weight of the trust area $\boldsymbol{\omega_i}$ (see Algorithm 1, lines 8–12). Thus, the low weighted trust areas are tolerated to have less space outside the GPS error tolerance area in order to be considered part of the ATRA. In the example of Fig. 4, let us assume that the weights of $L2$ and $L3$ are, respectively, 0.30 and 0.24. Let us also assume that the ratio of the non-overlapping areas $(A_{L_2} - \overline{A}_{L_2})$ and $(A_{L_3} - \overline{A}_{L_3})$ to their respective trust areas L_2 and L_3 are 0.28 and 0.30. Thus, the L_2 trust area will be included in ATRA (L_2 added to $\mathcal{T}$) but not the L_3 trust area.

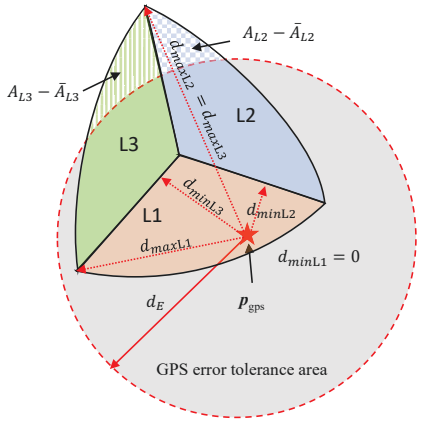


Fig. 4. Adaptive Trustable Residence Area.

*4) **ATRA-based GPS Spoofing Detection**:* To detect the GPS spoofing, the UTM compares the GPS location provided by the UAV with the ATRA while accounting for the GPS position measurement error. If the GPS position reported

Algorithm 1 ATRA Determination.

Input:
$\boldsymbol{S_{L_i}}$: The Li trust region, $i = \overline{1,3}$
$\boldsymbol{\omega_i}$: The weight of the trust level Li
$\boldsymbol{P_{gps}} = (P_{latitude}, P_{longitude})$: The GPS position planned by the UTM
$\boldsymbol{d_E}$: The tolerated GPS margin error
$\boldsymbol{R_j}$: The RSSI-based estimated distance between the UAV and the base station j

Output:
$\boldsymbol{\mathcal{T}}$: The adaptive trustable residence area

1: $(x_{gps}, y_{gps}) \leftarrow Get\_Cartisian(P_{gps})$
2: $\boldsymbol{T} \leftarrow \{\}$
3: **for each** L_i **do**
4: $\quad d_{minPi} \leftarrow Min\_Distance(S_{L_i}, (x_{gps}, y_{gps}))$
5: $\quad d_{maxPi} \leftarrow Max\_Distance(S_{L_i}, (x_{gps}, y_{gps}))$
6: $\quad$ **if** $d_{maxPi} \leq \boldsymbol{d_E}$ **then**
7: $\quad\quad \boldsymbol{\mathcal{T}} \leftarrow \boldsymbol{T} \cup \{\boldsymbol{L_i}\}$
8: $\quad$ **else if** $d_{minPi} < \boldsymbol{d_E}$ and $d_{maxPi} > \boldsymbol{d_E}$ **then**
9: $\quad\quad \boldsymbol{A_{L_i}} \leftarrow Area(\boldsymbol{S_{L_i}})$
10: $\quad\quad \overline{\boldsymbol{A}}_{\boldsymbol{L_i}} \leftarrow Area(\boldsymbol{S_{L_i}} \cap Circle(x_{gps}, y_{gps}, d_E))$
11: $\quad\quad$ **if** $\frac{A_{L_i} - \overline{A}_{L_i}}{A_{L_i}} < \boldsymbol{\omega_i}$ **then**
12: $\quad\quad\quad \boldsymbol{\mathcal{T}} \leftarrow \boldsymbol{T} \cup \{\boldsymbol{L_i}\}$
13: $\quad\quad$ **end if**
14: $\quad$ **end if**
15: **end for**
16: **Return** $\boldsymbol{\mathcal{T}}$

Algorithm 2 ATRA-based GPS Spoofing Detection.

Input:
$\boldsymbol{\mathcal{T}}$: The adaptive trustable residence area
$\boldsymbol{TL_{R_{gps}}}$: The trust level of the reported GPS tposition
$\boldsymbol{TL_{P_{gps}}}$: The trust level of the planned GPS position
$\boldsymbol{d_E}$: The tolerated GPS margin error
Output:
$\boldsymbol{Decision}$: The reported GPS position is spoofed (= 1) or not (= 0)
1: **if** $(\boldsymbol{TL_{R_{gps}}} \in \boldsymbol{\mathcal{T}})$ **then**
2: $\quad \boldsymbol{Decision} \leftarrow 0$
3: **else if** $(\mathbf{card}(\boldsymbol{\mathcal{T}}) == 3)$ and $(distance(R_{gps}, P_{gps}) < d_E)$ **then**
4: $\quad \boldsymbol{Decision} \leftarrow 0$
5: **else if** $(\boldsymbol{TL_{R_{gps}}} == \boldsymbol{TL_{P_{gps}}})$ and $(\boldsymbol{TL_{R_{gps}}} \neq L_0)$ **then**
6: $\quad \boldsymbol{Decision} \leftarrow 0$
7: **else**
8: $\quad \boldsymbol{Decision} \leftarrow 1$
9: **end if**
10: **return** $\boldsymbol{Decision}$

by the UAV is outside the residence area, a trust level $L0$ is assigned to this position. However, if the reported GPS position is inside the residence area, it will be assigned one of the trust levels $L1$, $L2$ and $L3$, depending on which trust area the GPS position is located in. The UTM considers a reported GPS position as authentic (i.e., not spoofed) if one of the following conditions is met:

1) The trust level of the reported position is included in the ATRA $\boldsymbol{\mathcal{T}}$ (see Algorithm 2, line 1);
2) Both the reported position and the whole residence area are inside the GPS error tolerance area. This case allows to reduce the number of false positives (i.e., a normal position considered as spoofed) due to uncertainty in GPS measurements (see Algorithm 2, line 3);
3) The GPS error tolerance area is inside the residence area and both the planned and reported GPS positions are located within the same trust area (see Algorithm 2, line 5).

Otherwise, the reported GPS position is considered spoofed.

III. Performance Evaluation

In this section, the performance of the proposed ATRA-based GPS spoofing detector is evaluated in both free-space and urban area environments.

A. Simulation Setup

We consider three base stations fixed at positions $(800, 800)$, $(750, 600)$, and $(600, 700)$ in a 2D space, respectively. The UAV's planned position is fixed at $(700, 700)$, while its real position is randomly generated within the range of the three base stations. The UAV's reported position is randomly selected within the GPS error tolerance area of the planned position. The uplink communication links between the UAV and the base stations are modeled using the log-normal shadowing model given in equation (1). The PLE n is randomly varied in $[1.9, 2.1]$ and $[2.7, 3.5]$ to model free space and urban area environments, respectively. The variance σ of the random shadowing effects χ_σ is set to $6dBm$ for free space and $10dBm$ for urban space. The UAV's GPS is considered spoofed when the distance between the real position and the planned position is bigger than the tolerated GPS margin error d_E. All simulations are implemented using Python.

B. Performance Results

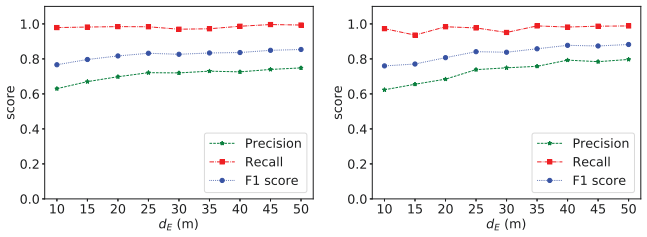
To evaluate the proposed ATRA-based GPS spoofing detector, the *precision*, *recall* and *F1-score*, defined in Eq (7), are measured. The *precision* is the percentage of detected spoofed positions that are truly spoofed positions. The *recall* refers to the percentage of actual spoofed positions that are correctly detected as spoofed. The *F1-score* is the harmonic mean of precision and recall.

$$\begin{cases} Precision = TP/(TP + FP) \\ Recall = TP/(TP + FN) \\ F1 = \dfrac{2 * Recall * Precision}{Recall + Precision} \end{cases} \tag{7}$$

Where TP (True Positive) is the correctly detected spoofed positions, FN (False Negative) is the spoofed positions detected as normal positions, FP (False Positive) is the normal positions considered as spoofed, and TN (True Negative) is the normal positions that are correctly detected as normal.

The evaluation of ATRA-based GPS spoofing detector is performed by varying the tolerated GPS margin error d_E. The performance measures depicted in Fig. 5 are obtained over 10000 positions for each d_E. The obtained results show that the proposed approach performs well in both free-space and urban area environments, which demonstrates that the shadowing effects have no impact on the detection accuracy. It is observed that the detection precision increases as the tolerated deviation from the planned position increases, to reach 80% for a tolerated deviation of $50m$. A recall rate

of above 95% is achieved, showing the high effectiveness of the proposed solution in detecting spoofed positions. It is worth noting that the recall metric is preferred in assessing the solution efficacy, as the unsuccessful detection of spoofed positions may lead to high risks of collisions and/or violation of no-fly zone regulation. The F1-score values indicate an overall performance that can reach 88%, which expresses a good balance between precision and recall.



(a) Free space (b) Urban space

Fig. 5. ATRA performance in free and urban space.

IV. Conclusion

This paper presented a novel method for detecting the GPS spoofing in an UAV environment. The proposed method leverages the uplink RSS measurements collected from the base stations to identify the adaptive trustable residence area (ATRA), which represents the region where the reported GPS positions need to be located in order to be considered as non-spoofed. The performances of the proposed method in terms of precision, recall and F1-score were evaluated through simulation. The obtained results showed the high effectiveness of the ATRA-based GPS spoofing detector in detecting spoofed positions in both free-space and urban area with a rate above 95%.

In the future, we will adopt the 3D LOS/NLOS path loss models for aerial vehicles, recently defined by 3GPP [22]. Furthermore, the proposed ATRA-based GPS spoofing approach will be extended to deal with situations where less than three base stations are in the vicinity of the UAV. Finally, Machine Learning (ML) will be leveraged for GPS spoofing detection based on channel quality metric.

V. Acknowledgement

This work was partially supported by the European Union's Horizon 2020 Research and Innovation Program through the 5G!Drones Project under Grant No. 857031, the Academy of Finland 6Genesis project under Grant No. 318927, It was also supported in the National Outstanding Youth Science Fund Project of China with grant No. 61825104 and the National Natural Science Foundation of China under grant agreement No. 61941105.

References

[1] H. Hellaloui, A. Chelli, M. Bagaa, and T. Taleb, "Towards Mitigating the Impact of UAVs on Cellular Communications," in *Proc. of the IEEE Global Communications Conf. (GLOBECOM)*, 2018, pp. 1 – 7.

[2] O. Bekkouche, T. Taleb, and M. Bagaa, "UAVs Traffic Control based on Multi-Access Edge Computing," in *Proc. of the IEEE Global Communications Conf. (GLOBECOM)*, 2018, pp. 1 – 6.

[3] 3GPP TS 22.125, "Unmanned Aerial System (UAS) support in 3GPP," Dec. 2018.

[4] K. Pärlin, M. M. Alam, and Y. L. Moullec, "Jamming of UAV Remote Control Systems using Software Defined Radio," in *Proc. of the International Conf. on Military Communications and Information Systems (ICMCIS)*, May 2018, pp. 1 – 6.

[5] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method using a Multi-Antenna Array," in *Proc. of the 25th ION GNSS*, Sept. 2012, pp. 1233 – 1243.

[6] J. Magiera and R. Katulski, "Detection and Mitigation of GPS Spoofing based on Antenna Array Processing," *Journal of Applied Research and Technology*, vol. 13, no. 1, pp. 45–57, 2015.

[7] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS Spoofing Detection via Dual-receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[8] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[9] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks," pp. 1018–1031, May 2018.

[10] K. D. Wesson, M. Rothlisberger, and T. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication," *NAVIGATION: Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[11] Z. Wu, Y. Zhang, and R. Liu, "BD-II NMA&SSI: An Scheme of Anti-Spoofing and Open BeiDou II D2 Navigation Message Authentication," *IEEE Access*, vol. 8, pp. 23 759–23 775, 2020.

[12] T. Liu, A. Hojjati, A. Bates, and K. Nahrstedt, "Alidrone: Enabling Trustworthy Proof-of-Alibi for Commercial Drone Compliance," in *Proc. of the IEEE 38th International Conf. on Distributed Computing Systems (ICDCS)*, Jul. 2018, pp. 841–852.

[13] H. Zhu, M. L. Cummings, M. Elfar, Z. Wang, and P. Pajic, "Operator Strategy Model Development in UAV Hacking Detection," *IEEE Transactions on Human-Machine Systems*, vol. 49, no. 6, pp. 540–549, 2019.

[14] 3GPP TS 22.825, "Study on Remote Identification of Unmanned Aerial Systems (UAS)," Sept. 2018.

[15] 3GPP TS 23.754, "Study on Supporting Unmanned Aerial Systems (UAS) Connectivity, Identification and Tracking," Dec. 2018.

[16] J. Jung and S. Nag, "Automated Management of Small Unmanned Aircraft System Communications and Navigation Contingency," in *AIAA Scitech 2020 Forum*, 2020.

[17] 3GPP TR 38.855, "Study on NR Positioning Support," March 2019.

[18] NGMN, "5G E2E Technology to Support Verticals URLLC Requirements," 2019.

[19] W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*. John Wiley & Sons, 2010.

[20] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 1996.

[21] J. Luomala and I. Hakala, "Analysis and Evaluation of Adaptive RSSI-based Ranging in Outdoor Wireless Sensor Networks," *Ad Hoc Networks*, vol. 87, pp. 100–112, 2019.

[22] 3GPP TR 36.777, "Enhanced LTE Support for Aerial Vehicles," Dec. 2017.