A Low-Cost UAV-Based Secure Location Verification Method

Marco Rasori*
University of Florence
DINFO
Via di S. Marta, 3
Florence, Italy 50139
marco.rasori@unifi.it

Pericle Perazzo
University of Pisa
Information Engineering
Largo Lucio Lazzarino, 1
Pisa, Italy 56122
pericle.perazzo@iet.unipi.it

Gianluca Dini
University of Pisa
Information Engineering
Largo Lucio Lazzarino, 1
Pisa, Italy 56122
gianluca.dini@iet.unipi.it

ABSTRACT

The capability to verify positions reported by devices is called secure location verification. The majority of the proposed solutions entail the use of many fixed anchors often along with special hardware, e.g., ultra-wideband and ultrasonic transceivers. However, the deployment and maintenance costs of such solutions make them scarcely attractive. A cheaper alternative is to use mobile entities as trusted infrastructure. In particular, Unmanned Aerial Vehicles (UAVs) represent a promising approach. Indeed, recent studies used them to face the secure location verification problem. In this paper, we introduce a low-cost approach based on a swarm of UAVs and a common radio frequency protocol, e.g., WiFi. By experimental simulations, we show that by using only three UAVs our system detects more than 99% of the attacks against an adversary that falsifies its position of at least 20 m. We also consider an adversary capable of tracking UAVs positions. The success probability of such an advanced adversary is smaller than 1% starting from a falsification distance larger than 35 m.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**; *Security services*; *Security protocols*;

KEYWORDS

Secure Location Verification, Unmanned Aerial Vehicles, UAV swarms, RSS-based localization

*Also with University of Pisa, Department of Information Engineering.

1 INTRODUCTION

Secure location verification is a process by which an infrastructure composed by one or more *verifiers* attempts to verify that a *prover* is actually placed where it claims to be. The problem of the secure location verification has been widely studied, and many different solutions have been proposed [14]. However, existing solutions make use of special hardware and/or many fixed verifiers, which entail high deployment costs and make them scarcely attractive. A promising and low-cost approach involves the use of *Unmanned Aerial Vehicles* (*UAVs*) as verifiers. In the last decade, UAVs employment has known a prosperous growth, especially in commercial and civil fields. UAVs have been used in swarms to accomplish disparate tasks [3, 11]. Recent studies addressed the problem of secure location verification by means of UAVs [5, 13]. However, they use special hardware, e.g., ultra-wideband (UWB) or stereo cameras, which makes them expensive and therefore hard to realize.

In this paper, we present a novel low-cost secure location verification approach based on a swarm of few UAVs equipped with common radio frequency (RF) transceivers (e.g., WiFi). This perfectly fits, for instance, a crowd sensing application in which a set of participants provided with smartphones share their positions to estimate the crowd density in some area. In this application, the UAVs can carry out random spot checks on participants in order to assure that their generated positions are genuine.

In our work, we suppose that a device claims its position and is reached by the swarm of UAVs, which places in formation around the device. Then, through an RF communication, a location verification protocol starts, and the device is asked to broadcast a message. By measuring the strengths of the

received signals by the UAVs, the system can establish if the device claimed its actual position.

The paper has several contributions. We first analyse a simple attack in which a malicious prover claims a false position. Then we introduce a stronger adversary that is capable of tracking UAVs' positions and adjusting its transmission power. By experimental evaluations, we investigate the impact of swarm cardinality and formation on the ability of detecting the presence of an adversary. The results of these tests show that a swarm of only three UAVs detects more than 99% of the attacks starting from a falsification distance of 20 m against a basic adversary, and 35 m against a stronger adversary.

The paper is organized as follows: in Section 2 we compare with related work. In Section 3 we introduce system and adversary models and describe the proposed location verification protocol. In Section 4 we evaluate the success probability of the adversary. Section 5 summarizes our results and concludes the paper.

2 RELATED WORK

The use of UAVs as mobile infrastructure represents a low-cost solution to the secure location verification problem. Yokohama et al. [13] use UAVs in a study related to secure positioning. They describe a method based on image processing to estimate the distances between the verifiers and the prover. This implies UAVs need to be equipped with high-resolution stereo cameras. In contrast, our approach is cheaper because it takes advantage of basic onboard components of a UAV and does not require additional hardware. Moreover, a visual technique entails a direct line of sight between every verifier and the prover. This constraint is not mandatory in our model.

Perazzo et al. [5, 6] approach the location verification problem using one UAV. They base their solution on UWB transceivers. However, at the present time these transceivers are neither widespread nor cheap.

Baker and Martinovic [2] describe an approach for secure location verification that employs a mobile verifier and at least one fixed verifier to determine prover's position by means of time difference of arrival (TDoA). This solution necessitates strict time synchronization between the base stations to achieve accuracy, and this requires technical effort and raises implementation costs. Our protocol is not subject to any rigid synchronization constraints, and thus it can be realized in a cheaper way.

Rasmussen et al. [8] describe an approach in which the verifiers are covert base stations, and another approach that employs a mobile base station. They both rely on time differences between RF and ultrasonic (US) signals sent by the prover in order to estimate the distances between verifiers and prover. Such a solution depends on US communication modules that are not off-the-shelf components in commercial UAVs. Our solution is more general and cheaper.

Other studies [7, 9, 10] deal with secure location verification by relying on infrastructures composed of many fixed verifiers whose locations are known. A fixed infrastructure is a huge constraint in terms of deployment and maintenance costs. In contrast, UAVs used as mobile verifiers are cheaper and more versatile since a few of them can cover wide areas. Moreover, the authors in [7, 9] make use of UWB transceivers that are currently not widespread. In contrast, our solution presumes the use of common wireless communication hardware (e.g., WiFi), which is often installed off the shelf on UAVs and mobile devices.

3 SYSTEM AND ADVERSARY MODELS

In our system, a swarm of UAVs forms the verification infrastructure where each UAV plays the role of verifier. UAVs are mobile stations and so they can autonomously reach given positions to start the location verification protocol. The *prover* is a device, for example a smartphone, claiming to be at a certain position (*claimed position*, p_C) that must be verified. We use n to indicate the *swarm cardinality*, i.e., the number of UAVs in the swarm.

We require UAVs to be equipped with a GPS module and an RF communication module (e.g., a WiFi transceiver). We assume that UAVs can determine their own positions by means of GPS. The RF module is used for the communication with the prover and the other UAVs. Moreover, we suppose that one UAV, the *leader*, shares a secret K (*shared secret*) with the prover. The secrets can be distributed to the provers in a secure manner through a generic key distribution scheme ([4]). The way in which this is deployed goes beyond the scope of this paper. We also assume the UAVs can communicate securely among one another. The UAVs move toward the claimed position and take positions within a *communication range* R from it, according to a given *swarm formation*. Then, the following location verification protocol, represented also in Figure 1, takes place:

$$
\begin{array}{lllll}
M1\text{:} & \text{leader} \rightarrow \text{prover:} & N & & \\
M2\text{:} & \text{prover} \not\rightarrow {}^{*}\text{:} & \text{sign}_K(N) & & \\
M3\text{:} & u_i \rightarrow \text{leader:} & \text{sign}_K(N), P_{Rx,i} & & \forall i,
\end{array}
$$

where the symbol $\not\rightarrow {}^{*}$ represents a broadcast message.

The leader starts the protocol by transmitting a nonce N to the prover, while the other UAVs remain passive. Then, the prover creates and broadcasts the message $M2$, which includes the nonce signed with the shared secret K. This is needed to authenticate the prover, and it is necessary to avoid that a malicious entity impersonates the actual prover. Additionally, we assume that the prover transmits $M2$ using a *nominal transmission power* P_{Tx}, which is known by the leader. Each UAV u_i is supposed to receive $M2$ with power

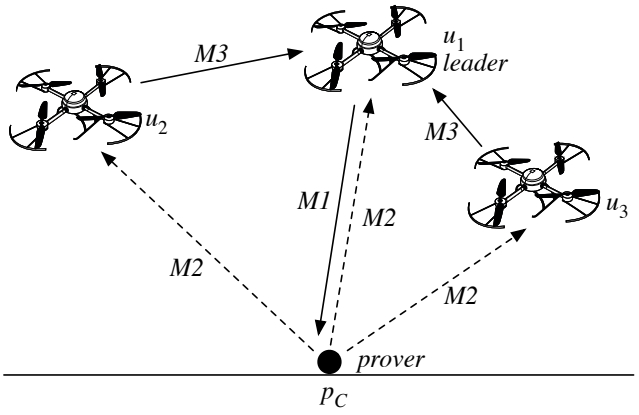


Figure 1: Location verification protocol. p_C is the *prover*'s claimed position; solid arrows indicate unicast messages, whereas dashed arrows indicate broadcast message.

$P_{Rx,i}$ (*received power*), and send the message $M3$ to the leader, including the signature and the received power. As soon as the leader receives all the messages from the other UAVs, it verifies the signature of all the received messages by using the shared secret K. Then, according to a path loss model, the leader computes the power that u_i should have received (*expected power*, $P_{Exp,i}$). The leader detects an attack if at least one absolute difference between the expected and the received powers is greater than a predetermined *consistency threshold* ΔP_{Rx}:

$$\begin{aligned}&\text{if } \left(\forall i \left|P_{Exp,i} - P_{Rx,i}\right| \leq \Delta P_{Rx}\right)\\ &\quad \text{then} \quad \text{no attack}\\ &\quad \text{else} \quad \text{attack detected.}\end{aligned}$$

In the following section, we will show how the system can fix a value for the consistency threshold.

3.1 Path Loss Model and Consistency Threshold Computation

The received power that each UAV experiences can be modeled through the standard log-distance path loss model [1], which follows the equation:

$$P_{Rx} = P_{Tx} - PL_0 - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) - X_g, \tag{1}$$

where P_{Tx} is the transmission power in decibel-milliwatt, PL_0 is the path loss in decibel (dB) at the reference distance d_0, γ is the *path loss exponent*, and X_g, in dB, represents the *shadowing effect term* and is modeled as a normal random variable with zero mean and standard deviation σ_g. We assume to know the parameters of the log-distance path loss model, namely the reference distance d_0, the path loss at the reference distance PL_0, the path loss exponent γ, and the standard deviation σ_g of the Gaussian random variable X_g.

By Eq. 1, the leader can estimate the expected power at u_i by setting $d = d_{C,i}$:

$$P_{Exp,i} = P_{Tx} - PL_0 - 10\gamma \log_{10}\left(\frac{d_{C,i}}{d_0}\right), \tag{2}$$

where $d_{C,i}$ is the distance between the u_i's position (which is known by the leader) and the prover's claimed position. Obviously, the shadowing effect term is not included in (2) because its value cannot be predicted by the system. Therefore, in case of an honest prover, the received power and the expected power differ only in the shadowing effect term.

We fix the consistency threshold in order to obtain a given probability of false positives, i.e., honest provers considered adversaries. The *false positive probability* (fp) coincides with the probability of warning an attack in the honest scenario:

$$fp = 1 - \prod_{i=1}^{n} \Pr\left(\left|P_{Exp,i} - P_{Rx,i}\right| \leq \Delta P_{Rx}\right), \tag{3}$$

where the product represents the probability that there are no inconsistencies between the expected and the received power at every UAV. Since the expected and the received powers differ only in the shadowing effect term $X_{g,i}$ (cfr. Eqq. 1 and 2), and since $X_{g,i}$ are Gaussian and identically distributed random variables with standard deviation σ_g, then Eq. 3 becomes:

$$fp = 1 - \left[2\,\Phi\left(\frac{\Delta P_{Rx}}{\sigma_g}\right) - 1\right]^n, \tag{4}$$

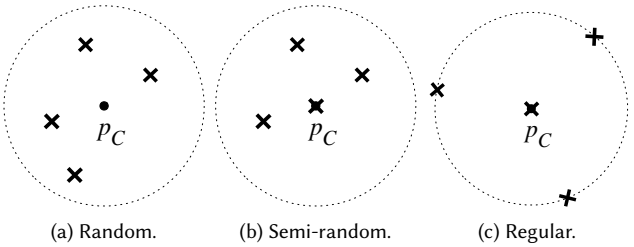
where $\Phi(\cdot)$ is the normal cumulative distribution function. It follows that:

$$\Delta P_{Rx} = \sigma_g \Phi^{-1}\left(\frac{1 + \sqrt[n]{1 - fp}}{2}\right). \tag{5}$$

3.2 Adversary Model

An attack occurs when a prover lies on its position. We assume the adversary claims to be at a distance d_f (*falsification distance*) from its *actual position* p_A, in a random direction. In other words, the falsification distance is the distance between the claimed position and the actual position. Such attack is known as the *false reported location attack* [14], and we will refer to this malicious prover as the *blind* adversary.

The second kind of attack that we consider extends the first one. The *observer* adversary is also able to estimate the position of every UAV. Using this information, it can adapt the transmission power of $M2$ in order to cheat the verification system. For each u_i, the observer adversary computes the transmission power $P_{TxA,i}$ for which the expected and the received power at u_i coincide ($P_{Exp,i} = P_{Rx,i}$), so



(a) Random. (b) Semi-random. (c) Regular.

Figure 2: Example of the swarm formations tested. Crosses represent the UAVs while the black dot is the claimed position. The dashed line represent the communication range R from p_C.

obtaining:

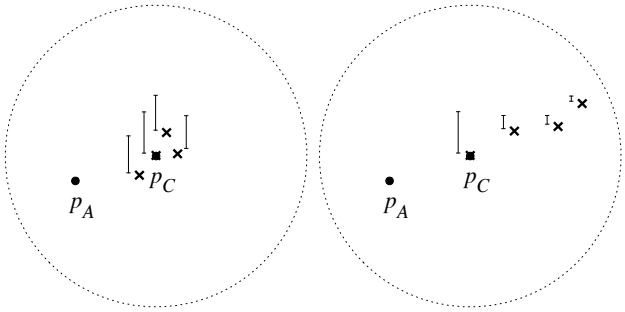
$$P_{TxA,i} = P_{Tx} + 10\gamma \log_{10}\left(\frac{d_{A,i}}{d_{C,i}}\right), \quad \forall i, \tag{6}$$

where $d_{A,i}$ and $d_{C,i}$ are the distances from u_i to the actual position and to the claimed position, respectively. We assume the adversary as a single entity which transmits from a unique position, hence no collusion attacks are considered. We further assume that the adversary does not have directional antennas by which it could send multiple copies of $M2$ with different transmission powers. Therefore, the adversary chooses the value P_{TxA}, that is the mean value of all the $P_{TxA,i}$, as transmission power.

3.3 Swarm Formations

The way the swarm places in the proximity of the claimed position plays an important role for the attacks detection. Our model considers UAVs placement in the 3D space. Initially, we assume a fixed altitude h for all the UAVs in the swarm, and their positions within R from the claimed position, according to a uniform random distribution. From now on, we will refer to this formation as the *random* formation (Figure 2a). It is the simplest formation and also makes UAVs' positions less predictable for the blind adversary. However, if all the UAVs happen to be far from both the claimed and the actual position, a blind adversary has high success probability. Indeed, all the expected and the received powers would be low, and thus similar. Of course, the same problem arises with the observer adversary too.

To solve this problem, we put one UAV in plumb line above p_C at altitude h_{pl} lower than h, while the others are randomly disposed as in the random formation. This change should improve system security because of the presence of a UAV near the claimed position, whose expected power should be high. We will refer to this formation as the *semi-random* formation (Figure 2b). However, this solution might be still vulnerable against the observer adversary in those cases in



(a) Cluster case. (b) Alignment case.

Figure 3: Critical cases for the semi-random formation. Crosses are the UAVs, and bars represent the expected powers $P_{Exp,i}$.

which UAVs are placed in a limited area near p_C, forming a *cluster* (Figure 3a). Indeed, all the expected powers are similar, and therefore the observer adversary can cheat the verification system by properly increasing the transmission power. Moreover, another critical case may happen when the UAVs are aligned and opposite to p_A as shown in Figure 3b. In this situation, a high transmission power by the observer adversary could result in received powers comparable with the expected ones. This means that in such a scenario the observer adversary has high success probability.

To solve these problems, we then analyze a third formation: one UAV is still placed in plumb line above the claimed position at altitude h_{pl}, and the others are evenly distributed on a circumference centered on p_C at altitude h; the radius is computed so that the distance between p_C and these UAVs is equal to the communication range R. By doing so, we avoid the weaknesses of the semi-random formation shown in Figures 3a and 3b. From now on, we will refer to this formation as the *regular* formation (Figure 2c).

4 EXPERIMENTAL EVALUATION

Our goal is to achieve a low *false negative probability* (fn), i.e., the percentage of adversaries considered honest provers, while keeping a low false positives probability. While fp was fixed a priori and set to 1 percent ($fp = 0.01$), fn was obtained through simulations of different scenarios.

The parameters of the log-distance path loss model mainly depend both on the environment and the obstacles that the signal encounters along its path. Yanmaz et al. [12] studied WiFi channel for UAV-to-ground link. Accordingly to their work, we set the path loss exponent γ to 2.6. The swarm cardinality was set from a minimum of 3 to a maximum of 6 to test whether acceptable outcomes could be obtained even with fewer UAVs. Moreover, we assumed $\sigma_g = 3$ dB, the

reference distance $d_0 = 1$ m, and a communication range R of 100 m.

Every formation was basically placed according to Section 3.3. In the random formation, UAVs were disposed with a fixed altitude, i.e., $h = 25$ m. In the semi-random and regular formations, the altitude for the plumb-line UAV was set to $h_{pl} = 5$ m.

We deployed our simulator in MATLAB. In order to obtain statistically sound results, 5000 independent trials with different seeds were run for each scenario. Within each trial, we firstly simulated the presence of an adversary by generating a claimed position and an actual position. Then, we placed the UAVs around p_C, according to the formation to be tested. At that point, the location verification protocol was simulated; the received powers by the various UAVs were simulated as well following Eq. 1, and a random value for the shadowing effect was generated for every value of $P_{Rx,i}$.

In our first set of simulations we set the falsification distance d_f to 30 m, and we tested swarm formations security in terms of false negative probability, varying the swarm cardinality. Figure 4a shows the formations' performances against the blind adversary. We observe that the random formation was the weakest one in detecting attacks. Indeed, fn was about 85% with the highest swarm cardinality tested. On the other hand, both semi-random and regular formations did not miss a single detection within every scenario tested.

Figure 4b shows the false negative probability with regards to the observer adversary; obviously, security lowers for all the formations if compared to the case of the blind adversary. However, semi-random and regular formations still exhibit excellent results. Their performance is clearly much better than the one provided by the random formation; specifically, with a swarm of 3 UAVs, the random formation did not detect 93% of the attacks whereas the semi-random and the regular formations did not detect 5.6% and 3% of the attacks, respectively. In this case, but also with higher swarm cardinalities, the regular formation outperforms the others and results as the best choice for the attacks detection. With the semi-random formation, cluster and alignment cases are more likely when the swarm cardinality is low. Therefore, as n increases, the performance of the semi-random formation improves to the point of performing almost equivalently to the regular formation. With a swarm of 6 UAVs, fn for the semi-random and the regular formations are 0.85% and 0.6%, respectively.

Figure 5 shows the results obtained varying d_f from 0 m to 50 m. The swarm cardinality was set to 3. Figure 5a confirms that the random formation is not suitable to make the system secure since fn is over 60% when $d_f = 50$ m. The other two formations perform equivalently against the blind adversary. Specifically, they both achieved a false negative probability of about 1% starting from a falsification distance of 20 m.

Figure 5b shows the results obtained with an observer adversary. It is noticeable how the regular formation outperforms the others; specifically, starting from $d_f = 20$ m the regular formation detects more attacks than the semi-random one. Indeed, the latter is vulnerable to the critical cases of Figures 3a and 3b, and this leads to a performance lowering. In contrast, the regular formation is more robust and avoids such critical cases. After the analysis varying the falsification distance, we can assert that the regular formation is the most secure among the ones we tested, achieving a false negative probability lower than 1% starting from a falsification distance of 35 m with a swarm of 3 UAVs.

5 CONCLUSIONS

We investigated a low-cost approach that uses a swarm of UAVs to securely verify devices' positions by means of received power in outdoor environment. We modeled the system and ran a set of experimental evaluations. The choice of the formation was a crucial point to make the system secure. With a swarm of only three UAVs, the regular formation detected more than 99% of the false reported location attacks starting from a falsification distance of 20 m. Moreover, the success probability of the observer adversary was smaller than 1% starting from a falsification distance larger than 35 m.

ACKNOWLEDGMENTS

This work has been supported by the research project "Analisi di dati sensoriali: dai sensori tradizionali ai sensori sociali" funded by "Progetti di Ricerca di Ateneo - PRA 2016" of the University of Pisa; the research project "Guida, Navigazione, Comunicazione e Controllo ad Elevata Sicurezza per Veicoli Senza Pilota" funded by "Progetti di Ricerca di Ateneo - PRA 2017" of the University of Pisa; and the SCIADRO project, cofunded by the Tuscany Region (Italy) and the Research Facilitation Fund (FAR) of the Ministry of Education, University and Research (MIUR).

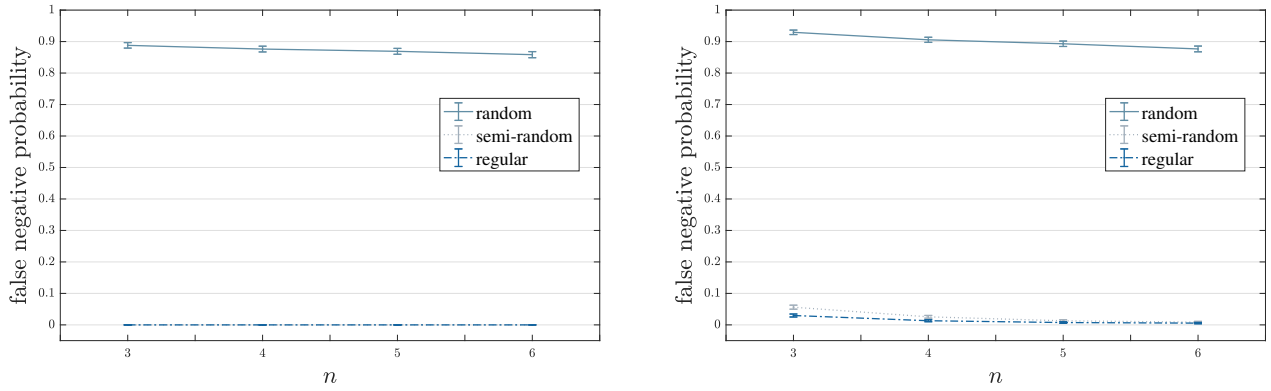
REFERENCES

[1] Jorgen Bach Andersen, Theodore S Rappaport, and Susumu Yoshida. 1995. Propagation measurements and models for wireless communications channels. *IEEE Communications Magazine* 33, 1 (1995), 42–49.

[2] Richard Baker and Ivan Martinovic. 2016. Secure Location Verification with a Mobile Receiver. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, 35–46.

[3] Fausto G Costa, Jó Ueyama, Torsten Braun, Gustavo Pessin, Fernando S Osório, and Patrícia A Vargas. 2012. The use of unmanned aerial vehicles and wireless sensor network in agricultural applications. In *2012 IEEE International Geoscience and Remote Sensing Symposium*. IEEE, 5045–5048.

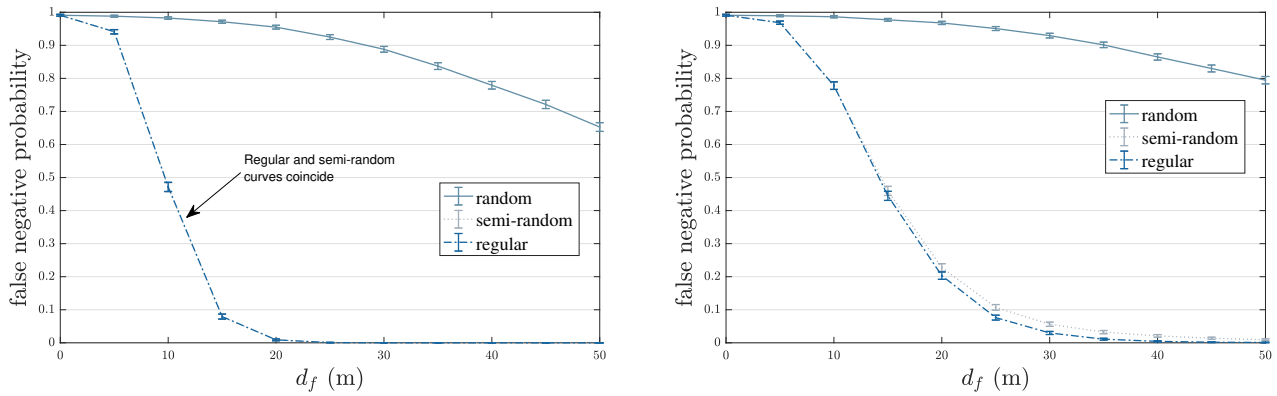
[4] Wenliang Du, Jing Deng, Yunghsiang S Han, Shigang Chen, and Pramod K Varshney. 2004. A key management scheme for wireless sensor networks using deployment knowledge. In *INFOCOM 2004*.



(a) Blind adversary.

(b) Observer adversary.

Figure 4: False negative probability and 95% confidence intervals for different number of UAVs. $d_f = 30\,\mathrm{m}$.



(a) Blind adversary.

(b) Observer adversary.

Figure 5: False negative probability and 95% confidence intervals as function of d_f, ranging from 0 m to 50 m. $n = 3$.

Twenty-third AnnualJoint conference of the IEEE computer and communications societies, Vol. 1. IEEE.

[5] Pericle Perazzo, Kanishka Ariyapala, Mauro Conti, and Gianluca Dini. 2015. The verifier bee: A path planner for drone-based secure location verification. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*. IEEE, 1–9.

[6] Pericle Perazzo, Francesco Betti Sorbelli, Mauro Conti, Gianluca Dini, and Cristina M Pinotti. 2016. Drone Path Planning for Secure Positioning and Secure Position Verification. *IEEE Transactions on Mobile Computing* (2016).

[7] Pericle Perazzo, Lorenzo Taponecco, Antonio A D'amico, and Gianluca Dini. 2016. Secure positioning in wireless sensor networks through enlargement miscontrol detection. *ACM Transactions on Sensor Networks (TOSN)* 12, 4 (2016), 27.

[8] Kasper Rasmussen, Mani Srivastava, et al. 2008. Secure location verification with hidden and mobile base stations. *IEEE Transactions on Mobile Computing* 7, 4 (2008), 470–483.

[9] Srdjan Čapkun and J-P Hubaux. 2006. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications* 24, 2 (2006), 221–232.

[10] Adnan Vora and Mikhail Nesterenko. 2004. Secure location verification using radio broadcast. In *International Conference on Principles of Distributed Systems*. Springer, 369–383.

[11] Sonia Waharte, Niki Trigoni, and Simon Julier. 2009. Coordinated search with a swarm of UAVs. In *2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops*. IEEE, 1–3.

[12] Evşen Yanmaz, Robert Kuschnig, and Christian Bettstetter. 2011. Channel measurements over 802.11a-based UAV-to-ground links. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 1280–1284.

[13] Roberto Sadao Yokoyama, Bruno Yuji Lino Kimura, and Edson dos Santos Moreira. 2014. Secure positioning in a UAV swarm using on-board stereo cameras. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing*. ACM, 769–774.

[14] Yingpei Zeng, Jiannong Cao, Jue Hong, Shigeng Zhang, and Li Xie. 2013. Secure localization and location verification in wireless sensor networks: a survey. *the Journal of Supercomputing* (2013), 1–17.