Anonymous Drone Swarm Identification Considering Dynamic Flight Plan

Soojin Lee[1] and Seung-Hyun Seo[2*]

[1] Dept. of Electrical Engineering, Hanyang University, Seoul, KOREA
tssn195@hanyang.ac.kr
[2] Dept. of Electrical Engineering, Hanyang University ERICA, Ansan, KOREA
seosh77@hanyang.ac.kr

Abstract

As the use of drone swarms becomes more widespread, there is a growing need for secure drone operations. Recently, the Federal Aviation Administration has introduced remote ID regulations to monitor aircraft and ensure the safe operation of aviation systems. However, the current regulations do not adequately protect drone privacy, as they reveal the drone's location and identifier in the remote ID message. To preserve the drone's privacy, a few anonymous drone identification and authentication protocols have been suggested. However, these protocols require high computational resources, making them less suitable for the drone environment, and they do not account for drone swarm scenarios. Therefore, we propose a lightweight drone swarm anonymous identification protocol. Furthermore, we introduce an identification scenario that takes into account changes in the drone's flight path. Each drone generates pseudonyms utilizing Physical Unclonable Functions (PUFs) and Henon maps. As a result, the proposed protocol offers low computational demands for drones while providing anonymity and ensuring security against drone impersonation attacks based on the characteristics of PUFs.

Keywords: identification, privacy, pseudonym generation

1 Introduction

Recently, as drone technology and communication technology have developed, the utilization of drones, which are also known as Unmanned Aircraft Systems (UAS), is increasing. Drones can collect necessary sensor data, reconnoiter surroundings, and serve as cargo ships, so they are used in various fields such as agriculture[1], urban monitoring[2, 3], and national defense[4]. With the advent of aerial mobility, the issues arising from objects moving in the airspace have expanded beyond just those on the ground. The lack of clear policies monitoring aerial objects has created issues where drones can fly into unauthorized areas or breach critical national facilities[5]. Therefore, it is crucial to enhance drone flight monitoring and identification.

The U.S. Federal Aviation Administration (FAA) proposed Remote ID regulation to improve airspace safety and operate drone networks efficiently[6]. Remote ID (Remote Identification) serves as the digital license plate for drones, allowing each drone to broadcast its identity and location information during flight. Drones should transmit their identity and location information to Zone Service Providers or air traffic control towers for every specified short term during flight, in accordance with the regulation.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.62
*Corresponding author : Department of Electrical Engineering, Hanyang University ERICA Campus, Ansan, 15588, Republic of Korea, Tel +82-31-400-5114

However, the Remote ID regulation does not include additional provisions for data security transmitted by drones. As a result, drone flight information is not securely protected, and malicious users can intercept and potentially deduce a specific drone's current location and flight path. In such cases, the privacy of the drone is not adequately safeguarded, and critical national flight objects like military drones may become vulnerable to physical attacks.

Research addressing the potential privacy exposure issues arising from remote ID regulation for drones has been ongoing[7, 8]. However, existing studies often demand significant computational resources for location protection or pseudonym generation. Drones typically have limited memory, relatively low computing power, and the need for battery efficiency, necessitating lightweight schemes. Additionally, as drone roles expand, there is a growing need for drone swarms, where multiple drones operate in groups to perform tasks efficiently. While previous work[9] proposed lightweight drone authentication methods using PUFs, they did not consider drone swarm identification.

Drones need to obtain permission in advance to visit certain areas for secure and efficient drone monitoring. At this time, drone swarms should share their identification information with the zone service provider of the areas they plan to visit in advance for identification. However, drone swarms may encounter situations where they need to change their flight paths abruptly due to factors such as weather changes or accidents. Therefore, there is a need for a mechanism to identify the drone swarm when a drone swarm operates differently from the pre-planned flight path.

To address the issues, we propose a lightweight drone swarm anonymous authentication model considering a dynamic flight plan. We leverage Physical Unclonable Functions (PUFs)[10] and a Henon map[11] known as one of the chaotic systems to enable each drone to generate one-time pseudonymous identifiers. The PUF has the characteristic of generating responses based on specific inputs, which is called a challenge. And each PUF has a unique response even if the designed circuit is the same. Thus, PUF Challenge and Response pairs can be used for identification. When generating new identification information using the Henon map[11], drones who is aware of shared parameters of henon map among the drone swarm and valid PUF Challenge and Response Pairs (CRPs) can create valid pseudonymous identifiers. When the flight path of the drone swarm changes, the drones generate new PUF CRPs and transmit them through the TA to the new ZSP they are planning to visit. The proposed drone swarm identification protocol offers anonymity for drones with minimal computational overhead, effectively concealing their flight paths from external observers. Additionally, it enhances security against drone spoofing attacks and physical tampering through the use of PUF.

2 Related Works

2.1 FAA remote identification regulation

The FAA (Federal Aviation Administration) in the United States announced the final regulations for remote identification in April 2021 in order to ensure safe airspace management and prevent indiscriminate flights by unauthorized drones[6]. Starting from September 2023, all drones in the United States are required to be registered with government agencies, and drone pilots must adhere to the regulations for standard remote ID drones and remote ID broadcast modules. According to the regulations, the main elements of the message that drones should broadcast at specific short intervals during flight are as follows:

- Drone's identification

- The control station's latitude and longitude
- An indication of the control station's barometric pressure altitude
- The drone's latitude and longitude
- An indication of the drone's barometric pressure altitude
- a time mark
- An indication of the emergency status of the drone.

The remote ID message sent by the drone to the Zone Service Provider (ZSP) contains the drone's location information and identity details. Third parties can obtain and read the remote ID message transmitted by a drone. Consequently, there is a concern that when someone unrelated to the drone collects and analyzes the remote ID message, it may reveal the drone's flight path. The existing FAA remote ID regulations do not provide specific privacy protection measures for drones. Therefore, strategies to protect the privacy of drones are necessary to ensure secure remote ID operations.

2.2 Anonymous drone identification and authentication

Tedeschi et al.[7] proposed the ARID (Anonymous Remote IDentification solution) protocol for providing anonymity to drones. In this protocol, drones periodically send remote identification information to the Critical Infrastructure (CI) operator, encrypted with a one-time secret key generated for each transmission. This information includes identity identifiers encrypted with the CI operator's public key. As a result, attackers cannot match multiple remote identification messages to a single drone, and the actual identity of the drone remains unknown.

Brighente et al.[8] introduced a method for encrypting drone location information through differential privacy techniques, enhancing privacy regarding the drone's location. Furthermore, in case an unauthorized drone intrudes into a specific area, the CI operator can request the Trusted Third Party (TTP) to reveal the malicious drone's location.

However, [7] and [8] did not consider the characteristics of drone hardware, such as low computational capabilities and limited memory capacity. Drones need a more lightweight anonymous identification protocol because they should transmit their remote identification information to the CI operator every few seconds.

Considering the hardware limitations of drones, pu et al.[9] proposed a lightweight drone pseudonym generation and authentication approach. Drones generate temporal pseudonyms using Physical Unclonable Functions (PUF) and chaotic systems, and they perform mutual authentication and key agreement with the Zone Service Provider (ZSP). The proposed protocol used PUF (Physically Unclonable Function) technology to counter physical attacks. However, it has been observed that adversaries may still infer PUF Challenge-Response Pairs (CRPs) from the stored identification information on drones. Chuang et al.[12] introduced a lightweight drone identity authentication method for multi-domain environments. The author proposed mutual authentication between multiple drones and multiple ground stations. The proposed model also used PUF and reusable fuzzy extractor for key agreement. However, the proposed scheme is primarily tailored to drone authentication and key establishment, making it less suitable for remote ID regulation.

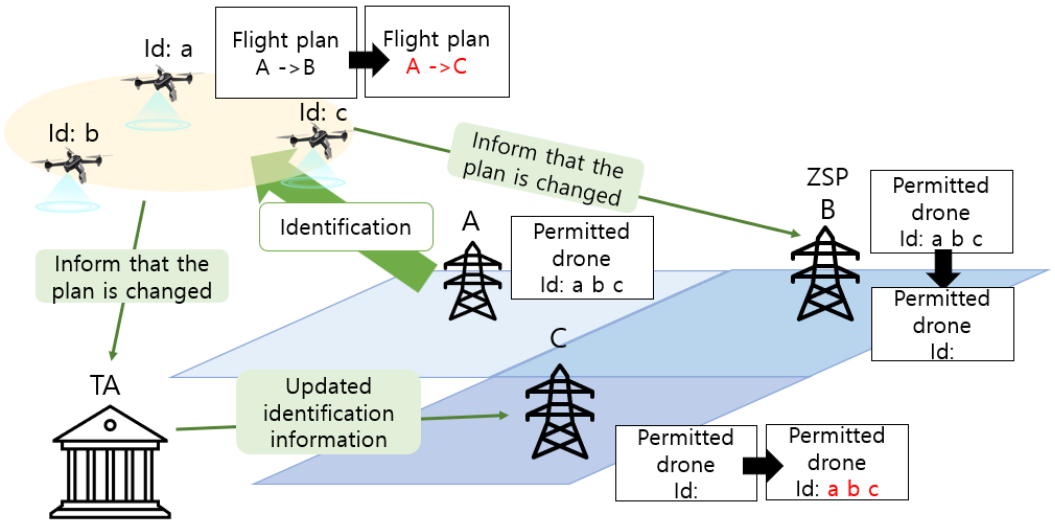

Figure 1: Proposed Scenario

3 Overall model

3.1 Scenario

In the proposed model, Trusted Authority (TA) organizes drones into groups to carry out tasks such as city monitoring, item deliveries, and sensor data collection. TA shares the zones to be visited and the flight routes required for performing these tasks with each drone swarm. The drone swarms should adhere to predefined flight schedules, and unauthorized areas should be restricted from flight.

Furthermore, the Zone Service Providers (ZSPs) receive information about which drone swarms are scheduled to visit their areas and when, as provided by TA. ZSPs detect unmanned aircraft entering their managed regions and verify the identities of these entities to check if their flights have been preauthorized. ZSPs confirm if the drone is a member of the designated drone swarm and validate the drone's identifier. If an unauthorized drone is found flying, ZSPs report it to TA and air traffic control authorities.

During drone swarm flights, if unexpected issues like bad weather conditions, accidents, or low battery levels to the original flight plan, the drone swarm informs the ZSP and TA that the flight path has been altered. TA, in turn, updates the relevant ZSPs with the modified drone swarm flight information and sends the necessary identification details for the new areas requiring flight authorization to the ZSPs. Figure 1 shows the overall drone scenario of the proposed model.

3.2 Entities

The proposed model has three main entities: a drone swarm, zone service providers, and a trusted authority. ZSP and TA are assumed to be trustworthy and have sufficient computational capabilities. Additionally, participants are capable of communication through LTE modules.

3.2.1 Drone swarm

Drones operate in swarms to enhance operational efficiency. In a drone swarm, multiple drones fly together, following predefined paths. If there are unexpected circumstances that require a change in the flight path, the leader drone within the swarm is responsible for communicating this change to both the Trusted Authority (TA) and the Zone Service Provider (ZSP). Each drone in the swarm adheres to the remote identification regulations and transmits a remote identification message to the ZSP located at waypoints along the flight path at regular intervals. Each drone is equipped with challenge-response Physical Unclonable Functions (PUF) for anonymous identification. Also, drones are equipped with communication modules for drone-to-drone, drone-to-ZSP, and drone-to-TA communication.

3.2.2 Zone Service Provider (ZSP)

Each Zone Service Provider (ZSP) is located in a specific region and monitors approaching flying objects in their vicinity. To prevent unauthorized drone flights, they identify the identities of drones approaching their jurisdiction. Each ZSP receives information about drones scheduled to fly in their area in advance from the Traffic Authority (TA). The ZSPs possess the actual identifiers and Challenge-Response Pairs (CRPs) for drones that are planning to visit their region. However, they do not have knowledge of the actual identities of drones that are not scheduled to visit their region.

3.2.3 Trusted Authority (TA)

Trusted Authority (TA) is the entity responsible for managing drones, scheduling their flight paths, and monitoring their operations. It assigns a unique identifier to each drone, ensuring that it complies with the requirements of the remote ID regulations. As TA is a government sector, it always behaves honestly.

3.3 Adversarial model

In the proposed model, malicious drones have the potential to behave as if they are members of an authorized drone swarm in order to access restricted areas. They may attempt impersonation attacks with other drones to bypass the identification process with the ZSP. Attackers with physical access can attempt to seize a drone to obtain the identification-related information it holds. Additionally, attackers may be interested in collecting personal information such as the flight paths and locations of drones in flight. To achieve this, attackers could eavesdrop on and intercept the identification information that each drone is transmitting to the ZSP.

4 Anonymous drone swarm identification protocol

The proposed anonymous drone swarm identification Protocol can be categorized as follows: Drone Registration, Drone Swarm Flight Path Setup, Broadcast of Remote ID Messages, Drone Swarm Identification, and Modification of Drone Swarm Flight Paths. We assume that TA and ZSPs have pre-generated private-public key pairs, and the public key information of TA and ZSPs is publicly available to all participants. Table 1 shows the main notations used in the protocol.

Table 1: Notations

Symbol	Description
$Drone_i$	The i-th drone within the drone swarm
D_i	The real identifier of the i-th drone within the drone swarm
N	The size of the drone swarm
J	The number of flight zones which a drone swarm will visit
ZSP_j	The ZSP of the j flying zone ($j = 0, 1, 2, ..., J-1$)
Z_j	The identifier of the ZSP_j
PD_i^t	The pseudonymous identifier of the $Drone_i$ at time slot t
(C_i^j, R_i^j)	The PUF CRP of the $Drone_i$ for j flying zone
$H(\cdot)$	Cryptographic hash function
(a, b)	Parameters of Henon map
(sk_e, pk_e)	A private key and public key pair of node e
$P(\cdot)$	A function of PUF ($R_i^j = P(C_i^j)$)
TS	A timestamp

4.1 Drone registration

In the drone registration phase, a drone, which is willing to join the proposed model. registers with the Trusted Authority. The drone should generate a Remote ID identifier following the Remote ID regulation.

- A new drone $Drone_i$ registers its Remote ID identifier with the Trusted Authority (TA). To do this, $Drone_i$ generates a private-public key pair $(sk_{Drone_i}, pk_{Drone_i})$ using a cryptographic key generation algorithm, assuming the use of a post-quantum secure encryption algorithm. $Drone_i$ then sends the generated public key pk_{Drone_i} to the TA.

- The TA verifies whether $Drone_i$ has been registered previously, and it signs the pk_{Drone_i} with its private key sk_{TA_i}, creating a certificate for the pk_{Drone_i}. TA generates a random number r and registers the drone's identifier $D_i = H(pk_{Drone_i}, r)$ along with the public key information and sends the generated certificate and D_i to $Drone_i$ through a secure channel.

4.2 Drone swarm flight path setup

In the drone swarm flight path setup phase, the TA assembles the drone swarm with the necessary drones for task execution. It schedules a flight path for the task and shares it with the drone swarm and the relevant Zone Service Providers (ZSPs). For anonymous drone identification, the TA obtains PUF CRP values from each drone swarm member and transmits them to the ZSPs in the areas where the flights are scheduled.

- The TA groups $drone_i (i = 0, 1, 2, ...N-1)$ into a single drone swarm. TA generates the parameters a and b for the pseudonymous Identifier creation and shares them with the members of the drone swarm. These parameters are known only to TA, the drone swarm

members, and the entities involved in identification. The a and b are used for drones to confirm that they are members of the drone swarm.

- The TA schedules the path FP for the drone swarm's flight based on the order in which the flying zones are traversed. For example, if the drone swarm is flying through $Zone_1$, $Zone_2$, and then $Zone_3$ in that sequence, the path FP would be represented as $FP = \{Zone_1, Zone_2, Zone_3\}$. The TA shares the FP to each drone swarm member $Drone_i (i = 0, 1, 2, .., N-1)$.
- The TA generates a set of PUF challenge values, C_i^j, for each drone, corresponding to the number of flying zones that the drone swarm needs to pass through, and provides these challenges to each drone. If $FP = \{Zone_1, Zone_2, Zone_3\}$, each $drone_i$, calculates PUF response values, $R_i^j = P(C_i^j)$, where j is 1,2, and 3. Each $drone_i$ sends them to the TA and deletes R_i^j.
- The TA shares $\{(a, b), (D_0, C_0^j, R_0^j), (D_1, C_1^j, R_1^j), ..., (D_{N-1}, C_{N-1}^j, R_{N-1}^j)\}$ to each ZSP_j through a secure channel. It also sends flight information to the Zone Service Providers (ZSPs), including details such as a visit date, flight time, and the purpose of the flight.

4.3 Broadcast of remote ID messages

Drone swarm members broadcast a remote ID message to the ZSP at the transit point every time slot t. At this time, each drone creates a one-time pseudonym identifier using its PUF CRP and a Henon map[11]. The Henon map is one of the chaotic systems that generate deterministic random numbers based on parameter values and initial conditions. Without knowledge of the parameters and initial conditions, it is impossible to regenerate a number sequence of the chaotic system. In the proposed model, the drones within a drone swarm use a shared secret value as the parameter for the Henon map, and each drone's PUF CRP serves as the initial condition.

- When the drone swarm is flying toward a $Zonej$, each $drone_i$ calculates its initial pseudonym identifier PD_i^0 as below.

$$R_i^j = P(C_i^j) \tag{1}$$

$$PD_i^0 = H(D_i, R_i^j, Z_j, TS) \tag{2}$$

  Each $drone_i$ uses the generated PD_i^0 as its drone identifier within the Remote ID message and sends this message to the ZSP_j during the first broadcast when flying towards $Zonej$.

- In the subsequent timeslot, each $drone_i$ updates its new pseudonymous identifier and uses it when sending the Remote ID message using a henon map and shared group parameters as follows:

$$x_i^t = \begin{cases} 1 - a(C_i^j)^2 + R_i^j, & \text{if } t = 1, \\ 1 - a(x_i^{t-1})^2 + y_i^{t-1}, & \text{if } t > 1. \end{cases} \tag{3}$$

$$y_i^t = \begin{cases} bC_i^j, & \text{if } t = 1, \\ x_i^{t-1}, & \text{if } t > 1 \end{cases} \tag{4}$$

$$PD_i^t = H(D_i, R_i^j \oplus y_i^t, Z_j, TS) \tag{5}$$

  A leader drone of the drone swarm collects each $drone_i$'s remote id message, which has a drone identifier as PD_i^t, and broadcasts to ZSP_j for every timeslot t.

4.4 Drone Swarm Identification

A ZSP verifies whether the identifier in the remote ID messages sent by the drone swam is valid and that the drone is authorized to fly.

- As a ZSP_j knows the drone swarm's group parameter a, b and PUF CRP of each drone, it can calculate each $PD_i^{t'}$ using the same formula as in section 4.3.
- if $PD_i^{t'} = PD_i^t$, the ZSP_j considers the $drone_i$ to be valid. If the drone's pseudonymous identifier is found to be invalid, ZSP_j reports the intrusion of an unauthorized drone to TA and the air traffic control authorities.

4.5 Modification of Drone Swarm Flight Paths

In this phase, when the drone swarm needs to deviate from the originally planned flight due to unexpected events, it shares the information required for anonymous identification with the ZSP of the new zone it intends to visit through TA.

- If the drone swarm, during its flight, encounters a situation where it cannot carry out the pre-scheduled flight due to special reasons and needs to go to another $Zone_k$ without prior authorization, the leader drone $drone_l$ first informs the ZSP and TA of the change in the flight path from the originally planned zone. At that time, the report should be encrypted and include $drone_l$'s signature for data security.
- The TA generates PUF challenge values $C_i^k (i = 0, 1, 2, ..., N-1)$ and sends the encrypted challenge values to the drone swarm.
- Each $drone_i$ computes $R_i^k = P(C_i^k)$ and encrypts it using TA's public key. The $drone_l$ collects the encrypted responses R_i^k and transfers them to the TA.
- The TA shares $\{(a, b), (D_0, C_0^k, R_0^k), (D_1, C_1^k, R_1^k), ..., (D_{N-1}, C_{N-1}^k, R_{N-1}^k)\}$ to the ZSP_k through a secure channel.
- The ZSP_k stores the group parameters and a set of PUF CRP. And it updates the list of drones with flight permits.

5 Security Analysis

This section provides a security analysis from the perspective of secure drone swarm identification and anonymity.

5.1 Resistance against drone impersonation attack

Malicious drones may attempt to enter unauthorized zones without detection by impersonating members of a specific drone swarm or by attempting to use the identity information of other drones. However, these malicious drones do not have knowledge of the parameters of the Henon map shared among the drone swarm members, and due to the properties of the PUF, they cannot generate responses corresponding to the challenges. Therefore, malicious drones would be unable to create valid pseudonymous identifiers. As a result, during the process of ZSP identifying the drone swarm through Remote ID messages, the unauthorized drone would be detected.

Furthermore, if a malicious drone attempted to steal the values necessary for identification from other drones through physical attacks, they could potentially discover the Henon map parameters shared by the drone swarm. However, due to the inherent complexity and unpredictability of PUFs, they would still be unable to derive the correct PUF CRPs. Therefore, the proposed model is secure against drone impersonation attacks.

5.2 Resistance against Sybil attack

Malicious drones may attempt to disrupt the aerial monitoring conducted by ZSP and TA by generating multiple fake IDs, making it appear as if multiple drones are operating together. To create valid pseudonymous identifiers PD that can pass ZSP's identification process, these drones need access to the drone identification information registered with TA. Furthermore, they would require access to the PUF CPR information registered with ZSP to generate valid pseudonymous identifiers PD. However, even if malicious drones were to accidentally obtain the PUF challenge values, they would be unable to generate the corresponding response values. Additionally, they do not possess the parameter information for the Henon map required for pseudonymous generation. Therefore, the proposed model is secure against Sybil attacks.

5.3 Preserving drone's privacy

Curious participants may attempt to collect the Remote ID messages sent by each drone to deduce the drone's destination and flight path. However, in the proposed model, drones generate unique pseudonymous identifiers for each time slot and use them to send Remote ID messages. Consequently, linking multiple Remote ID messages sent by a single drone becomes challenging, and other participants cannot ascertain the real identity of the drone. As a result, the proposed model preserves the privacy of the drone's flight information.

6 Conclusion and Future Work

In this paper, we proposed a solution to address the issue of exposing drone privacy, which was not considered in remote ID regulations. Additionally, we introduced a method for identifying drones when their flight paths are dynamically updated. Members of the drone swarm generate new pseudonymous identifiers each time they broadcast a remote ID message. To ensure protection against potential impersonation attacks by malicious drones, we leveraged the PUFs installed on each drone. Each drone swarm secretly shares the same Henon map parameter to prove whether a drone is a member of the drone swarm. By implementing a lightweight approach to pseudonymous drone identification, we reduced the computational burden on drones by designing a lightweight drone pseudonymous identification. We also ensured that other entities cannot infer the drone's flight information from its remote ID message, thereby preventing indiscriminate exposure of drone flight information. In future research, we plan to explore the application of blockchain technology to manage drone identification information and share information securely in this context.

7 Acknowledgments

This work was supported in part by the Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2023-00225201, Development of Control Rights Protection Technology to Prevent Reverse Use of

Military Unmanned Vehicles) and in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2023-2018-0-01417) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation)"

References

[1] S Ahirwar, R Swarnkar, S Bhukya, and G Namwade. Application of drone in agriculture. *International Journal of Current Microbiology and Applied Sciences*, 8(01):2500–2505, 2019.

[2] Lina Tang and Guofan Shao. Drone remote sensing for forestry research and practices. *Journal of Forestry Research*, 26:791–797, 2015.

[3] Ranganathan Rani Hemamalini, Rajasekaran Vinodhini, Balusamy Shanthini, Pachaivannan Partheeban, Mani Charumathy, and Karunakaran Cornelius. Air quality monitoring and forecasting using smart drones and recurrent neural network for sustainable development in chennai city. *Sustainable Cities and Society*, 85:104077, 2022.

[4] Yongho Ko, Jiyoon Kim, Daniel Gerbi Duguma, Philip Virgil Astillo, Ilsun You, and Giovanni Pau. Drone secure communication protocol for future sensitive applications in military zone. *Sensors*, 21(6):2057, 2021.

[5] Leila Hudson, Colin S Owens, and Matt Flannes. Drone warfare: Blowback from the new american way of war. *Middle East Policy*, 18(3):122–132, 2011.

[6] Federal aviation administration: Uas remote identification overview.

[7] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. Arid: Anonymous remote identification of unmanned aerial vehicles. In *Annual Computer Security Applications Conference*, pages 207–218, 2021.

[8] Alessandro Brighente, Mauro Conti, and Savio Sciancalepore. Hide and seek: Privacy-preserving and faa-compliant drones location tracing. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–11, 2022.

[9] Cong Pu, Andrew Wall, Kim-Kwang Raymond Choo, Imtiaz Ahmed, and Sunho Lim. A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment. *IEEE Internet of Things Journal*, 9(12):9918–9933, 2022.

[10] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

[11] Michel Hénon. A two-dimensional mapping with a strange attractor. *The theory of chaotic attractors*, pages 94–102, 2004.

[12] Chuang Tian, Qi Jiang, Teng Li, Junwei Zhang, Ning Xi, and Jianfeng Ma. Reliable puf-based mutual authentication protocol for uavs towards multi-domain environment. *Computer Networks*, 218:109421, 2022.