2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) | 979-8-3503-3667-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/WiMob58348.2023.10187758

Sec-PUF: Securing UAV Swarms Communication with Lightweight Physical Unclonable Functions

Wassila Lalouani
Department of Computer and Information Science, Towson University,
Towson, Maryland, USA
wlalouani@towson.edu

***Abstract*—UAV swarms are gaining popularity due to the reduced cost of deployment and their ability to perform complex tasks such as environmental monitoring, surveillance, and search and rescue operations. UAV swarms are characterized by a highly dynamic environment and continuous interaction with no guarantee of persistent connectivity to a trusted network infrastructure. Traditional cryptographic techniques can be inefficient in ensuring secure swarm communications due to the UAV resource constraints, the broadcast nature of wireless communication, and the vulnerability of UAVs to physical capture and cloning attacks. This paper aims to address these security issues by developing a novel lightweight secure and authenticated intra swarm communication. The approach incorporates Physically Unclonable Functions (PUFs) and the Chinese Remainder Theorem, which enables the seamless establishment and maintenance of group keys on the fly. Additionally, our mechanism supports implicit keys management using the pseudo-randomness proprieties of the chaotic map. We demonstrate the resiliency of our method against active and passive attacks, using formal analysis framework. We also validate the resiliency of our schema against key modeling attacks using FPGA-based PUF implementation. The results confirm a significant reduction in computational complexity compared to competing schemes.**

Keywords: Chaotic map, Chinese remainder theorem, UAV Swarms Group communication, Message Authentication, PUF.

I. INTRODUCTION

In recent years, Unmanned Aerial Vehicles (UAVs) have undergone significant advancements, with UAV swarm formation emerging as a novel paradigm. This revolutionary concept enables multiple UAVs to collaborate and coordinate their activities, resulting in high availability, greater connection density, and low end-to-end delay for various applications, including military surveillance, search-and-rescue missions, and goods delivery [1]. To support this level of collaboration between the UAVs, intra-swarm communication is crucial. By communicating with each other, the drones can collect data from multiple sensors, detect potential threats, optimize their routes, and avoid collisions, etc. To illustrate, in security surveillance, a group of swarm drones can be used to monitor a large area such as a border, a military base, or a critical infrastructure facility. Each drone can fly a specific pattern and share video footage and sensor data with the other drones to detect and respond to any potential security threats. Similarly, swarm drones can be used for delivering small packages in urban areas. The drones can communicate with each other to optimize their routes, avoid collisions, and share information about the delivery locations. Overall, communication between drones enables them to work together more efficiently and effectively as a group to achieve complex tasks that would be difficult or impossible for a single drone to perform alone.

Despite these advantages, UAVs rely on wireless channels for communications, which can easily be intercepted by malicious entities, posing a threat to the security of the drone network. Furthermore, the dynamic nature of UAV swarms' formation, where nodes can quickly join or leave the network, makes them even more susceptible to attacks. These attacks intend to obtain sensitive collected data stored in drones, exploit non-authorized connections, and extract cryptographic keys which may disrupt the proper operation of network. Hence, continual secure message exchange and authentication constitute the prime requirement towards secure intra-swarm communication. Traditional secure message exchange algorithms rely on encryption mechanism that can be classified into two main categories: symmetric and asymmetric. Symmetric techniques use the same key for both the sender and the receiver, necessitating the sharing of this key among all drones in the swarm. This poses a significant vulnerability to cryptoanalysis techniques and key leakage in a self-organized UAV network. Asymmetric techniques, on the other hand, provide a much higher level of security as they use different keys for the sender and the receiver. However, owing to the limitations of UAVs in terms of energy and computational resources, it becomes imperative to design an intra-swarm communication mechanism that is both efficient and lightweight. Recently, Physical Unclonable Functions(PUFs) have gained popularity, especially in UAV scenarios, thanks to their exceptional security features and computational efficiency. PUFs take advantage of the unique and non-reproducible randomness inherent in the fabrication process of chips to produce unique signature for the device, which cannot be cloned or forged. Traditional PUFs security mechanism, rely on the generation of a unique response (output) to a particular challenge (input), thereby resulting in a distinctive challenge-response pairs (CRPs). These CRPs are subsequently utilized to either authenticate the node or produce secure encryption keys [1]. However, applying conventional PUF security mechanisms to UAV swarm coordination is challenging due to the dynamic topology of communication and the unique characteristics of drones. PUFs are designed for individual UAV, while UAV swarm coordination requires group communication, making the implementation of PUF-based protocols more complex.

To address this issue, this paper proposes, Sec-PUF, a secure intra swarm message authentication and key agreement protocol. The proposed protocol utilizes physical unclonable functions to generate unique challenge-response pairs for each individual UAV, which are then used to form a collective

hardware fingerprint to generate a group key. Then, our protocol exploits the proprieties of Chinese Remainder Theorem (CRT) to ensures that each individual UAV can recover the group key using only its own fingerprint. To ensure the security and dynamism of the group key, the protocol leverages the inherent unpredictability of chaotic maps to dynamically vary the key over time in an implicit manner. Fundamentally the chaotic map utilizes the group key as a seed to generate a dynamic shuffling pattern and obscure the messages. Additionally, the flexibility of the CRT enables Sec-PUF to revoke and grant access to the group key in response to changes in the swarm's network setup. As the chaotic map is only used to dynamically update the group key, the key management process is implicitly updated with local coordination between drones in the swarm. We demonstrate that Sec-PUF is lightweight, scalable, and secure against active and passive attacks using formal analysis and experimental results. The contribution can be summarized as follows:

- We proposed a protocol for self-organized UAV networks, providing an energy-efficient encryption solution that does not necessitate the exchange of secret keys during operation.
- We proposed a lightweight continuous message authentication and verification mechanism.
- We have implemented the protocol using FPGA-based PUF implementation, proving its capability to sustain its resiliency against passive active attacks, with reduced computation costs compared to existing prominent protocols in the literature.

II. Related Work

Given the scope of this paper, we will focus on existing lightweight authentication and key agreement schemas. Specifically, we aim to delve into the exploration of schemes that are tailored to meet the specific requirements of UAV networks, particularly with respect to their dynamic topology and energy constraints. The authors [5] propose authentication and key agreement scheme for heterogeneous ad-hoc wireless sensor networks and IoT, whereas Tai et al. [6] presents a more secure solution for IoT, but it is vulnerable to several potential attacks, such as man-in-the-middle, replay attack, and forward secrecy. Additionally, Challa et al. [4] suggest a signature-based authenticated key establishment scheme that relies on Elliptic Curve Cryptography (ECC) and ElGamal-type digital signatures, but it is computationally more expensive than non-ECC-based methods. To deal with the complexity and ensure effective security, some work involve a third-party communication, allowing mobile edge computing service providers to authenticate UAVs [3]. Alladi et al. [2] propose a protocol for mutual authentication and secret key establishment in drone-assisted 5G networks. However, this may result in added latency, which could render it unsuitable for time-critical applications. Teng et al. [7] developed a protocol for inter-drone communication that uses ECC and PKI, but this results in a significant overhead. Pu et al.[8] proposed a lightweight protocol for mutual authentication and secret key establishment, but it is susceptible to PUF modeling attacks. The authors [9] proposed lightweight authentication schemes for Internet of Drones using biometric technology, but they require continuous connectivity to a trusted server. In contrast, TCALAS [10] employs lightweight hash functions and fuzzy extractor methods, with the latter used for local biometric verification purposes. D2D-MAP [13] utilizes simple hash functions and logical bitwise operators, resulting in a lightweight cryptographic complexity. However, D2D-MAP lacks scalability in UAV swarms since it requires mutual authentication to be established for each pair of drones in the swarm. Sec-PUF provides a flexible and comprehensive solution for secure intra-swarm communication that enables any two legitimate drones in the swarm to establish a secure communication link.

III. Background and System Model

A. System Model

This protocol enables Swarm of UAVs to share their data and coordinate their tasks securely and efficiently. The architecture consists of the following multi-tier players:

- UAVs: The UAVs are responsible for sensing and collecting data from the environment, coordinating with other UAVs, encrypting and authenticating their transmitted messages using a lightweight approach. In Sec-PUF, a Physically Unclonable Function will be integrated into each UAV to enable hardware-based identification.
- The ground station (GS) serves as a trusted base station that maintains a database of enrolled drones. During enrollment, it distributes security parameters to each drone and assigns mission tasks accordingly. Sec-PUF does not require the UAVs to be connected to the GS during operation; the GS is only used for initializing the swarm.

B. Attack Model

The aim of the adversary is to deceive the swarm operation by infiltrating the network, disrupting its normal operation, or gaining access to confidential information. The swarm network vulnerabilities can be exploited by the adversary to launch different attacks such as drone impersonation, replay attacks, and data manipulation. These actions are carried out to achieve the adversary's goals, which fall under two main threat scenarios. First, the wireless channels on which the swarm relies make it vulnerable to active attacks like impersonation, man-in-the-middle, and Sybil attacks. For example, in the case of swarm of UAVs coordinating to avoid collisions, the adversary can manipulate the messages exchanged between the drones. This can lead to the spread of false information about obstacles, resulting in the drones taking evasive actions and potentially increasing the risk of collisions. The second scenario involves the attacker's goal of hacking the drones either

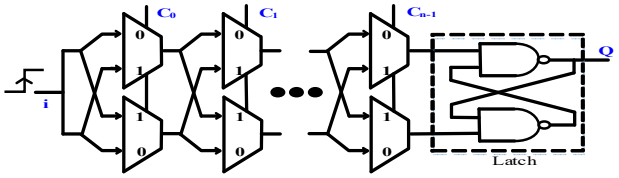

Fig. 1. The Arbiter PUF is represented in the schematic diagram, wherein the challenge bits regulate the operation of individual multiplexers. This results in discrepancies in the latched output value.

individually or in collusive way to expose the device secrets used for authentication and data encryption. Moreover, the attacker may physically capture the UAV, which poses a risk of cloning or tampering. Therefore, it is crucial to implement strong security measures to prevent such attacks and maintain the integrity and confidentiality of the data exchanged.

C. Security Goals

The challenges posed by UAV Swarms, including mobility, ad hoc network formation, limited device energy, and vulnerability to cloning attacks, necessitate effective security mechanism during UAVs task coordination. In light of these challenges, Sec-PUF aims to achieve the following design goals:

1) *Data integrity*: The communication among UAVs is primarily aimed at sharing tasks, which have a significant impact on the swarm's activity. Thus, it is crucial that messages are encrypted and authenticated. The system should ensure data confidentiality and be flexible enough to accommodate changes in the swarm's topology.
2) *Message source authentication*: The system should provide a means for the message recipient to verify the authenticity of the source for every communicated message.
3) *Physical protection*: The UAVs are vulnerable to hacking by malicious adversaries. Thus, it is crucial to generate keys on the fly instead of storing them, which will boost the confidentiality and integrity of the communication.
4) *Impersonation*: The identities of UAVs should not be falsified to gain privileges or participate in communication.

To meet these security goals, Sec-PUF generates unique session keys for each swarm with no correlation among keys generated across different swarms. Additionally, the protocol can detect any attempts to manipulate message integrity or authenticity.

D. Physically Unclonable Functions

A Physically Unclonable Function (PUF) is a hardware device that leverages the inherent random variations that occur during the fabrication process of integrated circuits to generate a unique, hardware-based fingerprint or signature of the device. The Arbiter PUF, depicted in Figure 1, is a Physically Unclonable Function that capitalizes on the differences in delay encountered by input signals as they travel through multiplexers to form a distinct hardware-based signature for the device. In other word, the configuration of the multiplexers using challenge bits, $c_0, c_1, .., c_{n-1}$, leads to the creation of a unique response that constitutes the signature. The randomness of the fabrication process makes it impossible to clone the PUF, and even if the device is compromised, its hardware identity remains secure. However, PUFs may be susceptible to modeling attacks, whereby machine learning techniques can be used to construct models of intercepted CRP pairs. Additionally, PUF are not designed for group communication.

IV. DETAILED APPROACH

A. Approach Overview

The aim is to devise a streamlined mechanism for generating keys and authenticating messages in UAV swarms, with a particular focus on minimizing resource consumption. Sec-PUF is a novel approach that distinguishes itself from existing methods by placing a higher emphasis on the use of hardware fingerprinting to guarantee system security during operation. This approach offers robustness against tampering attacks in fully dynamic swarm topologies. Moreover, our approach facilitates continual security over the network by enabling drones to dynamically update their keys without the need for security exchanges during swarm operation. Our methodology is designed around four phases: enrollment, message encryption, message authentication, and dynamic group membership– which align with the swarm's life cycle. During the enrollment phase, the UAVs establish communication with a trusted third party that generates the initial security parameters. Sec-PUF employs a trusted third party, such as a ground station, to authenticate each member of the swarm. This is achieved by utilizing a subset of CRPs to verify the hardware fingerprint of each UAV. In essence, the GS sends a set of randomly chosen challenges to each drone, and upon receiving the correct pre-shared response, the authentication process is successfully completed. Subsequently, the GS combines the UAVs responses using the CRT and generates the initial swarm key. Each UAV can individually derive the initial group key using its hardware fingerprint. During the data exchange phase, the UAVs utilize a lightweight encryption mechanism to securely transmit and receive data. Sec-PUF proposes a straightforward encryption method based on dynamic shuffling, where the shuffling pattern that represents the key is determined through sorting pattern of pseudo-random numbers generated by a chaotic map. The initial group key, acting as the seed for the chaotic map, results in unique keys for each swarm. To ensure high-level security for UAV swarms, Sec-PUF updates encryption keys implicitly during operation by dividing swarm operation into distinct periods during which drones autonomously generate new keys using the chaotic map. This strategy makes it difficult for an attacker to predict the encryption pattern. Furthermore, we utilize the chaotic map to generate an authentication token for each message, ensuring a secure and authenticated communication. Finally, Sec-PUF offers a critical advantage by supporting the dynamic addition or removal of nodes within the swarm. This is particularly important as UAVs may leave the swarm due to various factors such as environmental changes, or task requirements. To achieve this, Sec-PUF employs the CRT properties, which enable key updates without the need for communication with the GS. Overall, Sec-PUF provides an extra layer of security compared to existing solutions, allowing for lightweight, secure and authentic communication between UAVs. Additionally, our approach protects against tampering attacks, as the keys are generated on the fly using the unclonable hardware fingerprints. The approach details will be presented next.

B. Enrollment phase

The goal is to establish secure shared security parameters for UAVs in order to enable swarm members to authenticate and decrypt messages with minimal effort and rapid rekeying. This phase will involve the trusted ground station generating a group key and sending it to the authenticated UAV members, ensuring that only legitimate drones with corresponding hardware fingerprints can access the key. The GS will begin the process

by authenticating the swarm members using pre-shared hardware fingerprints. Specifically, the GS will contact each drone D_x in swarm S^j, during the task assignment phase at the start of the mission, the GS send a set of challenges to authenticate the individual drones. Let $\Upsilon^x(C_j^x, R_j^x)$ be the pre-shared CRPs of drone $D_x \in S^j$ with the GS. GS will randomly select a challenge C_j^x and expect its response from the UAV D_x to be authenticated. Once R_j^x is verified, the GS will use R_j^x to define the initial security parameters of the group communication. By leveraging the hardware fingerprints of each UAV in the swarm, the GS will generate the group key. The key generation would enable the individual UAV to automatically recover the group key without any knowledge of the other UAVs in the swarm's fingerprints. To accomplish this, we create a system of modulo equations from R_j^x and enable the legitimate UAV to recover the key by solving the modulo equations. We employ the Chinese remainder theorem, which states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime. In other words, the CRT provides a mathematical framework for securely generating and managing the swarm key for the UAV nodes. CRT involves the following. Given n drones, the GS uses R_j^x to form the following modulo equation:

$$\mu^j = \frac{\partial_g}{R_j^1}\gamma_1 + \cdots .. + \frac{\partial_g}{R_j^n}\gamma_n \ (mod\ \partial_g),\ i = 1, \dots, n. \quad (1)$$

Where $\partial_g = \prod_{i=1}^{n}(R_j^i)$, and y_i verify the following:

$$\frac{\partial_g}{R_j^i} * \gamma_i \equiv 1\ mod\ R_j^i \quad (2)$$

Subsequently, the GS can determine μ^j for each swarm *j*. Then it chooses a random key k_j of size τ bits, and computes:

$$\gamma_j = k_j * \mu^j. \quad (3)$$

GS sends γ_j to the UAVs within the swarm. Upon receiving γ_j, each drone $D_x \in S^j$ uses it proper PUF to compute R_j^x. Then, using the received γ_j the nodes will recover the key as follow:

$$\gamma_d mod\ R_j^x = k_j. \quad (4)$$

Therefore, Sec-PUF utilizes the CRT to validate the authenticity of UAVs, emphasizing the minimal computational requirements of the drones.

C. Message Authentication tokens generation

Sec-PUF further emphasizes the significance of message authentication in ensuring efficient operation of UAVs swarm. While the group key ensures message confidentiality, effective message authentication guarantees the authenticity and the integrity of the messages exchanged between drones, preventing any modifications, or tampering during transit and confirming the authenticity of the source of the messages. Without authentication, malicious actors can inject false instructions into the communication channels, leading to erroneous instructions being sent to the drones and thus jeopardizing their intended flight path or even resulting in collisions. By employing message authentication, the swarm drones can benefit from increased security, thereby allowing them to complete their tasks effectively and safely. Conventional message authentication techniques use cryptographic methods like digital signatures to authenticate a messages, but these approaches can introduce unnecessary complexity. Moreover, Identity based authentication mechanisms can be susceptible to impersonation attacks if the drone is captured. To address this vulnerability, we propose an innovative approach that utilizes chaotic maps to generate authentication information for UAV nodes. Chaotic systems are characterized by their dynamic and nonlinear behavior, displaying sensitivity to initial conditions and exhibiting a pseudo-random nature. While such properties can make the generated token unpredictable and difficult for an attacker to decipher, relying solely on chaotic maps is not sufficient, as the seed for the system can be captured if any drone within the swarm is cloned. Hence, Sec-PUF generates authentication tokens based on the initial group key k_j, which is dependent on the hardware fingerprint of the UAVs in the swarm. By using the group key as an initial condition for the chaotic map, only enrolled drones are able to produce valid authentication tokens. Once a UAV is enrolled and begins communicating with other drones in the swarm, it generates a message authentication code (MAC) for each message it sends. This MAC is created by combining the group key k_j, which is recovered from γ_j using a challenge-response pair of the UAV. Then, Sec-PUF determines the authentication token in each period $\boldsymbol{\eta}$, as follow[11]:

$$\begin{cases} x_{\eta+1} = y_\eta & (5) \\ y_{\eta+1} = -b * x_\eta + a * y_\eta - y_\eta^3 & (6) \end{cases}$$

Where *a* and *b* are constant parameters and the initial conditions represented by x_0 and y_0 are set to k_j, which represent the initial group key and serve to strongly influence the resulting authentication tokens y_η. The MAC is transmitted alongside the message to the receiving UAVs, and only nodes within the swarm can validate the messages. In other words, a drone must be able to produce the correct token to confirm its validity, implying that it possesses the accurate key k_j derived from correctly solving the eq. (4). Without validating the input stream using the PUF output, the chaotic map is incapable of generating the appropriate token y_η, thereby limiting attackers to brute force attacks. Similarly, only authorized drones can authenticate the tokens since both parties must be able to solve the same set of modulo equation. Additionally, the tokens are automatically updated using eq. $(5) - (6)$ without any implicit communication between the drones, thereby preventing eavesdroppers from inferring the next authentication tokens.

D. Message encryption

Sec-PUF incorporates a dynamic key generation mechanism to ensure the confidentiality of the data for various swarm configurations. Existing asymmetric encryption techniques are unsuitable due to their high overhead, while symmetric schemas may not provide adequate security against cryptanalysis. Sec-PUF stands out as a highly effective solution to the drawback associated with existing encryption techniques. Our approach employs a dynamic shuffling function that varies unpredictably over time, providing robustness against potential vulnerabilities. We utilize a randomized shuffling pattern generator to create a unique τ-bits sequence during each period $\boldsymbol{\eta}$, which varies per swarm and changes over time, resulting in

high resistance to cryptanalysis. More precisely, our technique exploits the effectiveness of chaotic maps to generate a complex sequence of pseudorandom numbers that follow a non-linear pattern. To obtain the shuffling pattern for the messages, we retrieve the index of the reordered pseudorandom numbers sequence in ascending order. By leveraging the chaotic system, every element in the sequence has an equal chance of being shuffled to any position, thereby minimizing biases and enhancing the randomness of the shuffling process. Additionally, chaotic maps are highly sensitive to initial conditions, making it difficult for attackers to predict the shuffling sequence or reverse-engineer the algorithm. However, the use of chaotic maps to generate a group key for the swarm is constrained by the susceptibility of drones to tampering attacks if the initial condition is stored in the drone's memory. This could enable an attacker to deduce the shuffling pattern key and decrypt all messages. To address this issue, Sec-PUF combines hardware fingerprinting and the non-repeatability of chaotic maps. Specifically, we use k_j as the initial condition for the chaotic map and enable the drones to retrieve it using eq. (4). The uniqueness of k_j by swarm, coupled with the sensitivity of the chaotic map to the initial condition, results in different shuffling patterns for each swarm. The scalability and computational efficiency of the chaotic map utilized by Sec-PUF enables it to manage a substantial volume of message exchanges seamlessly while preserving the confidentiality of the shuffling pattern.

E. Dynamic group membership

Drones may leave or join a swarm due to a variety of reasons, such as low battery or signal strength, changing mission objectives, or communication issues with other drones. The decision to join or leave a swarm can be made autonomously by the drone or by an operator based on resources availability and mission objectives. Hence, the swarm key and authentication tokens must be updated in accordance with the new swarm configuration, enabling legitimate access and barring illegitimate ones. Sec-PUF utilizes the properties of the CRT to manage the key update. When a new UAV, D_x joins the swarm, the current key, k_j, remains unaltered. The GS only needs to securely distribute the key to D_x using the following steps:

1- GS updates $\mu^x = \mu^x + \frac{\partial_g}{R_j^x}\gamma_j$, where $\frac{\partial_g}{R_j^x} * \gamma_j \equiv 1 \; mod \; R_j^x$

2- GS computes $\gamma_d = k_d * \mu^x$ and sends γ_d to D_x.

When a node D_x departs from the UAV swarm, we consider two scenarios. If the UAVs are connected to the GS, using 5G communication for example, the GS will update μ^x to revoke its access to the group key, by executing the following steps:

1- $\mu^x = \mu^x - \frac{\partial_g}{R_j^x}\gamma_j$, where $\frac{\partial_g}{R_j^x} * \gamma_j \equiv 1 \; mod \; R_j^x$

2- The GS selects a new group key $\overline{k_d}$ and sends $\overline{\gamma_d} = \overline{k_d} * \mu^x$ to the UAVs in the swarm

3- Upon receiving $\overline{\gamma_d}$, the UAVs use eq. (4) to recover $\overline{k_d}$.

When the UAVs are not connected to the GS, Sec-PUF uses the Exclusion Basis System (EBS) to exclude D_x from communication. EBS is a combinatorial optimization schema used for key management in group communication [12]. The idea is as follow, for each swarm with "k" UAVs, the GS generates C_{k+m}^k backup keys during enrollment and distributes them. Each drone stores a set of k keys and is unaware of m keys. The rekeying parameter, m, sets a threshold on the maximum number of new UAVs that can be included in the swarm. The remaining drones coordinate using the m backup keys that the departing drone D_x is unaware of, allowing them to securely communicate even after a node leaves. In Sec-PUF, the GS generates these keys using eq. (1)-(3) while applying different challenges for each backup key in C_{k+m}^k. The departure of D_x is broadcasted across the swarm, and the neighboring drone with the smallest ID selects a new key $\overline{k_j}$, computes $\overline{\gamma_j} = \overline{k_j} * k_j * \mu^x$, and sends it encrypted using the first key in the m backup keys set. This will exclude D_x from any further communication as it cannot decrypt the message to retrieve $\overline{\gamma_d}$. To efficiently disseminate the information, approach such as [13] can be employed. Subsequently, on receiving the updated $\overline{\gamma_d}$, the existing UAVs can obtain $\overline{k_d}$ using eq. 4, which ensures all security properties are verified.

V. VALIDATION EXPERIMENTS

To evaluate the effectiveness of our proposed approach, we conducted simulations using a 64-bit arbiter-PUF implemented in Xilinx ARTIX-7 FPGA. We assess the performance using embedded implementation on an Arduino microcontroller that has an active current of 1.23 mA when clocked at 16 MHz. We investigate the adversary's modeling capabilities to decrypt messages or impersonate authentication tokens by varying: (i) the number of messages intercepted by an eavesdropper or malicious drone, (ii) number of messages eminent from colluding UAVs across diverse swarms.

To gauge the effectiveness of our message authentication mechanism, we conduct a comparative evaluation of our approach with PUF-based authentication mechanisms and a discrete variant of Sec-PUF, namely DSec-PUF. Fundamentally, DSec-PUF discretizes the output of the chaotic map, thus reducing the computation complexity of the authentication tokens generation. We also assessed the encryptions keys similarity for same swarm over time and among different swarms using the Lavergian similarity metric, which checks the number of updates needed to make two keys identical. Furthermore, we evaluated the computation time complexity of our approach compared to lightweight PUF-based mechanisms proposed in the literature [1] [4-6] [9] [10]. We also validated the security properties of our approach using the formal verification framework AVISPA, which assesses vulnerability to active and passive attacks. We defined all the players, including the GS and UAVs, described the enrollment, encryption keys generation, and data exchange protocols using the High-Level Protocol Specification Language, and specified the security goals in terms of key secrecy and message authentication. The environment role involved multiple sessions of UAVs and one session for the GS and intruder. Figure 2 confirms that our schema is safe. Table1 demonstrates that using machine learning modeling techniques, an eavesdropper is unable to predict the authentication tokens, even after multiple rounds of training. This can be attributed to the hardware-dependent randomness of the authentication tokens, as well as the chaotic map output's tight dependence on the initial condition. Sec-PUF requires only 16 bits for authentication tokens, whereas DSec-PUF requires 128bits to

prevent adversaries from modeling the tokens. The excellent performance of Sec-PUF can be attributed to its use of floating-point tokens representation, making it difficult to predict the potential value range using machine learning. The evaluation of the effect of collusion among UAVs from different swarms on modelling the authentication tokens is shown in Table2. Despite an increase in the number of messages over time, the adversary is unable to accurately predict the tokens. The collusion increases slightly the accuracy of modelling for the DSec-PUF while our approach, Sec-PUF sustains its performance and prevents the adversary from inferring the authentication tokens. Figure 3 illustrates the dissimilarity of the encryption keys over time within the same swarm, while Figure 4 demonstrates the dissimilarity of the encryption keys between different swarms, with the matrix appearing diagonal, preventing the adversary from successfully guessing the keys. Figure 5 demonstrates a significant reduction in time complexity compared to existing schemes in the literature. The approaches proposed in [4][9][10] requires a larger number of cryptographic operations such as hash functions, and bitwise XORs. While the proposed protocol in [5][6][1] has comparable time complexity to Sec-PUF, yet they are limited to drone-to-drone communication and impose an increased complexity for swarm communication, whereas Sec-PUF enables lightweight secure cooperation among UAVs and achieves excellent scalability.

VI. CONCLUSION

This paper proposes Sec-PUF, a secure intra UAV swarm communication protocol which utilizes PUFs and the Chinese remainder theorem to generate initial group keys. The PUF response to a certain challenge bit pattern is employed to introduce randomness into the key management process, taking advantage of its tamper-resistance and low overhead. CRT is employed to distribute the key among group members, while Sec-PUF also exploits the non-uniformity of chaotic map output and its closed variability according to the initial condition, to generate updated keys. Validation results demonstrate Sec-PUF's resistance to modelling attacks from single or multiple colluding devices, as well as its lightweight design and resistance to other prominent hardware modeling attacks.

VII. REFERENCE

[1] K. Lounis, et al, "D2D-MAP:A Drone to Drone Authentication Protocol Using Physical Unclonable Functions," in IEEE Transactions on Vehicular Technology.

[2] T. Alladi et al.,"Drone-MAP: A Novel Authentication Scheme for Drone-Assisted 5G Networks", In IEEE INFOCOM WKSHPS: DroneCom 2021.

[3] P.Gope, et al.,"An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones," IEEE Transactions on Vehicular Technology,Vol. 69, pp.13621-13630, 2020.

[4] S.Challa et al.,"Secure signature-based authenticated key establishment scheme for future IoT applications,"IEEE Access, pp.3028–3043, 2017.

[5] M.Turkanovic, et al.,"A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," Ad Hoc Netw., vol. 20, pp. 96–112, 2014.

[6] W.-L.Tai, et al.,"An IoT notion-based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks," J. Inf. Security Appl., vol. 34, pp. 133–141, 2017.

[7] L.Teng, et al., "Lightweight Security Authentication Mechanism Towards UAV Networks" International Conference on Networking and Network Applications (NaNA), pp. 379–384, 2019.

[8] C.Pu and Y. Li, "Lightweight Authentication Protocol for Unmanned Aerial Vehicles using Physical Unclonable Function and Chaotic System," IEEE International Symposium on LANMAN, pp.1–6, 2020.

[9] M. Wazid, et al.,"Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment",IEEE Internet of Things Journal, Vol. 6, pp. 3572-3584, 2019

[10] J. Srinivas, et al., "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," IEEE Trans. Veh. Technol., vol. 68, no. 7, pp. 6903–6916, 2019

[11] J.Cui, et al., "Chaotic Map-Based Authentication Scheme Using Physical Unclonable Function for Internet of Autonomous Vehicle", IEEE Transactions on Intelligent Transportation Systems, vol.24, no.3, , 2023.

[12] M.Eltoweissy, et al.,"Combinatorial Optimization of Key Management in Group Communications," J. Network and Systems Management, vol. 12, no. 1, pp. 33-50, Mar. 2004.

[13] G.Bansal, et al, "S-MAPS: Scalable Mutual Authentication Protocol for Dynamic UAV Swarms," in IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 12088-12100, Nov. 2021.

Figure 2: Results of the formal verification using AVISPA.

Table 1: Accuracy of authentication token modeling attack.

	Modeling accuracy				
#messages	500	1000	2000	4000	5000
DSec-PUF-128	0.04	0.05%	0.073%	0.162%	0.204
Sec-PUF- 16 bits	≈0	≈0	≈0	≈0	≈0
Baseline	0.73	0.91	0.93	0.94	0.97

Table2: Effect of collusion on authentication tokens modeling attack

	Modeling accuracy			
# UAVs	1	2	3	4
DSec-PUF 128 bits	≈ 0.	≈ 0.223	≈ 0.46	≈ 0.327
DSec-PUF 256 bits	≈ 0	≈ 0.221	≈ 0.155	≈ 0.0366
Sec-PUF 16 bits	≈0	≈0	≈0	≈0

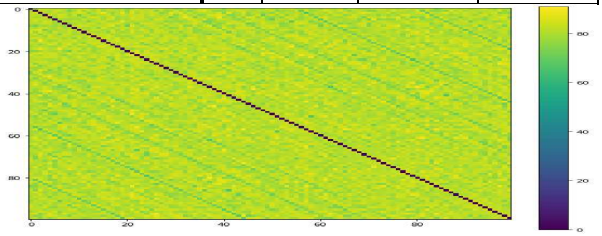

Figure 3: inter swarm key similarity.

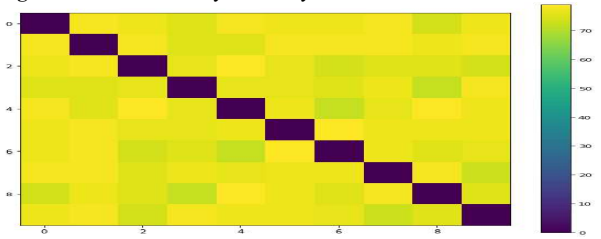

Figure 4: intra swarm key similarity.

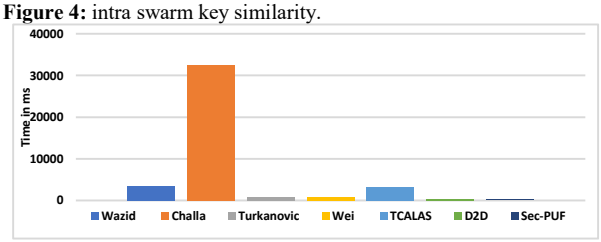

Figure 5: Runtime time complexity