Location Aware Clustering: Scalable Authentication Protocol for UAV Swarms

Gaurang Bansal, Biplab Sikdar, Senior Member, IEEE

***Abstract*—This letter proposes a scalable authentication protocol to address the security vulnerabilities in UAV-base station communication. UAVs are particularly vulnerable to multiple cyberattacks such as physical capture, cloning attacks, eavesdropping, and man-in-middle attacks. Current solutions propose to address these issues using one-to-one authentication. However, the approach is not scalable, especially in scenarios where a group of UAVs is deployed to provide services to end-users. The scalability is achieved using the K-Means clustering algorithm. The proposed protocol outperforms state-of-the-art approaches in terms of total authentication time.**

***Index Terms*—UAVs, Physical security, Authentication, PUFs.**

I. INTRODUCTION

UAVs have been used for a wide range of applications such as disaster surveillance, traffic monitoring, military operations, delivery services, task offloading, and many others [1]. Although UAVs have significant use cases, their deployment remains limited due to security threats that can disrupt/distort their communication. The communication messages from UAVs are susceptible to various attacks and can be intercepted by a malicious entity.

Addressing the issues, researchers have been working on amalgamating UAV communication with the digital identity of UAV. UAVs can be authenticated from time to time by a trusted entity to verify if the UAV carrying out the communication is the intended one or not. Among the existing literature works, Hooper presented a framework against network attacks such as man in middle by incorporating confidentiality and integrity [2]. Further, the model was improved by Blazy et al. in their work [3]. However, both of these protocols did not take into account user identification. They could identify whether the communication was not corrupted by any malicious entity but could not ascertain the origin UAV of communication. Later, an anonymous mutual authentication protocol was proposed in [4]. The work in [4] ensured authentication and anonymity in UAV networks. However, the major drawback of the approach was its dependency on Trusted Platform Modules (TPMs). These TPMs are specialized and expensive security co-processors, making them quite expensive.

Semal et al., [5] proposed a low-cost certificate-less group key authentication protocol that did not depend on any additional specialized hardware module. The use of bilinear pairing and elliptical curve cryptography (ECC) further enhanced the approach in [6]. The work in [7–9] moved from traditional security approaches to hardware security using Physically Unclonable Functions. Their approach not only reduced the computation overhead but also enhanced protection against physical attacks. These works are seen as seminal work for future work in UAV authentication using PUFs. All of these approaches discussed above have a significant drawback in that they are not scalable. Authentication of UAVs is carried in a one-by-one manner. Apart from these works, there are very few works that have tried to address scalability but have had no success, like SEDA [10] and DARPA [11].

Gaurang Bansal and Biplab Sikdar are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 119077, Singapore (e-mail: e0622339@u.nus.edu, bsikdar@nus.edu.sg)

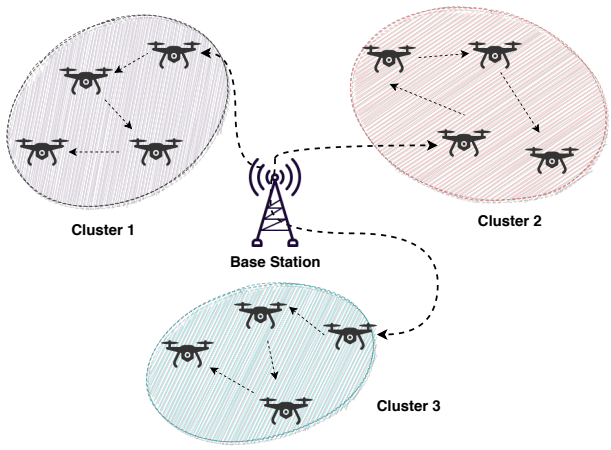

Fig. 1: System Model

In this letter, we bring the best of two worlds. We present a scalable authentication protocol for communication between UAVs and base stations. The scalability is enhanced by making the most of the topology and GPS location of UAVs. At the same time, the computational performance of the protocol is enhanced by using PUFs, inspired by the works of [7, 9]. The proposed protocol achieves confidentiality, authentication, physical security and ensures protection against replay, man-in-the-middle attacks (MITM), impersonation attacks, and node-tampering attacks.

The organization of the rest of the letter is as follows. We present our system model and adversarial model in Section II. The protocol description is presented in Section III. Section IV discusses the formal security analysis using Mao-Boyd logic. Finally, we compare the protocol with other state-of-art in Section V and conclude in Section VI.

II. SYSTEM MODEL

The system model (shown in Figure 1) consists of two types of entities: base stations (BSs) and UAVs. The base

station is stationary and trusted. UAV devices are deployed for operations and are vulnerable to security threats. Each UAV has an onboard computer (OBC) and is equipped with a PUF. A PUF can be considered as a digital fingerprint of integrated circuits of the OBC [12]. PUFs exploit the inherent randomness of hardware that is generated during the fabrication of the chip. A PUF is unique and cannot be cloned or forged. A PUF can be modeled as R=PUF(C). The PUF uses its internal characteristics to map a challenge C to a response R. Here, the challenge refers to binary input, and response refers to the output of the PUF corresponding to an input challenge. We assume that an adversary is granted complete control over the network (Dolev-Yao model) [13].

III. Proposed Protocol

This section describes the proposed protocol. UAVs are registered with the base station before they are deployed in the region. When a new UAV needs to be deployed, the base station stores the new UAV's ID along with a challenge and response pair generated by the UAV's PUF. This CRP helps with the identification of the UAV.

The base station identifies clusters based on the UAV's location using the K-means clustering algorithm. These clusters are used to determine the flow of protocol messages. The K-means algorithm partitions all the UAVs into k clusters. The algorithm for clustering starts by randomly choosing coordinates of k UAVs. These initial points form the centroid of k clusters. In each iteration, we evaluate the distance of each UAV from the centroids. After evaluation of distance, each UAV is assigned to the nearest cluster. Then, each cluster's centroid coordinates are updated by taking the mean of the coordinates of UAVs belonging to the cluster. This process continues until there is no change in centroids of clusters.

Once clusters are fixed, the base station generates a flow path for messages by choosing UAVs in the cluster at random. The communication from the BS to UAVs happens in a hop-by-hop manner. The BS sends a message to the UAV closest to it in a cluster. This UAV (closest to BS) forwards the communication to another UAV in the cluster and so on. These clusters are used to determine the flow of protocol messages. Thus, for k clusters we form k paths denoted by $\{P_1, P_2, \ldots, P_k\}$. P_j is the list of UAVs in the j^{th} path. Each of the paths starts from the base station and covers all the UAVs in its cluster. In each path, the message flows from the parent to child, originating from the base station. Here, the parent refers to the transmitting UAV, and the child refers to the receiving UAV. In the return path, the child responds to the parent, ultimately terminating at the base station.

The base station initiates the authentication protocol. It generates a secret message using a pseudo random number N_α and uses challenge-response pair (C_{ij}, R_{ij}) for the i^{th} device in the j^{th} path. Let M''_{ij} be the authentication message sent by BS for device i in j^{th} path. M''_{ij} is given as:

$$M''_{ij} = C_{ij} || E[N_\alpha || T_O || R_{ij}]_{R_{ij}}. \quad (1)$$

Base station sends challenge C_{ij} and encrypts its secret message N_α appended with current time stamp and PUF response with PUF response of the i^{th} device in the j^{th} path. The encrypted message is $E[N_\alpha || T_O || R_{ij}]_{R_{ij}}$

Rather than sending each device its authentication message M''_{ij} individually, the base station aggregates all the messages along a path to form M''_j. M''_j also includes a list of UAVs in the j^{th} path along with their relative position. Moreover, timestamp T_O is appended along with P_j to avoid replay or out-of-order messages. In here, M''_j refers to the aggregated authentication message sent by BS along the j^{th} path. M''_j is given by:

$$M''_j = M''_{1j} || M''_{2j} || \ldots || M''_{kj} || P_j || T_O. \quad (2)$$

When the message is propagated from the BS to UAVs, each UAV first checks if the current timestamp T_O on the message is the same as the expected timestamp T_O^{Ex} (timestamp refers to a period of time for an authentication period to occur). If yes, the authentication proceeds. Else the message is dropped. Once the time stamp is verified, using the P_j list, each UAV identifies its relative location in the path. Once the UAV has identified that it is the i^{th} device in the path, it extracts:

$$M''_{ij} = C_{ij} || E[N_\alpha || T_O || R_{ij})_{R_{ij}}. \quad (3)$$

Also, the i^{th} device forwards the entire message received from the BS to its child (evaluated using P_j). Using its PUF, the device generates R_{ij}^{Ex} on C_{ij} from M''_{ij}.

$$R_{ij}^{Ex} = PUF(C_{ij}). \quad (4)$$

R_{ij}^{Ex} is used to decrypt the encrypted message and extract N_α, ${T_O}^{Ex}$ and ${R_{ij}}^{Ex}$. The device compares the value of ${T_O}^{Ex}$ and ${R_{ij}}^{Ex}$ to the values of T_O and R_{ij}. This step ensures integrity check so that receiver is sure that message is not altered. Then, the device generates its secret message using a random generator as N_{Cij}. Moreover, it also generates a new set of random challenge-response pair (C'_{ij}, R'_{ij}) using its PUF. Once the device has ensured that the BS is authentic, it generates the session key Sk_{ij} using its secret message (N_{Cij}) and the secret message of BS (N_α). Sk_{ij} at the device is given as:

$$Sk_{ij} = R_{ij}^{Ex} \oplus N_\alpha \oplus N_{Cij}. \quad (5)$$

The device waits for a response from its child before sending its response to BS. The current device appends the reply of its decedent ($Q''_{(i+1)j}$) to its reply, which is given by:

$$Q''_{ij} = E(N_{Cij} || T_O || C'_{ij} || R'_{ij} || R_{ij}^{Ex})_{R_{ij}^{Ex}}. \quad (6)$$

Finally, the entire aggregated response reaches the base station. The base station breaks down the aggregated response into multiple messages, such that each message is a response for a device in a path. Like the decryption procedure followed by the device, the base station decrypts the message using R_{ij}. Note that the base station uses its memory to extract R_{ij} corresponding to C_{ij} instead of a PUF (as was the case in the device). The base station

evaluates the secret message N_{Cij}. The new challenge-response pairs (C'_{ij}, R'_{ij}) are stored in its memory. Then, it evaluates the session key as:

$$Sk_{ij} = R_{ij} \oplus N_\alpha \oplus N_{Cij}. \tag{7}$$

Once the session key is established, the BS and the device can communicate using the shared key.

IV. Formal Security Proof

In this section, we provide a formal security analysis of our protocol, by modelling the communication in the protocol using Mao-Boyd logic [14]. The notations for symbols as used by Mao-Boyd logic are presented as following:

1) $D_{ij} \models$ BS: D_{ij} believes BS.
2) $D_{ij} \overset{K_{ij}}{|\sim}$ M: D_{ij} encrypted M using the key K_{ij}.
3) $D_{ij} \overset{K_{ij}}{\triangleleft}$ M: D_{ij} extracts M using key K_{ij}.
4) $D_{ij} \overset{Sk_{ij}}{\leftrightarrow}$ BS: Sk_{ij} is a valid shared key.
5) #(N_α): Nonce N_α is unique and not used before.
6) sup(BS): BS is assumed to be secure and trustworthy.
7) $D_{ij} \triangleleft \| M$: D_{ij} cannot get the message M.

Claim 1. *D_{ij} knows that N_α is a valid shared and secure message between D_{ij} and* BS.

Proof: We assume that the PUF is secure, and R_{ij} is known only to the base station and the corresponding device. Also, we assume that the base station is trusted and cannot be compromised. Using the communication presented in Fig. 2, we now describe the proof for authentication. R_{ij} in the proof represents the PUFs response, D_{ij} represents the i^{th} device in path j. D_{ij} is able to obtain N_α. This can be mathematically represented as:

$$D_{ij} \models D_{ij} \overset{R_{ij}}{\leftrightarrow} \text{BS}, \tag{i}$$

$$D_{ij} \overset{R_{ij}}{\triangleleft} N_\alpha. \tag{ii}$$

Using the authentication rule (the Mao-Boyd rules are provided in [14]), we can combine (i) and (ii) to get (iii), which states that the D_{ij} knows BS encrypted N_α using the key R_{ij}:

$$D_{ij} \models \text{BS} \overset{R_{ij}}{|\sim} N_\alpha. \tag{iii}$$

Since the BS is trusted, D_{ij} knows that the nonce N_α must be fresh and unused. We have:

$$D_{ij} \models \#(N_\alpha), \tag{iv}$$

$$D_{ij} \models sup(\text{BS}). \tag{v}$$

Since R_{ij} was exchanged as part of the registration phase, D_{ij} knows that BS regards R_{ij} to be a valid shared key between D_{ij} and BS which can be expressed as:

$$D_{ij} \models \text{BS} \models D_{ij} \overset{R_{ij}}{\leftrightarrow} \text{BS}. \tag{vi}$$

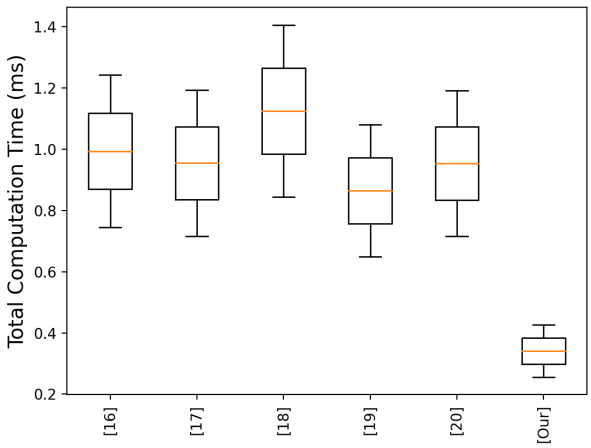

Fig. 2: Comparison of time taken for execution of protocol.

Moreover, D_{ij} knows BS is trusted from (v), so we get:

$$D_{ij} \models \text{BS} \models \{D_{ij}\}^c \triangleleft \| N_\alpha. \tag{vii}$$

Applying the confidentiality rule using (vi), (vii), and (iii), D_{ij} is convinced that no one else except itself and base station knows the secret nonce N_α, i.e.,

$$D_{ij} \models \text{BS} \models \{D_{ij}, \text{BS}\}^c \triangleleft \| N_\alpha. \tag{viii}$$

Applying the super principle rule, we can reduce (viii) to:

$$D_{ij} \models \{D_{ij}, \text{BS}\}^c \triangleleft \| N_\alpha. \tag{ix}$$

Finally, applying the good-key rule to (v) and (ix) we have,

$$D_{ij} \models D_{ij} \overset{N_\alpha}{\leftrightarrow} \text{BS}. \tag{x}$$

Hence, it is proved that D_{ij} is convinced of the shared secret N_α between D_{ij} and BS. ■

V. Simulation and Computational Performance

This section provides a comparison of the proposed technique with previous state-of-art works in authentication for UAVs. Our simulation considered 100 randomly deployed UAVs over 100 square km geographic area around a single base station. The base station is positioned at the center of the region. Simulation for the base station was performed on Apple Mac (1.8 GHz Dual-Core Intel Core i5, 8 GB 1600 MHz DDR3). UAV operations were performed on a Raspberry Pi 3B device. Python was used as the programming language for the execution of the protocol. Also, we consider the PUF proposed in [15] to be deployed in the UAVs for our protocol. The PUF generates a response of 320-bits and PUF operation time and is evaluated to 0.4 μs.

Figure 2 illustrates a boxplot comparison of the total computation taken per UAV for the execution of protocol with [16], [17], [18], [19] and [20]. Each boxplot shows the minimum, first quartile, median, third quartile, and maximum computation time per UAV for each protocol execution. The median time for [16], [17], [18], [19] and [20]

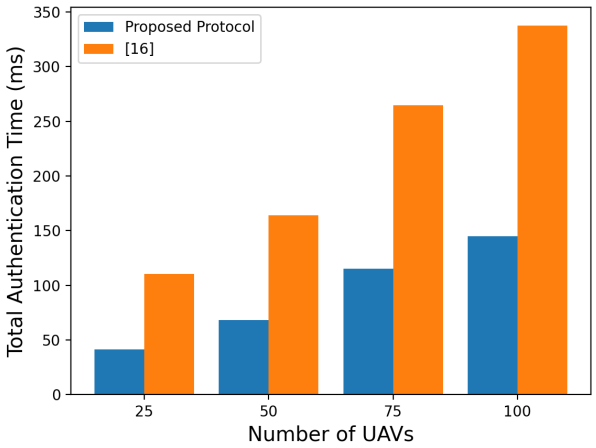

Fig. 3: Comparison of time taken for execution of protocol.

is 0.994 ms, 0.955 ms, 1.125 ms and 0.865 ms and 0.954 ms respectively. While, the median time for proposed protocol per UAV completes in 0.341 ms. This shows that proposed protocol is lightweight and computationally efficient.

Figure 3 depicts a bar graph comparison of the total authentication taken for the proposed protocol with [16]. The total authentication time includes time taken to generate topology, message propagation time, and product of computation time per UAV and number of UAVs. So as the number of UAVs increases, the total time of authentication increases. In Fig.3, we observe, the time taken for our proposed that our protocol is 41.28 ms, 68.14 ms, 115.32 ms and 144.76 ms for 25,50,75,100 UAVs. Whereas, the total time taken for protocol [16] is 110.43 ms, 163.95 ms, 264.78 ms and 337.40 ms. We can observe from the figure that our protocol consumes less than 50% of time than [16]. As the number of UAVs increases, the performance of the proposed protocol enhances.

VI. Conclusion

This letter presents a scalable protocol for mutual authentication between UAVs and a base station. We employed the K-Means clustering algorithm to form clusters based on UAV's location. Clustering of UAVs based on distance reduced the total propagation time and total propagation distance for messages than the previous state-of-the-art. The proposed protocol ensures physical security using PUFs and is also resistant to a man-in-the-middle attack, replay attack, physical attacks.

References

[1] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 899–922, 2016.

[2] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 1213–1218.

[3] O. Blazy, P.-F. Bonnefoi, E. Conchon, D. Sauveron, R. N. Akram, K. Markantonakis, K. Mayes, and S. Chaumette, "An efficient protocol for uas security," in *2017 Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, 2017, pp. 1–21.

[4] L. Chen, S. Qian, M. Lim, and S. Wang, "An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems," *China Communications*, vol. 15, no. 5, pp. 61–76, 2018.

[5] B. Semal, K. Markantonakis, and R. N. Akram, "A certificateless group authenticated key agreement protocol for secure communication in untrusted uav networks," in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*. IEEE, 2018, pp. 1–8.

[6] S. Jangirala, A. K. Das, N. Kumar, and J. Rodrigues, "Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Transactions on Vehicular Technology*, 2019.

[7] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for v2g using puf," *IEEE Transactions on Vehicular Technology*, 2020.

[8] G. Bansal, N. Naren, and V. Chamola, "Rama: Real-time automobile mutual authentication protocol using puf," in *Proceedings of IEEE International Conference on Information Networking (ICOIN), Barcelona, Spain*. IEEE, 2020.

[9] G. Bansal and V. Chamola, "Lightweight authentication protocol for inter base station communication in heterogeneous networks," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 871–876.

[10] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, and C. Wachsmann, "Seda: Scalable embedded device attestation," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 964–975.

[11] A. Ibrahim, A.-R. Sadeghi, G. Tsudik, and S. Zeitouni, "Darpa: Device attestation resilient to physical attacks," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 171–182.

[12] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 57–64.

[13] I. Cervesato, "The dolev-yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer Science—LICS*, vol. 1, 2001.

[14] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *[1993] Proceedings Computer Security Foundations Workshop VI*. IEEE Comput. Soc. Press, pp. 147–158. [Online]. Available: http://ieeexplore.ieee.org/document/246631/

[15] X. Zhao, Q. Zhao, Y. Liu, and F. Zhang, "An ultracompact switching-voltage-based fully reconfigurable rram puf with low native instability," *IEEE Transactions on Electron Devices*, vol. 67, no. 7, pp. 3010–3013, 2020.

[16] T. Alladi, V. Chamola, N. Kumar *et al.*, "Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks," *Computer Communications*, 2020.

[17] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.

[18] G. K. Verma, B. Singh, N. Kumar, and D. He, "Cb-ps: An efficient short-certificate-based proxy signature scheme for uavs," *IEEE Systems Journal*, vol. 14, no. 1, pp. 621–632, 2019.

[19] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43 711–43 724, 2020.

[20] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "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, no. 2, pp. 3572–3584, 2018.