Secure and Trusted Attestation Protocol for UAV Fleets

Gaurang Bansal, Member, IEEE and Biplab Sikdar, Senior Member, IEEE
Department of Electrical and Computer Engineering
National University of Singapore
Singapore, Singapore
e0622339@u.nus.edu, bsikdar@nus.edu.sg

***Abstract*—Unmanned Aerial Vehicles (UAVs) are capable of a wide variety of social, economic, and military applications. Due to the fact that UAVs communicate through wireless technology, they are vulnerable to security assaults. Establishing trust between the UAV and the base station is a vital component of reducing these hazards in UAV networks. Due to the restricted resources available to UAVs, adopting typical trust-building procedures in UAV networks becomes challenging. Additionally, as the number of unmanned aerial vehicles (UAVs) increases, this issue gets more critical. To address this issue, we offer a lightweight attestation mechanism for unmanned aerial vehicle swarms. Comparative analyses reveal that the proposed approach outperforms the state-of-the-art already available.**

***Index Terms*—UAVs, authentication, attestation.**

I. INTRODUCTION

While the development of UAV-based applications has accelerated dramatically over the last decade, the peak has not yet been reached. Numerous future applications need UAVs to operate close to end-users, which presents major security concerns. UAVs are vulnerable to physical assaults such as capture and manipulation, and numerous network-based attacks such as man-in-the-middle, replay, and device cloning attacks [1, 2].

Authentication and attestation are two critical security mechanisms for the proper operation and protection of UAV communications. Authentication is a process that communicating parties use to verify that each party is using a valid device [3, 4]. Authentication ensures that the messages being communicated are only accessible to authorized parties. However, malicious attackers may attempt to take control/compromise one or both communicating parties at any time in a dynamic network. As a result, periodic authentications are required to prevent malicious attackers from gaining access to communications [5].

Attestation is used to determine whether the memory/firmware of a device has remained unchanged [6]. The firmware of a UAV is susceptible to modification by malicious users who may attempt to reprogram it wirelessly or while interacting with it in an application-specific context (for example, drone delivery). Since a modified firmware can result in improper operation and security loopholes during UAV operations, attestation is also a critical security objective for UAV communications. A prover is an entity whose firmware is to be arrested, whereas a verifier is an entity that attests the prover [7, 8].

This paper proposes a hardware security-based authentication and attestation protocol for communication between unmanned aerial vehicles (UAVs). We consider the case of a swarm of unmanned aerial vehicles (UAVs) that must be attested and authenticated regularly following deployment. Because the size of a UAV swarm can vary significantly, the proposed protocol is designed to be scalable, lightweight, and distributed.

The major contributions of the paper are as follows:

1) We propose a scalable authentication cum attestation protocol for UAVs.
2) The proposed protocol uses a Physically Unclonable Function (PUF) to ensure speed and physical security.
3) The proposed protocol achieves message integrity, mutual authentication, attestation, confidentiality, and protection against denial of service, man-in-the-middle (MITM), replay, impersonation, and cloning attacks.

The rest of this paper is organized as follows. Related works are discussed in Section II. In Section III, we discuss the system and adversarial models. Section IV presents the proposed protocol. Security analysis of the protocol is presented in Section V. We provide a

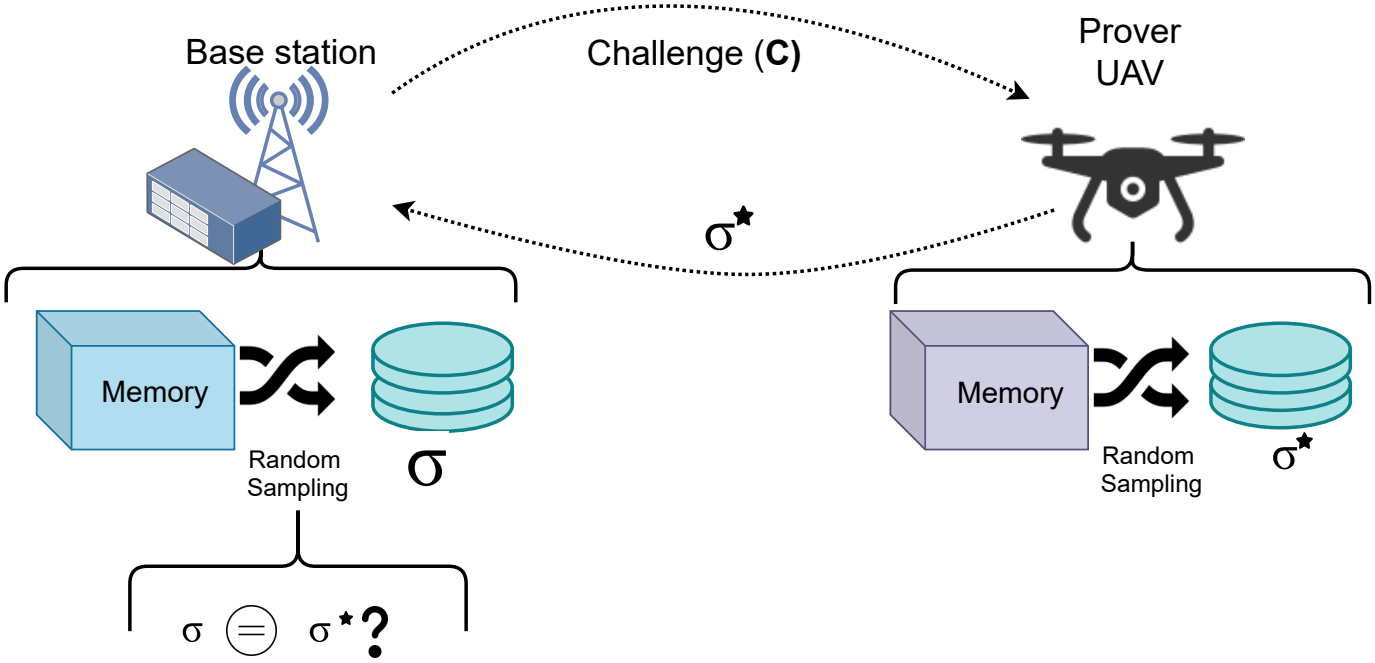

Fig. 1: Overview of proposed attestation technique.

performance analysis of the proposed protocol in Section VII. Finally, the conclusions of the paper are presented in Section VIII.

II. Related Works

The network characteristics of a UAV swarm are significantly different from other distributed networks mainly due to their mobility, which is higher than that of Mobile Ad-Hoc Networks (MANETs) and Vehicular Ad-Hoc Networks (VANETs). So traditional security mechanism of MANETs, VANETs can't be applied in UAV networks. There have been many works addressing the security concerns in UAV networks. In [9], the authors present a privacy-preserving authentication protocol for the Internet of Drones for authenticating a UAV with a UAV service provider through a mobile edge computing (MEC) device without loss of privacy. A point to note about this work is the use of PUFs to ensure physical security. Each UAV has two PUF devices that are used during the authentication. The authors of [1] present a UAV-Ground Station (GS) and a UAV-UAV authentication scheme using a single PUF device on each UAV. The authors of [10] present a PUF based authentication scheme for authenticating a two-layered swarm of drones. A larger leader drone controls several mini drones in its vicinity. Their protocol authenticates the leader drone with the Ground Station and a mini drone with the leader drone. Both [1], [10] provide security against physical attacks by the use of PUFs. However, [1] does not address scalability and [10] is applicable only to a fixed two-level scenario.

In [11–13], the authors present an authentication protocol for UAV swarms but they did not discuss anything regarding attestation. Chen et al. present a direct anonymous attestation protocol for network-connected UAV (NC-UAV) systems [14]. Their scheme utilizes Trusted Platform Modules (TPMs), dedicated microcontroller, or cryptoprocessor for storing secret credentials. These are generally highly expensive, and hence the feasibility of their usage in commercial UAVs is uncertain. In [15], the authors present Practical Attestation for Highly Dynamic Swarm Topologies (PADS). Their model is scalable and can be employed in unstructured networks. However, it is meant for use in networks of autonomous devices operating without a central controlling entity such as a base station.

As discussed above, most of the present works deal with either attestation or authentication, except for [14] which includes both attestation and authentication and uses expensive TPMs. The remaining works that deal with either attestation or authentication fall short in scalability and are limited in their usage scenarios. Moreover, most of these protocols do not ensure physical security. Hence, there is the need for a robust, distributed, and scalable authentication cum attestation protocol for UAV swarms that can quickly and in a lightweight manner

authenticate all the UAVs in a swarm among each other.

III. System Model

We consider a scenario where several UAVs in a swarm carry out a collective objective. Each UAV has to be repeatedly authenticated and attested at regular intervals to detect and prevent malicious entities from gaining control over one or more UAVs of the swarm. Each UAV in the swarm is equipped with a single PUF chip that acts as the basis for securely identifying each UAV and ensures protection against device tampering attacks. PUFs are derived from the randomness and process variations in the fabrication of an integrated circuit and serve as unique fingerprints for a particular chip [16, 17]. It is used in a challenge-response mechanism where a PUF device is evaluated with a challenge C to obtain a response R (C and R are together called the Challenge-Response Pair (CRP)). It is assumed that the construction of the PUF in the device is such that any attempt by the attacker/capturer of the UAV to extract/tamper with the PUF will render it unusable.

Apart from the PUF, the device is also equipped with a memory that stores the software. The memory is divided into blocks. Each block has multiple words, and each word is comprised of a series of bits. During the attestation process, the verifier UAV verifies a portion of the bits rather than verifying all the bits of code stored in memory (for efficiency). The overall working of our model is shown in Figure 1.

IV. Proposed Protocol

This section explains the working of the proposed authentication-attestation protocol. We assume that each of UAV has an associated PUF. Base station is trusted entity and can't be compromised. Challenge response pairs from the UAV are stored in the trusted base station server before the deployment. Each UAV has specific task of instructions that are loaded in its memory before the deployment. During the attestation process, the base station verifies if the memory locations where the code was located is unaltered or not. Note in here, we are only concerned with the area of memory where the code is stored and not other sections of memory. The authentication-attestation protocol shown in figure 2 works as follows:

1) The UAV, U, sends its ID ID_U, and a nonce χ_U^* to the base station S. S verifies if the software installed in U is correct or has been modified. The random nonce is generated to avoid replay attacks and ensure that each protocol iteration is unique.
2) Using the UAV ID ID_U, the base station extracts corresponding challenge C_U and response R_U pairs from its memory. It also generates three random sets ψ, ϕ, and ω using a pseudo-random generator function (PRNG). The random sets ψ, ϕ, and ω form the set of n blocks, m words and l bits, respectively. Thus, the verifier evaluates block locations $(\psi_1, \psi_2, \ldots, \psi_n)$, word location $(\Phi_1, \Phi_2, \ldots, \Phi_m)$ and bits location $(\omega_1, \omega_2, \ldots, \omega_l)$ using PRNG as follows:
$$\psi, \phi, \omega, \chi_S^* \leftarrow \text{PRNG}(),$$
$$\psi_1, \psi_2, \ldots, \psi_n \leftarrow \psi,$$
$$\Phi_1, \Phi_2, \ldots, \Phi_m \leftarrow \Phi,$$
$$\omega_1, \omega_2, \ldots, \omega_l \leftarrow \omega.$$
3) The base station also generates a nonce χ_S^* using a pseudo-random generator. This nonce is used to generate the session key after the authentication step.
4) The base station computes the attestation value σ_U^* using chosen memory location. The base station iterates over all the bits $\omega_1, \omega_2, \ldots \omega_l$ in the m words $\Phi_1, \Phi_2, \ldots \Phi_m$ of chosen blocks $\psi_1, \psi_2, \ldots \psi_n$ and concatenates them to form the value of σ_U^*. σ_U^* can thus be evaluated as:
```
σ*_U ← []
for i = 1, ··· , n do
    Choose block M_{ψ_i}
    for j = 1, ··· , m do
    Select memory word M_{ψ_i}[Φ_j]
        for k = 1, ··· , l do
        Choose bits in word M_{ψ_i}[Φ_j]{ω_k}
            σ*_U ← σ*_U ‖ M_{ψ_i}[Φ_j]{ω_k}
        end for
    end for
end for
```
5) The base station creates a message P by performing a XOR operation on $(\chi_S^* \| \psi \| \phi \| \omega) \oplus R_U$. Finally, the base station sends message P along with challenge C_U.
$$P = (\chi_S^* \| \psi \| \phi \| \omega) \oplus R_U.$$
6) On receiving the message (P,C_U) from base station S, UAV U uses C_U to generate R_U using its PUF. Then, it extracts the values of χ_S^*, ψ, ϕ, and ω from P using R_U as:
$$\chi_S^*, \psi, \phi, \omega \leftarrow (\chi_S^* \| \psi \| \phi \| \omega) \oplus R_U \oplus R_U.$$

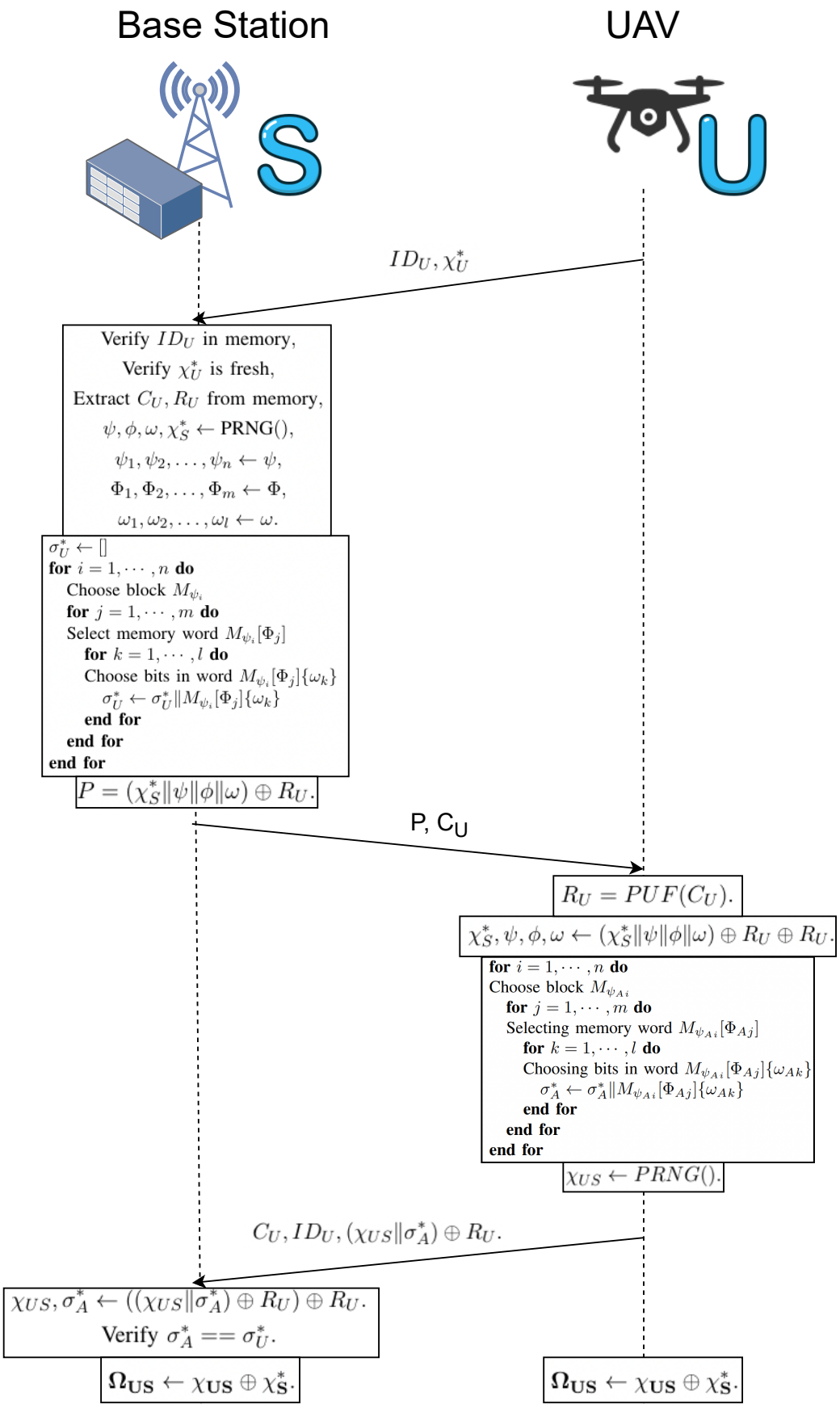

Fig. 2: Proposed protocol

7) Using the values ψ, ϕ, ω, UAV U evaluates the value of attestation (σ_A^*) as:
for $i = 1, \cdots, n$ **do**
Choose block $M_{\psi_{Ai}}$
for $j = 1, \cdots, m$ **do**
Select memory word $M_{\psi_{Ai}}[\Phi_{Aj}]$
for $k = 1, \cdots, l$ **do**
Choose bits in word $M_{\psi_{Ai}}[\Phi_{Aj}]\{\omega_{Ak}\}$
$\sigma_A^* \leftarrow \sigma_A^* \| M_{\psi_{Ai}}[\Phi_{Aj}]\{\omega_{Ak}\}$
end for
end for
end for

8) Once the UAV U generates its attestation value (σ_A^*), it generates another nonce χ_{US} using a pseudo random generator function. Using χ_{US} and χ_S^*, UAV U generates the session key Ω_{US} as:

$$\mathbf{\Omega_{US}} \leftarrow \chi_{\mathbf{US}} \oplus \chi_{\mathbf{S}}^*.$$

9) UAV U generates a message $(\chi_{US} \| \sigma_A^*)$ and performs a XOR operation with R_U to the trusted server. U sends the message $(\chi_{US} \| \sigma_A^*) \oplus R_U$ to the base station along with challenge C_U, and ID of UAV ID_U.

10) The base station extracts R_U corresponding to for UAV U from the memory. Using R_U, it extracts $(\chi_{US} \| \sigma_A^*)$, by performing a XOR operation on $(\chi_{US} \| \sigma_A^*) \oplus R_U$ with R_U. It then verifies the attestation value σ_A^* with its evaluated attestation value σ_U^*. If the value matches, the UAV is successfully attested, and session key Ω_{US} is generated as:

$$\chi_{US}, \sigma_A^* \leftarrow ((\chi_{US} \| \sigma_A^*) \oplus R_U) \oplus R_U.$$
$$\text{Verify } \sigma_A^* == \sigma_U^*.$$
$$\mathbf{\Omega_{US}} \leftarrow \chi_{\mathbf{US}} \oplus \chi_{\mathbf{S}}^*.$$

V. Results and Discussion

This section evaluates the proposed protocol's performance and compares it with other state-of-the-art works. The operation times for UAVs were evaluated on a Raspberry Pi 3B device. Figure 3 illustrates the comparison of the total time taken for the execution of our proposed protocol with the protocol in [10] for different number of UAVs. We can observe from figure that the performance of our protocol in comparison to [10] improves as the number of UAVs increase. For 25 UAVs, total execution time for proposed protocol is 5.33 ms which increases to 21.3 ms for 100 UAVs. While for [10], the increase is more steeper, from 9.59 ms to 38.4 ms. Similarly we show in Figure 4 the comparison of execution time with [18]. Similar to figure 3, as number of UAVs increase the difference of execution time of proposed protocol and [18] increase from 6.16 ms to 24.7 ms.

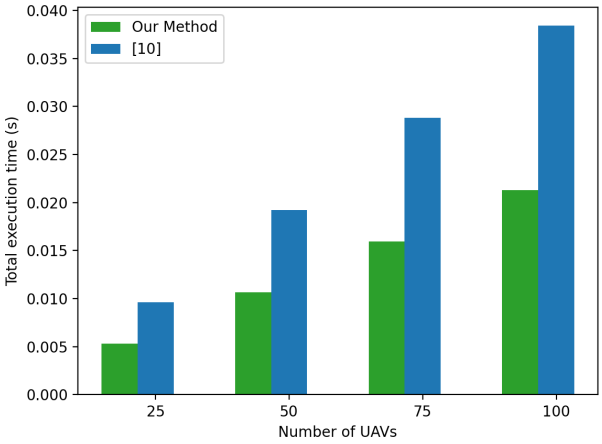

Fig. 3: Comparison of execution time with [10] for different number of UAVs.

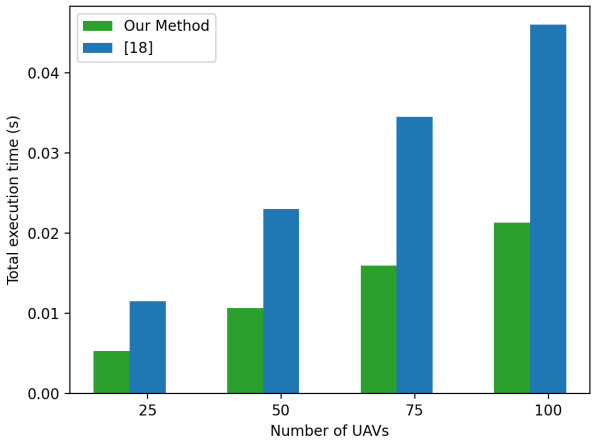

Fig. 4: Comparison of execution time with [18] for different number of UAVs.

VI. Conclusion

Unmanned aerial vehicles have a wide range of social, commercial, and military applications. Since they use wireless communication, UAVs are highly vulnerable to security threats. Establishing trust among UAVs is the most basic security requirement in UAV networks. Because UAVs have limited resources, deploying traditional trust establishment schemes in UAV networks is difficult.

This problem worsens as the number of UAVs increases. To address this, we proposed a lightweight authentication and attestation protocol for UAV swarms. The proposed protocol outperforms the current state-of-the-art.

REFERENCES

[1] T. Alladi, G. Bansal, V. Chamola, M. Guizani *et al.*, "Secauthuav: A novel authentication scheme for uav-ground station and uav-uav communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 068–15 077, 2020.

[2] G. Bansal, N. Naren, and V. Chamola, "Rama: Real-time automobile mutual authentication protocol using puf," in *2020 International Conference on Information Networking (ICOIN)*. IEEE, 2020, pp. 265–270.

[3] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2020.

[4] 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.

[5] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[6] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of the 11th ACM conference on Computer and communications security*, 2004, pp. 132–145.

[7] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," *International Journal of Information Security*, vol. 10, no. 2, pp. 63–81, 2011.

[8] Y. Zeng, S. Jin, Q. Wu, and F. Gao, "Network-connected uav communications," *China Communications*, vol. 15, no. 5, pp. iii–v, 2018.

[9] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 621–13 630, 2020.

[10] T. Alladi, V. Chamola, N. Kumar *et al.*, "Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks," *Computer Communications*, vol. 160, pp. 81–90, 2020.

[11] G. Bansal and B. Sikdar, "S-maps: Scalable mutual authentication protocol for dynamic uav swarms," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 12 088–12 100, 2021.

[12] G. Bansal and B. Sikdar, "A secure and efficient mutual authentication protocol framework for unmanned aerial vehicles," in *2021 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2021, pp. 1–6.

[13] G. Bansal and B. Sikdar, "Location aware clustering: Scalable authentication protocol for uav swarms," *IEEE Networking Letters*, vol. 3, no. 4, pp. 177–180, 2021.

[14] 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.

[15] M. Ambrosin, M. Conti, R. Lazzeretti, M. M. Rabbani, and S. Ranise, "Pads: practical attestation for highly dynamic swarm topologies," in *2018 International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2018, pp. 18–27.

[16] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A puf-based secure communication protocol for iot," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 3, pp. 1–25, 2017.

[17] T. Alladi, N. Naren, G. Bansal, V. Chamola, and M. Guizani, "Secauthuav: A novel authentication scheme for uav-base station scenario," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[18] 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.