A Secure and Efficient Mutual Authentication Protocol Framework for Unmanned Aerial Vehicles

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), commonly known as drones, are becoming increasingly popular owing to their wide application domain. However, the issue of security and privacy is a concern for these UAV-based applications. UAVs are susceptible to multiple threats like the man-in-the-middle attack, the replay attack, the physical attacks. To mitigate these threats and vulnerabilities, we propose a lightweight mutual authentication protocol that ensures network and communication security. The proposed protocol uses Physical Unclonable Function (PUFs), a digital fingerprint device to protect against physical and masquerade attacks. The proposed protocol is robust, secure, and fast compared to other state-of-the-art protocols previously proposed in the literature.**

***Index Terms*—Unmanned aerial vehicles, physical security, mutual authentication, security, and privacy.**

I. INTRODUCTION

UAVs have been used for various applications such as medical surveillance in natural disasters, traffic monitoring, military operations, delivery services, and task offloading. UAV technology has been one of the most rapidly advancing fields. UAV-based networks now can be used for traffic surveillance in the next generation Intelligent Transportation Systems [1]. In the domain of security, they could be used for tracking the movement of suspicious people and even for live streaming videos for security agencies [2]. Most UAV applications require a communication channel where drones and the base station can safely and quickly communicate.

Due to being deployed in an open environment, UAVs are also prone to several security threats. The threats to UAVs come in two types- natural phenomena and those caused by human interference. The quality of data transmitted is influenced by natural phenomena, whereas human interference affects the security aspect of the transmitted data. Some of these security threats could be modifying the communication data, blocking the channel, device capture, eavesdropping attack, flying away with the device, etc. The most challenging part of ensuring a secure communication channel is to make it lightweight and at the same time secure from all possible attacks such as network spoofing, man-in-the-middle attacks, replay attacks. The secure channel must ensure that it is not feasible for any adversary to exploit UAV devices to access sensitive information, disrupt the regular operation, corrupt the data, or cause malicious interference.

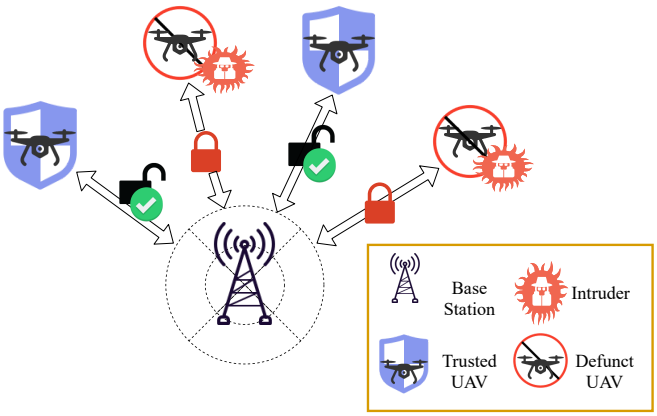

Fig. 1: System model

To ensure protection against external adversaries, one of the critical security requirements for UAV deployments in developing authentication techniques to the base station. In UAVs, it is essential to authenticate the devices frequently because of the dynamic nature of the environment. As UAVs move during their operation, their state (e.g., the links, the base station serving them, etc.) is likely to change with time. Continuous authentication of the devices is necessary to ensure that a malicious adversary cannot access the resources and information related to the UAV application or affect its regular operation.

For protection against environmental factors, there is a need to design a novel protocol that can understand the difference between changes due to external factors and adversaries [3–5]. With the rapid development of integrated circuit technology in recent years, PUFs are very promising in a wide range of security applications [6–8]. They utilize the inherent randomness introduced during the manufacturing process of a silicon device, thus making it very difficult to clone or reproduce them. However, due to external environmental factors, some randomness can be lost or error-prone. Thus it is necessary to design protocols that ensure the availability and authentication of UAV devices in such circumstances.

Section II highlights an overview of the network model, the security goals, attack model, and assumptions used in

this paper. Section III presents a detailed description of the proposed mutual authentication protocol. A comparison of performance analysis is provided in Section IV. Finally, the conclusion is presented in Section V.

II. System & Threat Model

A. System Model

According to Fig. 1, the system consists of three entities: legitimate UAVs and eavesdropper UAVs, as well as a base station (BS). As compared to the BS, UAVs have limited memory and computational capability. It is possible to connect multiple UAVs to a single base station in this model. When given a 32-bit challenge input, the computational device on every UAV responds with an output of 32 bits. When the UAV receives a response, it performs a key expansion on it to create session keys. Both the UAV and the BS use a non-linear public function to perform the key expansion procedure. The base station sends and stores a 64-bit challenge-response pair whenever a new UAV wants to register itself. In this network, the BS is the only trusted authority. A (C, R) pair is assigned to each UAV at registration by the BS. After this initial exchange, the UAV can operate independently without the assistance of technical personnel or a secure communication channel. - (C, R) pairs are generated on the fly by the UAV during each authentication attempt. However, the new (C, R) pair is securely transmitted and stored in the base station. After authentication, the ID of a UAV is dynamically changed. This new alias ID is stored in the base station and securely shared with the authenticated UAV after authentication is complete. In future communications, nothing else is assumed.

B. Security Goals

In this section, we highlight the security goals to be achieved by the proposed protocol

1) UAV and BS must achieve mutual authentication. UAV must identify whether the communication is occurring with the right BS and vice versa.
2) The communication between the UAV and the BS must be confidential. An attacker cannot get any information (whether complete or partial) from the communication.
3) Any unauthorized entity must not be capable of identifying/tracking any particular UAV. All the UAVs must be equally indistinguishable.
4) Each session key generated must be unique, and there must not exist any correlation among the session keys generated in different iterations.
5) The session keys generated must be safe against physical attacks like UAV node capture and node tampering.
6) Any message transmitted either by the UAV/BS is received by the BS/UAV without any change.

C. Attack Model

We assume that an adversary, either an authenticated UAV or an intruder UAV, can eavesdrop on any communication between the legitimate UAV and the BS. An attacker may change or tamper with the data being communicated in the UAV network, impersonate as a valid UAV or BS, store and replay the messages from previous sessions, inject its messages in the communication link, or initiate new sessions and authenticate with the BS. Moreover, in this model, the adversary may also have the capability to capture a fully functional UAV physically.

TABLE I: Notations

Notation	Description
U_i	ID of i^{th} UAV
B_i	ID of i^{th} BS
$\|$	Concatenation
$\oplus$	XOR operation
$MAC()$	Message Authentication Code
N_A, N_B, N_C	Nonces generated
Q	Cipher text prepared by BS
$F()$	Any public non-linear function with 32-bit input and output

D. Assumptions

Some of the assumptions that are made in this paper are discussed in this section. To support the creation of security keys on the fly, each UAV node in the network is endowed with a unique PUF circuit. When it comes to computing power and memory, UAV nodes are severely limited, while the BS has no such limitations. Tampering with the PUF circuitry after authentication will put the UAV into safe mode. Notations used in this paper are listed in the table I.

III. Proposed PUF-based Protocol

This section presents the proposed protocol between a UAV and the BS, which is depicted in Fig. 2.

A UAV U_1 sends its ID U_1 and a nonce N_A to B_1 when it wants to authenticate with a neighbouring BS B_1. B_1 uses the registration process to see if U_1 is already registered with it. It also verifies in memory if U_1 exists and if nonce N_A is new if it differs from the N_A generated during the previous authentication. The authentication request by U_1 is terminated if either of the requirements fails. The base station B_1 uses U_1 to locate the associated 64-bit challenge-response pair (C, R) in its memory. $N_A||N_B$. The function F could be any publicly available non-linear function that takes a 32-bit input and gives a 32-bit output, and it must be mutually agreed upon by both the BS and the UAVs. The value of m could be any even number greater than 2, which can be decided upon based on the speed of the algorithm required. Increasing the value of m leads to higher diffusion and confusion, thus making it harder

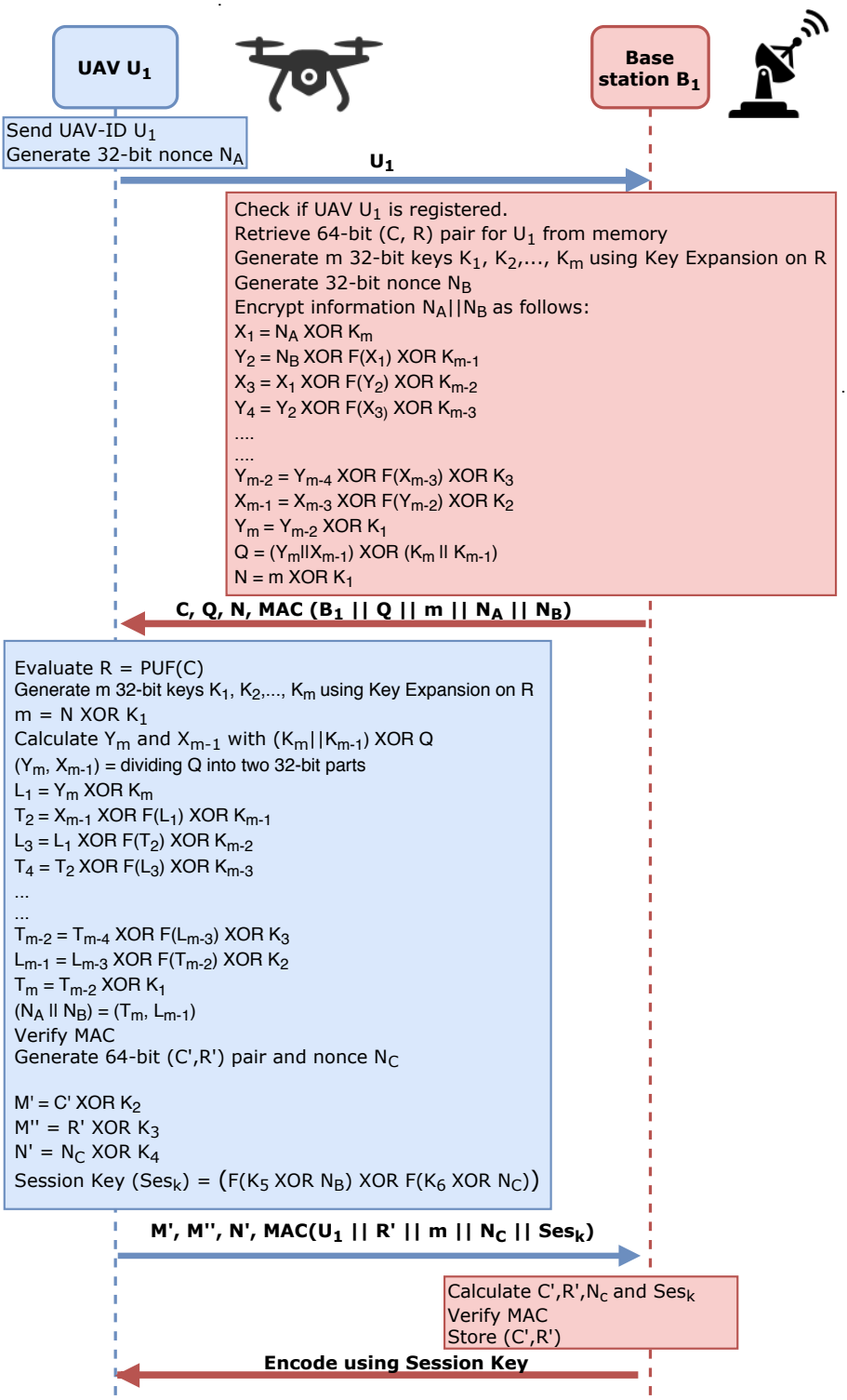

Fig. 2: Working of mutual authentication protocol between a UAV U and the Base Station BS

to break the encryption.

$$X_1 = N_A \oplus K_m$$
$$Y_2 = N_B \oplus F(X_1) \oplus K_{m-1}$$
$$X_3 = X_1 \oplus F(Y_2) \oplus K_{m-2}$$
$$Y_4 = Y_2 \oplus F(X_3) \oplus K_{m-3}$$
$$...$$
$$...$$
$$Y_{m-2} = Y_{m-4} \oplus F(X_{m-3}) \oplus K_3$$
$$X_{m-1} = X_{m-3} \oplus F(Y_{m-2}) \oplus K_2$$
$$Y_m = Y_{m-2} \oplus K_1$$

The base station sends the cipher-text Q to UAV U_1. Also, the value of m is xored to K_1 and sent to U_1 as N.

$$Q = (Y_m \| X_{m-1}) \oplus (K_m \| K_{m-1})$$
$$N = m \oplus K_1$$

Furthermore the base station also sends the challenge C and a Message Authentication Code: $MAC((B_1 \| Q \| m \| N_A \| N_B)$ to U_1. MAC is used to verify the integrity of message sent. UAV extracts the parameters and verifies, if data is tampered or not. To ensure the freshness of the base station, U_1 uses last two-parameter N_A, N_B. On receiving the message from the Base station, U_1 passes challenge C to the PUF. PUF generates the key R based on C [shown in (1)]. Using the same key generation and expansion procedure used by the base station, it regenerates m 32-bit keys: $K_1, K_2, K_3, ..., K_m$ from the response R. It calculates m and evaluates $Y_m \| X_{m-1}$ as shown below.

$$R = PUF(C) \tag{1}$$
$$m = N \oplus K_1 \tag{2}$$
$$(Y_m \| X_{m-1} (= (K_m \| K_{m-1}) \oplus Q \tag{3}$$

Y_m and X_{m-1} form the two parts of 64-bit string, where each part is of 32 bits. The decryption procedure is as follows:

$$L_1 = Y_m \oplus K_m$$
$$T_2 = X_{m-1} \oplus F(L_1) \oplus K_{m-1}$$
$$L_3 = L_1 \oplus F(T_2) \oplus K_{m-2}$$
$$T_4 = T_2 \oplus F(L_3) \oplus K_{m-3}$$
$$...$$
$$T_{m-2} = T_{m-4} \oplus F(L_{m-3}) \oplus K_3$$
$$L_{m-1} = L_{m-3} \oplus F(T_{m-2}) \oplus K_2$$
$$T_m = T_{m-2} \oplus K_1$$

Now, the original information $N_A || N_B$ is recovered as $T_m \| L_{m-1}$. From this, N_B is retrieved, and the MAC is recomputed. Once the base station is verified. The device generates a random challenge C' and using PUF evaluates corresponding response R'. It also generates a new nonce N_C. Finally U_1 creates messages $M', M'' and N'$ as:

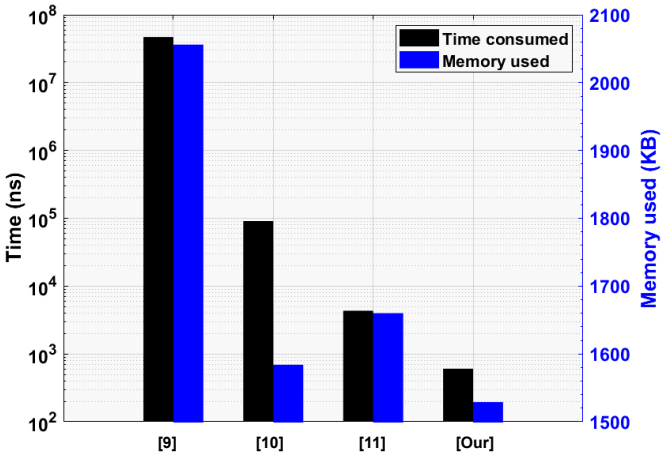

Fig. 3: Performance comparison with popular encryption schemes

$$M' = C' \oplus K_2$$
$$M'' = R' \oplus K_3$$
$$N' = N'_C \oplus K_4$$

The session key Ses_k is evaluated using:

$$Ses_k = ((F(K_5 \oplus N_B) \oplus F(K_6 \oplus N_C)) \tag{4}$$

U_1 sends M', M'' and N' to B_1. B_1 calculates C', R', N_C and Ses_k as:

$$C' = M' \oplus K_2$$
$$R' = M'' \oplus K_3$$
$$N'_C = N' \oplus K_4$$
$$Ses_k = ((F(K_5 \oplus N_B) \oplus F(K_6 \oplus N_C))$$

As a result, B_1 first verifies MAC. If the verification fails, B_1 terminates the authentication process. A 64-bit "challenge-response pair" is stored in the memory of the UAV if it is verified $((C', R')$ replaces (C, R). In order to communicate with U_1 until B_1 moves out of range, their communication is encoded with the Ses_k code. U_1 and B_1 compute the new alias ID (AID) for U_1 for next iteration.

$$AID = U_1 \oplus Ses_k \tag{5}$$

Untraceability is ensured by changing the UAV's ID as shown in equation (5). If an adversary cannot match the AID with any of its previous authentication records, the AID will be unmatchable by the adversary.

IV. Results

In Fig. 3, we have compared the time consumed and memory used for the encryption process in our protocol with the schemes in [9], [10] and [11]. The protocol was implemented in C and compiled using GCC v7.4.0 on the Ubuntu 18.04

operating system. The simulation environment used was a 64-bit Intel(R) Core(TM) i7-5500 CPU with 8GB RAM. While [9], [10] and [11] took 4.7×10^7 ns, 90890 ns and 4340 ns, our protocol took just 605 ns to execute. Thus, our protocol performs exponentially better than the schemes mentioned above in terms of execution time. While [9], [10] and [11] consumed 2056 KB, 1584 KB and 1660 KB of memory respectively, our protocol required only 1429 KB showing that our protocol consumes memory more efficiently. Therefore, our scheme is a better choice considering both the processing capabilities and the memory constraint of UAVs.

V. Conclusions

As part of the UAV network, this paper proposed a PUF-based mutual authentication protocol. PUFs enable a challenge-response scheme, which means that no secret information is stored in the UAV nodes. One challenge-response pair per UAV can be stored in the base station. Every time the base station and UAV attempt to authenticate, an unencrypted session key is established. On top of that, we showed protection against various attacks such as masquerading, Man in the middle attack, replay, and node tampering attacks. Aside from that, it has been shown to outperform other solutions in terms of time consumption and memory usage. Because of this, our proposal is a very effective solution for UAV networks, which is why we believe it is a viable one.

References

[1] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, 2017.

[2] 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.

[3] D. Bhattacharya, S. Misra, N. Pathak, and A. Mukherjee, "Idea: Iot-based autonomous aerial demarcation and path planning for precision agriculture with uavs," *ACM Transactions on Internet of Things*, vol. 1, no. 3, pp. 1–21, 2020.

[4] P. K. Deb, A. Mukherjee, and S. Misra, "Xia: Send-it-anyway q-routing for 6g-enabled uav-leo communications," *IEEE Transactions on Network Science and Engineering*, 2021.

[5] N. Pathak, S. Misra, A. Mukherjee, A. Roy, and A. Y. Zomaya, "Uav virtualization for enabling heterogeneous and persistent uav-as-a-service," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6731–6738, 2020.

[6] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Springer, 2010, pp. 3–37.

[7] A. Bera, S. Misra, and C. Chatterjee, "Qoe analysis in cache-enabled multi-uav networks," *IEEE Transactions on vehicular technology*, vol. 69, no. 6, pp. 6680–6687, 2020.

[8] S. Intrinsic-ID, "Puf: the secure silicon fingerprint," *White Paper*, 2016.

[9] A. Abdallah, M. Z. Ali, J. Mišić, and V. B. Mišić, "Efficient security scheme for disaster surveillance UAV communication networks," *Information (Switzerland)*, vol. 10, no. 2, 2019.

[10] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on UAV network," in *Proceedings - 2017 1st IEEE International Conference on Robotic Computing, IRC 2017*. IEEE, apr 2017, pp. 393–398.

[11] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, and A. A. Elngar, "Secure authentication protocol based on machine-metrics and RC4-EA hashing," *International Journal of Network Security*, vol. 18, no. 6, pp. 1080–1088, 2016.