Fault Resilient Authentication Architecture for Drone Networks

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*—Wireless communication technology, particularly in Unmanned Aerial Vehicle (UAV) applications, has advanced rapidly recently. However, owing to security flaws, UAV-based applications have not reached their full potential. Interception of drone-based station communication is possible. Many authentication mechanisms, including Physical Unclonable Functions (PUF) based protocols, have been developed to address this problem. However, prior studies require noise-resistant and theoretically perfect PUF. This assumption restricts the usage of UAV-based authentication. This assumption limits the use-cases for UAV-based authentication systems. So we propose a novel distributed authentication approach based on Shamir's secret sharing that is resistant to noisy PUFs.**

***Index Terms*—UAVs, Authentication, Availability.**

I. INTRODUCTION

UAVs have been utilized for a wide range of purposes, including medical surveillance during natural catastrophes, traffic monitoring, military operations, delivery services, and task offloading, to name a few. In recent years, unmanned aerial vehicle technology has emerged as one of the most quickly developing sectors. The majority of UAV applications need the establishment of a communication channel via which drones and base stations may securely and swiftly connect. Because they are deployed in an open environment, unmanned aerial vehicles (UAVs) are vulnerable to various security risks. The dangers to UAVs arise in two forms - human involvement and environmental variables [1, 2].

The presence of a human being degrades the security of transmitted data. These security risks might include things like altering communication data, blocking a channel, seizing a device, or launching an eavesdropping attack, among others. As a consequence, there is a need to build a safe route for communication. The secure channel must assure that an attacker will not utilize unmanned aerial vehicles (UAVs) to access sensitive information, disrupt the regular operation, corrupt data, or otherwise cause malicious interference [3].

A critical security need for UAV deployment is to verify devices regularly to protect them from external attacks. Because UAVs are mobile during operation, their status (e.g., the connections, the base station that serves them, and so on) is likely to change over time. Continuous device authentication is necessary to ensure that an attacker cannot access the UAV application's resources and information or disturb its regular operation [4].

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. With the rapid development of integrated circuit technology, PUFs are very promising in many security applications. The inherent randomness is utilized, which is 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.

This article discusses a challenge-response pair authentication system based on PUFs. The base station issues a series of challenges to the UAV, and the UAV answers through its PUF response with an output that matches the challenges. When the base station gets responses from all UAVs, it verifies them using a threshold-based technique. This threshold-based approach takes advantage of the Shamir secret sharing algorithm [5]. Each device must appropriately answer to at least t of the k challenges presented by the k verification UAVs. The advantage of the Shamir secret key is that it eliminates the need for k^2 comparisons. Rather than that, it uses mathematical field concepts to reduce the protocol's

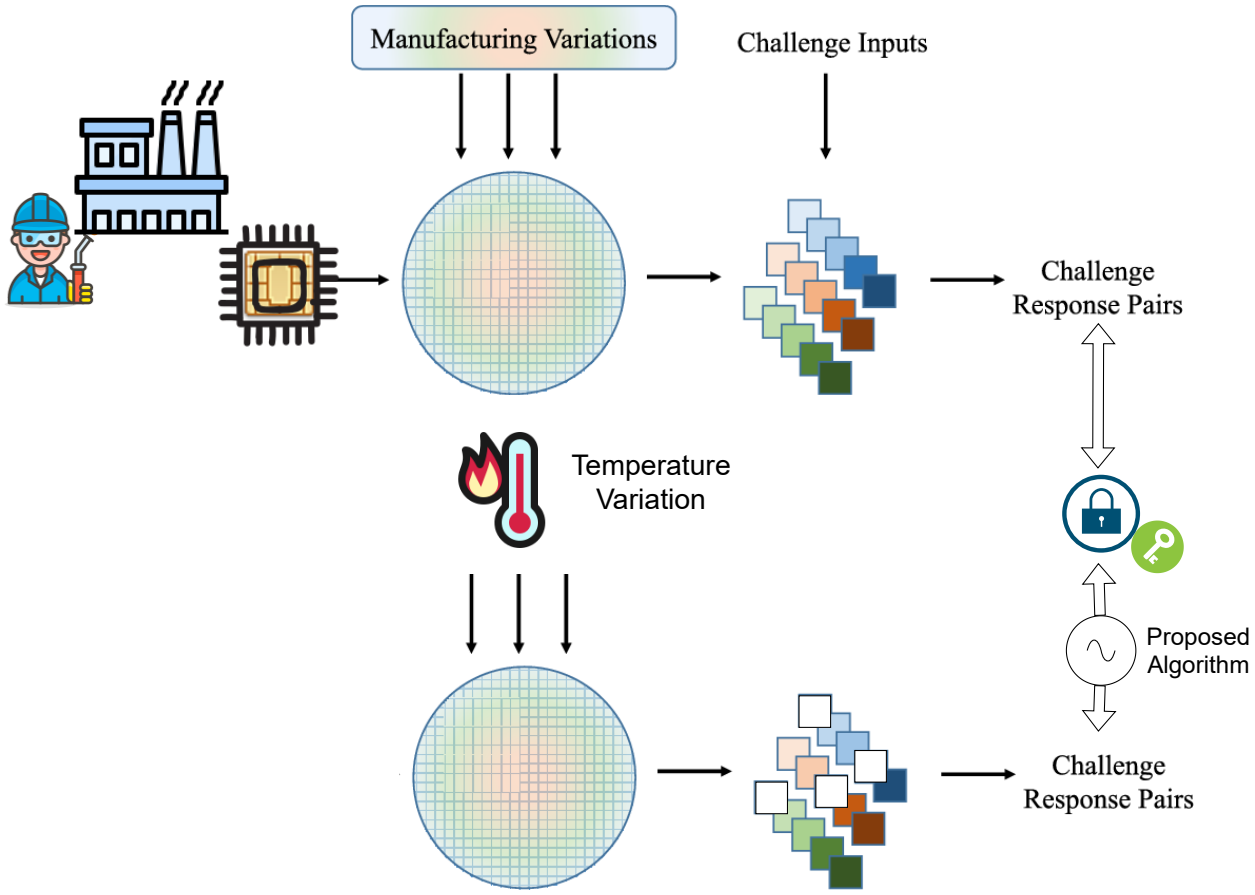

Fig. 1. Proposed model

execution time to $O(k)$. As a consequence, the system exhibits a high tolerance for failure.

The major contributions of this paper are as follows:

1) In this paper, we present a lightweight authentication mechanism based on Physical Unclonable Functions (PUFs).
2) The suggested protocol is tolerant of minor PUF errors caused by ambient circumstances outside the user's control. It also dispels the assumption that PUFs are infallible and unbreakable.
3) Our protocol guarantees secrecy, authentication, physical security, and protection against replay attacks, man-in-the-middle attacks, impersonation attacks, and node tampering attacks. It also protects against DoS attacks, confidentiality, and authentication.

The organization of the rest of the paper is as follows. Section II discusses the previous related works in the area of UAV authentication protocols. Next, we present the proposed protocol in Section III. Section IV discusses the result and finally conclusion is presented in Section V.

II. Related Work

UAVs differ significantly from other distributed network systems regarding topology, mobility, consumer service, degree of availability, complexity, and other characteristics. Traditional security provisioning for distributed networks does not produce the same results for UAVs [6, 7]. As stated in the introduction, various security concerns have hampered UAV adoption on a large scale [8, 9]. There has been much research towards implementing lightweight security provisioning for UAVs in recent years [10].

Hooper et al. [11], offered a lightweight framework for attack resilience in the authentication area. This framework was further extended in [12, 13]. The protocols in [12, 13] had a disadvantage that authors did not take into

account for all security parameters. The authors in [14] recommended using a secure channel with an array of random numbers to offer continuous authentication. In the paper, the base station uses this array as a challenge to authenticate the UAVs during the protocol execution. An PUF-based architecture is used in [15–17]. Using cryptographic identities, this approach provides privacy and device uniqueness. However, the work had a critical flaw which was discovered later.

In [18], the first distributed key authentication solution with a Certification Authority was suggested (CA). The research made a major contribution by addressing the issue of multi-party key management in a wireless mesh network. Each participant entity is assigned a unique identification or serial number that is used to build a public and private key pair via the application of cryptographic operations. The CA regularly changes the unique identification and creates new private and public keys for authentication after each authentication cycle. The primary disadvantage of this method is its dependence on centralised trustworthy organisations and high costs associated with vital computing. The authors of [19] and [20] respectively introduced authentication algorithms based on bilinear pairing and elliptical curve cryptography (ECC). While they boosted security, their methods are far from scalable. The creators of [16] offered an authentication solution for edge-assisted UAV applications. The suggested technique takes into account third-party communication, allowing mobile edge computing service providers to validate UAVs. All of the protocols discussed above regarded authentication to be an aim but lacked fault tolerance.

So we propose a fault-tolerant authentication mechanism that can handle changes in PUF due to environmental factors. We employ Shamir's secret sharing scheme to provide availability, fault tolerance, and complete security. In Shamir's secret sharing scheme [5], the concerned authority divides the secret into shares and distributes them among the shareholders. The secret can be reconstructed if there is a subset of shares, then thresholds are available. If less than the threshold of shares are available, it is impossible to reconstruct the secret. In our authentication protocol, rather than validating all responses from PUF, we verify a subset of responses based on the threshold. This allows resistance against variability in PUF due to environmental factors. We also show that the approach is mathematically secure and complete.

III. Proposed Protocol

In this section, we will describe the working of our proposed protocol as shown in figure 1.

- The base station generates a device identifier *id* for the UAV and this is stored in the device in a one-time programmable (OTP) memory. This is a kind of non-volatile memory, i.e, it is not erased when power supply is stopped.
- The base station creates a polynomial:

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1}$$

  where $a_i \in$GF(2^q), $i = (1, \ldots, t-1)$. q is a constant chosen by network administrator.
- In here, constant term a_0 acts as secret value. We denote secret value as S. Once the base station creates this S, it stores it inside its memory.
- Devices need to correctly find the value of S to authenticate themselves during the authentication phase.
- The base station generates k random challenges $C_1, C_2, \ldots, C_k$ which are randomly created to evaluate the PUFs in the device. During the enrollment phase, these challenges are given to a device. Device using its PUF generates k responses are $R = R_1, R_2, \ldots, R_k$ for k challenges.
- There exists only one response per challenge, and the response is unique for each device. The responses would be completely different if two devices were given the same challenge due to randomness generated during chip fabrication.
- Once the base station receives all the responses from the UAV. The base station calculates $f(R_i), i = 1, 2, \ldots, k$. Finally, base station stores the challenge set, response set $Q = \{f(R_j), j = 1, 2, \ldots, k\}$ and the secret a_0 as hash(a_0). We assume that the adversary has access to the data stored at the base station in the adversary model. As a result, we store the secret a_0 as a hash (a_0). So any adversary can't get a value of a_0 even by accessing the base station's memory.

In the authentication process, the device is verified when the base station can regenerate the secret based on the responses from the device, as shown in Figure 2. The aggregation of responses is turned into a Shamir Secret Key problem. The threshold is set as t, where the total number of responses is k. The rationale behind this threshold is that knowledge of any correct t responses allows the base station to authenticate the device successfully. If less than t responses are correct,

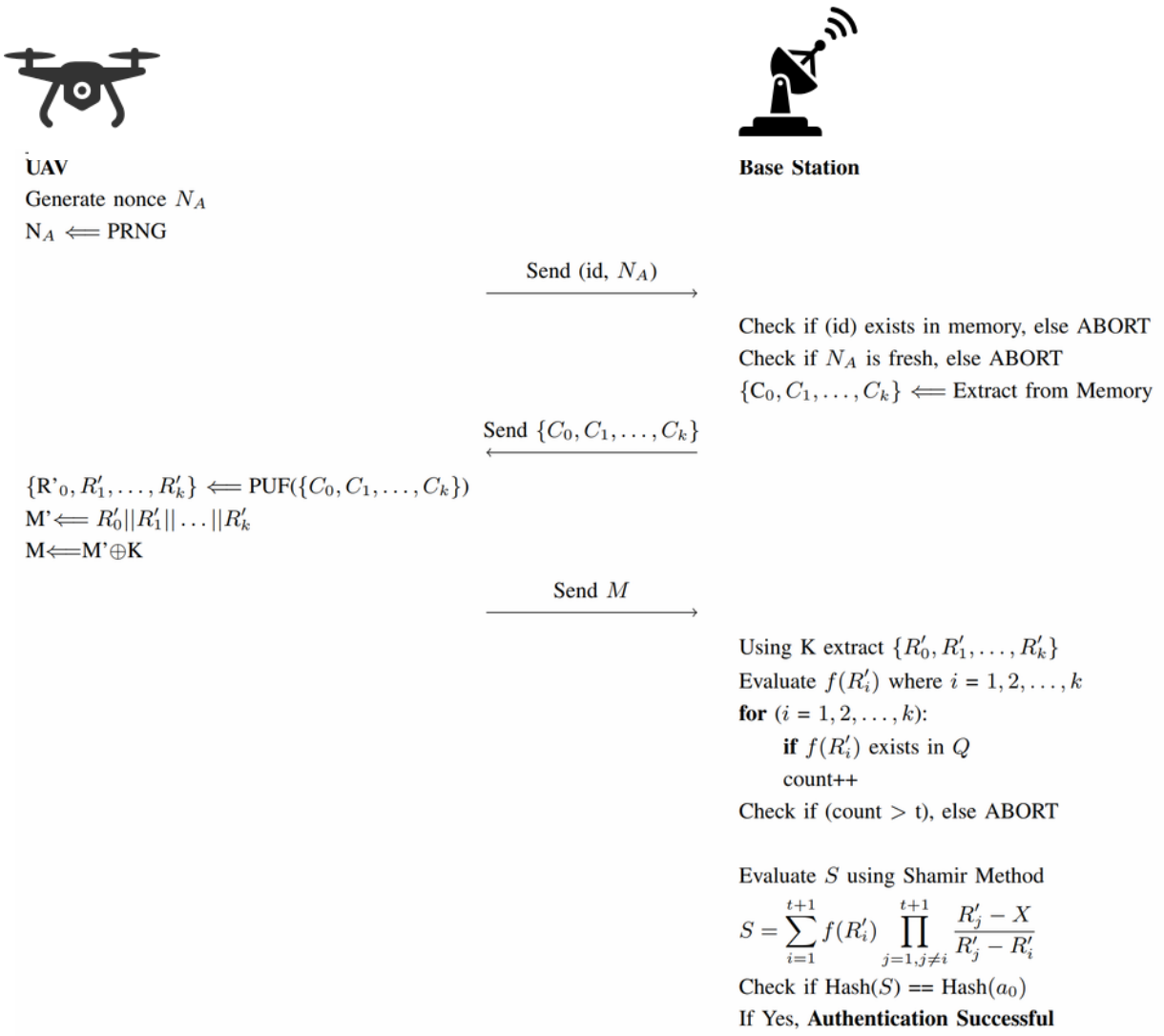

Fig. 2. Device Authentication Phase

it leaves the secret completely undetermined or reveals no information about the secret. This schema is called Shamir (t, k) scheme.

- The device initiates the authentication process by sending over its id to the base station. If the device's id is present in the base station's database, it begins the authentication process.
- The base station sends out a challenge set $C = \{C_1, C_2, \ldots, C_k\}$ to the device which is stored in memory. The device generates k responses $R'_1, R'_2, \ldots, R'_k$ corresponding to challenges given by the base station.
- Device then concatenates all the responses to form a new message M' and performs XOR operation with mutually shared nonce K.

$$M' = R'_0||R'_1|| \ldots ||R'_k,$$
$$M = M' \oplus K.$$

K ensures that no one except the base station or the device can extract the exact responses sent by the device to the base station.
- Due to environmental changes, it is possible that a valid PUF may be altered than it was during the enrollment phase. Some of the responses generated by the PUF would not match the original response during the enrollment phase. Hence we denote the response generated by PUF as R' in the authentication phase rather than R in the enrollment phase.
- Base station using the shared nonce K extracts the

responses. Then base station computes $f(R_i')$ where $i = 1, 2, \ldots, k$.

- To facilitate better computation, base station counts the occurrences of $f(R_i')$ that exists in Q or not. If the count is less than the threshold, the authentication stage is aborted, and the device is declared to fail the authentication. The authentication failure can occur in two circumstances. The PUF is drastically changed that it can no longer be authenticated or captured by an adversary.
- On the other hand, when the count of $f(R_i')$ is greater than t. We compute secret using any of t responses such that $f(R_i')$ exists in Q.

$$S = \sum_{i=1}^{t+1} f(R_i') \prod_{j=1, j\neq i}^{t+1} \frac{R_j' - X}{R_j' - R_i'}$$

- The base station evaluates Hash(S) and compares it with Hash(a_0) stored in the memory. If Hash(S) equals Hash(a_0), authentication is successful, else authentication request fails.

IV. Results & Discussion

This section evaluates and compares our suggested protocol's performance to that of existing state-of-the-art research. The operation times of UAVs were investigated using a Raspberry Pi 3B device. On a Mac OS (1.8 GHz Dual-Core Intel Core i5, 8 GB 1600 MHz DDR3) computer, the base station actions were analysed. In our system model, we utilise a Raspberry Pi 3B to imitate UAVs and execute typical mathematical and cryptographic operations like as XOR, pseudo-random number generation (PRNG), hash (SHA-1), HMAC (SHA-1), and concatenations.

Figure 3 illustrates the comparison of the total time taken for the execution of our proposed protocol with the protocols in [19, 21, 22]. While [19], [21], [22] have computation costs of $394\mu s$, $355\mu s$, $525\mu s$ respectively, our protocol has a cost of only $223\mu s$. Thus we show how the proposed model is far more superior to state-of-the-art.

V. Conclusion

We described a secure authentication system for unmanned aerial vehicles (UAVs) that we created throughout this article. The suggested approach employs a Shamir Secret Key sharing mechanism to ensure that the protocol continues to work even when PUF values are subject to change due to external influences. The proposed protocol, which employs Physical Unclonable

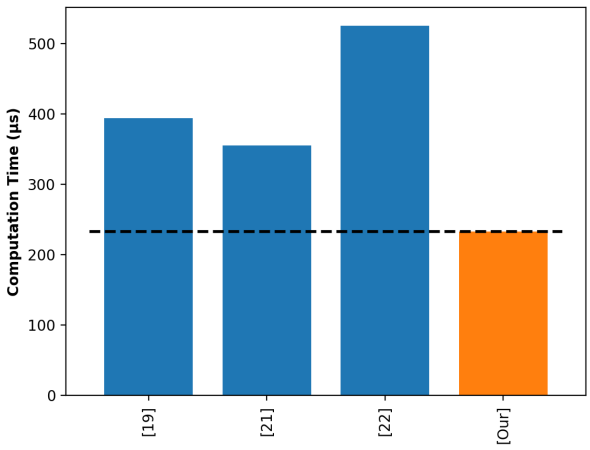

Fig. 3. Comparison of Total Authentication Time

Functions, provides physical security while resisting man-in-the-middle, replay, and denial-of-service attacks. We demonstrate via simulations that the proposed protocol outperforms existing state-of-the-art protocols in terms of computation time while being the only one that can customize to give multiple degrees of security depending on network administrator demands.

References

[1] 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.

[2] 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.

[3] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2014.

[4] D. Rudinskas, Z. Goraj, and J. Stankūnas, "Security Analysis of Uav Radio Communication System," *Aviation*, vol. 13, no. 4, pp. 116–121, 2009.

[5] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[6] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution

architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[7] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.

[8] S. Garg, K. Kaur, G. Kaddoum, P. Garigipati, and G. S. Aujla, "Security in iot-driven mobile edge computing: New paradigms, challenges, and opportunities," *IEEE Network*, 2021.

[9] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. F. Alhamid, "An intelligent uav based data aggregation algorithm for 5g-enabled internet of things," *Computer Networks*, vol. 185, p. 107628, 2021.

[10] A. Birk, B. Wiggerich, H. Bülow, M. Pfingsthorn, and S. Schwertfeger, "Safety, security, and rescue missions with an unmanned aerial vehicle (uav)," *Journal of Intelligent & Robotic Systems*, vol. 64, no. 1, pp. 57–76, 2011.

[11] 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.

[12] 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.

[13] 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.

[14] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on uav network," in *2017 First IEEE International Conference on Robotic Computing (IRC)*. IEEE, 2017, pp. 393–398.

[15] G. Bansal and B. Sikdar, "Location aware clustering: Scalable authentication protocol for uav swarms," *IEEE Networking Letters*, 2021.

[16] G. Bansal and B. sikdar, "S-maps: Scalable mutual authentication protocol for dynamic uav swarms," *IEEE Transactions on Vehicular Technology*, 2021.

[17] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight authentication and attestation scheme for in-transit vehicles in iov scenario," *IEEE Transactions on Vehicular Technology*, 2020.

[18] H. Nicanfar, P. Jokar, and V. C. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *2011 IEEE PES Innovative Smart Grid Technologies*. IEEE, 2011, pp. 1–8.

[19] 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.

[20] 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.

[21] 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.

[22] 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.