CIS-TC Newsletter

Communications and Information Security Technical Committee

http://cis.committees.comsoc.org/

Issue 10 – December 2022

Contents

MESSAGE FROM THE CHAIR

Dear CISTC Members,

I would like to sincerely welcome you to the present issue of CIS-TC Newsletter. Due to the global pandemic since 2020, our CIS-TC meetings have been virtual events for 6 times, hope we can move back to in-person TC meetings in 2023. While we cannot have in-person meetings in the past 3 years, our Newsletter has already been served as one of essential ways to reshape relationships within our communities via a wider and more structured social internetworking. Thanks to our Newsletter Chair, Professor Francesco Chiti, great effort, our Newsletter has become an open and inclusive platform for our TC members. Please feel free to send us any scientifical, technical contributions or even news that you believe could be beneficial to our community. I do hope you will enjoy in reading this Issue.

Finally, let me conclude this message wishing you and your loved ones, on behalf of all the CIS-TC Officers, peaceful and healthy season holidays together with a renewed and prosperous 2023.

Sincerely,
Rongxing Lu
Chair of CIS-TC

CISTC OUTSTANDING SERVICE AWARD 2022

The Award Committee chaired by Professor Francesco Chiti, with unanimous consent decided to give CIS-TC Outstanding Service Award 2020 to Professor Abderrahim Benslimane at University of Avignon (France) for "his excellent contribution to security field, to ComSoc and to CISTC, where he has been Secretary, Vice-Chair and Chair".

The Committee congratulate with the Awarded and he will be awarded during the CIS-TC meeting held at Globecom 2022 in Rio de Janeiro (Brasil).

CIS-TC Newsletter
Communications and Information Security Technical Committee
http://cis.committees.comsoc.org/

Abderrahim Benslimane *[Senior Member, IEEE] received the B.S. degree in computer science from the University of Nancy, Nancy, France, in 1987, the DEA (M.S. degree) and the Ph.D. degree in computer science from the Franche-Comte University of Besanon, Besanon, France, in 1989 and 1993, respectively. Since 2001, he has been a Full Professor of computer-science with the Avignon University, Avignon, France. He is currently the Vice Dean of the Faculty of Sciences and Technology and the Head of the Master Degree SICOM, Communicating Systems. He has been nominated in 2020 as IEEE VTS Distinguished Lecturer. He has the French award for Doctoral supervision and Research during 2017–2021. Since September 1994, he has been as an Associate Professor with the University of Technology of Belfort-Montbliard, Belfort, France. He has more than 220 refereed international publications, such as books, conference proceedings, journals and conferences, and more than 20 Special issues. All publications are in his research topics. He supervised more than 20 Ph.D thesis and more than 40 M.Sc. research thesis. He was the recipient of the title to supervise researches (HDR 2000) from the University of Cergy-Pontoise, Cergy, France. He has been nominated IEEE ComSoc Steering Chair of Multimedia Communications TC during 2022–2024 and was the Vice Chair during 2020–2022. During 2017–2019, he was the past Chair of the ComSoc Technical Committee of Communication and Information Security. He is the EiC of Inderscience International Journal of Multimedia Intelligence and Security (IJMIS), the Area Editor of Security in IEEE Internet of Things journal, the Editorial Member of IEEE Transaction on Multimedia, IEEE Wireless Communication Magazine, IEEE System Journal, Elsevier Ad Hoc Networks, Springer Wireless Network Journal, and the Past Area Editor of Wiley Security and Privacy journal during 2017–2019. He has been the Co-Founder and is the General-Chair of the IEEE WiMob since 2005 and iCOST and MoWNet international conference since 2011.*

FEATURED TOPICS

"Blockchain-based Authentication on IoD"

Julio C. Pérez-García[1] and Abderrahim Benslimane[1]

[1]Laboratoire Informatique d'Avignon (LIA), Avignon University, Avignon, France.

Abstract—The Internet of Drones (IoD) manages and coordinates communications among drones in the Internet of Things (IoT) applications. Ensuring security and privacy in Unmanned Aerial Vehicles (UAV), i.e., Drones, networks is critical to protecting data from cyber-attacks. Providing authentication in this context is challenging because drones are energy-limited devices, given that they are powered by batteries, which are shared for flight functions, communication, and onboard processing. Blockchain technology allows for addressing the problem of centralizing existing authentication protocols. New secure and efficient authentication protocols relying on Blockchain to store, manage and control drone authentication should be proposed.

Index Terms: Authentication, Blockchain, µTesla, UAV, IoD

I. INTRODUCTION

Unmanned Aerial Vehicles have been essential allies in preserving social distance during the fight against the COVID-19 pandemic. Drones allow access to hard-to-reach places with low energy, time, and manpower consumption. As a result, drone applications have expanded rapidly in various branches of human development, ranging from rescue operations or agriculture to military applications.

The Internet of Drones (IoD) paradigm is a layered network architecture that coordinates and manages communications among drones. Given the economic and social losses that could result from the leakage of information in most IoD applications, it is essential to preserve the security and privacy of the data exchanged by drones. In particular, authentication of legitimate IoD devices is a very important feature.

Drones have limited power, computational, and storage resources. The battery is used simultaneously for flight functions and to power communications and onboard processing systems. These limitations, combined with the high mobility of drones, make ensuring authentication a significant challenge. Therefore, optimizing the power and time consumption of authentication protocols maximizes flight time and the level of operability in the missions.

Authentication is generally addressed through a centralized solution, where digital certificates are issued by a Certificate Authority (CA). Conventional centralized solutions have scalability issues as the network expands. In addition, they often have a single point of failure, being susceptible to disruption in the event of denial of service attacks (DOS) or technical failures.

Taking into account the drawbacks of centralized solutions, several authentication protocols, assisted by Blockchain technology, have been proposed in the literature to tackle the centralization and security issues

of typical solutions. Blockchain is a Distributed Ledger Technology (DLT) in which data is recorded with immutable cryptographic properties. The information is stored in blocks, which are stored on all nodes of a peer-to-peer network. Peers do not need to trust each other and maintain a local copy of a ledger. A consensus algorithm, developed by the peers, is responsible for adding new data blocks to the Blockchain, in a distributed manner, among the peers in the network.

A. Research Motivation

Most communications in IoD networks are conducted over a public channel in a broadcast fashion, so it is required to authenticate all source devices in the network for all messages during the communication. In addition, due to the high mobility of drones, it is possible to lose some packets during communication, and also drones can change from one cell (domain) to another. Thus, the authentication protocol must consider possible handover, operate in a distributed manner, and support packet losses.

Given the limitations of drones and the fact that many IoD applications are sensitive to delays, it is essential that the authentication protocol is efficient in terms of energy consumption, authentication time, and computational complexity. Several existing works have proposed authentication protocols for IoD networks. However, they are still not robust enough against packet losses and possible handovers during communication, and in some cases are vulnerable to specific attacks.

II. RELATED WORKS

A. Security Requirements of Broadcast Authentication

The main objective of attacks on IoD networks, as in other networks, is to gain access and modify messages to satisfy an attacker's purpose. On the other hand, attacks on drones, compared to typical cyber-attacks usually occur due to serious design flaws and a lack of wireless security protection mechanisms. Given the high number of reported IoD attacks, it is necessary to classify them in order to explore their effects in detail and find solutions to them. Fig. 1 shows different types of IoD network attacks with different targets. A detailed explanation of such attacks can be found in [1].

Broadcast communications are critical in many applications because multiple receivers can be reached with the same packet, enabling rapid and efficient information exchange. Unfortunately, packet injection attacks and eavesdropping are easy to implement in a wireless environment, hence source authentication is necessary to avoid these security issues.

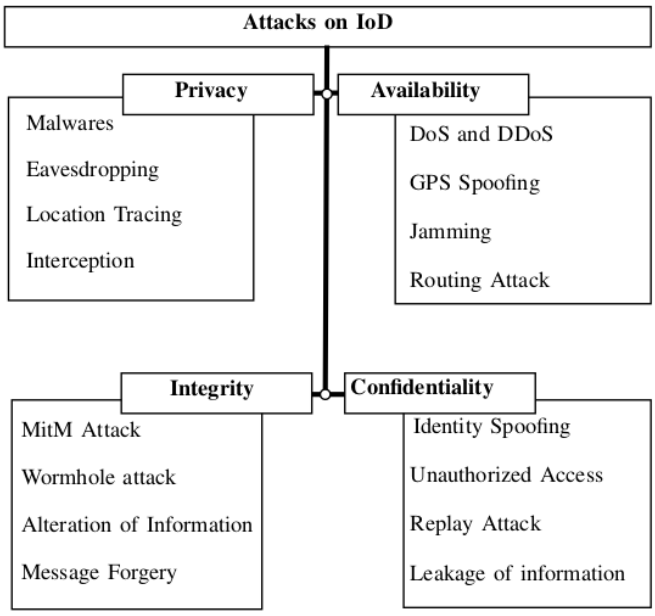

Figure 1. Typical attacks on IoD Networks

In the context of IoD, an authentication scheme should provide resilience against various attacks. Most point-to-point solutions are not secure against these attacks in broadcast transmissions and in some cases are not efficient enough. In IoD networks, authentication schemes must consider their dynamic and heterogeneous nature, as well as the resource constraints of drones. Therefore, it is necessary to authenticate the source of broadcast packets efficiently. A broadcast authentication protocol in IoD networks must meet the following performance and security requirements:

- Secure and attack-resistant
- Low computational cost for generation and verification of authentication information
- Low communication overhead, and robust to packet loss and handover
- Scalable for a large number of receivers
- Decentralized architecture

B. Centralized Authentication

Several protocols have been proposed in the literature for authentication in IoT and IoD networks that present a centralized

architecture. Deploying the standard point-to-point authentication mechanism only, (e.g., adding a message authentication code (MAC) to each packet, computed using a shared secret key), does not allow secure broadcast authentication.

The problem is that any receiver with a secret key can forge the data and impersonate the sender. Consequently, solutions based on asymmetric cryptography are preferred to avoid this problem; a digital signature scheme is an example of an asymmetric cryptographic protocol to achieve authentication.

For the management of secret keys used in digital signatures, authentication protocols often use public key infrastructures (PKI), i.e., asymmetric cryptography, or symmetric cryptographic solutions. In [2], an authentication protocol based on public key cryptography is presented, proposing a privacy-preserving authentication scheme with the help of Mobile Edge Computing (MEC). In their solution, an RSA inspired digital signature is applied for message integrity checking and, as a result, their scheme is secure although computationally expensive.

Elliptic curve cryptography (ECC) has shown to be more efficient than other schemes, e.g., RSA-based since the same security levels are obtained with lower bandwidth consumption and computational cost. In [3], an ECC-based authentication scheme for UAV networks is proposed to enable bidirectional identity authentication between drones. In [4], the authors create a scheme with mutual authentication (Mutual authentication Direct anonymous attestation MA-DAA), which is designed considering the limitations of low bandwidth and computational capacity of UAV networks. In [5], Hyperelliptic Curve Cryptography (HECC) is used to present a certificate-based access control and key agreement scheme for Flying Ad hoc Networks (FANETs), demonstrating the feasibility in terms of computational costs, security features, and functionalities of the proposed solution.

In any case, traditional PKI management is generally complex, certificate handling and maintenance costs are high, and certificates contain redundant information, which is not favorable for transmission in a low-bandwidth network environment or on devices with little storage. The cross-certification management is often used among multi-domain CAs, which is not in favor of the rapid construction of the cross-domain trust system. Therefore, solutions based on symmetric cryptography are generally preferable when devices are limited.

In [6], the Timed Efficient Stream Loss-tolerant Authentication (Tesla) protocol is introduced. Tesla allows all receivers to check the integrity and authenticate the source of each packet in broadcast data streams. Tesla does not require trust between receivers, uses low-cost computational operations at both the sender and receiver, and can tolerate any level of loss without retransmissions. The Tesla protocol achieves asymmetric properties by delaying the disclosure of secret keys, even though it is based on a symmetric message authentication protocol (MAC).

Perrig et al. proposed µTesla in [7], designed for resource constrained networks. This protocol communicates the initial key in the key chain to all receivers, reducing the size of transmitted packets compared to Tesla, and saving time and energy. In addition, it restricts the number of authenticated senders by not storing the one-way key chain in all the nodes. Unlike the original Tesla, where a digital signature is used for initial packet authentication, it instead sends the initial key commitment to all receivers by unicasting.

Traditional PKI configurations are mostly centralized and, despite being well established, face some security issues, such as malicious certificates that could be undetected and allow attackers to impersonate a user through a man-in-the-middle attack. Centralized services in turn present the problem of a single point of failure, which makes them vulnerable to Denial of Service attacks or technical failures that could disable the network. In addition, centralized solutions present scalability problems due to the deterioration in performance when the number of users that the server has to serve simultaneously increases. That is why in recent years distributed solutions have gained the attention of academia and industry. The following section presents some existing works where distributed solutions to the authentication problem are proposed, specifically those based on Blockchain.

C. Blockchain-based Authentication

A Blockchain is essentially a distributed ledger on a peerto-peer network that allows transactions, and any other data, to be securely stored and verified without the need for any centralized authority. The information is stored in blocks and each block is linked to the immediately preceding block through a hash pointer. Thus, it is impossible to modify a block without being detected, since the hash value of the modified block is significantly different from that of the same block without modifications. Moreover, since the Blockchain is distributed among all peers in the network, any local change made by a dishonest node to the data in a block can be easily discovered by other nodes in the network.

Every new block of information is added to the existing Blockchain through a consensus protocol developed by all peers in the network. The consensus protocol allows validating the trustworthiness of the block in a decentralized and untrusted peer-to-peer environment, without requiring a trusted third party. In summary, Blockchain technologies are decentralized, fault-tolerant due to multiple copies of information, immutable, and allow traceability and auditability of stored transactions.

Blockchain has been applied to distribute services in applications where traditionally a centralized trusted entity is required to create and maintain records. It replaces trusted entities with a publicly verifiable,

tamper-proof, peer-to-peer distributed data store that maintains its integrity using various consensus protocols. Several works employ Blockchain to store, query, and verify the validity of the identity and public key of devices (users), or some representation, e.g., hash, of them. Using Blockchain alleviates PKI management without a third party while ensuring the security and privacy of the system [8].

In [9], practical challenges in building PKI systems based on smart contracts are studied. Providing a complete and formal security proof of the RSA-based smart contract PKI, which had been presented by the authors themselves in previous works. In [10], a Blockchain-assisted secure authentication and key agreement and cross-domain key agreement mechanism are presented in the context of industrial IoT (IIoT). Specifically, consortium Blockchain is introduced as a trusted platform for sharing domain-specific information. In [11], a secure user authentication system with fine-grained access control is proposed for Industry 4.0 applications.

These protocols proposed for IoT are generally lightweight and could be easily adapted to IoD networks. However, recently, novel authentication protocols for IoD have been proposed. In [12], a secure and low latency authentication of drones using Blockchain-based security is addressed. The proposed architecture provides a transparent and efficient mechanism for data security as well as the secure migration of drones between different zones.

In addition, a cross-domain authentication scheme for 5G-enabled UAVs based on Blockchain is proposed in [13]. The identity of each drone is dynamically managed by applying a multi-signature smart contract. Entities from different domains can authenticate each other without knowing their true identities. The Blockchain enables security auditing and the establishment of an accountability mechanism for the involved entities.

Table I
COMPARISON OF AUTHENTICATION SCHEMES

Req.	[5]	[14]	[15]	[16]	[11]	[17]	[18]
EA	●	●	●	●	●	●	●
DII	●	●	●	●	●	●	●
DIF	●	●	●	●	●	●	●
ESL	●	●	●	●	●	●	●
MITM	●	●	●	●	●	●	●
DoS	●	●	●	●	●	●	●
Des	○	●	●	●	●	●	●
SKB	○	●	○	○	○	○	○
HA	○	○	○	○	○	○	●
MLT	○	○	○	○	○	○	○

● Provides ○ Does not provide

Requirements: **EA:** Eavesdropping Attack, **DII:** Drone Identity Impersonation, **DIF:** Drone Identity Forgery, **ESL:** Ephemeral Secret Leakage Attack, **MITM:** Man-in-the-Middle Attack, **DoS:** Denial of Service Attack, **Des:** Decentralization, **SKB:** Symmetric Key Based, **HA:** Handover Authentication, **MLT:** Message Loss-Tolerant.

Based on the above literature review, we observe that many practical authentication mechanisms have been designed for IoT and specifically for UAV networks. Most of them consider the privacy preservation of the participants and successfully resist different attacks caused by internal or external attackers, while they are suitable for authentication for resource constrained devices due to their computational efficiency. However, not all of these solutions offer resistance to the packet losses that occur in wireless networks and to the possibility of handovers, either due to technical problems or mobility. Table I overviews these solutions, highlighting their differences in terms of the security requirements provided (or not) by these existing protocols.

III. BROADCAST AUTHENTICATION WITH µTESLA-INSPIRED BLOCKCHAIN

This section presents a Blockchain-based authentication scheme that is under revision in IEEE IoT Journal. In this solution, we adapt µTesla to be used in an IoD scenario. We present the considered network architecture and the processes involved in the proposed protocol, which include configuration, drone registration, communication authentication, and authentication revocation. In this model the Blockchain stores the information necessary for the authentication of each entity in the network, so we consider a private Blockchain that anyone can access but only registered GS can add new blocks. In the blocks, the information for validating the authentication of each drone as well as the data for synchronization and other protocol processes will be stored. Like in [9], smart contracts are used in our solution to achieve automation of all Blockchain services. The following subsections describe the network architecture and discuss some of the building blocks used in the proposed scheme.

A. IoD Network Scenarios

A classic IoD network architecture is shown in Fig. 2, in which drones coexist in different flight zones. These zones may represent different domains, zones in a smart city, or sectors in a disaster zone. Generally, drones can communicate with each other and with a Ground Station (GS) through broadcast messages, as long as they are in the same zone. Each GS is responsible for controlling and managing the drones, including the processes of registration, authentication revocation, handover management, and drone communication with the Blockchain. Generally, in each flight zone, there is at least one GS with which the drones flying over that zone can communicate, and in turn, the GSs communicate with each other through the P2P network provided by the Blockchain.

Most drones are limited in terms of energy, processing, and storage capacity. On the other hand, GSs are provided with much more computational and energy resources than drones, then could be a good idea that those entities carry out the Blockchain storage and maintenance, using the Fog and Edge computing paradigms.

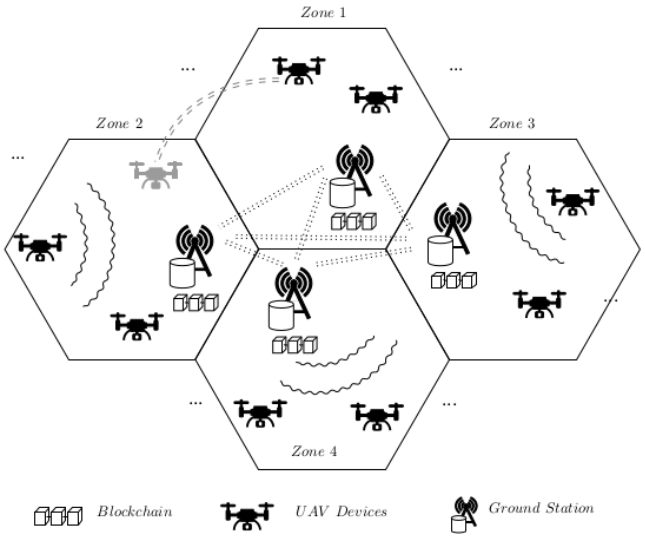

Figure 2. Blockchain enabled IoD Architecture

In this scenario, Blockchain could store the information necessary for the authentication of each entity in the network, a private Blockchain is suitable for that purpose, thus, anyone can access the Blockchain information but only registered GS can add new blocks. Smart contracts could be used to achieve automation of all Blockchain services.

B. One-Way cryptographic Hash Functions

Hash functions are an important cryptographic primitive and are widely used in security protocols to guarantee the integrity of information. They compute a digest of a message that is a short, fixed-length string of bits. For a particular message, the message digest, or hash value, can be thought of as the fingerprint of a message, i.e., a unique representation of a message. A small change in the input string results in a completely different output string. One-Way cryptographic Hash Functions were defined in [5] as follows.

Definition 1. A cryptographic One-Way hash function $\mathrm{H}: \{0,1\}^{*} \rightarrow \{0,1\}^{\mathrm{n}}$ is a deterministic function that produces a fixed length output string of n bits against a variable length input string.

A cryptographic One-Way hash function must have some properties such as:

1) The hash value is easy to compute: so that it is computed quickly and its hardware implementation cost is low.

2) Preimage resistance or unidirectionality: for a given y it is computationally impossible to find a value x such that $\mathrm{H}(\mathrm{x}) = \mathrm{y}$.

3) Preimage resistance or weak collision resistance: for a given x and $\mathrm{y} = \mathrm{H}(\mathrm{x})$ it is computationally impossible to find a value $\mathrm{x}' = \mathrm{x}$ such that $\mathrm{H}(\mathrm{x}') = \mathrm{H}(\mathrm{x})$.

4) Collision resistance or Strong collision resistance: it is computationally impossible to find two distinct values $x' \neq x$ such that $H(x') = H(x)$.

C. µTesla Authentication

µTesla improves the performance of the Tesla protocol, making it possible to implement it in devices with limited resources. µTesla is lighter because of the elimination of digital signatures, which are computationally expensive. The main idea of µTesla is to broadcast an authenticated packet through a MAC protocol and a small period of time later publish the key used to compute the MAC. In this way, it is impossible to forge the broadcast packets before the key is published.

Figure 3 shows an example of µTesla, first, the sender generates a sequence of secret keys (or key chain), for which it chooses the last K_n key randomly and generates the remaining values by successively applying a one-way function H, that satisfies Definition 1. Hence, the key in the interval i can be obtained by applying i times the function H to K_1 , i.e., $K_i = \mathrm{H}^{\mathrm{i}}(K_1)$. The one-way function gives the key chain the characteristic that anyone can compute in one direction, it is impossible

to compute $K_1, K_1, K_2, \ldots, K_{j-1}$ for a given K_j , but it is easy to compute in the other direction, i.e., $K_{j+1}, Kj +_2, \ldots, K_N$ for a given K_j.

The time is divided into intervals of equal length (T_{slot}) and the sender associates each key of the one-way key chain with a time interval. In this way, the sender uses the key K_i in the interval i to calculate the MAC code of all the packets in this interval. However, in order for the receivers to verify the MAC code of each received packet q in the interval i (P_i^q), they must eventually know the key K_i . The Sender publishes K_i during the next interval, after some time (τ) has elapsed, then the receivers can verify the packet Piq without the risk of impersonation attack since the Sender uses in this interval the key K_{i-1} to calculate the new packet.

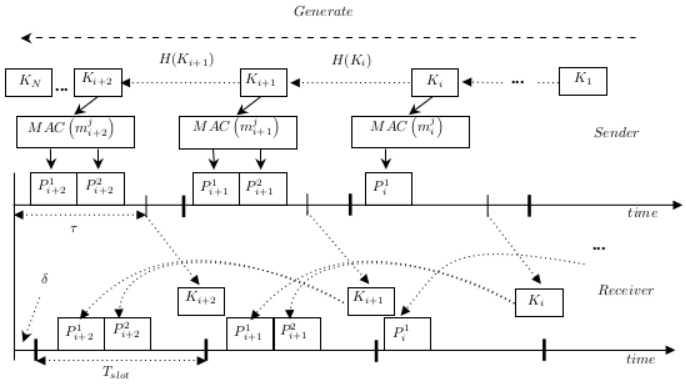

Figure 3. µTesla Authentication Protocol

For µTesla to work properly requires that the sender and receivers are synchronized in time and that the receivers know the key distribution scheduling. µTesla does not require a strong synchronization, some error is permissible without affecting the protocol, but it is necessary to choose a time delay interval in the key revelation (τ) that is greater than any round-trip time between the sender and receivers in the network and the possible synchronization error (δ).

Weak time synchronization as the authenticated key chain commitment is established in µTesla by a mechanism that provides strong freshness and point-to-point authentication [7]. For this purpose when joining the network each receiver sends a random nonce (N_A) in the request packet to the sender (D_{REQ}). The sender responds with the message (T_S |K_i |T_i |T_{slot} |τ) and its corresponding MAC, which contains its actual time (T_S)(allowing synchronization), the corresponding key (K_i) of the one-way key chain for interval i, and the start time (T_i) of the interval i, the duration of a time interval (T_{slot}), and the disclosure delay (τ). Note that those last three values are sufficient to determine the timing of key disclosure unambiguously.

D. Setup and Registration

In this phase, the public parameters for the subsequent authentication process are generated and all drones must be registered to obtain the Blockchain-assisted authentication services in the respective flight zones. System setup: In this phase each drone is prepared for a specific mission, it happens offline and without the risk that any attacker can have access to the data generated during the course of the mission. Before each mission, the user who owns a drone must generate a hashchain of length N in a similar way as in µTesla. The following procedure is followed to perform this computation.

1) Choose a random number K_N of 128 bits from the set $\{1, 2, \ldots 2^{128} - 1\}$ as private key.

2) Choose a cryptographic One-Way hash function H (see Definition 1), which meets the properties discussed in Section III.B.

3) Compute and store $K_i = \mathrm{H}^{\mathrm{i}}(K_N), \mathrm{i} \in (1, \mathrm{N})$, where K_1 will be the first value to be stored in the blockchain doing public key functions.

Note that this process does not consume power from the drone because it can be executed on another computing medium, e.g., laptop, or with the drone on the ground, the battery charge can be completed again. Once the key chain has been stored in the drone and the mission has been programmed, it proceeds to register it in the Blockchain through one of the GS.

Registration: The drone owner must receive through a secure channel a unique identifier, i.e., pseudonym, from the GS and send the information generated in the Setup phase, i.e., K_1 , H. When the GS receives and validates this information, it invokes the smart contract Register UAV, thereby creating a new entry in the list of Registered drones (WL, White list), once validated and included in the Blockchain of all GS, the drone can start the mission in any area. The keys of each drone can be accessed by a simple query to any of the GSs in the different zones, which is responsible for searching the local copy of the Blockchain and responding to the query.

E. Broadcast Authentication

Once the mission of each drone starts, all sent packets will be authenticated by a MAC code added to each message. As in µTesla, in each time slot i a different key K_i will be used to calculate the MAC code of all messages transmitted by the drone during this time slot. Fig. 4 shows an example of the authentication protocol of a packet Pi sent by the drone A.

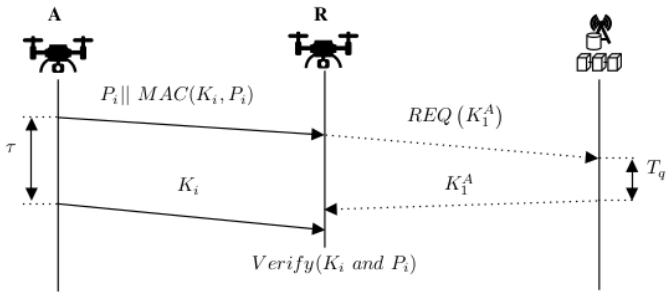

Figure 4. Blockchain-assisted µTesla Authentication Protocol

When a receiver R receives the packet (P_i), coming from A, with its corresponding MAC, it needs to make sure that the packet could not have been spoofed by an adversary. The threat is that the adversary already knows the key revealed for this time slot and could therefore forge the packet since it knows the key used to calculate the MAC. Therefore, the receiver needs to be sure that the sender has not yet revealed the key that corresponds to an incoming packet, which implies that no adversary could have spoofed the content. This is called the security condition, in which receivers check for all incoming packets.

In addition, each receiver must verify which key corresponds to the current time slot, which is calculated from the last key of the drone A stored in drone R, denoted as K_l^A. The verification process is performed using Algorithm 1. In the case that some receiver has never had communication with the drone A, it must make a request to the blockchain through GS of its zone, which will respond with the value of the key of A stored in the BC in the Registration phase.

Algorithm 1 Authentication Algorithm

Input: t, i, K_i, K_l, P_i, MAC(K_i, P_i)
Output: **bool** A

```
if: t < i * τ                          % Check security condition
    Verify MAC(K_i, P_i)
    if: K_l == F^(i-l)(K_i)            % Key verification
        A = True                       % Successfully authentication
        Store K_i                      % K_l = K_i
    else: A = False
return A
```

IV. FUTURE DIRECTION AND OPEN CHALLENGES

Designing secure and lightweight authentication schemes: In most IoD network-based applications, existing authentication methods suffer from real-time latency issues as well as security vulnerabilities. On the other hand, the computational complexity of cryptographic protocols is a major factor limiting their use in battery-powered and processing-limited UAVs. Therefore, there is a great necessity to propose secure and computationally lightweight authentication schemes.

Effective solutions for intrusion detection and prevention: An adversary can launch different types of attacks in the IoD environment. Therefore, there is a need for efficient intrusion detection and prevention solutions to protect against these malicious attacks which could complement cryptographic solutions for authentication and authorization. Due to the dynamism and heterogeneity of IoD networks, it is a great challenge to design robust intrusion detection algorithms.

Physical Layer Security solutions: While conventional cryptographic techniques have inherent difficulties in managing secret keys, Physical Layer Security (PLS) is a promising solution for secure IoD communication. PLS takes advantage of the randomness in the physical properties of wireless channels. This channel randomness can contribute to communication security by masking the communication in the form of pseudo-noise and it can be used to generate symmetric keys between drones. This technology is computationally efficient which makes it very attractive for application in IoD networks, also benefiting from the channel dynamism caused by the mobility of drones.

V. CONCLUDING REMARKS

Ensuring security and privacy in IoD networks is critical to protect data from cyberattacks. Securing authentication is challenging because drones are power-limited devices and because of the nature of wireless broadcast communications. Blockchain technology could address the drawback of typical centralized solutions for authentication. Blockchain could be used to store, manage and control the cryptographic information needed to authenticate communication between drones. In the future, new decentralized authentication protocols supported by Blockchain are needed, which guarantee security and computational lightness, and are resistant to packet loss and handover present in IoD networks.

VI. REFERENCES

[1] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, “Internet of drones security and privacy issues: Taxonomy and open challenges,” IEEE Access, vol. 9, pp. 57 243– 57 270, 2021.

[2] Y. Tian, J. Yuan, and H. Song, “Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones,” Journal of Information Security and Applications, vol. 48, p. 102354, 2019.

[3] T. Li, J. Ma, X. Ma, C. Gao, H. Wang, C. Ma, J. Yu, D. Lu, and J. Zhang, “Lightweight secure communication mechanism towards UAV networks,” 2019 IEEE Globecom Workshops, GC Wkshps 2019 Proceedings, pp. 0–5, 2019.

[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] M. A. Khan, I. Ullah, N. Kumar, O. S. Oubbati, I. M. Qureshi, F. Noor, and F. Ullah Khanzada, “An Efficient and Secure CertificateBased Access Control and Key Agreement Scheme for Flying Ad-Hoc Networks,” IEEE Transactions on Vehicular Technology, vol. 70, no. 5, pp. 4839–4851, 2021.

[6] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, 2000, pp. 56–73.
[7] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins Security protocols for sensor networks," Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.
[8] L. Wang, Y. Tian, and D. Zhang, "Toward Cross-Domain Dynamic Accumulator Authentication Based on Blockchain in Internet of Things," IEEE Transactions on Industrial Informatics, vol. 18, no. 4, pp. 2858–2867, 2022.
[9] C. Patsonakis, K. Samari, A. Kiayias, and M. Roussopoulos, "Implementing a Smart Contract PKI," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1425–1443, 2020.
[10] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT," IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 942–954, 2020.
[11] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," Journal of Network and Computer Applications, vol. 116, pp. 42–52, 2018. [12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling Drones in the Internet of Things with Decentralized Blockchain-Based Security," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6406–6415, 2021.
[13] B. Liu, K. Yu, C. Feng, and K. K. R. Choo, "Cross-domain authentication for 5G-enabled UAVs: A blockchain approach," DroneCom 2021 Proceedings of the 4th ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, pp. 25–30, 2021.
[14] M. W. Akram, A. K. Bashir, S. Shamshad, M. A. Saleem, A. A. AlZubi, S. A. Chaudhry, B. A. Alzahrani, and Y. B. Zikria, "A Secure and Lightweight Drones-Access Protocol for Smart City Surveillance," IEEE Transactions on Intelligent Transportation Systems, pp. 1–10, 2021.
[15] T. Hewa, A. Bracken, M. Ylianttila, and M. Liyanage, "Blockchain-based Automated Certificate Revocation for 5G IoT," IEEE International Conference on Communications, vol. 2020-June, 2020.
[16] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K. K. R. Choo, "Homechain: A blockchain-based secure mutual authentication system for smart homes," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 818–829, 2020.
[17] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," IEEE Internet of Things Journal, pp. 1–1, 2022.
[18] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones," IEEE Internet of Things Journal, vol. 9, no. 8, pp. 6224–6238, 2022.

FORTHCOMING MEETING

The next IEEE ComSoc's Communication & Information Security TC (CISTC) meeting will be held at IEEE ICC 2023 "Sustainable Communications for Renaissance", 28 May – 01 June 2023 in Rome (Italy).

You are more than welcome to join it and to provide your valuable contribution.

CIS-TC ORGANIZED SYMPOSIA

- *Communications and Information System Security Symposium* – **Globecom2022,** 4-8 December 2022, Rio de Janeiro, Brazil - Hybrid: In-Person and Virtual Conference "*Accelerating the Digital Transformation through Smart Communications*" (https://globecom2022.ieee-globecom.org)
- *Communications and Information System Security Symposium* – **ICC2023**, 28 May - 01 June 2023 - Rome, Italy "*Sustainable Communications for Renaissance*" (https://icc2023.ieee-icc.org)

CIS-TC AFFILIATE CONFERENCES

- **Conference: WiMob 2022**
  - 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2022)
  - October 10-12, 2022, Thessaloniki, Greece
  - http://www.wimob. org/wimob2022/
- **Conference: CITS2022**
  - International Conference on Computer, Information, and Telecommunication Systems (CITS2022)
  - July 13-15, 2022, Athens, Greece
  - http://atc.udg.edu/ CITS2022/
- **Conference: WTS 2023**
  - Wireless Telecommunications Symposium of WTS 2023
  - April 19-21, 2023, Boston, Massachusetts, USA (Virtual Conference)
  - https://www.cpp.e du/~wtsi/
- **Conference: CCCI 2022**
  - International Conference on Communications, Computing, Cybersecurity, and Informatics, (CCCI 2022), October 17-19, 2022, Dalian, China
  - http://atc.udg.edu/CCCI2022/

- **Conference: ITNAC-2022**
  - 32nd International Telecommunication Networks and Applications Conference (ITNAC)
  - 30 Nov – 2 Dec 2022, Wellington, New Zealand
  - https://itnac.org.au/

- **Conference: ICACT 2023**
  - 25th International Conference on Advanced Communications Technology
  - Feb. 19-22, 2023, Pheonix Pyeongcahng, Korea
  - https://icact.org/

- **Conference: ICISCTI 2022**
  - 4th International Conference on Intelligent Systems for Cyber Threat Intelligence (ICISCTI 2022)
  - 13-15 October 2022, Marrakech, Morocco
  - https://iciscti.com

- **Conference: CSNet 2022**
  - 6th Cyber Security in Networking Conference
  - October 24- 26, 2022 (Rio de Janeiro, Brazil)
  - https://csnet-conference.org/2022/