A Review on Authentication Schemes for the Internet of Drones

Muskan Sharma, Bhawna Narwal, and Richa Yadav

Abstract Internet of Drones (IoD) is the newly emerging field of IoT. Over the years, various advancements in IoD have attracted the attention of researchers and engineers. It has very promising applications in various fields like smart city, military, education, medical, industries, etc. Drones being a critical part of IoD have also evolved over time. So, they are equipped with sensors and high-resolution cameras, providing better data with increased accuracy and precision. But, with growing popularity and advancements, they are prone to many security attacks. Day-to-day, the IoD environment faces many attacks like man-in-the-middle, impersonation, drone capture, node tampering, modification, replay, eavesdropping, cloning attack, etc. Hence, there comes a need for authentication schemes that authenticate the network entities before communicating the data. This paper reviews some of the latest authentication schemes on the basis of their network models, proposed scheme, advantages and disadvantages. These schemes work on similar or different network models, but ensure that basic security requirements of the IoD environment are fulfilled. Moreover, along with a comparative report of these existing schemes, a brief about various formal proofs used by these schemes to verify the security of their scheme is also given.

Keywords Internet of drones · Security · Authentication

M. Sharma (✉) · R. Yadav
ECE Department, Indira Gandhi Delhi Technical University for Women, Delhi, India
e-mail: muskan98111@gmail.com; muskan027btece18@igdtuw.ac.in

R. Yadav
e-mail: richayadav@igdtuw.ac.in

B. Narwal
IT Department, Indira Gandhi Delhi Technical University for Women, Delhi, India
e-mail: bhawnanarwal@igdtuw.ac.in

V. Goar et al. (eds.), *Advances in Information Communication Technology and Computing*,
Lecture Notes in Networks and Systems 628,
https://doi.org/10.1007/978-981-19-9888-1_35

1 Introduction

Over the years, we have seen great advancements in various fields ranging from agriculture, and military to industries. The backbone of these advancements is technology comprising newer and more efficient hardware and software designs. In this development, IoT has received significant attention. Internet of Things (IoT) or a network of connected devices gathers huge chunks of data from the environment, stores it and analysis it [1]. This information can then be used in various applications.

Internet of Drones is a recent encroachment in the field of IoT. Similar to IoT, it consists of a network of connected devices where the key role is played by drones. Drones are the ones in direct contact with the environment, they scan, store and deliver the information to fulfil a requirement. Figure 1 represents various applications of IoD.

Drones are an important part of smart city designs. IoD ensures efficient traffic surveillance and real-time notifications, which provides assistance using accidents. Climate monitoring is another benefit that helps in analyzing the environment and provides information about temperature, humidity, rainfall, etc. In rural areas as well, IoD proves to be extremely helpful. Like in the case of agriculture surveillance to look after crops, their regular watering etc. [2].

Along with never-ending applications and advantages, IoD has several security challenges. Since the whole network runs wirelessly, adversaries can attack the communication paths and cause damage to the network.

Various attacks like man-in-the-middle, replay, denial-of-service, etc. occur when an unauthorized person/entity gets access to the network.

Hence an authentication mechanism is very essential in any IoD environment.

An adversary can capture the messages being communicated in the network and then attempt to impersonate an authorised network entity, to affect other entities in the network. Also, drones are prone to drone capture attacks since they are remotely

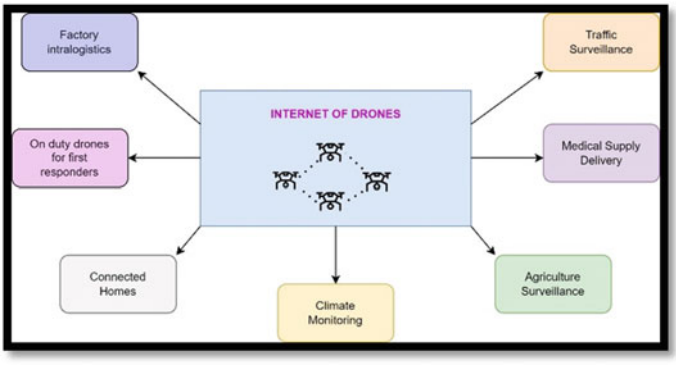

Fig. 1 IoD applications

allocated. And due to the low storage and computational power of drones, there is a need for secure and lightweight authentication schemes.

Over the years, many authentication schemes are proposed with regard to the above-mentioned concerns [2–7]. Researchers have come up with innovative and efficient methods to propose authentication schemes. They have used hash functions, XOR operations, elliptic curve cryptography (ECC) and concatenation operations. Recently, with advancements in technology, schemes have used blockchain and physically unclonable functions (PUFs). Blockchain is basically a chain of blocks, and these blocks are immutable and they store shared information.

They virtually keep track of all the assets of the network. Whereas, the PUF provide a unique fingerprint to every drone, helping in uniquely identifying the drones. It is based on a challenge-response pair. A PUF will generate a response for a challenge passed to it which will be completely different from other PUFs gone through the same fabrication process.

The main objective of this paper is to review the existing authentication schemes for IoD environment. The paper is organized as follows. In Sect. 2, an overview of IoD environment and its network model is discussed. The section also highlights the basic security requirements and formal proofs of an authentication scheme. Section 3 depicts a comparative report of the recent authentication schemes proposed in the field of IoD. Then, the final conclusion along with future scopes is given in Sect. 4.

2 IoD Overview, Requirements and Proofs

2.1 Overview

Internet of Drones (IoD) is a network of drones or Unmanned Aerial Vehicles (UAVs) deployed and controlled by a central authority that is usually named the Ground Station.

These drones are deployed in some remote locations and work on limited battery power. They extract specific information from the environment and transmit it to the ground station or user. Drones are composed of various sensors and high-resolution cameras to collect efficient data. This whole big network and process of transmitting information need to be protected from various security threats. Over years, several security complications have arisen. For example, establishing session-key agreement, authentication, resistance to attacks, and privacy.

A typical network model of IoD is shown in Fig. 2. It contains the entities that are key participants in any IoD environment.

These network entities are as follows:

- **Ground Station (GS)**: It is the central authority of the network. It contains all the databases and secret information about the whole network. It first registers the drones and then allots them to a particular remote location. In case, a user wants

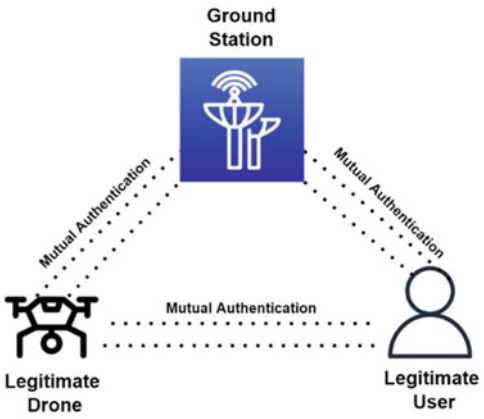

Fig. 2 IoD network entities

to connect with the drone, GS acts as an intermediate. It first authenticates the user and then assigns a drone to it.

- **Drones**: They are the key entities of the IoD environment, they are responsible for getting the most essential part of IoD network, i.e. data. Once deployed, they use their sensors and cameras to capture the required information from the environment and then transmit it to GS or the user.
- **Users**: They are the ones who use the data collected by drones. They can connect with the drone via GS and obtain the required information.

Before establishing the network, drones are registered on the GS and similarly, interested users get themselves registered. Then, in any session, before transmitting data, every entity validates each other using an authentication scheme. In case, any condition in the authentication scheme is not fulfilled, the connection is not established and information is not transmitted.

2.2 Requirements in IoD Environment

Hence, it is essential to design a secure authentication scheme in order to protect the IoD network from any possible attacks. The basic security requirements for an authentication scheme are:

- **Anonymity**: It ensures the identity of sender and receiver remains unknown.
- **Untraceability**: Any message communicated should not reveal anything about the sender and receiver.
- **Mutual Authentication**: Every entity should authenticate that the incoming request is from a legitimate entity. Once confirmed then only it takes respective action.

- **Integrity**: It signifies that the received message remains unmodified and intact. Anonymity and Untraceablity together ensures integrity.
- **Session-key Agreement**: It requires a session key to be established between the user and drone before exchanging the information so that the information remain protected.

2.3 Formal Proofs

After a rigorous review of various authentication schemes, it seems along with fulfilling the above basic requirements, the proposed scheme should also exercise some formal proofs in order to verify its security. There are various proofs being defined over the years like ROR Model, coding simulations, BAN Logic, Boyd etc. But, in this paper, we will review three widely used formal proofs and those are BAN Logic [9], AVISPA Simulations [11] and ROR Model [10].

These are briefly described as follows:

- **BAN Logic**: It is a formal proof that defines certain rules and identities. In order to prove a particular scheme ensures key agreement and mutual authentication, it should pass these rules.
- **AVISPA Simulation**: AVISPA is a software to test cryptographic protocols. All the entities present in the network are represented using objects in code. And respective message communications also need to be coded. Then, on running simulation, it tells whether a particular scheme is safe or not.
- **ROR Model**: It is the most used Model for verification purposes. It actually verifies the security of the session key. It also contains a theorem that is to be proved by exercising certain games. These games are assumed to be played by the adversary in a compromised situation.

3 Comparative Report for Existing Authentication Schemes in IoD

Table 1 shows a brief comparison between the various schemes in terms of the proposed scheme, network model, advantages and disadvantages.

Wazid et al. [3] proposed a scheme for mutual authentication between user and drone. They used hash-function, XOR operations along with fuzzy extractor method. Their scheme is composed of 7 stages. The first stage is a pre-Deployment stage, in which GS generates a unique ID for the drone and stores it in its database with other information. Whereas the drone also stores its ID, GS ID and other information in its memory. Then comes, the user registration stage, for user to be able to access the drone from anywhere, it sends its ID to GS, and GS then creates a pseudo-identity for the user. A fuzzy extractor is used for biometric verification, once the password is

Table 1 Authentication schemes comparison

Ref.	Year	Network model	Proposed scheme	Pros	Cons
[3]	2018	Ground station server, drones, user, control room, Internet	Proposed a secure scheme based on one-way hash-functions and XOR operations using random nonces and timestamps	– Lightweight – Lower cost requirements – Ensures forward secrecy – Security against man-in-middle and replay attacks	– Prone to privileged insider attack – Prone to cloning and node-tampering attacks – Lacks basic security requirements
[4]	2019	Ground station server, drones, user, control room, Internet	Lightweight authentication scheme using one-way cryptographic hash-function and fuzzy extractor	– Ensures three-factor authentication (smart card, password and biometric) – Lightweight – Balances trade-off between storage and cost needs	– Prone to known session key attacks – Prone to cloning and node-tampering attacks
[5]	2020	User, Drone, Ground Station	An authentication Scheme based on creation of session key between user and drone using only one-way hash-function and XOR operations	– Security against impersonation, man-in-middle and replay attacks – Ground Station is secure against server proofing attacks	– Prone to cloning and node-tampering attacks
[6]	2020	Drone, Ground Station	A lightweight authentication scheme for mutual authentication between drone and ground station using only one-way hash-function, XOR operations and PUFs	– Ensures security against cloning and node-tampering attacks – Lightweight – Ensures mutual authentication between network entities	– No formal proof is used to confirm security of scheme – Less practical model
[7]	2021	Ground station server, drones, user, control room, Internet	An authentication Scheme for user-drone communication based on ECC, passwords and biometrics	– Ensures session-key agreement – Ensures security against impersonation attacks – Ensures security against password guessing and lost/stolen user device attacks	– Prone to cloning and node-tampering attacks

(continued)

Table 1 (continued)

Ref.	Year	Network model	Proposed scheme	Pros	Cons
[8]	2021	User, Drone, Ground Station	An authentication scheme proposed using biometrics, passwords, ECC, random numbers, timestamps, cryptographic one-way hash-functions and XOR and concatenation operations	– Ensures all basic security requirements – Secure against man-in-middle, replay and impersonation attacks – Secure against drone capture attack – Secure against modification attack – Secure against password guessing and lost/stolen user device attacks	– Prone to cloning and node-tampering attacks – AVISPA simulation not used for security verification – High-cost requirements

chosen by the user. The exchanged information is stored safely in GS and the user's device memory.

Then, in login phase, user inputs his ID, password and biometric and computations are run to verify the user. If the calculated value matches the stored value, user is authenticated else session is terminated and the login fails. Then, comes the authentication phase, where user first runs certain computational expressions consisting of hash functions and XOR and concatenation operations. And directs certain messages to GS, GS first valid the user and then generates new messages to direct to drone. Similarly, drone validates the incoming messages using stored information in its memory, once verified, drone computes the session key. And directs certain messages to user so that user can also compute the session. It is only when each entity validates the incoming message, it performs further computations. Hence, mutual authentication is ensured.

Last three steps are: Password/Biometric updation, through which user can update his/her password or biometric by first verifying the existing password/biometric, then generating new ones; Dynamic Drone Addition Phase, through this drones can be dynamically be added to IoD network and Drone Key Management, in case two drones need to communicate with each other.

From a security perspective, this scheme is resistant to various attacks like man-in-the-middle, replay, stolen smart device, modification and offline/online password guessing attacks. Moreover, AVISPA Simulations show that this scheme is safe against adversary attacks in a real-life IoD environment.

Srinivas et al. [4]'s proposed scheme also works on the same network model and it consists of 6 stages: pre-deployment, user registration, login and authentication, password/biometric update, revocation and reissue and dynamic node addition. Here, drones are deployed in clusters called flying zones. The first four stages are similar

to [3]. Stage 5 is helpful in case, user's smart device is lost or stolen, the user can contact GS with same ID but different password and the process repeats and the new mobile of the user becomes part of IoD network. This scheme seems quite promising as it overcomes attacks like Known Session Key, modification, impersonation, etc. The security of [4] is proved by ROR Model and AVISPA simulation.

Zhang et al. [5] propose a lightweight authentication scheme using just 4 stages: the set-Up stage, user registration, drone registration and authentication phase. It is centric to establish a key-agreement between user and drone. In the set-Up stage, GS creates a pseudonym for itself and chooses a secret key. Then in user registration, interested user conveys his/her ID and password to GS to get a pseudonym and secret key. GS after certain computations creates a pseudo-identity and pseudo secret key for the user which is visible to the public. Both these things are stored in user's device memory and GS also stores this information with respect to user. A similar thing happens between GS and Drone in the drone registration phase. In authentication phase, Zhang et al. [5] doesn't use anything apart from hash functions and XOR (and concatenation) operations. This is a very effective scheme as apart from resistance against cloning and node tampering attacks, it provides security against impersonation, known session key, modification and many more attacks. Its security is ensured by ROR Model.

Alladi et al. [6] propose a very lightweight authentication scheme with a slightly different network model, it consists of only GS and drones. And it ensures providing mutual authentication between drone and GS as well as between two drones. For implementing the scheme, Alladi et al. [6] uses basic hash functions and XOR, concatenation operations. It uses the latest technology of Physically Unclonable Functions (PUFs) [12–16] which protects the scheme in case of cloning and node tampering attacks. PUF basically assigns uniqueness to every drone. It comprises a challenge-response (C-R) pair, so for every C, there will an R as output. And this R will be unique for every drone given with the same C. PUF has the property that in case, an adversary tries to tamper with the drone, this PUF will be completely unusable and hence adding an extra layer of security to the information stored in the drone's memory.

It assumes that drones have limited storage and power supply whereas GS has unlimited storage and power supply since GS is stationary and drones are in remote locations. It includes three stages: Drone registration, Drone-GS authentication and Drone-Drone Authentication. The drone registration phase is somewhat different from the above-discussed schemes as it uses PUF. So, GS generates a C-R pair for the drone along with a temporary ID. GS stores this information for the drone and the drone stores C, GS ID and its temporary ID.

Then, the authentication process starts post-registration, where R plays the key role. Using substrings of R, XOR, concatenation and hash-functions, a lightweight scheme is proposed with a communication cost of 1600 bits and storage cost of 352 bits. For, Drone-Drone communication, first Drone A authenticates with GS and then GS authenticates Drone B and provides a session key for both drones to communicate with each other. This scheme is resistant to various attacks like eavesdropping, replay,

man-in-the-middle, etc. The security of the scheme is also proved by formal proof of Boyd Logic followed by informal cryptoanalysis.

Hussain et al. [7] proposes an Elliptic curve cryptography (ECC) based authentication scheme for the network model that contains Drones, users, the Internet, Ground Station Server, and Control Room. This scheme is also focused on securing the user-drone communication through computational authentication. It contains around 6 stages. First is the set-Up phase, where GS decides the Elliptical Curve and a base point and announces them publically. Then, in the pre-deployment phase, pseudonym or pseudo-identity is calculated for drone and is stored in its memory. Then a user, who wants real-time data from the data, needs to register with GS. For registration, both password and biometric security are used. Now comes the authentication stage, user first inputs his/her user ID and password and then convey some messages to GS so that GS can validate the user. GS follows the same flow, first verifying the user then computing messages that are to be conveyed to drone. Once, drone receives the messages and verifies them, it generates a session key and sends encrypted messages to user so he/she can also generate the session key. Once, the session key is created by both user and drone, session-key agreement is ensured. The last two steps are biometric/password updation and dynamic drone addition which are already discussed above.

Ali et al. [8] the proposed scheme consists of 4 steps: initialisation, registration, login and authentication and password update. Its network consists of user, drone and ground station. The setUp phase is implemented by GS by selecting a master key and computing the pseudonym for itself. GS uses this master key to compute pseudonyms for users and drones as well. Then, the registration of user and drone is similar to [4] and it uses hash functions, XOR and concatenation operations.

The registration happens via a secure channel whereas the authentication phase happens via a public channel so this scheme like all other schemes makes sure to use pseudonyms in transmitting messages instead of real identities. For password updation, it is interesting to note that user don't require connecting with GS, instead, he/she can do it at their own end.

No matter what technologies are being employed in creating the authentication scheme, its important to fulfil basic security requirements. So, Table 2 shows the comparison based on security requirements.

4 Conclusion and Future Scope

In this paper, recently proposed authentication schemes for IoD were reviewed. A comparative report was provided to emphasize their proposed scheme, network model, advantages and disadvantages. The comparison showed us that every scheme tried to balance the trade-offs and there is no perfect solution. Moreover, since security is a major concern in the IoD environment, the schemes were compared on the basis of security requirements fulfilled. In the coming future, we will get to see more

Table 2 Comparison based on security requirements

Ref.	Anonymity	Untraceability	Mutual authentication	Integrity	Session key agreement
[3]	–	–	–	–	–
[4]	–	–	+	–	+
[5]	+	+	+	+	+
[6]	+	+	+	+	+
[7]	+	+	+	+	+
[8]	+	+	+	+	+

+: Supported; –: Not Supported

secure schemes with much higher security and the incorporation of advanced technologies like machine learning and artificial intelligence to make IoD even more robust.

References

1. Dizdarević J, Carpio F, Jukan A, Masip-Bruin X (2019) A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Comput Surv (CSUR) 51(6):1–29
2. Abualigah L, Diabat A, Sumari P, Gandomi AH (2021) Applications, deployments, and integration of internet of drones (IoD): a review. IEEE Sens J (2021)
3. Wazid M, Das AK, Kumar N, Vasilakos AV, Rodrigues JJ (2018) Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment. IEEE Internet Things J 6(2):3572–3584
4. Srinivas J, Das AK, Kumar N, Rodrigues JJ (2019) TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. IEEE Trans Veh Technol 68(7):6903–6916
5. Zhang Y, He D, Li L, Chen B (2020) A lightweight authentication and key agreement scheme for Internet of Drones. Comput Commun 154:455–464
6. Alladi T, Bansal G, Chamola V, Guizani M (2020) Secauthuav: a novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Trans Veh Technol 69(12):15068–15077
7. Hussain S, Chaudhry SA, Alomari OA, Alsharif MH, Khan MK, Kumar N (2021) Amassing the security: an ECC-based authentication scheme for Internet of drones. IEEE Syst J 15(3):4431–4438
8. Ali Z, Alzahrani BA, Barnawi A, Al-Barakati A, Vijayakumar P, Chaudhry SA (2021) TC-PSLAP: temporal credential-based provably secure and lightweight authentication protocol for IoT-enabled drone environments. Secur Commun Netw (2021)
9. Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc Lond A Math Phys Sci 426(1871):233–271
10. Narwal B, Mohapatra AK (2021) SAMAKA: secure and anonymous mutual authentication and key agreement scheme for wireless body area networks. Arab J Sci Eng 46(9):9197–9219
11. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuéllar J, Drielsma PH, Heám PC, Kouchnarenko O, Mantovani J, Mödersheim S, von Oheimb D, Rusinowitch M, Santiago J, Turuani M, Viganò L, Vigneron L (2005) The AVISPA tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification, pp 281–285. Springer, Berlin, Heidelberg

12. Alladi T, Chamola V, Kumar N (2020) PARTH: a two-stage lightweight mutual authentication protocol for UAV surveillance networks. Comput Commun 160:81–90
13. Gope P, Sikdar B (2020) An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. IEEE Trans Veh Technol 69:13621–13630
14. Pu C, Li Y (2020) lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. In Proceedings of the 2020 IEEE international symposium on local and metropolitan area networks (LANMAN), Orlando, FL, USA, pp 1–6
15. Zhang L, Xu J, Obaidat MS, Li X, Vijayakumar P (2021) A PUF-based lightweight authentication and key agreement protocol for smart UAV networks. IET Commun, 1–18
16. Lei Y, Zeng L, Li Y-X, Wang M-X, Qin H (2021) A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access 9:53769–53785