drones

MDPI

Article

Anonymous Mutual and Batch Authentication with Location Privacy of UAV in FANET

Arun Sekar Rajasekaran [1,*], Azees Maria [1], Fadi Al-Turjman [2], Chadi Altrjman [2,3] and Leonardo Mostarda [4]

[1] Department of ECE, GMR Institute of Technology, Rajam, Srikakulam 532127, Andhra Pradesh, India; azees.m@gmrit.edu.in
[2] Artificial Intelligence Engineering Department, Research Center for AI and IoT, AI and Robotics Institute, Near East University, Mersin 10, Turkey; fadi.alturjman@neu.edu.tr
[3] University of Waterloo, Waterloo, ON N2L 3G1, Canada; cmfaltrj@uwaterloo.ca
[4] Computer Science Department, University of Camerino, 62032 Camerino, Italy; leonardo.mostarda@unicam.it
* Correspondence: arunsekar.r@gmrit.edu.in or rarunsekar007@gmail.com

Abstract: As there has been an advancement in avionic systems in recent years, the enactment of unmanned aerial vehicles (UAV) has upgraded. As compared to a single UAV system, multiple UAV systems can perform operations more inexpensively and efficiently. As a result, new technologies between user/control station and UAVs have been developed. FANET (Flying Ad-Hoc Network) is a subset of the MANET (Mobile Ad-Hoc Network) that includes UAVs. UAVs, simply called drones, are used for collecting sensitive data in real time. The security and privacy of these data are of priority importance. Therefore, to overcome the privacy and security threats problem and to make communication between the UAV and the user effective, a competent anonymous mutual authentication scheme is proposed in this work. There are several methodologies addressed in this work such as anonymous batch authentication in FANET which helps to authenticate a large group of drones at the same time, thus reducing the computational overhead. In addition, the integrity preservation technique helps to avoid message alteration during transmission. Moreover, the security investigation section discusses the resistance of the proposed work against different types of possible attacks. Finally, the proposed work is related to the prevailing schemes in terms of communication and computational cost and proves to be more efficient.

Keywords: authentication; privacy; security; FANET

Citation: Rajasekaran, A.S.; Maria, A.; Al-Turjman, F.; Altrjman, C.; Mostarda, L. Anonymous Mutual and Batch Authentication with Location Privacy of UAV in FANET. *Drones* **2022**, *6*, 14. https://doi.org/10.3390/drones6010014

Academic Editor: Vishal Sharma

Received: 13 December 2021
Accepted: 5 January 2022
Published: 7 January 2022

1. Introduction

Aerial drone technology may be utilized for a variety of reasons to improve our lives due to its rapid invention and modification as well as the shrinking of integrated sensors, CPU processing speed, and widespread connectivity of wireless systems. Moreover, UAVs are known as drones used in numerous applications ranging from civilian to military platforms [1]. There has been a significant improvement in the number of drone applications, as the advancement in drone technology increases. Drone application in the field of the military is boundless, as they are a vital asset on the modern battlefield. Internet-connected drones provide accurate and efficient flying strategies to ensure the quality of service. Using the drone's sensors, the assigning field's physical parameters are collected [2]. In addition, the drone's cameras and microphones transmit real-time video to the service provider or user via a wireless medium. By controlling a drone, a service provider/user can obtain real-time information from a remote location [3]. A drone's data collection poses new security and privacy risks as technology advances.

Manpower is saved when the drones are used to deliver packages via airways. Moreover, for short-distance delivery of goods, drones are very obliging. Drones can be used to record video, which was previously impossible due to the need for expensive aircraft and scaffolding to capture the images. The current pandemic situation can be addressed

with the help of drones as they are used to transport medicine and necessary items to the contaminated zones. The Internet of Drones (IoD) environment helps to monitor crops and provide the required water facilities frequently, thus helping in smart farming. During the occurrence of any natural calamities, drones will be helpful for collecting the required disaster information. Further, drones are used to monitor a large group of people during public meetings/gatherings as a surveillance and to record the data to guarantee public safety. Drones are not only useful for searching operations but also help to rescue a person in danger from war fields and provide them with food, clothing, and medicine. Moreover, the vital role of safeguarding each country's border surveillance can be also performed by drones.

In addition to the above-mentioned applications, a drone's location and other sensitive data are also to be collected and preserved [4]. An adversary can easily intercept the information sent by a drone due to IoD's public, insecure network connection. Wireless networks are more vulnerable to cyber-attacks than wired networks due to their open nature. To reduce this risk in MANET, predominantly in the IoD environment, various approaches based on single or combined security mechanisms have been proposed. Currently, drones face several issues related to security, privacy, and authentication, which makes them an appealing research topic [5]. IoD is susceptible to several kinds of security attacks. Before exchanging confidential data via an unreliable channel, security precautions should be taken [6]. In this paper, drones are used for providing information related to obstruction on pathways in hilly and other highly populated areas. Roadside infrastructure is desperately required for the sake of safety to help quickly transmit and livestream necessary details about the path ahead in real time. Some of the services that drones can provide include monitoring of low-altitude, disaster relief, and data transmission assistance. It is believed that drones have the greatest potential for providing connectivity and solutions because of their ease of access. A blended wireless protocol is used in mountain ranges and rural places where there are weak signals or interferences. Moreover, if any fault occurs in the current existing drone, it should be replaced with another drone exactly at the same position. Hence, the current location of the drone should be preserved from adversaries.

Authentication and privacy are two of the prevalent security issues with IoD communications [7–9]. Drones are attractive targets for adversaries because they are used for sensitive applications. Along with drone data, adversaries may also try to track down geographic location to obtain confidential data. The main challenge is the security between the users and drones during the exchange of information. Due to the open nature of the communication medium, an adversary can read, alter, or respond to the message communicated and send fake information. Moreover, another important vital challenge is to preserve the privacy of the user/drone from an adversary [10]. If the real identity of the drone is revealed, then there may be a possibility for an adversary to perform an impersonation attack and steal the original confidential information of the drone. Though most of the currently existing schemes provide authentication, these are vulnerable to several possible attacks.

Drones are mainly used for aerial surveillance and monitoring operations. During natural disasters and emergency periods, drones play a significant role. The integrity of the collected sensitive data should be preserved without any modification. In addition, privacy of the drone and end user should be preserved. Thus, the main significance of the proposed scheme is that the drone and the end user should be authenticated anonymously without revealing its privacy. Therefore, a simple cryptographic pairing and hashing operations are used for privacy preservation in our work during both mutual and batch authentication. Thus, the computational cost, communication cost, and storage cost are reduced significantly when compared to the prevailing existing works. Moreover, to avoid tracing of the authenticated drones, a location privacy scheme is proposed in this work. The proposed scheme is applicable in the following ways: privacy and anonymity are preserved and the computational cost for verifying a group of drones is significantly reduced. Finally, an intruder will be unable to track the authenticated drones' location.

The research impact of this manuscript are as follows:

- To develop a privacy-preserving anonymous mutual authentication scheme between a drone and a user.
- To authenticate a group of drones anonymously based on batch authentication protocol to reduce the total computational overhead.
- To ensure the privacy of the confidential information from the authenticated drone to the authenticated user.
- To guarantee location privacy for the authenticated drones from an adversary.

The systematic flow of a research article is as follows. Section 2 deals with the related prevailing works which deal with security and privacy. The overview of the entire system is described in Section 3. This section describes the basic system model, bilinear pairing, and security measures of the proposed work. Section 4 explains the proposed scheme. This section explains the initialization of the system, registration of the end-user and drone, key exchange protocol, mutual and batch authentication, integrity preservation, and location privacy. Some conceivable security attacks are described in Section 5. Performance analysis is explained in Section 6. This section deals with the analysis of computational cost, communication cost, storage cost, and drone service providing capability. Finally, Section 7 concludes the work.

2. Related Work

Security and privacy are the major concern in the IoD environment [11–14]. There are many works focused on security issues concerning drones [15], but this work not only discusses the security issues but also focuses on the location privacy of the drones. Turkanovic et al. [16] suggested a mutual authentication framework between the drones and the end-user without the involvement of any third-party node. However, the scheme suffers from several security threats such as the man in the middle attack and the impersonation attack. Amin et al. [17] suggested a strong authentication protocol based on the smart card. However, this scheme suffers from password guessing attacks and damage to smart cards, etc. Challa et al. [18] suggested a signature-based authentication scheme using elliptic curve cryptography (ECC). Though ECC is used in this scheme, this work suffers from increased computational and storage costs for storing the required keys. A certificateless scheme was suggested by Won et al. [19] for the security of drones. In this scheme, three scenarios for communication are taken into consideration. They are one-to-one, many-to-one, and one-to-many communication between drones and smart devices. Moreover, the conditional tracking mechanism is also adopted in this scheme. However, the scheme lacks location privacy and has increased communication cost during batch authentication.

Tai et al. [20] suggested a two-factor authentication scheme. This work is mainly based on user passwords and smart card systems. It generally uses a hash function based on cryptography. However, this work fails to provide resistance against several well-known attacks such as replay attack, privileged-insider attack, etc. Wazid et al. [21] recommended a three-factor authentication scheme. This scheme is based on three parameters such as biometrics, smart card, and password. Though a one-way hash function is used, it lacks conditional tracking and revocability. Yue et al. [22] suggested a technique based on AI for drone surveillance. This work focused on wireless networking protocol. Different features of the drone and the exact location of the drone are traced using this scheme. However, this work does not focus on security issues and latency. Bouman et al. [23] proposed a traveling salesman problem based on a drone. A solution was achieved based on dynamic programming for this problem. The communication cost of this work is significantly lower but it has high computational complexity. Hong et al. [24] suggested a new model of recharging station for the spatial drone. A heuristic algorithm was used in this work which for maximum coverage and to avoid range restriction. There was no analysis regarding the storage cost and security threats. Shavarani et al. [25] proposed an effective method for the delivery of the essential components with less time. A mathematical model based on a biobjective was designed in this work. The drawback of this work

is the non-deterministic polynomial time-hard problem and computational complexity. Aggarwal et al. [26] suggested an authentication scheme based on blockchain topology. The framework focuses on etherem based protocol. Though this work ensures privacy and security, the computational complexity of this work is very high. Huang et al. [27] proposed a new method of implementing the charging stations for the drones. A triangular-based approach was used in this work. Moreover, the charging stations with less or no customers were recursively removed. This work does not focus on the communication and storage cost. Shavarani et al.'s [28] work deals with reducing the transportation cost during the delivery time of the goods by drones. A fuzzy logic-based approach was used in this work. Security and privacy concerns were not discussed in this work. Automated swapping of the battery method was suggested by Cokyasar et al. [29]. This work focused on the selection of optimal automated battery swapping machine location and minimized the delivery cost. Although communication cost was reduced in this work, it increased the computational cost. This work does not deal with major security threats. A secure authentication framework was presented from the human-centered industrial internet of things (IIoT) perspective by Singh et al. [30]. When a node first joins the network, a registration hub generates the required credentials for the node. Moreover, nodes are involved in further complex operations such as mutual authentication, exchange of keys, etc., and the registration hub is no longer required to perform these functions. However, this scheme writhes from hefty computational cost, and there is no location privacy. Tian et al. [31] proposed an authentication protocol that integrates both efficiency and security. This framework relies on a compact online/offline signature layout, and it can be deployed on resource-restricted small-scale unmanned aerial vehicles. Moreover, in this work, due to the high mobility of UAVs, the investigation of an extrapolative authentication approach using mobile edge computing (MEC) was performed to decrease authentication costs for possible authentication accomplishments. However, this work suffers from high computational and storage costs.

Gope et al. [32] suggested a scheme that ensures the physical security of the drone. Physically unclonable function and hash operations are used in this scheme. Though the physical security of drones is ensured, it lacks location privacy. Zhang et al. [33] suggested a compact authentication and key agreement (AKA) scheme that relies solely on a one-way secure hash function where drones and users authenticate one another mutually. Though this scheme is robust to different security threats, it lacks location privacy and physical threats. Ever et al. [34] suggested a secure authentication framework based on ECC. Though several potential attacks were defended using this work, it lacks preservation of the location privacy and involves high communication cost. Hussain et al. [35] proposed a three-factor authentication scheme. This work mainly compares the drawback of Wazid et al. [21] but it involved high computational time. Table 1 shows the summary of the different existing approaches.

Table 1. Summary of different existing approaches.

Existing Works	Publication Year	Techniques	Drawbacks
Turkanovic et al. [16]	2014	One way hash fuction is utilized.	User anonymity is not preserved. Impersonation attack on sensor node is possible.
Amin et al. [17]	2016	Secured authentication protocol for smart card.	Suffers from password guessing attack.
Challa et al. [18]	2017	Signature-based authentication scheme using ECC.	High computational and storage costs.
Won et al. [19]	2017	Secured certificateless scheme. Conditional tracking mechanism.	Lacks location privacy. High communication cost.
Tai et al. [20]	2017	Two-factor authentication scheme	Cannot withstand replay attack and privileged-insider attack.

Table 1. *Cont.*

Existing Works	Publication Year	Techniques	Drawbacks
Wazid et al. [21]	2018	Three-factor authentication. One way hash fuction is utilized.	No mutual authentication. Privileged insider attack and impersonation attack.
Yue et al. [22]	2018	Secured AI-based technique.	Not focussed on security issues. Latency problem.
Bouman et al. [23]	2018	Dynamic programming approach.	Computational cost is high.
Hong et al. [24]	2018	A heuristic algorithm approach.	Lacks security analysis and privacy.
Shavarani et al. [25]	2019	Biobjective mathematical model.	Non deterministic polynomial time-hard problem.
Aggarwal et al. [26]	2019	Authentication scheme based on blockchain topology.	High computational complexity.
Huang et al. [27]	2020	Triangular-based approach.	High communication and storage cost.
Shavarani et al. [28]	2021	Fuzzy logic-based approach.	Lacks security and privacy concerns.
Cokyasar et al. [29]	2021	Automated swapping approach.	Prone to security attacks.
Singh et al. [30]	2019	Secure authentication framework based on IIoT.	High computational cost, and there is no location privacy.
Tian et al. [31]	2019	Secured authentication protocol.	High computational and storage costs.
Gope et al. [32]	2020	Physically unclonable function and one way hash operation is utilized.	Lacks location privacy.
Zhang et al. [33]	2020	Two factor authentication. One-way hash fuction is utilized.	It does not offer untraceability.
Ever et al. [34]	2020	Secure authentication framework with ECC.	High communication cost. Lacks location privacy.
Hussain et al. [35]	2022	Three-factor authentication.	High communication cost.

3. System Overview

In this section, system model, bilinear pairing, and security measures are described in detail.

3.1. System Model

The proposed work's system model comprises of three major entities, namely, trusted server, end user, and drone [36]. Figure 1 portrays the system model of the proposed work. The role of each entity is described as follows.

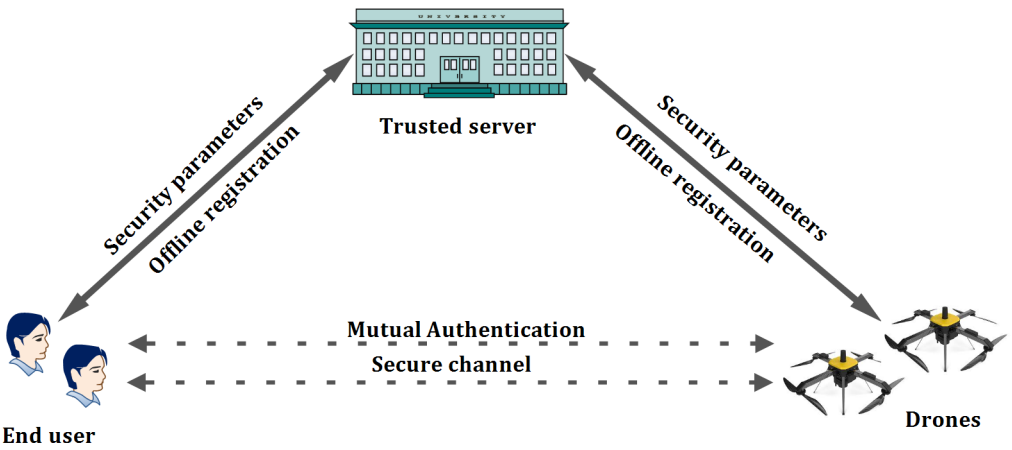

Figure 1. System model of proposed work.

Trusted server (*TS*)

TS is the key entity in our proposed work. Initialization, secret key generation, drone and end-user registrations are performed by *TS*. Moreover, unique keys are generated during the key generation process to avoid collision attacks. Initially, both the drone and the end-user should register to the *TS* through an offline registration. Only after the successful registration, *TS* provides the required credentials to the drone and end-user.

End-user (*EU_i*)

EU_i is the participant in the FANET network. The required credentials for the *EU_i* to participate in the network are provided by *TS*. The *EU_i* is able to communicate with the control device of the drone through the specialized equipment with him. This highly sophisticated equipment of *EU_i* is capable of performing the computational operations efficiently. Moreover, the information collected from the controlling device of the drone is stored in the specialized equipment *EU_i*.

Drone (*D_j*)

The *D_j* is embedded with a control device which has high computational competence. Moreover, specialized sensors are implanted in the controlling device which helps to capture the image of long-distance. The control device of *D_j* is capable of generating the short life session keys during key exchange protocol. In addition, the controlling device of *D_j* is provided with a large storage capability to store the secret keys provided by *TS* during the initial registration.

3.2. Bilinear Pairing

Let G_x, G_y, and G_T be the cyclic multiplicative group of prime order a. Moreover, let $e: G_x \times G_y \rightarrow G_T$ be the asymmetric bilinear map that gratifies the condition

Bi-linearity: $e\left(g_x^p, g_y^q\right) = e(g_x, g_y)^{pq}$, $(g_x, g_y) \in G_x \times G_y$ and $\forall p, q \in Z_a^*$, where $Z_a^* = [1, 2, \ldots, a-1]$

Non-degeneracy: $(g_x, g_y) \in G_x \times G_y$, $e(g_x, g_y) \neq 1$.

Computability: The bilinear map $e: G_x \times G_y \rightarrow G_T$ is computable.

No effective isomorphism between G_x and G_y.

3.3. Security Measures

Four security measures must be met by a proposed system to ensure secure communications in FANET.

Mutual authentication: To protect the FANET system from impersonation attacks, the *EU_i* and controlling device of *D_j* should authenticate each other. Moreover, during the exchange of confidential information from *D_j* to *EU_i*, mutual authentication between vehicle users and RSUs is indispensable.

Exchange of session key: The session key should be shared in an efficient anonymous way between the *EU_i* and *D_j* to maintain confidentiality. Secure communication can be ensured only with the help of the short life session key.

Privacy preservation: The unique identity of *EU_i* and *D_j* should be preserved during the exchange of data. Here, anonymous identity is used during mutual authentication which helps to protect the real identity of both *D_j* and *EU_i* from the adversary.

Performance analysis: This mainly depends on communication and computational cost. The proposed work mainly focuses on a faster message verification time (shorter delay) for the *D_j* with less communication and computational cost.

4. Proposed Scheme

In this article, a proficient anonymous mutual and batch authentication with location privacy is presented. System initialization, *EU_i* registration, *D_j* registration, key exchange, mutual and batch authentication, integrity preservation, and location privacy are the stages in our proposed scheme. Table 2 describes the list of notations and descriptions used in this work.

Table 2. List of notations and abbreviations.

Notations	Explanation
TS	trusted server
EU_i	end user
D_j	drone
G_1, G_2	cyclic multiplicative group
g_1, g_2	generator of groups G_1 and G_2
Z_a^*	non-zero elements of a finite field Z_a, where Z_a^* = [1,2, ... ,$a-1$]
a	prime order
e	asymmetric bilinear map
m	master key for the trusted server
q	private key for the trusted server
α_{ts}	public key for the trusted server
$H : \{0,1\}$	secure hash function
u_j	private key for the end user
α_{eu}	public key for the end user
FID_{eu}	fake identity for the end user
UBK_j	batch authentication key for the end user
∂_f	secret key to trace exact location
d_j	private key for the drone
α_{D_j}	public key for the drone
FID_{D_j}	fake identity for the drone
DBK_j	drone batch key
DTK_j	drone tracking key
T, $T1$	timestamps
$\oplus$	EXOR operation
sk	session key for the end user
c_j	short life private key for drone
e_j	short life public key for drone
φ	x axis (latitude)
λ	y axis (longitude)
h	z axis (altitude)

4.1. System Initialization

The TS selects the master key $m \in Z_a^*$ from a large prime number a. The private key for the TS is chosen as q such that, $\in Z_a^*$, where Z_a^* = [1,2, ... ,$a-1$]. Here, Z_a^* is the non-zero elements of a finite field Z_a and it forms the group under the modulo multiplication a. The corresponding public key for TS is calculated as $\alpha_{ts} = g_1^{m+q}$. Here, G_1, G_2, and G_T are the multiplicative cyclic groups and g_1, g_2 are the corresponding generators of the group G_1 and G_2, respectively. The secure hash function chosen by TS is $H : \{0,1\} \rightarrow Z_a^*$ and the bilinear mapping is given by $e : G_1 \times G_2 \rightarrow G_T$. Then, the TS publishes the parameters (G_1, G_2, g_1, g_2, α_{ts}, e, H, a) as the required credentials after computing $Z = e(g_1, g_2)$.

4.2. EU_i Registration

The EU_i provides his required credentials to TS during his initial offline registration. The genuine credentials provided by EU_i are verified by TS. Once the offline registration is completed, the private key for the EU_i is chosen by TS as u_j from the random number such that $u_j \in Z_a^*$. Moreover, the public key and the fake identity for the EU_i are calculated as $\alpha_{eu} = g_2^{\frac{1}{m+q+u_j}}$ and $FID_{eu} = g_1^{\frac{1}{(m+q)u_j}}$, respectively. To perform batch authentication, the EU_i batch authentication key is calculated as $UBK_j = g_2^{m+q}$. Moreover, to trace the exact location of the D_j, the TS provides the secret key ∂_f, such that $\partial_f \in Z_a^*$ to the EU_i.

4.3. D_j Registration

The TS chooses the private key for the D_j as d_j such that $d_j \in Z_a^*$. Based on the private key, the public key is calculated as $\alpha_{D_j} = g_2^{\frac{1}{m+q+d_j}}$. The fake identity for the D_j is calculated as $FID_{D_j} = \frac{(m+q)^2}{d_j}$. During batch authentication process, to authenticate a large number of drones, the drone batch key and the drone tracking key are calculated as $DBK_j = g_2^{m+q+d_j}$ and $DTK_j = g_2^{-m-q}$, respectively.

4.4. Mutual Authentication

Anonymous mutual authentication must be conceded in an efficient way between the D_j and the EU_i to perform effective communication. The following steps are to be followed.

Step 1: If an EU_i requires a specific service from the D_j, then the EU_i calculates $\gamma = g_1^{u_j}$. Moreover, after calculating the value of γ, the parameters $(\gamma, \alpha_{eu}, FID_{eu})$ are sent to D_j.

Step 2: The controlling device in the D_j checks $e(\gamma.\ \alpha_{ts}, \alpha_{eu}) = Z$. If the condition is gratified, then the EU_i request is accepted, else the request from the EU_i is rejected.

Proof of correctness

$$e(\gamma.\ \alpha_{ts},\ \alpha_{eu}) == e(g_1^{u_j}.\ g_1^{m+q},\ g_2^{\frac{1}{m+q+u_j}})$$

$$= e(g_1^{u_j+m+q},\ g_2^{\frac{1}{m+q+u_j}})$$

$$= e(g_1, g_2) = Z$$

Step 3: Similarly, the controlling device in the D_j calculates the value of $\gamma' = g_1^{d_j}$ and sends the parameters $(\gamma', \alpha_{D_j}, FID_{D_j})$ to the EU_i.

Step 4: Then, the EU_i checks $e(\gamma'.\ \alpha_{ts},\ \alpha_{D_j}) = Z$. If the condition is gratified, the communication with D_j is accepted, else it is rejected.

Proof of correctness

$$e(\gamma'.\ \alpha_{ts},\ \alpha_{D_j}) = e(g_1^{d_j}.\ g_1^{m+q},\ g_2^{\frac{1}{m+q+d_j}})$$
$$= e(g_1^{d_j+m+q},\ g_2^{\frac{1}{m+q+d_j}})$$
$$= e(g_1, g_2) = Z$$

4.5. Session Key Exchange Protocol

In this phase, session key generation request, session key integrity preservation, and session key exchange are discussed. Once the mutual authentication scheme is successfully performed, the key exchange should be carried out between the D_j and EU_i. The session key generation request is carried out as follows:

Step 1: Initially, the EU_i chooses a random number x such that $x \in Z_a^*$ and calculates s_0, s_1 and s_2 respectively, where $s_0 = g_1^{(m+n)u_j}$, $s_1 = \left(FID_{D_j}\right) \oplus x$ and $s_2 = H(s_0 \parallel s_1 \parallel x)$

Step 2: Finally, EU_i sends (s_0, s_2, x, T) to the D_j where T is the timestamp.

Step 3: Initially, the controlling device of D_j checks for the validity of the T, if it holds then the controlling device of D_j calculates $e(FID_{eu}, s_0)$. If $e(FID_{eu}, s_0) = e(g_1, g_1)$, the session key generation request is accepted.

Proof of correctness

$$e(FID_{eu}, s_0) = e\left(g_1^{\frac{1}{(m+q)u_j}},\ g_1^{(m+q)u_j}\right)$$
$$= e(g_1, g_1)$$

Step 4: Moreover, the integrity of session key is verified by checking $s_1' = s_1$. The value of s_1' is calculated by the controlling device of D_j as $s_1' = FID_{D_j} \oplus x$.

Step 5: By using s_1', the value of $s_2' = H(s_0 \parallel s_1' \parallel x)$ is calculated. Thus $s_2' = s_2$, then the integrity is preserved, else request is discarded.

Step 6: Once the session key generation request is accepted and session key integrity is preserved, the session key is generated by the controlling device of D_j as $sk = (FID_{eu})^{d_j}$ and sends $(sk,\ T1)$ to EU_i.

Step 7: The EU_i first checks the validity of the timestamp $T1$. Once, the validity is validated, EU_i checks $(sk)^{u_j.FID_{d_j}} = \alpha_{ts}$. If the condition is satisfied, then the session key exchange is performed between the EU_i and D_j for effective communication of data.

Proof of correctness

$$
\begin{aligned}
(sk)^{u_j \cdot FID_{d_j}} &= \left((FID_{eu})^{d_j}\right)^{u_j \cdot FID_{d_j}} \\
&= \left((g_1^{\frac{1}{(m+q)u_j}})^{d_j} \right)^{(u_j \cdot \frac{(m+q)^2}{d_j})} \\
&= \left(g_1^{\frac{1}{(m+q)u_j}} \right)^{u_j \cdot (m+q)^2} \\
&= g_1^{m+q} = \alpha_{ts}
\end{aligned}
$$

4.6. Batch Authentication

The end user cannot rely on only one D_j for gathering the required information. If the EU_i requires more data, then a greater number of drones should be authenticated at the same time to reduce the computational cost and to increase the performance. The steps involved in batch authentication are as follows

Step 1: Initially, the controlling device of D_j picks a random number c_j as its short life private key such that $c_j \in Z_a^*$. The short life public key is calculated as $e_j = g_2^{c_j}$. Moreover, if there are j number of drones, their short life private keys are calculated as $c_1, c_2, c_3 \ldots\ldots\ldots c_j$.

Step 2: To make an effective communication, the controlling device of D_j calculates $E_j = g_2^{c_j - d_j}$ and $F_j = E_j \cdot DBK_j$ where $DBK_j = g_2^{m+q+d_j}$ is the batch authentication key for D_j.

Step 3: Moreover, the controlling device of D_j computes the $G_j = H(e_j || F_j)$ to preserve the integrity of the confidential information. Then, the quadruple is calculated as $(F_j,\ G_j,\ e_j,\ DTK_j)$, where $DTK_j = g_2^{-m-q}$ is the drone tracking key, and it is sent to the EU_i.

Step 4: To validate the number of individual messages sent by each D_j, the EU_i first checks the integrity of each message by calculating the hash value of F_j and e_j.

Step 5: If the integrity is verified, then the EU_i gathers $F_1, F_2, F_3 \ldots F_j$ as $F = \prod_{i=1}^{j} F_j$. Similarly, $e_1, e_2, e_3 \ldots\ldots e_j$ are accumulated as $e = \prod_{i=1}^{j} e_j$.

Step 6: Finally, EU_i checks $\frac{F}{e} = \left(UBK_j\right)^j$. If this condition is satisfied, then the messages send by j number of drones are batch authenticated.

Proof of correctness

$$F = \prod_{i=1}^{j} F_j = \prod_{i=1}^{j} E_j.DBK_j$$
$$= E_1.DBK_1.E_2.DBK_2 \ldots E_j.DBK_j$$
$$= g_2^{c_1-d_1}.g_2^{m+q+d_1}.g_2^{c_2-d_2}.g_2^{m+q+d_2} \cdots g_2^{c_j-d_j}.g_2^{m+q+d_j}$$
$$= g_2^{c_1+m+q} g_2^{c_2+m+q} \cdots g_2^{c_j+m+q}$$
$$= g_2^{c_1+m+q+c_2+m+q....c_j+m+q}$$
$$e = \prod_{i=1}^{j} e_j = \prod_{i=1}^{j} g_2^{c_j}$$
$$= g_2^{c_1}.g_2^{c_2} \cdots\cdots g_2^{c_j}$$
$$= g_2^{c_1+c_2+....c_j}$$
$$\frac{F}{e} = \frac{g_2^{c_1+m+q+c_2+m+q....c_j+m+q}}{g_2^{c_1+c_2+....c_j}}$$
$$= g_2^{c_1+m+q+c_2+m+q....c_j+m+q-(c_1+c_2+....c_j)}$$
$$= g_2^{(j*m+J*q)} = g_2^{j(m+q)} = (UBK_j)^j$$

4.7. Location Privacy

In case of any energy loss or fault in the current active D_j, it should be replaced by the EU_i. However, the real location of the is anonymous. Therefore, in order to retrieve the actual real location, the TS sends the real location of the D_j to the authenticated EU_i anonymously. To perform the location privacy, the three coordinates of the D_j location are to be known. The three coordinates are generally represented as latitude, longitude, and altitude. Since the D_j is placed at a certain distance from the ground surface, the altitude is to be incorporated as the third coordinate. Figure 2 shows the schematic location of drone in the three-coordinate system.

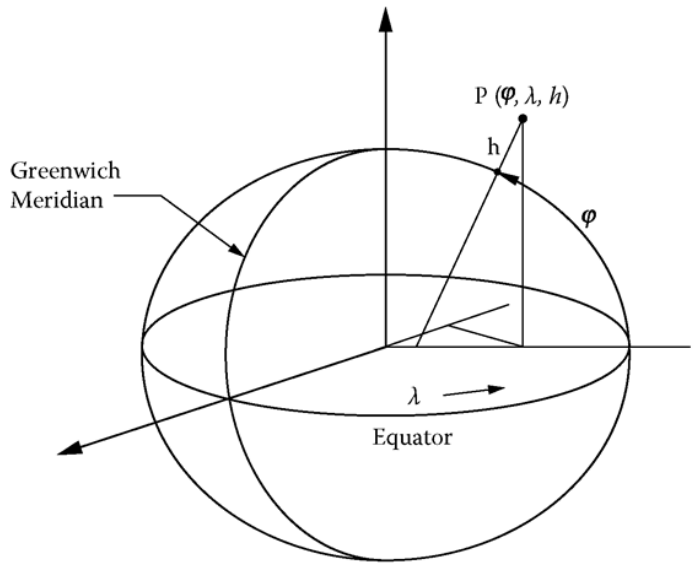

Figure 2. Three coordinate system representation.

For instance, let us consider the D_j geographic location as (15.92,80.18,400). Here, x, y, and z represent latitude (φ), longitude (λ), and altitude (h), respectively. The TS executes the following steps as follows, TS calculates

1. $\mathbb{Q}_i = \frac{\partial_f}{\partial_i}$
2. $\mathbb{Q}_i\mathbb{R}_i \equiv 1 \; mod \; \partial_i$
3. $\varnothing_i = \mathbb{Q}_i\mathbb{R}_i$
4. $\mu = \sum \varnothing_i$

5. $\mathcal{M} = \mu \times \omega$, here $\omega = E_r(\varphi| \ |\lambda| \ |h)$.

Finally, the value of $\mathcal{M}$ is provided to the EU_i. The value of secret key ∂_f is provided to the EU_i by TS during initial offline registration. The EU_i calculates ω as $\mathcal{M}$ *mod* ∂_i. By decrypting ω with the public key of the TS, the three required coordinates can be retrieved by the EU_i. This protocol is mainly based on Chinese remainder theorem (CRT) [37].

5. Security Analysis

Analysis of some conceivable security attacks is described in this section.

5.1. Impersonation Attack

When an adversary efficaciously imitates a legitimate EU_i or D_j in the FANET, it is called an impersonation attack. In our suggested scheme, security parameters such as private key (α_{eu}), fake identity (FID_{eu}), end-user batch key (UBK_j), and the secret key for finding the exact location $\left(\partial_f\right)$ are provided by the TS during offline registration. To regenerate the exact replica of the keys, an adversary should have knowledge regarding the master key and private key of TS. However, the confidentiality of these keys is high, and it is hard for an attacker to compute these keys. Moreover, to compute the value of the public key $\alpha_{eu} = g_2^{\frac{1}{m+q+u_j}}$, the value of the private key of the EU_i (u_j) should be known. However, it is a randomly chosen number, and the computation involves a discrete logarithm problem (DLP) [38].

5.2. Bogus Message Attack

The adversary should be capable of sending a bogus message in place of the real message to the EU_i. To perform this task, the adversary should compromise the controlling device of the D_j. However, this is practically not possible since the drone is registered with TS and any misbehavior of the D_j leads to its revocation from the network by TS. Thus, our suggested work shows resistance against fake message attack.

5.3. Message Modification Attack

The collected confidential information/data from the D_j to EU_i are3 transferred in a secured way. Here, short time session keys are generated for transferring the information to the EU_i. It is very difficult for an adversary to generate the equivalent short life session key and to perform the message modification attack. Moreover, the integrity of the session key is also ensured in our suggested work. As a result, our scheme is resistant to message alteration attack.

5.4. Reply Attack

When an adversary is capable of capturing the transferred information, modifying it and sending to the EU_i in the same stipulated time, it is called a reply attack. However, in this proposed work, timestamps are attached during the session key exchange. During initial session key generation request, EU_i sends (s_0, s_2, x, T) to the D_j; here, D_j checks the validity of the current timestamp (T). If the minimum delay is not satisfied, then the request is discarded. Moreover, after the session key generation, D_j sends $(sk, \ T1)$ to EU_i. Here also, the validity of $(T1)$ is checked to ensure the legitimacy of the session key. Since the information is transferred with the assistance of the session key, without capturing the session key, it is hard for an adversary to perform a reply attack. Thus, our scheme is resistant to reply attack.

5.5. Privacy Preservation

Anonymous dummy identities are used to hide the real identities of the D_j and the EU_i in this proposed scheme. Mutual authentication uses only the dummy EU_i identity and dummy D_j identity. Therefore, even if the adversary discovers the dummy identity of the EU_i/D_j, it is difficult for the adversary to determine the original identity of the

EU_i/D_j. In addition, the fake identity of EU_i and D_j are calculated as $FID_{eu} = g_1^{\frac{1}{(m+q)u_j}}$ and $FID_{D_j} = \frac{(m+q)^2}{d_j}$, which involves the master key, the private key of TS, and the private key of EU_i and D_j. Tracing of the private keys of EU_i/D_j is hard due to DLP. As a result, privacy is preserved in this suggested work.

5.6. Repudiation Attack

In this suggested framework, repudiation of the EU_i is not possible. Here, the EU_i is registered with the TS offline. Only after the successful authentication, the security parameters are transferred to EU_i and the authenticated EU_i becomes the part of the network. As a result, only the authenticated EU_i can request information/data from the authenticated drone. Therefore, on receiving the confidential data from the controlling device of D_j, the EU_i cannot repudiate.

5.7. Unlinkability

Confidential information is transferred using the short life session key. These session keys have a limited life span. As a result, once the information is transferred with this short life session key, the validity of this session key expires. During the next/successive information transfer, a new session key is to be generated for efficient transfer of information. Thus, there exists an unlinkability between the two successive messages. Therefore, it is hard for an adversary to link the two messages from the same user.

5.8. Man in Middle Attack

If an adversary is capable of deceiving both the D_j and the EU_i, a man in the middle attack is possible. In our suggested work, even if an adversary captures $(\gamma', \alpha_{D_j}, FID_{D_j})$ from D_j, it is difficult for an adversary to alter the parameters in the list. Even if the adversary modifies the credentials, EU_i checks the condition $e(\gamma'. \alpha_{ca}, \alpha_{D_j}) = Z$. If the condition is not gratified, then the current authentication request is aborted. Thus, our work is resistant to man in the middle attack.

5.9. Privileged Insider Attack

The required credentials for the D_j and EU_i are provided by TS during the initial offline registration in a secure way. Therefore, it is impossible for an inside attacker to generate fake credentials for D_j/EU_i. Moreover, TS is a completely trusted authority and it is difficult for an inside attacker to compromise it. The validity of the session key generated is only for a limited period and it is hard for an inside attacker to crack it. Thus, our proposed work is resistant to insider attack.

6. Performance Analysis

The performance investigation of the suggested scheme is described in terms of computational cost, communication cost, storage cost, and drone's service providing capability. The following subsections briefly explain the aforementioned analysis.

6.1. Computational Cost

In the analysis of the computational cost, the cost involved in the generation of public key, fake identity generation, and key exchange protocol is examined. The cryptographic operations involved in the analysis of computational cost are hashing operation, exponential operation, multiplication operation, one-point addition operation, pairing operation, and reverse fuzzy extraction operation. The execution time representations of the above-mentioned operations are Ex_h, Ex_e, Ex_m, Ex_a,Ex_p, and Ex_{fe}, respectively. To accomplish these operations, the cryptographic library based on pairing is utilized with Type-A curve. Moreover, Cygwin version 1.7.35 [39] is used with the system requirements of Core i7, 3.4GHz processor, 8GB memory, and gcc version 4.9.2. The implementation time for performing Ex_h, Ex_m, Ex_e, Ex_a, Ex_p, and Ex_{fe} are calculated as 2.6 ms, 1.2 ms,

0.6 *ms*, 2.6 *ms*, 1.72 *ms*, and 2.13 *ms*, respectively, where *ms* represents the execution time in milliseconds. Table 3 clearly shows the comparison of the computational cost for various schemes in terms of the execution time for different cryptographic functions. A total of $(3Ex_e + 2Ex_p + Ex_h = 7.84\ ms)$ is required as the computational time at the D_j side. The suggested work is compared with the related existing schemes such as Singh et al. [30], Tian et al. [31], Wazid et al. [21], Gope et al. [32], Zhang et al. [33], Ever et al. [34], and Hussain et al. [35] schemes, respectively. The computational cost for the schemes [21,30–35] are 9.6 *ms*, 9 *ms*, 18.2 *ms*, 19.04 *ms*, 18.2 *ms*, 31.64 *ms*, and 18.2 *ms* which are high when compared to the suggested work. Similarly, a total of $(4Ex_e + Ex_p + Ex_h = 6.72\ ms)$ is required as the computational cost at the EU_i side, whereas the prevailing schemes such as [21,30–35] require 7.2 *ms*, 7 *ms*, 43.73 *ms*, 18.2 *ms*, 26 *ms*, 16.44 *ms*, and 41.13 *ms*, respectively. Figures 3 and 4 show the graphical representation of computational cost both at D_j side and EU_i side for different schemes. From the figures, it is clear that the suggested work has less computational cost both at the drone and user side. Table 4 shows the computational cost analysis for the batch authentication process. The investigation is performed for 100 simulations and performance is evaluated. Figure 5 shows the pictorial representation of batch authentication for the large number of drones. The graph portrays that the suggested work outperforms the prevailing works.

Table 3. Computational cost at drone and end user side for different schemes.

Schemes	Drone (D_i)	End User (EU_i)	Total Cost
Singh et al. [30]	$2Ex_e + 7Ex_m$	$2Ex_e + 5Ex_m$	$4Ex_e + 12Ex_m$
Tian et al. [31]	$Ex_m + Ex_a + 2Ex_h$	$Ex_e + Ex_m + 2Ex_h$	$Ex_m + Ex_a + Ex_e + 4Ex_h$
Gope et al. [32]	$2Ex_p + 6Ex_h$	$7Ex_h$	$2Ex_p + 13Ex_h$
Zhang et al. [33]	$7Ex_h$	$10Ex_h$	$17Ex_h$
Ever et al. [34]	$2Ex_p + 9Ex_h + 4Ex_m$	$2Ex_p + 5Ex_h$	$4Ex_p + 14Ex_h + 4Ex_m$
Hussain et al. [35]	$7Ex_h$	$15Ex_h + 1Ex_{fe}$	$22Ex_h + Ex_{fe}$
Wazid et al. [21]	$7Ex_h$	$16Ex_h + 1Ex_{fe}$	$23Ex_h + Ex_{fe}$
Proposed Scheme	$3Ex_e + 2Ex_p + Ex_h$	$4Ex_e + Ex_p + Ex_h$	$7Ex_e + 2Ex_p + 2Ex_h$

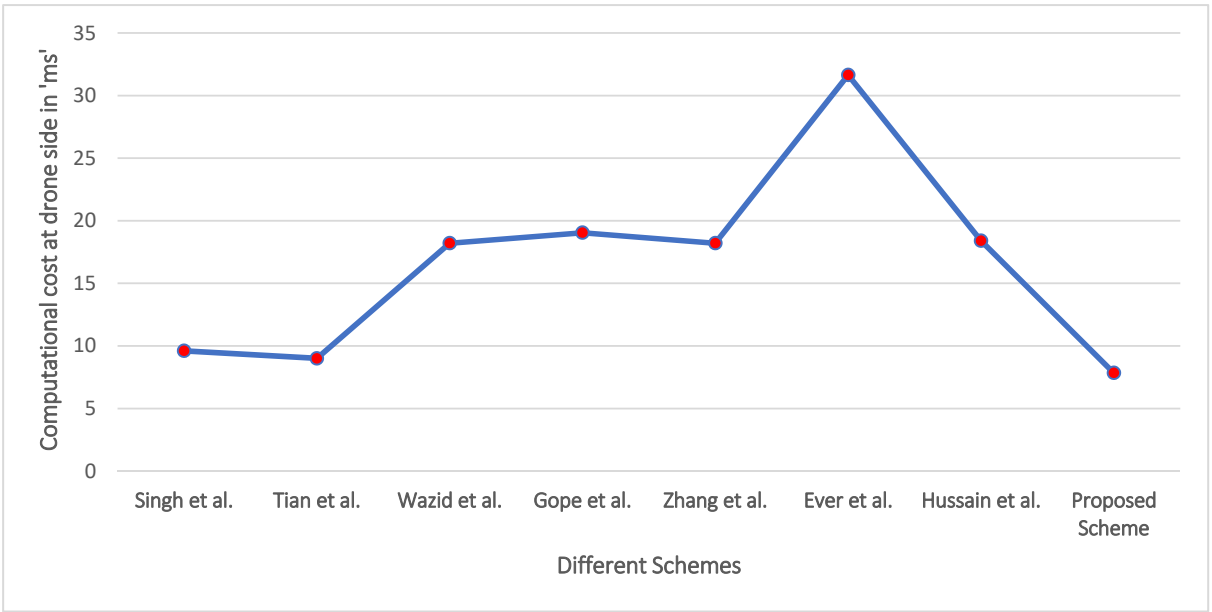

Figure 3. Computational cost at drone side for different schemes.

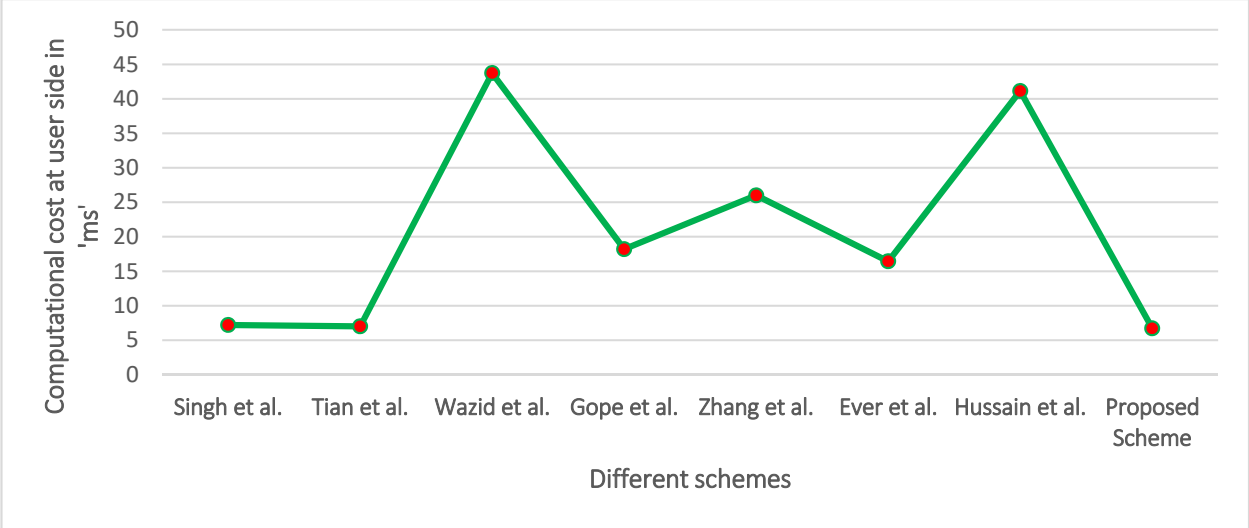

Figure 4. Computational cost at end user side for different schemes.

Table 4. Computational cost analysis for the batch authentication process.

Schemes	Batch Authentication at the D_i Side
Singh et al. [30]	$(n+1)Ex_e + 5Ex_m$
Tian et al. [31]	$nEx_m + nEx_a + (n+1)Ex_h$
Gope et al. [32]	$(n+1)Ex_p + 6nEx_h$
Zhang et al. [33]	$7nEx_h$
Ever et al. [34]	$(n+1)Ex_p + (4n+5)Ex_h + (n+3)Ex_m$
Hussain et al. [35]	$7nEx_h$
Wazid et al. [21]	$(4n+3)Ex_h$
Proposed Scheme	$(n+2)Ex_e + (n+1)Ex_p + nEx_h$

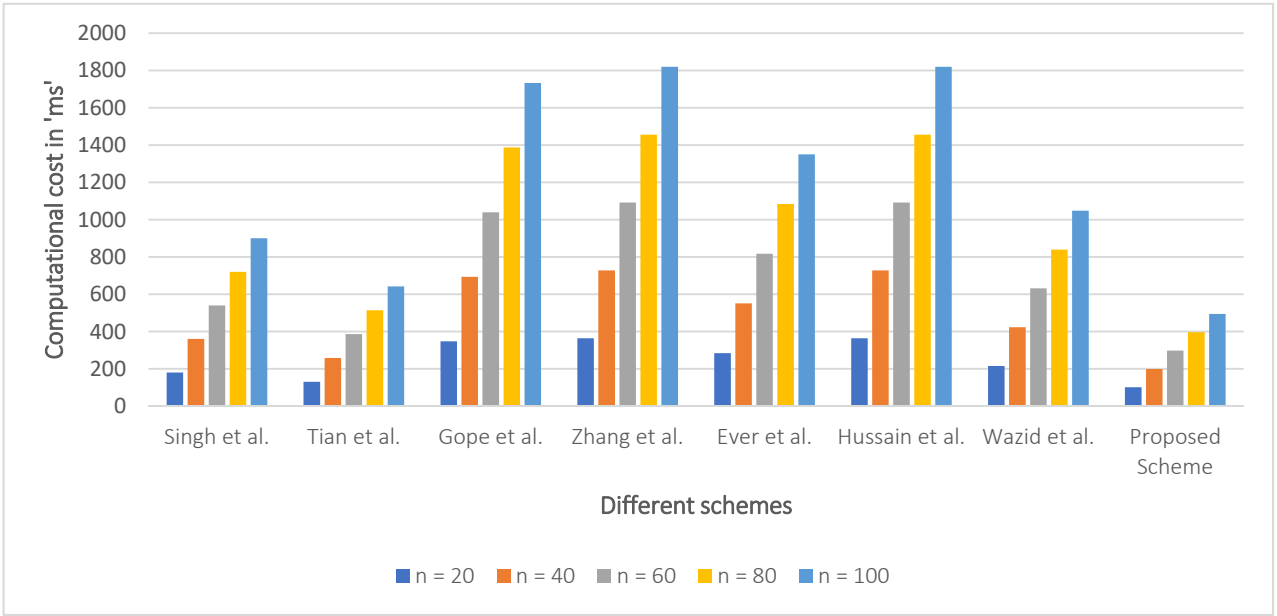

Figure 5. Graphical representation of batch authentication for large number of drones.

6.2. Communication Cost

Once the mutual authentication is accomplished between the EU_i and D_j, exchange of session key takes place. During session key exchange protocol, the EU_i sends (s_0, s_2, x, T) to D_j. Here, (s_0, s_2, x, T) are the elements of Z_a^*. Moreover, the returns the value of $(sk,\ T1)$ to the EU_i after successful validation. The communication cost for the key exchange protocol is calculated as $(5 * 32 + 1024 = 1184\ bits)$. Table 5 portrays the assessment of communication cost for various schemes. From the table, it is clear that the suggested scheme consumes minimum cost when compared to the prevailing schemes. Figure 6 clearly displays the graphical representation of communication cost for various prevailing schemes with our proposed work.

Table 5. Assessment of communication cost for various schemes.

Various Schemes	Communication Cost for Single Authentication	Communication Cost for '*n*' Authentication
Singh et al. [30]	4256	4256*n*
Tian et al. [31]	7328	7328*n*
Gope et al. [32]	1792	1792*n*
Zhang et al. [33]	1472	1472*n*
Ever et al. [34]	1920	1920*n*
Hussain et al. [35]	2061	2061*n*
Wazid et al. [21]	1696	1696*n*
Singh et al. [30]	1184	1184*n*

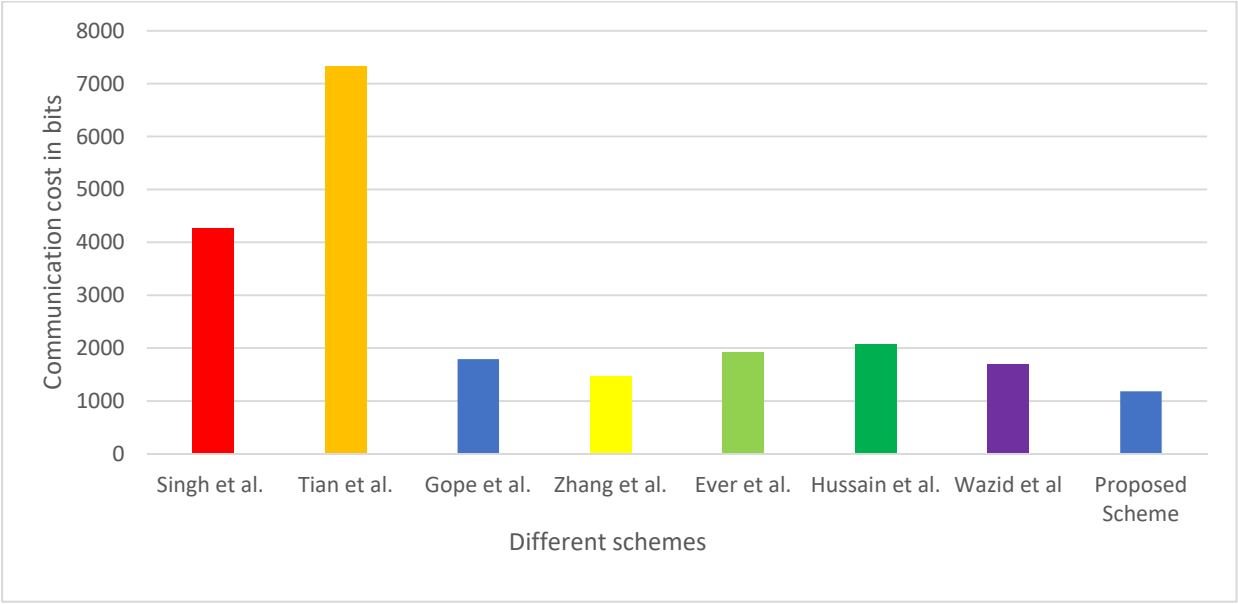

Figure 6. Communication cost for various schemes.

6.3. Storage Cost

The capacity of the D_j to store the keys in its controlling device is termed as the storage cost. Since the memory capacity is related to the resource constraint of D_j's design. The keys generated should be small enough to be accompanied in the design. In this suggested framework, the D_j is equipped to store the value of session key and timestamp values for a period. The memory storage for the proposed protocol is calculated as 1046 bits. Table 6 shows the comparison of the storage cost of the proposed work with the existing

schemes. The suggested work is compared with prevailing works such as Singh et al. [22], Tian et al. [23], and Zhang et al. [25] and found to have lower storage cost. Figure 7 depicts the graphical illustration of the storage cost of different prevailing works with the suggested work.

Table 6. Assessment of storage cost for different schemes.

Different Schemes	Total Storage Cost (bits)
Singh et al. [30]	1152
Tian et al. [31]	2368
Zhang et al. [33]	2752
Proposed Scheme	1046

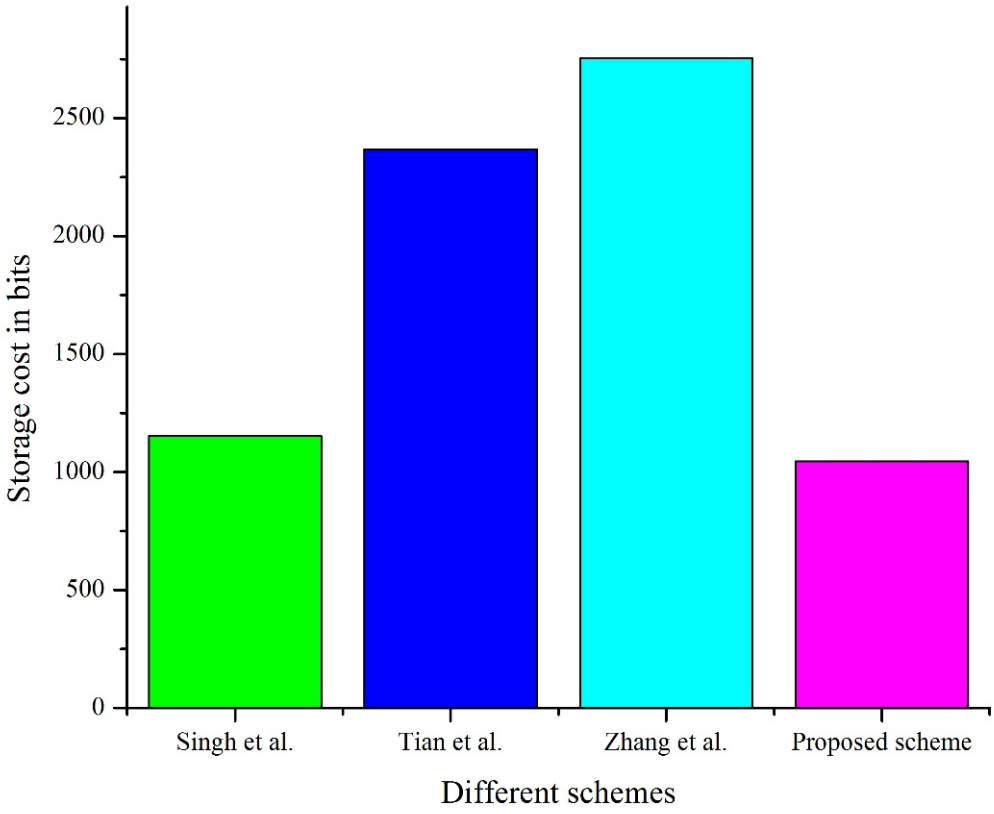

Figure 7. Graphical illustration of the storage cost for different schemes.

6.4. Drone's Serving Capability

The number of drones efficiently providing service to the end-user determines the drone's serving capability. Let P be the probability of $\aleph$ number of drones that provide service to the EU_i. The total computational time incurred in this suggested work is calculated as $\Lambda\mathcal{M} = 7Ex_e + 2Ex_p + 2Ex_h$. Thus, the service providing competency of the D_j is calculated as $\varpi = \frac{\mathrm{P}}{\aleph.\Lambda\mathcal{M}*\aleph}$. Figure 8 shows the serving capability of D_j. From the figure, it clearly indicates that the service-providing competency decreases with the increase in the number of drones. Moreover, the figure s if the computational time is low, the serving capability is high.

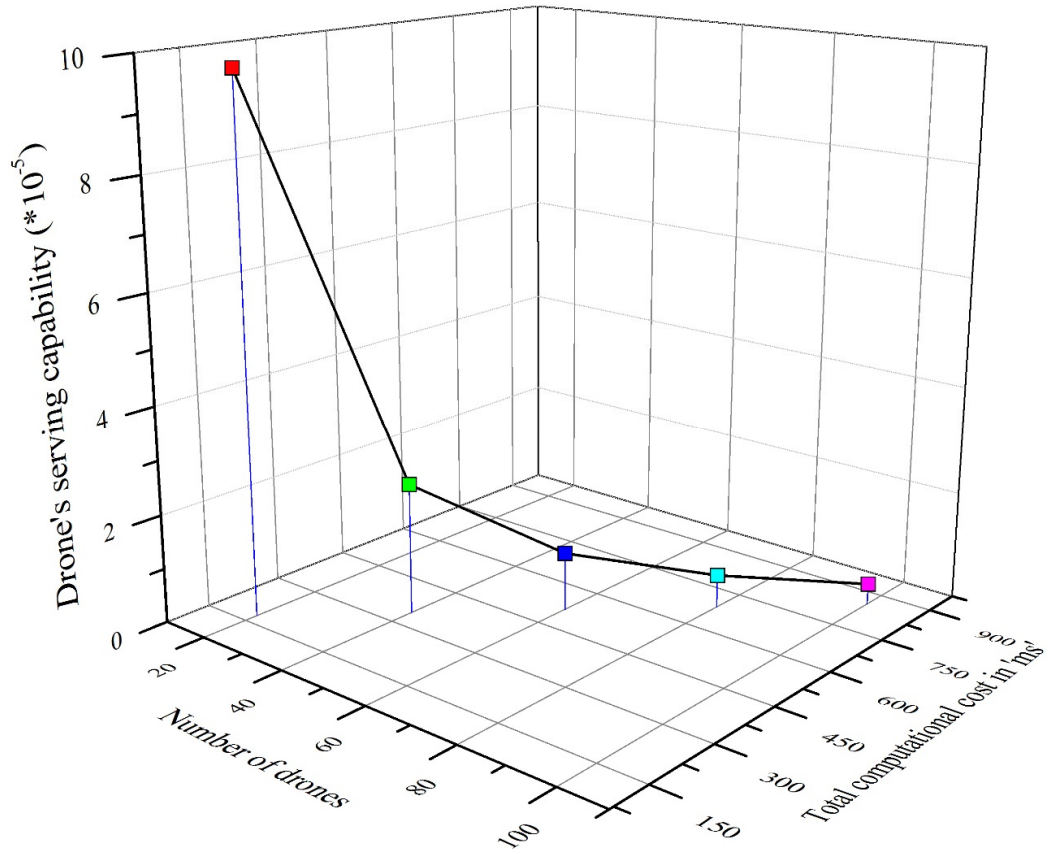

Figure 8. Graphical illustration of the drone's serving capability.

7. Conclusions

A competent mutual and batch anonymous authentication scheme with location privacy is suggested in this article. This work suggests an effective secure communication in the IoD environment. In case of critical situations, the location privacy of D_j is preserved in this suggested work. The security investigation section ensures the resistance of the proposed work against various well-known attacks. Finally, D_j's serving capability to the EU_i is also deliberated. The main contribution of privacy preservation between the end users is achieved. Moreover, for authenticating groups of drones, batch authentication with reduced computational overhead is implemented. In addition, integrity preservation of the confidential information from the drone and location privacy of the drone is preserved.

The suggested work uses only a simple cryptographic pairing and hashing operations for both privacy preservation during mutual and batch authentication which reduces the computational cost, communication cost, and storage cost significantly when compared to prevailing existing schemes. Session keys are generated the preserve the integrity and privacy of the confidential information. Moreover, a simple EXOR operation is utilized during the session key generation request, session key integrity preservation, and key exchange. Finally, location privacy can be achieved by efficiently by utilizing the CRT algorithm. The future scope of this work can be extended to the incorporation of artificial intelligence (AI) and blockchain technology into the authentication protocol.

Author Contributions: A.S.R.: proposed work, security analysis, paper writing. A.M.: experimental work, literature survey, paper writing. F.A.-T.: performance analysis, system model. C.A.: literature survey, computational cost, paper writing. L.M.: proposed work, system model. All authors have read and agreed to the published version of the manuscript.

Funding: The authors declare no funding received for this research.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors appreciate the support from Artificial Intelligence Engineering Dept., Research Center for AI and IoT, Near East University, Mersin 10, Turkey, University of Waterloo, Waterloo, Ontario, Canada, and Computer Science Division, Camerino University, Italy. The authors thank GMR Institute of Technology, Rajam, Andhra Pradesh for the technical assistance to complete this experimental work.

Conflicts of Interest: The authors declare that they have no conflict of interest regarding the publication of this paper.

References

1. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1123–1152. [CrossRef]
2. Labib, N.S.; Brust, M.R.; Danoy, G.; Bouvry, P. The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 115466–115487. [CrossRef]
3. Filkin, T.; Sliusar, N.; Ritzkowski, M.; Huber-Humer, M. Unmanned Aerial Vehicles for Operational Monitoring of Landfills. *Drones* **2021**, *5*, 125. [CrossRef]
4. Lin, C.; He, D.; Kumar, N.; Choo, K.-K.R.; Vinel, A.; Huang, X. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [CrossRef]
5. Wu, Q.; Xu, J.; Zeng, Y.; Ng, D.W.K.; Al-Dhahir, N.; Schober, R.; Swindlehurst, A.L. A Comprehensive Overview on 5G-and-Beyond Networks with UAVs: From Communications to Sensing and Intelligence. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2912–2945. [CrossRef]
6. Nait-Abdesselam, F.; Alsharoa, A.; Selim, M.Y.; Qiao, D.; Kamal, A.E. Towards enabling unmanned aerial vehicles as a service for heterogeneous applications. *J. Commun. Netw.* **2021**, *23*, 212–221. [CrossRef]
7. Iqbal, A.; Rajasekaran, A.S.; Nikhil, G.S.; Azees, M. A Secure and Decentralized Blockchain Based EV Energy Trading Model Using Smart Contract in V2G Network. *IEEE Access* **2021**, *9*, 75761–75777. [CrossRef]
8. Raja, G.; Anbalagan, S.; Subramaniyan, A.G.; Selvakumar, M.S.; Bashir, A.K.; Mumtaz, S. Efficient and Secured Swarm Pattern Multi-UAV Communication. *IEEE Trans. Veh. Technol.* **2021**, *70*, 7050–7058. [CrossRef]
9. Arasan, A.; Sadaiyandi, R.; Al-Turjman, F.; Rajasekaran, A.S.; Karuppuswamy, K.S. Computationally efficient and secure anonymous authentication scheme for cloud users. *Pers. Ubiquitous Comput.* **2021**, *566*, 1–11. [CrossRef]
10. Shafique, A.; Mehmood, A.; Elhadef, M. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 46927–46948. [CrossRef]
11. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [CrossRef]
12. Subramani, J.; Azees, M.; Sekar, A.; Al-Turjman, F. Lightweight Privacy and Confidentiality Preserving Anonymous Authentication Scheme for WBANs. *IEEE Trans. Ind. Informatics.* **2021**, *9*, 7759. [CrossRef]
13. Sanjab, A.; Saad, W.; Basar, T. A Game of Drones: Cyber-Physical Security of Time-Critical UAV Applications with Cumulative Prospect Theory Perceptions and Valuations. *IEEE Trans. Commun.* **2020**, *68*, 6990–7006. [CrossRef]
14. Subramani, J.; Maria, A.; Neelakandan, R.B.; Rajasekaran, A.S. Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification. *IET Commun.* **2021**, *15*, 1187–1197. [CrossRef]
15. Wu, T.; Guo, X.; Chen, Y.; Kumari, S.; Chen, C. Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks. *Drones* **2022**, *6*, 10. [CrossRef]
16. Turkanović, M.; Brumen, B.; Hölbl, M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Network* **2014**, *20*, 96–112. [CrossRef]
17. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Comput. Netw.* **2016**, *101*, 42–62. [CrossRef]
18. Challa, S.; Wazid, M.; Das, A.K.; Kumar, N.; Reddy, A.G.; Yoon, E.-J.; Yoo, K.-Y. Secure signature-based authenticated key establishment scheme for future IoT applications. *IEEE Access* **2017**, *5*, 3028–3043. [CrossRef]
19. Won, J.; Seo, S.-H.; Bertino, E. Bertino, Certificateless cryptographic protocols for efficient drone-based smart city applications. *IEEE Access* **2017**, *5*, 3721–3749. [CrossRef]
20. Tai, W.-L.; Chang, Y.-F.; Li, W.-H. An IoT notion-based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. *J. Inf. Secur. Appl.* **2017**, *34*, 133–141. [CrossRef]
21. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Conti, M.; Jo, M. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet Things J.* **2018**, *5*, 269–282. [CrossRef]
22. Yue, X.; Liu, Y.; Wang, J.; Song, H.; Cao, H. Software defined radio and wireless acoustic networking for amateur drone surveillance. *IEEE Commun. Mag.* **2018**, *56*, 90–97. [CrossRef]

23. Bouman, P.; Agatz, N.; Schmidt, M. Dynamic programming approaches for the traveling salesman problem with drone. *Networks* **2018**, *72*, 528–542. [CrossRef]
24. Hong, I.; Kuby, M.; Murray, A.T. A range-restricted recharging station coverage model for drone delivery service planning. *Transp. Res. Part C: Emerg. Technol.* **2018**, *90*, 198–212. [CrossRef]
25. Shavarani, S.M.; Mosallaeipour, S.; Golabi, M.; İzbirak, G. A congested capacitated multi-level fuzzy facility location problem: An efficient drone delivery system. *Comput. Oper. Res.* **2019**, *108*, 57–68. [CrossRef]
26. Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M. A new secure data dissemination model in Internet of drones. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
27. Huang, H.; Savkin, A.V. A method of optimized deployment of charging stations for drone delivery. *IEEE Trans. Transp. Electrif.* **2020**, *6*, 510–518. [CrossRef]
28. Shavarani, S.M.; Golabi, M.; Izbirak, G. A capacitated biobjective location problem with uniformly distributed demands in the UAV-supported delivery operation. *Int. Trans. Oper. Res.* **2021**, *28*, 3220–3243. [CrossRef]
29. Cokyasar, T. Optimization of battery swapping infrastructure for e-commerce drone delivery. *Comput. Commun.* **2021**, *168*, 146–154. [CrossRef]
30. Singh, J.; Gimekar, A.; Venkatesan, S. An efficient lightweight authentication scheme for human-centered industrial Internet of Things. *Int. J. Commun. Syst.* **2019**, *2*, e4189. [CrossRef]
31. Tian, Y.; Yuan, J.; Song, H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. *J. Inf. Secur. Appl.* **2019**, *48*, 102354. [CrossRef]
32. Gope, P.; Sikdar, B. An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13621–13630. [CrossRef]
33. Zhang, Y.; He, D.; Li, L.; Chen, B. A lightweight authentication and key agreement scheme for Internet of Drones. *Comput. Commun.* **2020**, *154*, 455–464. [CrossRef]
34. Ever, Y.K. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* **2020**, *155*, 143–149. [CrossRef]
35. Hussain, S.; Mahmood, K.; Khan, M.K.; Chen, C.M.; Alzahrani, B.A.; Chaudhry, S.A. Designing secure and lightweight user access to drone for smart city surveillance. *Comput. Stand. Interfaces* **2021**, *80*, 103566. [CrossRef]
36. Bigazzi, L.; Basso, M.; Boni, E.; Innocenti, G.; Pieraccini, M. A Multilevel Architecture for Autonomous UAVs. *Drones* **2021**, *5*, 55. [CrossRef]
37. Zhou, J.; Ou, Y.-H. Key tree and chinese remainder theorem based group key distribution scheme. *J. Chin. Inst. Eng.* **2009**, *32*, 967–974. [CrossRef]
38. Blake, I.; Seroussi, G.; Smart, N. The Elliptic Curve Discrete Logarithm Problem. In *Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 79–100. [CrossRef]
39. Cygwin: Linux Environment Emulator for Windows. Available online: http://www.cygwin.com/ (accessed on 10 December 2021).