ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks

Xiaoyu Du1 · Yinyin Li1,3 · Sufang Zhou1 · Yi Zhou2

Received: 12 July 2021 / Accepted: 29 April 2022 / Published online: 27 May 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
With the rapid development of wireless communication and edge computing, UAV-assisted networking technology has great significance in many application scenarios such as traffic forecasting, emergency rescue, military reconnaissance. However, due to dynamic topology changes of Flying Ad-hoc Networks (FANET), frequent identity authentication is easy to cause the instability of communications between UAV nodes, which makes FANET face serious identity security threats. Therefore, it is an inevitable trend to build a secure and reliable FANET. In this paper, we propose a lightweight mutual identity authentication scheme based on adaptive trust strategy for Flying Ad-hoc Networks (ATS-LIA), which selects the UAV with the highest trust value from the UAV swarm to authenticate with the ground control station (GCS). While ensuring the communication security, we reduce the energy consumption of UAV to the greatest extent, and reduce the frequent identity authentication between UAV and GCS. Through the security game verification under the random oracle model, it is proved that the proposed method can effectively resist some attacks, effectively reduce the computational overhead, and ensure the communication security of FANET. The results show that compared with the existing schemes, the proposed ATS-LIA scheme has lower computational overhead.

Keywords FANET · UAV · Mutual authentication · Trust strategy · Random oracle model

1 Introduction
In recent years, the development of the UAV industry has experienced explosive development. UAVs are more widely used in detectives, scientific research, smart cities [1], adventure rescue and other fields, bringing huge convenience to people’s lives and production [2]. With the sudden outbreak of new coronavirus pneumonia in 2020, UAVs actively responded to the call and played a huge role [3], and the development and planning of the UAV industry also has ushered in new opportunities and challenges [4]. According to [5] statistics, it is estimated that by 2025, the global UAV market will reach 42.8 billion U.S. dollars, and it is estimated that by 2030, the global UAV market will reach 150 billion U.S. dollars.

FANET has become a new development direction. An aerial network composed of dozens of UAVs can perform more complex flight missions in diverse scenarios. Both FANET and Internet of vehicles (VANET) are special categories of mobile ad hoc network (MANET), which are composed of some highly mobile nodes. The characteristics and security requirements are shown in Fig. 1. UAV network can be regarded as a subset of MANET and VANET, which is composed of mobile devices and on-board devices to solve point-to-point communication, but their only difference is moving in the air.

Both security and privacy are the main problems in FANET environments. Since the communication between UAVs is built on an open channel (radio propagation, WiFi, e.g.), malicious attacks often occur in such kind of networks. These will have a major impact on the privacy and safety of UAVs. In addition to the data collected by the UAV,
malicious attackers will also be interested in the UAV’s identity and flight path. In this way, malicious attackers obtain confidential data from UAVs and their monitoring facilities. In addition, the weight, energy, and communication technology of UAVs are the main factors affecting its services, such as communication methods, flight distance, flight endurance, load capacity, etc. [6, 7]. Specifically, the security and privacy issues mainly include the following aspects:

- The dynamic FANET is easy to cause a situation, which is data loss. Due to the relatively fast speed and relative movement speed of the UAV, the network topology of the UAV changes quickly. This causes serious data loss in the communication process, which has a great impact on the reliability and security of communication.
- UAVs have limited storage and computing power, as well as the energy they can carry. The complex encryption algorithm will increase the UAV’s resource consumption and energy consumption, resulting in a long communication response time and affecting the performance of UAV communication. Therefore, it is necessary to allocate resources and energy reasonably and supplement them in time.
- There is no direct trust relationship between UAV nodes. Since the nodes in FANETs mainly communicate through the wireless transmission, the network is often interrupted and reconnected during the movement of UAV nodes. Therefore, attackers easily interfere with the network and obtain the data information transmitted between nodes.

For the above security issues, the main contributions of this article are as follows:

1. A credible computing scheme is designed in this paper. We aggregate the direct trust value, global trust value, and energy trust value of UAVs in the drone fleet into a comprehensive trust value. UAV representatives are selected from the drone fleet based on the comprehensive trust value.
2. A lightweight security authentication scheme is designed in this paper, the scheme based on elliptic curve encryption algorithm to ensure the identity authentication of the representative UAV and road station.
3. We uses a random oracle model to analyze the provable security. At the same time, we conducted an informal safety analysis. Through security analysis, we have judged the security performance of this solution and the attacks that can be resisted.

2 Related work

UAV is vulnerable to malicious factors when it performs specified tasks in the network. In terms of privacy and security, such as network coverage [8], UAVs responsible for point-to-point traffic are vulnerable to data security threats, malicious attacks, and interference [9]. In terms of communication, malicious UAVs use a specific bandwidth of the air network to perform frequency interference on the system’s secure channel to intercept UAV data. Most of the existing solutions are mainly based on the ideas of Ad Hoc or Internet of Vehicles security networking [10–12]. However, due to the highly dynamic mobility of UAVs, the security threats it faces are even more special. The safety and privacy of UAVs have also attracted more and more attention. He et al. [13] proposed an enhanced anonymous user authentication and key agreement scheme for roaming in a global environment, security analysis shows that this solution has important security attributes such as prevention of various attacks, single registration, user anonymity, and high password authentication efficiency. In the literature [14], the author’s scheme provides a key agreement for the global mobile network environment and ensures the security and fairness of communication. This has contributed to the research on UAV communication and privacy security.

In [15], the authors proposed a software-defined network (SDN) that can facilitate the flexible deployment and management of new services, which helps reduce costs and improve network security and availability. Finally, the author gave a comprehensive description of the problems of FANET security. In [16], the author mainly studied the security and privacy of FANET architecture, and outlines potential solutions to these challenging problems, such as privacy leakage, data confidentiality protection, and flexible accessibility, etc. In [17], the author proposed a certificate-based privacy protection authentication scheme to protect FANET. The scheme realizes the privacy protection of UAV identity, location, and flight route. The author also proved
the feasibility of this scheme in terms of security, privacy, and efficiency through in-depth analysis. Chen et al. [18] and Semal et al. [19] proposed a mutual authentication scheme for FANET deployment based on asymmetric bilinear pairing. The purpose is to achieve confidentiality, information integrity and authenticity in UAV-to-UAV communication.

Zhang et al. [20] proposed a lightweight authentication scheme for FANETs. When UAVs and users authenticate each other, only a secure one-way hash function and odor operation can resist various attacks. Gope and Sikdar [21] pointed out that the scheme of Zhang et al. is insecure against forgery attacks. The attacker can intercept the first message between the user and the control server. The attacker modifies the timestamp so that the control server cannot recognize the message. The scheme proposed by the author in [22] is also vulnerable to the above-mentioned similar attacks. Wazid et al. [23] also proposed a new type of lightweight authentication scheme. When users want to access UAV data, they need to apply for authorization to achieve the security verification of users and UAVs. But Wazid et al. only used fuzzy extractors and hash functions. Although they have lightweight features, the authentication protocol is vulnerable to session-specific temporary information attacks. Yahuza et al. [24] and Zhang et al. [25] proposed a secure and lightweight authentication key agreement technology for FANET deployment, and evaluated the security of the technology from theoretical methods and formal methods.

Although these authors have proposed data privacy protection schemes for UAVs, they have not solved their privacy security issues based on the special network environment of UAVs. Moreover, these solutions still cannot solve the problems of UAV communication delay and complicated calculation. In order to ensure the security identity of drones from the source, we can conduct credibility assessments in the drone fleet. Therefore, a Bayes-based reputation management model was proposed in the literature [26]. This model obtains the comprehensive trust value of the node through the global trust iteration method, which improves the trust convergence speed, but increases the energy consumption of trust calculation. In order to reduce the energy consumption of trust computing, the literature [27] combines historical trust value of nodes, the statistical trust value and direct trust value to calculate the comprehensive trust value of nodes to balance the subjective and objective nature of trust. The literature also proposes a method for evaluating the trust degree of the Internet of Things based on node behavior. Some scholars introduce social relationships into the trust evaluation model to fully mine the trust relationship between node and node [28, 29].

In order to design an effective and credible FANET authentication framework with privacy protection capabilities, it is necessary to consider the following aspects. First, in order to reduce the communication overhead, which is caused by the simultaneous identity authentication of multiple UAVs in FANET, it is necessary to select a representative UAV and the GCS for one-to-one authentication. Secondly, since UAVs usually have resource constraints in terms of computing and energy, the identity authentication scheme must be lightweight. Finally, the designed scheme must protect the privacy of UAVs.

3 System model

3.1 FANET model

FANET mainly includes drone fleet, ground control station (GCS), and trusted center (TC). The drone fleet needs to select the representative UAV (RUAV) with the highest trust value. The drone fleet and the GCS have communication tasks, so a two-way identity authentication is required. Their mutual authentication needs to rely on the storage and verification of their private identity information by the trusted center. After the UAV and the road station are successfully authenticated, the UAV receives the message from the road station and executes the message task. Figure 2 shows the scene and relationship diagram of FANET.

The main functions are:

UAV: Every UAV is equipped with communication equipment, which can communicate with UAV and road station in real time.

Trusted Center (TC): TC is trusted by all nodes of the UAV system and has sufficient computing, communication, and storage capabilities. TC is also responsible for generating system parameters and registering UAVs and GCSs.

Ground Control Station (GCS): The GCS is an infrastructure that is deployed on the side of the road or is a movable man-operated infrastructure. Before the GCS establishes a call with the UAV, the identity information must be authenticated.

When UAVs perform tasks, they usually perform collaborative operations within the UAV fleet. Therefore, there will be situations where the drone fleet and the GCS initiate an identity authentication request at the same time.

3.2 Trust management method

This article makes the following presuppositions for the trust value calculation management model adopted:

• The UAV fleet network environment has been running for a period, and a moderate amount of interaction experience has been accumulated among UAVs;

• The position of each UAV in the UAV fleet is fixed, that is, the adjacent nodes are also determined. There-
fore, the node has formed a relatively stable "circle of acquaintances" according to the historical interaction degree of the UAV.

- In the trust value evaluation stage, the status of each drone node in the drone network is equal, and they must evaluate each other after each task is executed;
- All UAV nodes in the system can be considered as cooperative nodes, and there are no uncooperative nodes that do not provide services or provide evaluation. Here, malicious UAVs are also cooperative nodes.

We first evaluate the reputation of the UAV in the drone fleet. The direct trust value, global trust value, and energy trust value of each UAV are evaluated through the historical communication records of the UAV nodes. We comprehensively calculate the three types of trust values to obtain the comprehensive trust value of each UAV. Due to the energy limitation of the UAV, when the energy of the UAV is greater than the energy threshold, we evaluate the reputation of the UAV. Otherwise, we will kick the UAV out of the fleet for energy replenishment. The system selects the UAV with the highest reputation value through the UAV trust list as RUAV, which represents the real-time communication between the drone fleet and GCS. Figure 3 shows the system frame diagram of FANET in this scheme.

4 ATS-LIA scheme

This paper proposes an identity protection scheme based on trusted UAVs. This section mainly introduces the scheme in detail. The program is mainly divided into four parts, which are security goals, the most trusted UAV selection, the privacy protection of the UAV's identity, and the identity privacy protection of the GCS. The choice of the most trusted UAV is mainly based on the UAV's local trust value, global trust value, capability trust value and comprehensive trust value. The identity privacy protection scheme mainly includes system initialization, anonymous identity setting, message signature and message authentication.

4.1 Security requirements

We make the following assumptions based on the characteristics of FANET system in reality:

1. The Trusted Center (TC) in FANET is completely credible;
2. The communications of UAV→UAV and UAV→GCS is spread on open propagation channels, so it is very likely to be attacked by a wide range of attackers.
Table 1 is the security goal of the trusted FANET designed in this paper.

4.2 Selection of RUAV

The main influencing factors of the direct trust value of each UAV in the drone fleet are: the relevance of data transmission, the sending rate of data packets, the freshness of data, and the successful delivery rate of packets. The entity trust of UAVs is mainly judged by the quality scores of other UAVs in the UAV group and the credibility of the scores. The comprehensive trust value of UAV is mainly composed of local trust value, global trust value and energy trust value. The trust value is calculated as follows:
Table 1 safety objectives of the design scheme

| Type                          | Describe                                                                 |
|-------------------------------|--------------------------------------------------------------------------|
| Identity privacy protection   | UAVs, road stations, and malicious UAVs cannot obtain the UAV’s identity information from the communication messages |
| Message authentication and integrity | When the UAV communicates with the road station, both parties must be authenticated, so it can detect whether the message has been tampered with or fabricated |
| Traceability                  | The Trusted Center (TC) is the only institution that can know the identity of the UAV |
| Un-linkability                | UAVs, road stations, and third-party participants cannot track UAVs by analyzing communication data because they cannot link and determine whether two messages are from the same UAV |
| Impersonation attack          | This attack is mainly aimed at malicious UAVS forged into trusted UAVS to send fake messages |
| No certificate management     | The complexity and cost of certificate management increase with the increase in the number of UAVS. In order to reduce the complexity of certificate verification and ensure the communication performance of the UAV, the solution needs to design certificateless management |
| Demonstrable safety           | The program needs to use a widely recognized safety certification model for safety analysis |

- Local trust value

In the process of judging the data of $U_i$( The i-th UAV), we mainly judge the task instructions received from RUAV as the receiver and the shared information received by RUAV from other member UAVS. The shared information mainly includes the location of the UAV, the flying speed of the UAV, and the flying direction of the UAV. We mark the received shared information of $U_i$ (The j-th UAV) as $X_j = \{x_1, x_2, \cdots, x_n\}$, and mark the flight status information of $U_i$ as perceived by $U_j$ as $Y_j = \{y_1, y_2, \cdots, y_n\}$. The $U_i$ perceives the data information $Y_j$ of $U_j$ and the shared information $X_j$ of $U_j$ in a one-to-one correspondence. We calculate the error result of the same variable of the two data sets to get the error set $E_j = \{e_1, e_2, \cdots, e_n\}$, where $e_i = |x_i - y_i|$. In the following sigmoid function, $o_{th}$ represents the influence weight of various shared information on the overall trust value, $o_{th}$ is the threshold of the model, and $t$ represents the hovering time. In this function, the input is each value in the corresponding error set $E_j$, and the output is trust value evaluation result $R_{ij}$ of $U_i$ to $U_j$ transmission information, which is calculated as:

$$R_{ij}(t) = \frac{1}{1 + \exp(-\sum_{k=1}^{n} o_{th} \cdot e_k - o_{th})}$$  \hspace{1cm} (1)

- Global trust value

The global trust value is mainly judged based on the quality of the mission performed by the UAV. The judgment basis is mainly the trust value of the judged UAV provided by neighbor nodes. The set of neighbor nodes is represented by $u_k$, where $u_k = \{u_{i_1}, u_{i_2}, \cdots, u_{i_k}\}$, $k$ represents the number of neighbor nodes, $k$ represents the total number of UAVs. Figure 4 shows the aggregation process of the trust value of neighbor nodes.

The mission execution quality $Q_{ij}(t)$ of the UAV is expressed as:

$$Q_{ij} = \frac{1}{n} \sum_{u \in V_u} (R_{iu} \cdot R_{uj})$$  \hspace{1cm} (2)

where $U_i$, represents the trusted public neighbor node of $U_i$ and $U_j$, $R_{iu}$ represents the direct trust value of $U_i$ to $U_u$, and $R_{uj}$ represents the direct trust value of $U_u$ to $U_j$.

The global trust value of the UAV is expressed as:

$$S_j(t) = Q_{ij}(t - 1) + R_{ij}(t) + \sum_{u=1,u \neq i,j}^{n} Q_{uj}(t - 1)$$ \hspace{1cm} (3)

- Energy trust value

The energy consumption of UAV is mainly determined by the flight distance and flight time. We assume that $U_j$ flies in a
straight line at a uniform speed of $v$, the influence of the flight
distance of $U_j$ on flight energy consumption is calculated as:
$E_d(t) = \int_0^t P(v) dt$. The energy consumption of $U_j$ when hover-
ing is: $E_h(t) = \int_0^t P(h) dt$. Among them, $P(v)$ represents the
power when the $U_j$ is flying at the speed $v$, and $P(h)$ represents
the power when the flying height is $h$ at the hovering time $t$. There-
fore, the energy trust value of the UAV can be obtained as:

$$E(t) = E_d(t) + E_h(t)$$  \hspace{1cm} (4)

- Comprehensive trust value

We have considered the data security, entity trust and
energy consumption of UAV nodes, and the comprehensive
trust value formula of $U_j$ is as follows:

$$C(t) = \lambda_1 \cdot (\varphi \cdot R_p(t)) + \lambda_2 \cdot S_p(t) + \lambda_3 E(t)$$  \hspace{1cm} (5)

where $\lambda_1 + \lambda_2 + \lambda_3 = 1$. To prevent the previous malicious
behavior from being forgotten by the UAV, we introduce the
activation factor $\varphi$, so that the previous bad behavior of the
$U_j$ will be strongly remembered, and it will take a long time
to establish a new trust next time.

### 4.3 Identity authentication

The authentication scheme based on anonymous identity of
UAV is shown in Fig. 5, and the specific steps are as follows:

A  Identity authentication scheme of UAV

---

**Fig. 5** The working diagram
of the proposed authentication
process

| Stages               | TC          | $U_i$          | GCS          |
|----------------------|-------------|----------------|--------------|
| System Initialization| TC $\leftarrow$ \{ID\} $U_i$ | 1. TC generates a group G and four
encrypted hash functions $h_0 - h_3$
2. TC selects two random numbers $a$ and $b$, and calculates $A_{pub} = g^a$
and $B_{pub} = g^b$
3. TC broadcasting system parameter $Params = \{q, G, g, A_{pub}, B_{pub}, h_0, h_1, h_2, h_3\}$ |
| Anonymity Settings for UAVs| TC $\leftarrow$ \{ID\} $U_i$ | 1. TC generates an anonymous FID
and computes $PK_{i,j} = g^{k_{i,j}}$
2. TC computes $SK_{i,j} = a \cdot h_k(FID_{i,j})$
3. TC packages $\{FID^*_i, SK^*_i, PK^*_i\}$
and sends it to $U_i$
| TC $\leftarrow$ \{ID\} $U_i$ | 1. TC computes $RPK_{i,j} = g^{m_{i,j}}$
2. TC computes $RSK_{j,i} = a \cdot h_k(SID_j)$
3. TC packages $\{SID_j, RSK^*_j, SPK^*_j\}$ and sends it to GCS |
| Identity generation and key extraction for GCS| TC $\leftarrow$ \{ID\} $U_i$ | 1. TC computes $RPK_{i,j} = g^{m_{i,j}}$
2. TC computes $RSK_{j,i} = a \cdot h_k(SID_j)$
3. TC packages $\{SID_j, RSK^*_j, SPK^*_j\}$ and sends it to GCS |

© Springer
### Step 1 System initialization phase

1. Given a system parameter $k \in \mathbb{Z}^*$, TC generates a prime number $q$ and an elliptic curve group $G$ of order $q$, where $g$ is the generator of $G$. TC also chooses $4$ cryptographic hash functions $h_q, h_1, h_2, h_3$, of which $h_q : G \times G \rightarrow \mathbb{Z}_q^*$, $h_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_2 : \{0,1\}^* \times \{0,1\}^* \times G \times G \rightarrow \mathbb{Z}_q^*$, $h_3 : G \rightarrow \mathbb{Z}_q^*$.

2. TC chooses a random number $a \in \mathbb{Z}_q^*$ and sets $A_{pub} = g^a$. $a$ is the master key that only TC knows to extract the private key. TC chooses a random number $b \in \mathbb{Z}_q^*$ and sets $B_{pub} = g^b$, $b$ is the traceable master key that only TC knows.

3. TC announces system parameters $Params = \{q, g, A_{pub}, B_{pub}, h_q, h_1, h_2, h_3\}$.

### Step 2 Anonymous Identity Setting

1. A legal $U_i$ transmits the real identity $ID_i$ to TC, and after confirming that the identity $ID_i$ is valid, TC selects a set of private random numbers $\{k_{i,1}, k_{i,2}, \ldots, k_{i,z}\}$ and calculates the public key $PK_i = \{PK_{i,1}, PK_{i,2}, \ldots, PK_{i,z}\}$, where $PK_{i,j} = g^{k_{i,j}}$ and $j \in \{1,2,\ldots, z\}$. TC generates a set of pseudo-identities $FID_i, FID_i^* = \{FID_{i,1}, FID_{i,2}, \ldots, FID_{i,z}\}$, and $FID_{i,j} = ID_i \oplus h_q(PK_{i,j}^b, B_{pub})$ for $U_i$. The real ID of the UAV is hidden in the $FID$.  

2. After calculating $FID_i^*$, TC calculates the private key $SK_i^* = \{SK_{i,1}^*, SK_{i,2}^*, \ldots, SK_{i,z}^*\}$, where $SK_{i,j} = a \cdot h_q(FID_{i,j}), j \in \{1,2,\ldots, z\}$.

3. TC sends the system parameters $Params$ and $\{FID_i^*, SK_i^*, PK_i^*\}$ to $U_i$.

### Step 3 UAV message signature

1. $U_i$ selects a private key $SK_{i,j}$, a corresponding public key $PK_{i,j}$, and pseudo-identity $FID_{i,j}$ from $SK_i^*, PK_i^*$, and $FID_i^*$ respectively.

2. $U_i$ selects a random number $s_i \in \mathbb{Z}_q^*$ and calculates $S_i = g^{s_i}, f_j = h_2(M_j, FID_{i,j}, PK_{i,j}, S_i, T_i) \in \mathbb{Z}_q^*$, and $Sig_i = (h_3(S_i) - SK_{i,j} \cdot f_j) \cdot s_i^{-1}$, where $T_i$ represents the current timestamp that supports the freshness of the valid signature message.

3. $U_i$ sends a signed message $Msg = \{M_i, FID_{i,j}, PK_{i,j}, S_i, T_i, Sig_i\}$ to a nearby GCS.

### Step 4 UAV authentication

1. When receiving the $Msg$ signed by $U_i$, the receiver checks the freshness of the timestamp $T_i$. If $T_i$ is not fresh, the receiver deletes the message.

2. If $T_i$ is fresh and effective, the receiver (RUAV) will calculate $h_1(FID_{i,j})$ and $f_j = h_2(M_j, FID_{i,j}, PK_{i,j}, S_i, T_i) \in \mathbb{Z}_q^*$, and then verify whether the formula $h(S_i) \cdot A_{pub} = g^h(S_i)$ is valid. The theoretical basis is as follows:

$$
\begin{align*}
S_i^{h_1(FID_{i,j})} & = S_i^{h_2(M_i, FID_{i,j}, PK_{i,j}, S_i, T_i)} \cdot g^{h_2(M_i, FID_{i,j}, PK_{i,j}, S_i, T_i)} \\
& = g^{h_2(M_i, FID_{i,j}, PK_{i,j}, S_i, T_i)} \cdot g^{h_2(M_i, FID_{i,j}, PK_{i,j}, S_i, T_i)} \\
& = g^{h_2(M_i, FID_{i,j}, PK_{i,j}, S_i, T_i)} \\
& = g^{h_2(M_i, FID_{i,j}, PK_{i,j}, S_i, T_i)}
\end{align*}
$$

### B Identity authentication scheme of GCS

The authentication scheme of GCS is shown in Fig. 6, and the specific steps are as follows:

1. **Step 1 Identity generation and key extraction of GCS**

   - Given $RID_j$ of the GCS, the trusted center TC selects a set of random numbers $\{m_{j,1}, m_{j,2}, \ldots, m_{j,z}\} \in \mathbb{Z}_q^*$ and calculates the corresponding public value $RPK_j = \{RPK_{j,1}, RPK_{j,2}, \ldots, RPK_{j,z}\}$, where $RPK_{j,l} = g^{m_{j,l}}, l \in \{1,2,\ldots, z\}$.

   - TC calculates the private key $RSK_j = \{RSK_{j,1}, RSK_{j,2}, \ldots, RSK_{j,z}\}$ of GCS, where $RSK_{j,l} = a \cdot h_1(SID_j)$ and $l \in \{1,2,\ldots, z\}$.

   - TC sends $Params$ and $\{SID_j, RSK_j^*, SPK_j^*\}$ to GCS through a secure transmission channel, and GCS stores all its private keys $\{RSK_j^*, RPK_j^*\}$ and its corresponding representation $RID_j$ in the system memory.

2. **Step 2 The message signature of GCS**

   When GCS broadcast's location information to UAVs in range, the signature of command message $Msg_j$ issued by GCS is as follows:

   1. GCS selects a private key $RSK_{j,l}$ and corresponding public key $RPK_{j,l}$ from $RSK_j^*$ and $RPK_j^*$ respectively, and selects a random number $w_j \in \mathbb{Z}_q^*$ to calculate $W_j = g^{w_j}, RF_j = h_2(Msg_j, RID_j, RPK_{j,l}, W_j, T_j) \in \mathbb{Z}_q^*$, and $R_SIG_j = (h_3(W_j) - RSK_{j,l} \cdot RF_j) \cdot W_j^{-1}$, where $T_j$ is the timestamp of the current time.

   2. The GCS broadcasts the signature information $Msgs = \{M_j, RID_j, RPK_{j,l}, W_j, T_j, R_SIG_j\}$. 
3. **Step 3** The UAV verifies the identity information of GCS.

4. After the UAV receives the signature message $\textit{Msg}_s$ sent by the GCS, $U_i$ checks the freshness of the timestamp $T_j$, if it is not fresh, deletes the information; otherwise, the road area station is authenticated.

5. If the timestamp is fresh, $U_i$ calculates $h_1 (\textit{RID}_j)$ and $RF_j = h_2 (M_j, \textit{RID}_j, \textit{RPK}_j, W_j, T_j)$ to determine whether...
\[ W_i^{\text{sign}} \cdot a_{\text{pub}}^{h_i(BID_i) \cdot RF_i} = g^{h_i(w_i)} \] is established. If the equation is established, \( U_i \) receives the task instruction message \( Msg_i \) from GCS.

5 Security analysis

5.1 Security requirements

The definition of security for our proposed solution is given by a game executed between a polynomial-time adversary \( \Lambda \) and a challenger \( \Gamma \). The game process is as follows:

1. Setup: The challenged person generates the system private key and public parameter params, and sends the params to \( \Lambda \).

2. Query: \( \Gamma \) creates an initially empty list \( L_{\text{UAV}_1} \), and the tuple \( \{ M_i, FID_i, PK_i, S_i, T_i, \Sigma_i, \sigma_i \} \) is stored in \( L_{\text{UAV}_1} \), where \( \sigma_i \in Z_q^* \). \( \Lambda \) and \( \Gamma \) conduct the following query game.

\( h_i = \text{Oracle} \): In this query, \( \Gamma \) chooses a random number \( \mu_i \in Z_q^* \), inserts tuple \( (m, \mu_i) \) into table \( L_{\text{UAV}_1} \), and returns \( \mu_i \) to \( \Lambda \).

\( \text{Sign} = \text{Oracle} \): In this query, \( \Lambda \) inputs information about the UAV mission information \( M_i \), \( \Gamma \) generates forged signature information \( \{ M_i, FID_i, PK_i, S_i, T_i, \Sigma_i \} \).

5.2 Provable security of ATS-LIA

Definition If the advantage of function \( Adv_{\Gamma}^{\text{Auth}}(\Lambda) \) is negligible for any polynomial adversary \( \Lambda \), then the ATS-LIA scheme in this paper is used for UAV chosen-identity and chosen-message secure security.

\( Adv_{\Gamma}^{\text{Auth}}(\Lambda) \) is defined as the advantage of adversary \( \Lambda \) in destroying the identity authentication scheme designed in this paper. According to definition, the identity, and messages security with random oracles for the presented ATS-LIA scheme is argued as shown below.

Theorem Assuming that the discrete logarithm problem (ECDLP) is difficult to solve, the authentication scheme proposed in this paper is secure in random language and model.

Proof Assuming polynomial time adversary \( \Lambda \) can forge a message \( Msg = \{ M_i, FID_i, PK_i, S_i, T_i, \Sigma_i \} \), then \( \Gamma \) can execute the forged message of \( \Lambda \) as a sub-project to solve ECDLP. Assuming that \( A_{\text{pub}} = g^a \) is an instance of ECDLP, the purpose of \( \Lambda \) is to calculate \( a \). \( \Lambda \) obtains the system params \( \text{Params} = \{ q, G, g, A_{\text{pub}}, B_{\text{pub}}, h_0, h_1, h_2, h_3 \} \), and \( \Gamma \) follows the request of \( \Lambda \) and performs the following query.

\( h_0 = \text{Oracle} \): \( \Gamma \) maintains a tuple \( \{ PK_i, B_{\text{pub}}, h_0 \} \) in the list \( L_{\text{UAV}_2} \) which is initialized to be empty. When receiving a request from \( \Lambda \) to query \( \{ PK_i, B_{\text{pub}} \} \), \( \Gamma \) queries whether tuple \( \{ PK_i, B_{\text{pub}}, h_0 \} \) is in list \( L_{\text{UAV}_2} \). If this tuple exists in the list, \( \Gamma \) calculates \( h_0 = h_0(PK_i, B_{\text{pub}}) \) and returns \( h_0 \) to \( \Lambda \). Otherwise, \( \Gamma \) chooses a random \( \mu_0 \in Z_q^* \), calculates \( h_0 = h_0(PK_i, B_{\text{pub}}) \), sends \( \mu_0 \) to \( \Lambda \) and adds \( \{ PK_i, B_{\text{pub}}, h_0 \} \) to \( L_{\text{UAV}_2} \).

\( h_1 = \text{Oracle} \): \( \Gamma \) is maintained as a tuple \( \{ FID_i, \mu_1 \} \) in the list \( L_{\text{UAV}_1} \) which is initialized to be empty. When receiving a request from \( \Lambda \) to query \( \{ FID_i \} \), \( \Gamma \) queries whether tuple \( \{ FID_i, \mu_1 \} \) is in list \( L_{\text{UAV}_1} \). If this tuple exists in the list, \( \Gamma \) calculates \( \mu_1 = h_1(FID_i) \) and returns \( \mu_1 \) to \( \Lambda \). Otherwise, \( \Gamma \) chooses a random \( \mu_1 \in Z_q^* \), calculates \( \mu_1 = h_1(FID_i) \), sends \( \mu_1 \) to \( \Lambda \) and adds \( \{ FID_i, \mu_1 \} \) to \( L_{\text{UAV}_1} \).

\( h_2 = \text{Oracle} \): \( \Gamma \) maintains a tuple \( \{ M_i, FID_i, PK_i, S_i, T_i, \mu_2 \} \) in the list \( L_{\text{UAV}_2} \) which is initialized to be empty. When receiving a request from \( \Lambda \) to query \( \{ M_i, FID_i, PK_i, S_i, T_i \} \), \( \Gamma \) queries whether tuple \( \{ M_i, FID_i, PK_i, S_i, T_i, \mu_2 \} \) is in list \( L_{\text{UAV}_2} \). If this tuple exists in the list, then \( \Gamma \) calculates \( \mu_2 = h_2(M_i, FID_i, PK_i, S_i, T_i) \) and returns \( \mu_2 \) to \( \Lambda \). Otherwise, \( \Gamma \) chooses a random \( \mu_2 \in Z_q^* \), calculates \( h_2 = h_2(M_i, FID_i, PK_i, S_i, T_i) \), sends \( \mu_2 \) to \( \Lambda \) and adds \( \{ M_i, FID_i, PK_i, S_i, T_i, \mu_2 \} \) to \( L_{\text{UAV}_2} \).

\( h_3 = \text{Oracle} \): \( \Gamma \) maintains a tuple \( \{ S_i, \mu_3 \} \) in the list \( L_{\text{UAV}_2} \) which is initialized to be empty. When receiving a request from \( \Lambda \) to query \( \{ S_i \} \), \( \Gamma \) queries whether tuple \( \{ S_i, \mu_3 \} \) is in list \( L_{\text{UAV}_2} \). If this tuple exists in the list, then \( \Gamma \) calculates \( \mu_3 = h_3(S_i) \) and returns \( \mu_3 \) to \( \Lambda \). Otherwise, \( \Gamma \) chooses a random \( \mu_3 \in Z_q^* \), calculates \( h_3 = h_3(S_i) \), sends \( \mu_3 \) to \( \Lambda \) and adds \( \{ S_i, \mu_3 \} \) to \( L_{\text{UAV}_2} \).

\( \text{Sign} = \text{Oracle} \): When \( \Gamma \) receives a request from \( \Lambda \) that contains a message \( M_i \) and an anonymous identity \( FID_i \), \( \Gamma \) chooses a random number \( s \) and calculates \( S_i = g^s \) and \( \Sigma_i = (\mu_3 - SK_i) \cdot s^{-1} \). \( \Gamma \) stores \( \{ M_i, FID_i, PK_i, S_i, T_i, \mu_2 \} \) in \( L_{\text{UAV}_2} \) and stores \( \{ S_i, \mu_3 \} \) in \( L_{\text{UAV}_2} \) and then sends the signature information \( Msg = \{ M_i, FID_i, PK_i, S_i, T_i, \Sigma_i, \sigma_i \} \) to \( \Lambda \). \( \Lambda \) is easy to verify Eq. (6):

\[ S_i^{\Sigma_i}, A_{\text{pub}}^{h_i(FID_i) \cdot RF_i} = g^{h_i(S_i)} \] (7)

If the equation does not hold, \( \Gamma \) interrupts the game, otherwise through the bifurcation principle [30], \( \Gamma \) only changes \( h_2 \) to repeat the above query process, \( \Lambda \) can obtain a new \( \Sigma_i' \) as \( \{ M_i, FID_i, PK_i, S_i, T_i', \Sigma_i' \} \), so it is easy to get the Eq. (8):

\[ S_i^{\Sigma_i'}, A_{\text{pub}}^{h_i(FID_i) \cdot RF_i'} = g^{h_i(S_i)} \] (8)
Through Eqs. (7) and (8), we can get:

\[
S_i^{\text{Sig}_{i}'} - \text{Sig}_{i} = A_{\text{pub}}^{h_i(\text{FID}_{i})}(f_i' - f_i) \tag{9}
\]

\[
g^{s_i(\text{Sig}_{i} - \text{Sig}_{i}')} = g^{a(\text{FID}_{i})}(f_i' - f_i) \tag{10}
\]

Through Eq. (10), we can get:

\[
s_i = a(\text{FID}_{i}) \cdot (f_i' - f_i)(\text{Sig}_{i} - \text{Sig}_{i}')^{-1} \tag{11}
\]

According to Eq. (11), \( \Lambda \) outputs \( s_i = a(\text{FID}_{i}) \cdot (f_i' - f_i)(\text{Sig}_{i} - \text{Sig}_{i}') \). This contradicts the difficulty of the ECDLP problem. Therefore, under the random oracle model, the privacy protection scheme based on anonymity proposed in this paper is safe under adaptive message selection attacks.

5.3 Security and attributes analysis

Message identity authentication According to the theorem, we can analyze and get that based on the difficulty of the ECDLP problem, no polynomial opponent can forge a valid message. The receiver can easily verify the integrity of the message \( \text{Msg} = \{\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i, \text{Sig}_{i}\} \) from the sender through a formula \( S_i^{\text{Sig}_{i}} \cdot A_{\text{pub}}^{h_i(\text{FID}_{i})} = g^{h_i(S_i)} \). Therefore, the attacker cannot obtain the signature information of the UAV, and thus cannot generate legal information.

Privacy protection The real identity \( \text{ID}_{i} \) of the UAV proposed in this paper is related to its anonymous identity \( \text{FID}_{i} = \text{ID}_{i} \oplus h_0(\text{PK}_{i}, \text{B}_{\text{pub}}) \). To find the true-identity \( \text{ID}_{i} \) of the UAV, the attacker needs to calculate \( \text{PK}_{i} = g^{k_{i}, b} \), \( \text{PK}_{i} = g^{h_{i}, b} \), \( \text{PK}_{i} = g^{h_{i}, b} \). However, due to the difficulty of ECDLP, the attacker cannot calculate \( \text{PK}_{i} \). Therefore, the ATS-LIA scheme proposed in this paper can protect the privacy of the UAV’s identity.

Traceability The real identity \( \text{ID}_{i} \) of the UAV proposed in this paper is related to its anonymous identity \( \text{FID}_{i} = \text{ID}_{i} \oplus h_0(\text{PK}_{i}, \text{B}_{\text{pub}}) \). Through the private key of the system, TC can calculate the real identity \( \text{ID}_{i} = \text{FID}_{i} \oplus h_0(\text{PK}_{i}, \text{B}_{\text{pub}}) \) of the UAV. Therefore, the solution proposed in this paper provides traceability functions.

Un-linkability UAV generates \( \{\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i, \text{Sig}_{i}\} \), \( \text{FID}_{i} = \text{ID}_{i} \oplus h_0(\text{PK}_{i}, \text{B}_{\text{pub}}) \), \( \text{PK}_{i} = g^{k_{i}, b} \), \( S_i = g^{h_{i}} \), \( \text{Sig}_{i} = (h_{i}(S_i) - \text{SK}_{i} \cdot f_i) \cdot s_i^{-1} \). Due to the randomness of \( k_{i} \) and \( s_i \), the attacker cannot find the correlation from the random information generated each time, so it is impossible to determine whether it is a message sent by the same UAV. Therefore, the solution proposed in this paper achieves non-connectivity.

Modification attack The UAV will broadcast message \( \text{Msg} = \{\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i, \text{Sig}_{i}\} \) to GCS. It is easy for an attacker to modify the information \( M \), which is eavesdropped on from the wireless communication channel. If the message sent by the UAV to the GCS is modified, we will verify whether the formula \( S_i^{\text{Sig}_{i}} \cdot A_{\text{pub}}^{h_i(\text{FID}_{i})} = g^{h_i(S_i)} \) is satisfied according to \( f_i = h_2(\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i) \) and \( \text{Sig}_{i} = (h_{i}(S_i) - \text{SK}_{i} \cdot f_i) \cdot s_i^{-1} \). If the broadcast information is found to be untrue, therefore, the solution proposed in this paper can resist message modification attacks.

Impersonation attack To impersonate the identity of a GCS or UAV, the attacker must have a legal message \( \text{Msg} = \{\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i, \text{Sig}_{i}\} \) and must pass verification \( S_i^{\text{Sig}_{i}} \cdot A_{\text{pub}}^{h_i(\text{FID}_{i})} = g^{h_i(S_i)} \). Therefore, it is difficult for an attacker to generate a legally signed message. UAVs and GCSs can easily detect whether the sender is being impersonated by the above equation. Therefore, the ATS-LIA scheme proposed in this paper can resist impersonation attacks.

Replay attack The timestamp of the scheme proposed in this paper is contained in \( \text{Msg} = \{\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i, \text{Sig}_{i}\} \). Because of the signature \( \text{Sig}_{i} = (h_{i}(S_i) - \text{SK}_{i} \cdot f_i) \cdot s_i^{-1} \), \( f_i = h_2(\text{M}_i, \text{FID}_{i}, \text{PK}_{i}, S_i, T_i) \) also contains a timestamp. UAVs and GCSs can easily determine whether the message is rebroadcast by verifying the freshness of the timestamp. Therefore, the solution proposed in this paper can resist replay attacks.

Man-in-the-middle attack This solution provides identity authentication for UAVs and GCSs during their communication. Therefore, the ATS-LIA scheme proposed in this paper can resist man-in-the-middle attacks.

The checklist is stolen attack Neither the UAV nor the GCS maintains a validator table for authentication, so they only need to store their private key. The attacker cannot steal any verification form for malicious attacks. Therefore, the solution proposed in this paper can resist the attack of checklist theft.

6 Implement analysis

In this section, we will analyze the performance of the identity based ATS-LIA scheme proposed for UAVs. It is mainly divided into two parts, including analysis computation cost and communication cost. We mainly analyze
the computational overhead of the identity-based privacy protection scheme in the UAV self-organizing network. We mainly calculate the computational overhead consumed in the message signature generation and message authentication phases. Compared with the Internet of Vehicles and sensor networks, the UAV self-organizing network has similar characteristics. Therefore, this paper mainly compares the schemes adopted by Bayat et al. [12], Gope and Sikdar [21], and Tian et al. [17].

In order to make a fair comparison, we use the famous password library MIRACL to calculate the execution time of password operations. We calculate the encryption time in the following environment: on a desktop computer with Intel (R) core (TM) i5-8500 CPU, frequency of 3.00 GHz and 8 GB RAM. Table 2 lists the symbol settings for the above operations and the average time required. Table 3 shows the calculation cost comparison of each step of these three schemes and the total calculation cost comparison.

This section mainly compares the time cost of the UAV message signature generation (MSG) phase and the UAV identity authentication (IA) phase verification.

For the NEAS scheme adopted by Bayat et al. in the MSG stage, there are mainly five bilinear correlation scalar multiplication operations and a hash function \(5T_m + T_h \approx 6.048ms\). In the IA stage, there are three bilinear pairing operations and one bilinear correlation addition operation, which is calculated as \(3T_p + T_a \approx 12.0609ms\). The total computational cost is \(Total \approx 18.1089ms\).

For the scheme adopted by Gope and Sikdar, in the MSG phase, there are mainly a bilinear correlation scalar multiplication operation, a bilinear correlation addition operation and a hash function \(T_m + T_a + T_h \approx 1.2189ms\). In the IA phase, it is mainly a bilinear pairing operation, a bilinear correlation scalar multiplication operation and two hash functions, which are calculated as \(T_p + T_m + 2T_h \approx 5.233ms\). The total computational cost is \(Total \approx 6.4529ms\).

The scheme adopted by Tian et al. in the MSG stage, mainly a bilinear correlation scalar multiplication operation, a bilinear correlation addition operation and a hash function, which are calculated as \(T_m + T_a + T_h \approx 1.2189ms\). In the IA phase, it is mainly a bilinear pairing operation, two bilinear correlation scalar multiplication operations and two hash functions, which are calculated as \(T_p + 2T_m + 2T_h \approx 6.442ms\). The total computational cost is \(Total \approx 7.6609ms\).

The scheme adopted in this paper is mainly based on an elliptic curve correlation scalar multiplication and two cryptographic hash functions in the MSG process, so the computational cost is \(3T_m + 2T_h \approx 0.426ms\). In the IA stage, there are mainly four scalar multiplication operations based on elliptic curves, one addition operation based on elliptic curves, and two encrypted hash functions, so the computational cost is \(3T_m + T_a + 2T_h \approx 1.246ms\). The total computational cost is \(Total \approx 1.6906ms\).

It can be seen from Fig. 7 that in the MSG, the program designed in this paper has an increase of about 92.96% in the time percentage of Bayat et al. program, and an increase of 65.05% in the time percentage of the program compared with Gope and Sikdar and Tian et al. In the IA, the time percentages of the ATS-LIA scheme designed in this paper are about 89.51%, 75.83%, and 80.37% higher than those of Bayat et al., Gope and Sikdar, and Tian et al. The total time cost of our program is 90.66% higher than that of Bayat et al. the percentage of time is about 73.80% higher than that of Gope and Sikdar, and the percentage of time is about 77.93% higher than that of Tian et al.

### Table 2: Execution time of different encryption operations

| Encryption operation | Definition                                    | Execution time (ms) |
|----------------------|-----------------------------------------------|---------------------|
| \(T_p\)              | Bilinear pairing operation                     | 4.018               |
| \(T_m\)              | Bilinear correlation scalar multiplication operation | 1.209               |
| \(T_a\)              | Bilinear correlation addition operation        | 0.0069              |
| \(T_m-ecc\)          | ECC related scalar multiplication operations  | 0.419               |
| \(T_a-ecc\)          | ECC related addition operations               | 0.0016              |
| \(T_h\)              | Cryptographic hashing                          | 0.003               |

### Table 3: Comparison of the calculation cost at each step

| Comparative literature | MSG                  | IA                  | Total                |
|------------------------|----------------------|---------------------|----------------------|
| Bayat et al. scheme [12]| \(5T_m + T_h \approx 6.048ms\) | \(3T_p + T_a \approx 12.0609ms\) | \(Total \approx 18.1089ms\) |
| Gope and Sikdar scheme [21]| \(T_m + T_a + T_h \approx 1.2189ms\) | \(T_p + T_m + 2T_h \approx 5.233ms\) | \(Total \approx 6.4529ms\) |
| Tian et al. scheme [17]| \(T_m + T_a + T_h \approx 1.2189ms\) | \(T_p + 2T_m + 2T_h \approx 6.442ms\) | \(Total \approx 7.6609ms\) |
| ATS-LIA scheme         | \(T_m-ecc + 2T_a \approx 0.426ms\) | \(3T_m-ecc + T_a-ecc + 2T_h \approx 1.246ms\) | \(Total \approx 1.6906ms\) |
The size of the element in $G$ which we selected in this paper is 40 bits, and the size of the output and timestamp of the general hash function are 20 bits and 4 bits respectively. Therefore, in this paper, the UAV sends $\{M_i, FID_{ij}, PK_{ij}, S_i, T_i, Sig_i\}$ to GCS, where $\{PK_{ij}, S_i, Sig_i\} \in G$ and $FID_{ij}$ are the hash operation results and $t$ is the timestamp. In all identity-based authentication schemes, the messages about the instruction status are similar, so this paper does not calculate the $M_i$ with instructions transmitted by UAV. Thus, the communication overhead is calculated as: $3 \times 40 + 20 + 4 + M_i = 144 + M_i$ bits.

7 Conclusion

As the application of UAVs becomes more and more widespread, it has also received more and more attention in the industry and academia. For the particularity of FANETs, this paper proposes a trust-based identity authentication scheme of UAV. Compared with other solutions, we consider the communication overhead of drone fleet certification, and choose the most credible representative UAV in the drone fleet to establish a communication link with the ground station. It can avoid the potential safety hazards caused by UAV nodes because of their moving speed fast and frequent access to the network. At the same time, this scheme designs two-way authentication based on elliptic curve for UAV and road station, which ensures that the authentication scheme is lightweight. Through the random oracle model, it is proved that the scheme proposed in this paper can resist various attacks. By comparison, the computational cost of this solution is also competitive.

Acknowledgements This work was supported by National Natural Science Foundation of China (61701170). Special project for key R & D and promotion of science and Technology Department of Henan Province (222102210052,222102210007,222102210062,222102210272)

Declarations

Conflict of interest We declare that we have no conflict of interest.

References

1. Ismail A, Bagula BA, Tuyishimire E (2018) Internet-of-things in motion: A UAV coalition model for remote sensing in smart cities. Sensors 18(7)
2. Xu C, Liao X, Tan J, Ye H, Lu H (2020) Recent research progress of unmanned aerial vehicle regulation policies and technologies in urban low altitude. IEEE Access 8:74175–74194. https://doi.org/10.1109/ACCESS.2020.2987622
3. Shao Z, Cheng G, Ma J, Wang Z et al. Real-time and Accurate UAV pedestrian detection for social distancing monitoring in COVID-19 pandemic. IEEE Trans Multimed. https://doi.org/10.1109/TMM.2021.3075566
4. Zhao J, Gao F, Ding G et al (2018) Integrating Communications and Control for UAV Systems: Opportunities and Challenges. IEEE Access 1–1
5. Shafique A, Mehmood A, Elhadef M (2021) Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access 9:46927–46948. https://doi.org/10.1109/ACCESS.2021.3066778
6. Vergouw B, Nagel H, Bondt G, Custers B (2016) Drone technology: types, payloads, applications, asser press, frequency spectrum issues and future developments. T.M.C
7. Saharan S, Bawa S, Kumar N (2019) Dynamic pricing techniques for Intelligent Transportation System in smart cities: A systematic review. Comput Commun 150
8. Guo W, Devine C, Wang S (2014) Performance analysis of micro unmanned airborne communication relays for cellular networks. Int Symp Commun Syst 658–663
9. Alsamhi SH, Ansari O, Ansari SM, Gupta SK (2019) Collaboration of drone and internet of public safety things in smart cities:
An overview of QoS and network performance optimization.

Drones

10. Li W, Meese C, Guo H et al (2020) Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof. CoRR 18–24

11. Song L, Sun G, Yu H et al (2020) FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles. IEEE Trans Veh Technol 69(5):5403–5415

12. Bayat M, Barmsboory M, Rahimi M et al (2015) A secure authentication scheme for VANETs with batch verification. Wirel Netw

13. He D, Ma M, Zhang Y et al (2011) A strong user authentication scheme with smart cards for wireless communications. Comput Commun 34(3):367–374

14. Gope P, Hwang T (2016) An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. J Netw Comput Appl 62(Feb.):1–8

15. Gupta L, Jain R, Vaszkun G (2016) Survey of Important Issues in UAV Communication Networks. EEE Commun Surv Tutor 18(2):1123–1152

16. Lin C, He D, Kumar N et al (2018) Security and privacy for the Internet of Drones: Challenges and solutions. IEEE Commun Mag 56(1):64–69

17. Tian Y, Yuan J, Song H (2019) Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. J Inf Secur Appl 48:102354

18. Chen L, Qian S, Ming L et al (2018) An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems. China Commun 15(005):61–76

19. Semal B, Markantonakis K, Akram RN (2018) A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)

20. 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

21. Gope P, Sikdar B (2020) An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of Drones. IEEE Trans Veh Technol

22. Jangirala S, Das AK, Kumar N et al (2019) TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment. IEEE Trans Veh Technol 1–1

23. Wazid M, Das AK, Kumar N et al (2018) Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones Deployment. IEEE Internet Things J 1–1

24. Yahuza M, Idris M, Wahab A et al (2021) An edge assisted secure lightweight authentication technique for safe communication on the Internet of Drones network. IEEE Access 99:1–1

25. Zhang N, Jiang Q, Li L et al (2021) An efficient three-factor remote user authentication protocol based on BPV-FourQ for internet of drones. Peer Peer Netw Appl 14(5):3319–3332

26. Ganeriwal S, Srivastava MB (2004) Reputation-based framework for high integrity sensor networks. ACM Trans Sensor Netw 4(3, article 15):66–77

27. Liu YanB, Gong XueH, Feng YanF (2014) Trust evaluation method based on behavior detection of Internet of Things nodes. J Commun 35(005):8–15

28. Abderrahim OB, Elhdbili MH, Saidane L (2017) TMCol-SIOT: A trust management system based on communities of interest for the social Internet of Things. Wirel Commun Mob Comput Conf (IWCMC) 747–752

29. Adewuyi AA, Cheng H, Shi Q, Cao J et al (2019) CTRUST: A dynamic trust model for collaborative applications in the Internet of Things. IEEE Internet Things J 6(3):5432–5445. https://doi.org/10.1109/JIOT.2019.2902022

30. Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. J Cryptol 361–396

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Xiaoyu Du received the BS degree in automation specialty from Henan University, Kaifeng, China, in 2003, and the PhD degree in information network from Nanjing University of Posts and Telecommunication, Nanjing, China, in 2015. She is an associate professor with the computer science and technology, Henan University. Her research interests include information security, wireless sensor networks and data center networks.

YinYin Li is currently pursuing the master’s degree with the computer science and technology, Henan University, China. Her research interests are information security and cryptography protocol.

Sufang Zhou received the B.S. degree in computer science from Henan Normal University in 2013, and the Ph.D. degree in computer software and theory from Shaanxi Normal University in 2019. She is currently a master supervisor within the School of Computer and Information Engineering, Henan University. Her research interests include secure multiparty computation, privacy-preserving machine learning.
Yi Zhou (M’15) received the B.S. degree in electronic engineering from the First Aeronautic Institute of Air Force, China, in 2002, and the Ph.D. degree in control system and theory from Tongji University, China, in 2011. From 2002 to 2005, he was a Research & Development Engineer with Beijing Centergate Technologies Co, Ltd., China. He was a Visiting Researcher with the Telecommunications Research Center (f.w.), Vienna, Austria, in 2009, and the National Institute of Informatics, Tokyo, Japan, in 2010. From 2014 to 2015, he was a Post-Doctoral Fellow with the University of Waterloo, Waterloo, ON, Canada. He is currently a professor with the School of Artificial Intelligence, Henan University, China. He is the Director of the International Joint Research Laboratory for Cooperative Vehicular Networks, Henan, China. He also leads the Institute of Collaborative ITS, Henan University, China. His research interests include vehicular cyber-physical systems, multi-agent cooperation for vehicular networks and internet of thing security.