Zhao *et al. Cybersecurity* (2024) 7:50
https://doi.org/10.1186/s42400-024-00247-3

Cybersecurity

RESEARCH

Open Access

Lightweight ring-neighbor-based user authentication and group-key agreement for internet of drones

Zhuo Zhao[1], Chingfang Hsu[2,3*], Lein Harn[4], Zhe Xia[5], Xinyu Jiang[6] and Liu Liu[3]

Abstract

As mobile internet and Internet of Things technologies continue to advance, the application scenarios of peer-to-peer Internet of Drones (IoD) are becoming increasingly diverse. However, the development of IoD also faces significant challenges, such as security, privacy protection, and limited computing power, which require technological innovation to overcome. For group secure communication, it is necessary to provide two basic services, user authentication and group key agreement. Due to the limited storage of IoD devices, group key negotiation requires lightweight calculations, and conventional schemes cannot satisfy the requirements of group communication in the IoD. To this end, a new lightweight communication scheme based on ring neighbors is presented in this paper for IoD, which not only realizes the identity verification of user and group key negotiation, but also improves computational efficiency on each group member side. A detailed security analysis substantiates that the designed scheme is capable of withstanding attacks from both internal and external adversaries while satisfying all defined security requirements. More importantly, in our proposal, the computational cost on the user side remains unaffected by the variability of the number of members participating in group communication, as members communicate in a non-interactive manner through broadcasting. As a result, the protocol proposed in this article demonstrates lower computational and communication costs in comparison to other cryptographic schemes. Hence, this proposal presents a more appealing approach to lightweight group key agreement protocol with user authentication for application in the IoD.

Keywords IoD, Secure group communications, Group key agreement, User authentication, Asymmetric bivariate polynomial, Lightweight ring-neighbor-based

Introduction

Since the emergence of the Internet, the number of connected devices has been continuously skyrocketing. This upward trend is fueled by increasing reliance on and pursuit of the Internet, driving the expansion of network connections across various types of devices. From smartphones and computers to household appliances and cars, almost all technological domains are rapidly integrating with the Internet, making our daily lives closely intertwined with the digital world. These interconnected devices will generate, share, collect, and enable varied data utilization, further promoting the transmission, communication, and interaction of information.

*Correspondence:
Chingfang Hsu
cherryjingfang@gmail.com
[1] Faculty of Artificial Intelligence in Education, Central China Normal University, Wuhan 430079, China
[2] Hubei Provincial Key Laboratory of Artificial Intelligence and Smart Learning, Central China Normal University, Wuhan 430079, China
[3] School of Computer, Central China Normal University, Wuhan 430079, China
[4] Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO 64110, USA
[5] Department of Computer Science, Wuhan University of Technology, Wuhan 430071, China
[6] Joint Wollongong Institute, Central China Normal University, Wuhan 430079, China

The widespread application of IoT technology has facilitated the seamless integration of drones with various devices, systems, and platforms, significantly advancing the development of Internet of Drones (IoD) (Derhab et al. 2023). This advancement has attracted considerable attention in academia and industry. Due to their exceptional flexibility, convenience, and efficiency, the Unmanned Aerial Vehicles (UAVs) (Drones) have replaced human involvement in mechanical and high-risk activities across numerous fields, thereby substantially improving work efficiency and quality of life (Badshah et al. 2024; Cui et al. 2020). For instance, drones can be deployed for the rapid delivery of pharmaceuticals and medical supplies to enhance the efficiency of emergency responses. Similarly, they can precisely locate missing persons during search and rescue operations. Moreover, drones are also employed in critical tasks such as military reconnaissance and traffic monitoring, providing timely and essential information to prevent and manage emergency situations.

A typical application scenario of IoD is illustrated in Fig. 1. These drones collect data via their integrated sensors, cameras, and microphones, and then use their own communication modules such as Wi-Fi, Bluetooth, and WLAN to transmit these data to the control center through public channels. Hence, drone technology offers an efficient means for users to obtain relevant information in real-time from a distance. In most application scenarios, drones often collect data containing sensitive private information, rendering these drones highly vulnerable to physical interception and data tampering when operating in public spaces. This leads to significant data security challenges. Additionally, as devices constrained by limited resources, the restricted memory and computational power of drones limit their ability to implement complex security protocols. Therefore, how to achieve lightweight computational and communication costs while ensuring robust security for data has become a critical issue that urgently needs addressing in this technological domain.

Drone communications in IoD face two principal data security challenges, authentication and privacy (Gupta et al. 2015; Lin et al. 2018). In open environments, besides the data gathered by drones, adversaries might also aim at the identities of drones and their geographic locations (that is, their flight routes) to acquire confidential information concerning the usage of drones and the facilities they are monitoring. Therefore, it is imperative that all entities participating in drone communications are thoroughly authenticated, and that encryption protocols are employed on the communication data to protect drones against attacks targeting their privacy, thus averting the leakage of sensitive information.

Due to the limited operational range of individual drones, practical scenarios often require the simultaneous deployment of multiple drones for collaborative purposes. In this circumstance, group communication among drones becomes essential. Considering the serious risk of information leakage while transmitting data to recipients in a public and open environment, establishing a confidential group key among different group members is fundamental to ensuring the security of group communications (Zhang et al. 2020; Gope and Sikdar 2020; Hsu et al. 2023c, 2021). This approach to group-based

Fig. 1 The typical application scenario of IoD

key negotiation requires the preliminary dissemination of one-time session key to all users. This one-time session key plays a pivotal role in creating a confidential group key among the group members. It is imperative to ensure that the generated group key is kept confidential and is only known to the members participating in the current session. This group key is subsequently used to encrypt all information transmitted in later communications, thus ensuring secure group communications.

In secure communications, the aim of key negotiation schemes is to distribute session keys to users securely. Researchers have utilized various cryptographic technologies to propose effective group key negotiation strategies that meet the security needs for confidentiality and integrity, among other aspects, within group communications. The initially proposed Diffie-Hellman scheme (Diffie and Hellman 1976) is a distinctive key exchange solution that enables encrypted communication between two users by agreeing upon a shared key without the requirement of transmitting it over an open public channel. This protocol laid the cornerstone for the advancement of modern key exchange algorithms and has become a popular tool for establishing keys. However, due to the limitation of the Diffie-Hellman proposal being applicable only to two users, numerous scholars have built upon this foundation to design new group key distribution protocols (Joux 2000; Boneh et al. 2001). Laih et al. (1989) proposed a group key distribution scheme, which employs secret sharing technique. Its core idea is to have a trusted group administrator distribute tokens to authorized group members and broadcast them to all participating members, thereby establishing a shared key. A conference key distribution system was introduced by Burmester and Desmedt (1994), which utilizes public-key cryptography to generate a group key for the attending members. Subsequently, Harn and Lin (2010) presented another group key agreement protocol where the group key is concealed within a polynomial and broadcasted simultaneously to all members within the group. This innovative approach proves to be more cost-effective and efficient compared to point-to-point communication.

As an increasing number of smart devices integrate into the IoD, the presence of millions of devices and the wireless data transmission across various systems markedly elevate the risks associated with cybersecurity (Abualigah et al. 2021; Derhab et al. 2023; Tanveer et al. 2021). To ensure the security of data within the IoD, there is a necessity for the efficient authentication of a multitude of nodes. This process guarantees that only authorized users can access the data, thus preserving the confidentiality of information. Due to several factors, traditional one-to-one authentication schemes are no longer suitable for the current complex IoD environment (Hsu et al. 2023b). On one hand, the low power consumption constraints of nodes within the IoD limit their ability to process complex computations and communications. Conventional group key protocols in this environment require constant-round communication with lightweight computation overhead on each group member side (Zhang et al. 2020; Gope and Sikdar 2020). On the other hand, the extensive number of devices poses a challenge for servers to process numerous authentication requests concurrently (Zhang et al. 2020; Hussain et al. 2021). Consequently, there is an urgent need to design lightweight group authentication protocols for the IoD environment that can simultaneously verify the legitimacy of group members and ensure secure communication among different members within the group.

Sharma and Purushothama (2022) designed a lightweight membership-authenticated group key establishment for resource-constrained smart environments using symmetric bivariate polynomials. By using symmetric binary polynomials, Hsu et al. (2023a) presented a structure for lightweight authentication in conjunction with joint arithmetic computation within the context of 5G IoT networks. This framework incorporates both member authentication and collaborative arithmetic computation functionalities, ensuring efficient computation and communication for each group member. Tian et al. (2019) introduced a privacy protection strategy for the IoD environment, utilizing an online/offline signature design. Additionally, they also proposed an authentication method by employing mobile edge computing. Zhang et al. (2020) presented an alternative lightweight authentication and key negotiation scheme for IoD. The verification process within this scheme only utilizes one-way hash functions and XOR operations. However, in the protocol, drones are required to store security credentials to authenticate their identities to other participants. This introduces a potential vulnerability, in the event of a physical assault on a drone, it becomes feasible for adversaries to access the preserved credentials. The existing authentication protocols (Zhang et al. 2020; Tian et al. 2019; Srinivas et al. 2019; Cho et al. 2020) designed for IoD uniformly confront a similar threat, that is, the privacy and security concerns arising from physical attacks on drones. PMAP is a lightweight and privacy-preserving protocol designed by Pu et al. (2022). It consists of two components: the first part authenticates the identities of drones and service providers and establishes a secure session key, while the second part authenticates the drone identities and establishes a secure session key. Notably, the latter employs Physical Unclonable Functions (PUFs) and chaotic systems to support the negotiation process.

Based on the analysis of the security and privacy challenges prevalent in IoD, this paper proposes a novel and

efficient scheme for user authentication and key negotiation. Unlike existing drone security solutions, the proposed approach employs asymmetric binary polynomials and addition operations to simultaneously support member authentication and the establishment of a group key. Furthermore, it provides the necessary security features for privacy protection without the need to store any keys on the devices. In registration stage, the membership registration center (MRC) is responsible for distributing a token for each registered member. The token refers to the univariate polynomial calculated by the asymmetric bivariate polynomial, which is used to distribute paired shared keys and verify the identity of the member. Subsequently, each group member uses addition to blend the secret key shared by her/him and the two neighbors in the group ring with his secret input value to obtain an output value. This output value is encrypted with the pairwise keys that she/he shares with other members of the group ring, generating a secret value that is then broadcasted to the corresponding group members. Finally, the participating members utilize all the received values to compute the group key, so as to facilitate subsequent secure communication. The presented ring-neighbor-based lightweight protocol is especially suitable for IoD environments.

The main contributions of this research are as follows.

- An efficient scheme for membership authentication and group key agreement is presented for secure communication in IoD environment, which is constant-round communication with lightweight computation overhead for each group member side.
- Tokens, initially derived from asymmetric binary polynomials, are employed for authenticating members and distributing pairwise shared keys.
- The principal computational method of the proposed scheme is addition, substantially reducing the computational burden on users.
- A distinctive feature of our scheme is that the computational overhead on the side of each group member does not increase linearly or logarithmically with the size of the group membership.
- The security analysis clearly demonstrates that our scheme can effectively withstand internal and external attacks, while satisfying all defined security requirements.

Organization: "Preliminaries" section introduces the relevant preliminaries. The models of the presented protocol are described in "Model of our proposed protocol" section. In "Our proposed protocol" section, a comprehensive outline of our proposal is provided. We analyze the security of this proposal in detail and discuss various aspects of its performance in "Analysis" section. Finally, "Conclusion" section summarizes this study.

Preliminaries

The Shamir's threshold secret sharing scheme SS (Shamir 1979) is a classic encryption algorithm. Its implementation principle involves obtaining t points on a polynomial curve for any $t-1$ degree polynomial function. These points can be used to determine the function through polynomial interpolation methods. The specific process begins with the secret owner selecting an arbitrary polynomial $f(x)$, where $f(0)=s$, with s representing the secret information. Subsequently, the share $f(x_i) mod\ p$, is generated for each participant and distributed to the corresponding participant, where $i=1,2,\ldots,n$, p is a prime satisfying $p>s$, x_i denotes the identifier of the participant. It should be noted that the recovery of the secret information s requires a collective combination of at least t shares from the participating parties.

Due to the limitation in Shamir's SS where shareholders cannot ascertain the validity of shares received from the dealer, Chor et al. (1985) extended this SS in 1985 to devise the first verifiable secret sharing (VSS). This scheme allows shareholders to authenticate the validity of shares received from the dealer. If the shares are found to be invalid, shareholders are entitled to request the dealer to regenerate new shares. Subsequently, researchers (Cramer et al. 1592; Cheng and Agrawal 2005; Desmedt and Frankel 1991; Katz et al. 2008; Kumaresan et al. 2010; Knuth 1981a) have broadened the application from univariate polynomial functions to bivariate functions to design more efficient schemes, BVSSs. Suppose there is a $t-1$ degree bivariate polynomial $F(x,y)=\sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{i,j}x^i y^j mod\ p$, where $a_{i,j}\in GF(p)$, and p is a prime. Bivariate polynomials are further classified into two types: symmetric and asymmetric, similarly, BVSSs are divided into two categories, SBVSSs (Cheng and Agrawal 2005; Katz et al. 2008; Knuth 1981a) and ABVSSs (Cramer et al. 1592; Desmedt and Frankel 1991; Kumaresan et al. 2010). The former refers to polynomials where the coefficients satisfy the condition $a_{i,j}=a_{j,i}, \forall i,j\in[0,t-1]$. Similar to the univariate polynomial-based secret sharing protocol mentioned above, in SBVSS, the secret owner randomly defines a polynomial $F(x,y)$ of degree $t-1$, where $F(0,0)=s$. Each share $F(x_i,y) \bmod p, i=1,2,\ldots,n$ is distributed to the corresponding participant U_i and kept securely. The share is a univariate polynomial of degree $t-1$ generated based on the symmetric polynomial $F(x,y)$, and satisfies $F(x_i,x_j)=F(x_j,x_i)$, $\forall i,j\in[0,t-1]$. Consequently, participants U_i and U_j can posse a shared key

$F(x_i, x_j) = F(x_j, x_i)$. Similarly, in ABVSS, each shareholder U_i can obtain a pair of shares, $F(x_i, y)$ mod p and $F(x, x_i) mod\ p, i = 1, 2, \ldots, n$, generated by the secret owner, and establish a shared pairwise secret key, $F(x_i, x_j)$ or $F(x_j, x_i)$, with other shareholder U_j.

This paper aims to design a lightweight and efficient membership authentication and group key negotiation scheme for IoD. The three solutions of verifying membership, distributing pairwise shared keys, and negotiating group keys are integrated into our construction. In contrast to most current secure communication solutions (Yang et al. 2023; Bai et al. 2022; Wang et al. 2022; Roy and Bhattacharya 2022) that require additional steps for member authentication and shared key distribution, as well as interactive communications or complex computations for encryption and decryption, our approach presents considerable benefits in communication and computational expenses owing to its integrated and non-interactive characteristics. Furthermore, utilizing a method based on ring neighbors ensures that the computational burden for each group member does not increase linearly or logarithmically with the size of the group. That is, regardless of the number of participants in group communication, the computational cost for individuals within the group remains constant.

Model of our proposed protocol

We design models of the presented proposal from two perspectives of network and security respectively. The following is a detailed introduction.

Network and communication model

In resource constrained environments, for example, in a typical Internet of Drones (IoD) model, there are typically three foundational elements: trusted authority (TA), IoD infrastructures (II) and smart devices (SD). Through IoD, these three types of participants are able to interconnect and form a vast communication network. Smart Devices can share various types of information with each other and with the IoD infrastructure, thus enhancing the efficiency of IoD information processing. Communication between Smart Devices and everything else represents one form of intelligent environment communication, referring to the interactions between Smart Devices and any entity. In addition, there are other types of communications, such as SD-to-SD communication, SD-to-II communication. The typical IoD model is

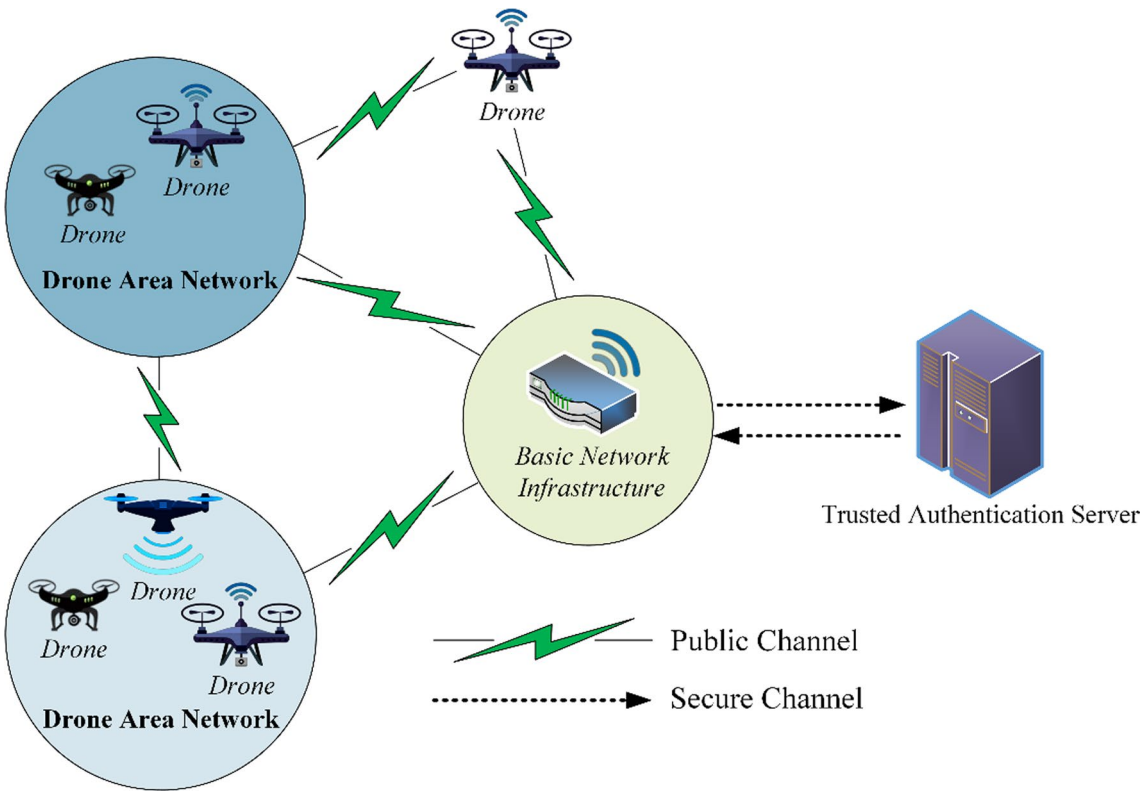

Fig. 2 Typical Internet of Drones (IoD) model

illustrated in Fig. 2, featuring both SD-to-SD and SD-to-II communication. The protocol we propose is designed to secure group communications within this network model, where the TA is fully trusted and responsible for member registration. Participants in group communication can include smart devices such as drones, as well as IoD infrastructure.

In this IoD model, it is assumed that there there are n users $\{U_1, U_2, \ldots, U_n\}$, who belong to a communication group. The proposed scheme is primarily divided into three steps: user registration, authentication of group members, and group key agreement. Firstly, all users who want to participate in the application need to register with TA. TA is responsible for user management, including deletion of unregistered users and registration of new users. Upon completion of the registration process, TA assigns each user a unique secret token. Before engaging in actual communication, users are required to authenticate their identity to ensure the legitimacy of those intending to participate in group communications. Typically, if all users involved in the communication are legitimate members of the group and act honestly, the protocol executes successfully, meaning that only legitimate members of the same group can obtain the session key for that group. Otherwise, the protocol fails to execute, meaning that no secret information will be disclosed to the group members. Therefore, member authentication is necessary before establishing a group key. Group key negotiation refers to the collaborative process by which all members establish a shared key before participating in group communication, ensuring the confidentiality of data transmitted during the communication process.

The specific process of our model is briefly outlined below. Suppose that a group ring is formed m (i.e., $2 \leq m < n$) members $\{U_{v_1}, U_{v_2}, \ldots, U_{v_m}\}$ in a certain fixed order as shown in Fig. 3, where $m = 6$. First, interactive authentication is performed among all participating members to demonstrate their membership in the communication group. Specifically, each member broadcasts a randomly selected integer within the group. The generated value, obtained by inputting the key shared with other member and the received random value from this member into a hash function, serves as the authentication response for this member. This response value is then used to verify the identity of the member, that is, whether they belong to the same communication group. Subsequently, each member adds their secret share to the paired keys shared with their two neighboring members, and the resulting output value is broadcasted to the entire group. The group key is reconstructed by combining all the received values, and used for subsequent secure communication. Our solution employs lightweight operations, such as addition, to achieve group member authentication and group key negotiation. Most importantly, it is a non-interactive protocol that enables the construction of a group key without the need for direct interactions among the members. These significantly enhance the efficiency of our scheme, with a detailed analysis and discussion of the performance evaluation to be presented in "Analysis" section.

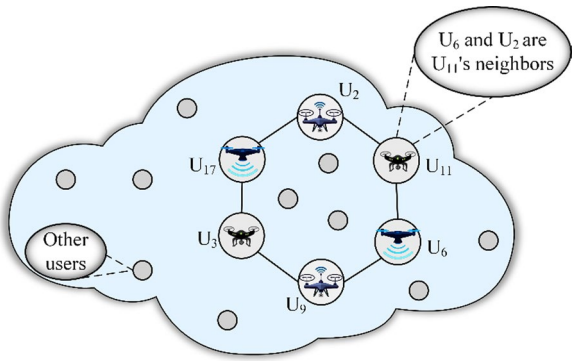

Fig. 3 A group ring of five members

Security model

Considering the highly sensitive nature of the information collected in the IoD environment, the data transmitted by drones over open networks are vulnerable to security risks. Hence, ensuring that the presented group key negotiation protocol meets the security required for IoD is of utmost importance. This subsection presents the security model of our proposal, and the corresponding proof analysis process is provided in "Analysis" section.

Type of adversaries

This paper discusses two distinct forms of attacks: internal attacks and external attacks. Internal attacks refer to the attempts made by registered users, who have obtained tokens, to launch attacks by utilizing their own tokens with the aim of recovering the polynomial and gaining access to secret information. In contrast, external attacks involve illegal adversaries without valid tokens trying to generate valid tokens in order to impersonate legitimate members and gain access to information beyond their authorized knowledge.

Security features

To ensure a robust group key agreement, it is crucial to fulfill the following essential security criteria.

(1) *Correctness* In the case where all members participating in group communication comply with to the protocol rules, the authentication of members

and the correct recovery of the group key can be achieved.

(2) *Freshness of authentication response* Each member is required to send a one-time response to other members within the group as proof of their identity, which is only used for this round of communication.

Freshness of group key The group key used in each session is unique to prevent malicious adversaries from exploiting a previously used key to deceive the system.

Freshness of the group key authentication The verification message utilized to validate the correctness of the group key is also disposable and cannot be reused.

(3) *Forward secrecy of group keys* Users who have not taken part in the ongoing group communication are incapable of recovering the key that has been established solely for the current group communication.

Backward secrecy of group keys Participants in the current group communication are unable to retrieve previously used group key.

Security assessment

This section outlines the security assessment criteria that a group key agreement (GKA) protocol should meet. The specific standards are as follows:

- *Resistant to key compromise impersonation attack* Even if a member U_i's token is disclosed, an adversary cannot impersonate any legitimate group member when U_i is present, such as the adversary in a man in the middle (MITM) attack.
- *Key authentication* Ensures that every group member is assured that no entities other than the current participants in the key negotiation can know the established session key.
- *Contributiveness* Every group member is confident that their contribution, that is one-time key, has been used in computing the group key.
- *Known-key security* Even if a session key is compromised and disclosed to an adversary, they cannot derive the keys of other sessions based on that key.

At the same time, we can clearly see that in the IoD scenario, the authentication of group membership and the establishment of group keys also need to meet all the above security requirements, as follows:

(1) Mutual authentication can be achieved through Group membership authentication;
(2) Session key agreement can be achieved through Group key agreement;
(3) Effectively interception for illegal login can be achieved through Freshness of authentication response;
(4) Resist device loss attack and Resist physical attack can be achieved through Known-key security;
(5) Resist impersonation attack can be achieved through Resistant to key compromise impersonation attack;
(6) Resist privileged insider attack It can be achieved by resisting inside attack;
(7) Resist de-synchronization attack can be achieved by ensuring Freshness of group key and group key authentication;
(8) Forward and backward secrecy can be achieved by Forward and Backward secrecy of group keys.

Our proposed protocol

This paper presents an innovative approach for establishing secure sessions within the IoD environment, which is a lightweight group key agreement proposal with user authentication based on ring neighbors. It utilizes binary asymmetric polynomial for constructing group keys and primarily employs addition as the main mathematical operation. The detailed procedure of the scheme is illustrated in Fig. 4. The notations used in our protocol is shown in Table 1.

Analysis

This section will provide a detailed discussion and analysis of the security and performance of the presented scheme.

Security analysis

Firstly, a comprehensive analysis of the security features and two distinct attack scenarios discussed in "Security Model" section is conducted.

Security features

Theorem 1 (Correctness) *The presented scheme can verify the legitimacy of the identities of all participants in group communication and then successfully negotiate a secret group key among them.*

Proof *Membership authentication* The value $Auth_{i,j} = h(k_{i,j} \parallel r_j)$ for each member U_{v_i} to verify membership is calculated based on his token and selected random integer, which is used to verify the membership of U_{v_i} to U_{v_j}. Only registered users possess secret tokens,

Token generation

Suppose there are n users $U_1, U_2, \ldots, U_n$.

TA randomly selects an asymmetric bivariate polynomial, $F(x,y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{1,1}xy + a_{2,0}x^2 + a_{0,2}y^2 + a_{1,2}xy^2 + a_{2,1}x^2y + a_{2,2}x^2y^2 + \ldots + a_{t-1,h-1}x^{t-1}y^{h-1} mod\ p$, where $a_{i,j} \in GF(p), \forall i \in [0, t-1], \forall j \in [0, h-1]$, and p is a prime integer with $p > n$. $F(x,y)$ is $t-1$ degree in x and $h-1$ degree in y, and satisfies $h > 2t-2$, which will be proven in Theorem 1. Each registered member U_i will get a token $(s_i(y), s_i(x))$ secretly transmitted by TA, where $i = 1,2,\ldots,n$. The token is a pair of shares generated by TA, $s_i(y) = F(x_i, y)$ and $s_i(x) = F(x, x_i)$, where $x_i \notin \{0,1\}$ is the public information associated of user U_i.

Membership authentication

Suppose there are m users $\{U_{v_1}, U_{v_2}, \ldots, U_{v_m}\}$ who want to participate in group communication of IoD applications, and these m members are connected in a sequential order to form a group ring, as depicted in Fig. 3, where $2 \le m < n$.

Step 1. Each member U_{v_i} randomly picks an integer $r_i \in GF(p)$, and broadcasts it in the group, where $i = 1,2,\ldots,m$.

Step 2. Member U_{v_i} calculates the shared pairwise key $k_{i,j} = s_{v_i}(x_{v_j}) = F(x_{v_i}, x_{v_j})$, with other members in the group by using one share of his token, $s_{v_i}(y)$ or $s_{v_i}(x)$, where $j = 1,2,\ldots,m, j \neq i$ and $x_{v_i} < x_{v_j}$. $k_{i,j}$ refers to the shared pairwise key between member U_{v_i} and member U_{v_j}.

Step 3. In order to verify his identity with other members, member U_{v_i} needs to calculate $Auth_{i,j} = h(k_{i,j} \| r_j)$, where $h()$ represents a cryptographic hash function with irreversible properties, and $j = 1,2,\ldots,m, j \neq i$. Then, the value $Auth_{i,j}$ is used as an authentication response and sent publicly to member U_{v_j}.

Step 4. After receiving the response $Auth_{i,j} = h(k_{i,j} \| r_j)$ from member U_{v_i}, the member U_{v_j} calculates $h'(k_{i,j} \| r_j)$ by using the pairwise shared key $k_{i,j} = s_{v_i}(x_{v_j}) = F(x_{v_i}, x_{v_j})$ to verify the identity of member U_{v_i}. And then U_{v_j} checks if $Auth_{i,j} = h'(k_{i,j} \| r_j)$. If the verification is successful, it means that member U_{v_i} is legitimate; otherwise, member U_{v_j} regards U_{v_i} as an illegal member. Repeat the above process until all members $U_{v_i}(i = 1,2,\ldots,m)$ in the group have been verified.

Fig. 4 Membership authentication and group key establishment

Group key establishment and authentication

Assuming that all members $\{U_{v_1}, U_{v_2}, \ldots, U_{v_m}\}$ have passed the above-mentioned identity verification and are recognized as legitimate members. And then, the group members perform the group key agreement process by using addition operations. In this process, all transmitted secret information is required to be encrypted with the shared keys $k_{i,j}$.

Step 1. Member U_{v_i} randomly selects a secret value $s_i \in GF(p)$ and an integer, $l_i \in GF(p)$, and then broadcasts l_i to other members of the group.

Step 2. Member U_{v_i} $(i \neq 1, m)$ uses the paired keys that she/he shares with her/his two neighbors in the group ring to compute

$$q_{v_i} = s_i + (-1)^a k_{i,i-1} + (-1)^b k_{i,i+1} mod\ p,$$

where $\begin{cases} if\ v_i < v_{i-1}, then\ a = 0; \\ if\ v_i > v_{i-1}, then\ a = 1, \end{cases}$ and $\begin{cases} if\ v_i < v_{i+1}, then\ b = 0; \\ if\ v_i > v_{i+1}, then\ b = 1, \end{cases}$.

The member U_{v_1} uses the paired keys that she/he shares with her/his two neighbors in the group ring to compute

$$q_{v_1} = s_1 + (-1)^a k_{1,m} + (-1)^b k_{1,2} mod\ p,$$

where $\begin{cases} if\ v_1 < v_m, then\ a = 0; \\ if\ v_1 > v_m, then\ a = 1, \end{cases}$ and $\begin{cases} if\ v_1 < v_2, then\ b = 0; \\ if\ v_1 > v_2, then\ b = 1, \end{cases}$.

The member U_{v_m} uses the paired keys that she/he shares with her/his two neighbors in the group ring to compute

$$q_{v_m} = s_m + (-1)^a k_{m,m-1} + (-1)^b k_{m,1} mod\ p,$$

where $\begin{cases} if\ v_m < v_{m-1}, then\ a = 0; \\ if\ v_m > v_{m-1}, then\ a = 1, \end{cases}$ and $\begin{cases} if\ v_m < v_1, then\ b = 0; \\ if\ v_m > v_1, then\ b = 1. \end{cases}$

Step 3. Member U_{v_i} encrypts q_{v_i} by using the pairwise shared keys $k_{i,j}$, and obtains $u_{i,j} = E_{k_{i,j}}(q_{v_i})$. Then this ciphertext $u_{i,j}$ is sent to member U_{v_j}.

Step 4. By using the pairwise shared key $k_{i,j}$, member U_{v_i} decrypts the received ciphertext $u_{j,i}$, and obtains $q_{v_j} = E_{k_{i,j}}(u_{j,i})$.

Step 5. Each member U_{v_i} uses the decrypted q_{v_j} to calculates $\sum_{j=1}^{m} q_{v_j} mod\ p = \sum_{j=1}^{m} s_j mod\ p = K_i$, where $i = 1,2,\ldots,m,\ j = 1,2,\ldots,m, j \neq i$.

Step 6. Each member U_{v_i} calculates $H(K_i||L)$ $(i = 1,2,\ldots,m)$ and transmits it to other group members through broadcast. And then member U_{v_i} checks if $H(K_1||L) = H(K_2||L) = \cdots = H(K_i||L) = \cdots = H(K_m||L) mod p$, where $L = \sum_{i=1}^{m} l_i$ and $H()$ represents a unidirectional hashing function with irreversible characteristics. If it is so, K_i obtained by each member U_{v_i} is used as the secret key for group communication, that is $K_i = K$. All group members U_{v_i} $(i = 1,2,\ldots,m)$ repeat this step to obtain the group key for communication.

Fig. 4 continued

Table 1 Notations table

Notation	Description
U_i	User *i*
MRC	Membership registration center
GKA	Group key agreement
p	A prime integer with p > n
F(x, y)	A random asymmetric polynomial
$k_{i,j}$	Pairwise shared key between U_{v_i} and U_{v_j}
E(•)	Encryption algorithm using pairwise shared key
D(•)	Decryption algorithm using pairwise shared key
h(•), H(•)	One-way hash functions
K	Secret group communication key
||	String concatenation operation

making it impossible for unauthorized adversaries without tokens to pass identity authentication using counterfeit ones.

Group key establishment The correctness of this process is determined by the rules of addition operation. Since $q_{v_i} = s_i + (-1)^a k_{i,i-1} + (-1)^b k_{i,i+1} mod\ p$,

where $\begin{cases} if\ v_i < v_{i-1},\ then\ a = 0; \\ if\ v_i > v_{i-1},\ then\ a = 1, \end{cases}$ and $\begin{cases} if\ v_i < v_{i+1},\ then\ b = 0; \\ if\ v_i > v_{i+1},\ then\ b = 1. \end{cases}$

we can obtain $\sum_{i=1}^{m} q_{v_i}\ mod\ p = \sum_{i=1}^{m} s_i\ mod\ p = K_i i = 1, 2, \ldots, m.$

Group key authentication After the group members compute the key, they further verify its correctness using the computation formula $H(K_1||L) = H(K_2||L) = \cdots H(K_i||L) = \cdots = H(K_m||L) \bmod p$. If all the equations are satisfied, it confirms the correctness of the obtained group key, allowing for subsequent secure communication.

Theorem 2 *The presented scheme features security characteristics including freshness of authentication response, freshness of group keys and freshness of the group key authentication.*

Proof *Freshness of authentication response* The message $Auth_{i,j} = h(k_{i,j} \parallel r_j)$, used to verify user identity authentication, is produced by employing a hash function on the combination of the paired key $k_{i,j}$ and a random number r_j. $k_{i,j}$ is shared between user U_{v_i} and user U_{v_j}, and r_j is selected by U_{v_j}. As r_j is different for each session, it effectively withstands the replay attack from adversaries.

Freshness of group keys As shown in equation $K = \sum_{i=1}^{m} s_i\ modp$, the group key is derived from the secret input s_i of U_{v_i}. Since s_i is randomly selected, it ensures the one-time nature of the group key K. That is, our protocol meets the goal of *Contributiveness.*

Freshness of the group key authentication The verification message $H(K_i||L)$ is computed by applying a unidirectional hashing function to the sum of the secret inputs s_i of all members and the sum of random integers l_i. The randomness of K_i and L ensures the freshness of the authentication message, making it impossible to authenticate the current key based on past messages.

Theorem 3 *The proposed protocol achieves the backward and forward secrecy of group keys. i.e., the newly joined members cannot recover past group keys, and members who have left the group cannot access the future group keys.*

Proof *Forward secrecy of group keys* In each session, the group key K used for encrypting communication data is collaboratively generated by the members who are currently involved in the negotiation. Therefore, members who have already left are unable to obtain the random numbers required to establish the key, and thus cannot acquire the group key used for the current session. We can see that the group key is different in every session. In other words, each member involved in the current group is convinced that his/her contribution has been used to calculate the group key. Simultaneously, individuals outside the group are unable to fabricate the authentication response, as they lack knowledge of the current members' secret tokens. Furthermore, this group key establishment process can against inside and outside attacks (see Theorems 4 and 5). Therefore, the members who have left the group cannot access the future group keys.

Backward secrecy of group keys Similarly, the members who are currently involved in the session are also unable to access the random numbers required to establish the keys used in the past, which means they cannot be aware of the key used in previous group communications. The group key is exclusively known by the members who participated in its establishment process. We can see that the group key is different in every session. In other words, each member involved in the current group is convinced that his/her contribution has been used to calculate the group key. Simultaneously, individuals outside the group are unable to fabricate the authentication response, as they lack knowledge of the current members' secret tokens. Furthermore, this group key establishment process can against inside and outside attacks (see Theorems 4 and 5). Therefore, the newly joined members cannot recover past group keys.

Possible attacks

Theorem 4 (Inside Attack) *In the case of* $h > 2t - 2$, *it is necessary to have a minimum of t internal attackers to restore the tokens. The polynomial* $F(x, y)$ *of the proposed scheme can withstand a joint attack from up to* $t - 1$ *internal adversaries.*

Proof The internal attackers in our scheme are legitimate registered users who possess valid secret tokens. Asymmetric bivariate polynomial, $F(x,y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{1,1}xy + a_{2,0}x^2 + a_{0,2}y^2 + a_{1,2}xy^2 + a_{2,1}x^2y + a_{2,2}x^2y^2 + \ldots + + a_{t-1,h-1}x^{t-1}y^{h-1} modp$, has *th* different coefficients. Each token $\{s_i(y), s_i(x)\}$ can be used to generate $t + h$ linearly independent equations based on the coefficients of $F(x, y)$, because $s_i(y)$ is $h - 1$ degree and $s_i(x)$ is $t - 1$ degree. If there are $t - 1$ users colluding jointly, $(t + h)(t - 1)$ equations can be obtained. Meanwhile, $t - 1$ colluding users also have $2C_2^{t-1}$ pairs of secret keys. Therefore, they can obtain $(t + h)(t - 1) - 2C_2^{t-1}$ linear independent equations. In order to make the colluding users unable to recover the bivariate polynomial $F(x, y)$, it is essential to ensure that the number of linear independent equations owned by colluding adversaries cannot exceed the number of terms in polynomial $F(x, y)$, that is $th > (t + h)(t - 1) - 2C_2^{t-1}$. Simplifying the above inequality, we can get $h > 2t - 2$. Accordingly, in the case of $h > 2t - 2$, it is impossible for $t - 1$ colluding users to recover the original polynomial $F(x, y)$. In other words, our scheme prevents at most $t - 1$ colluding users from recovering the polynomial $F(x, y)$ and obtaining the secret. We can select appropriate values for t and h according to the security level requirements of the application scenario. As an example, in the case of $n = t - 1$, even if all users collude, the polynomial $F(x, y)$ cannot be recovered. This situation belongs to information-theoretic secure.

Here, it is evident that internal attackers are incapable of recovering the polynomial $F(x, y)$, because, even if the token of member U_i is compromised, they still cannot obtain the tokens of other members and the corresponding paired shared keys. Thus, our protocol meets the goal of *Resistant to key compromise impersonation attack*.

Theorem 5 (Outside Attack) *No confidential information can be obtained by external attackers.*

Proof Outside attacks refer to the attempts made by unauthorized adversaries without valid tokens to generate valid tokens in order to impersonate legitimate members and gain access to information they are not supposed to know. Suppose there is an external adversary attempting to acquire the group key by pretending to be an authentic group member. Before negotiating the group key, group members undergo identity verification with all other members. This is achieved by combining their secret inputs with paired keys shared with two neighbors, and broadcasting the resulting output to other members. Due to the absence of valid token, the external attacker is unable to pass the verification of other members. Furthermore, the shared keys among legitimate members are unknown to this adversary, preventing him from extracting any confidential information from the broadcasted messages. Consequently, external adversaries are incapable of recovering the group key or obtaining any confidential information associated with the key.

As a result, each group member is convinced that no other entities except all group members can learn the established session key, our protocol meets the goal of *Key authentication.* At the same time, combined with the freshness of group key, even if the adversary compromises one session key, he/she cannot compute other session keys, our protocol meets the goal of *Known-key security*.

Performance evaluation

Many of the most recent schemes (Yang et al. 2023; Bai et al. 2022; Wang et al. 2022; Roy and Bhattacharya 2022) are designed to offer either user authentication or group key establishment independently. Such schemes require further membership verification and distribution of shared keys, in addition to necessitating multiple rounds of interactive communication and intricate calculations for encryption and decryption. Below, we first examine the performance characteristics of our protocol.

(1) *Function feature* Compare with the existing schemes, ours achieves both member authentication and group key negotiation simultaneously. Users can verify the validity of their identity to other members based on the tokens received during registration, and negotiate a group key for secure communication. The secret token of each group member, $(s_i(y), s_i(x))$, required for member authentication and group key establishment, is generated using his unique public information, associated with each user, through an asymmetric bivariate polynomial. Therefore, the dynamic joining and exit of members can be flexibly realized.

(2) *Non-interactive feature* According to the definitions of most communication protocols, "interactive communication" refers to one party acting in response to or in conjunction with another. In the protocol we propose, members do not need to "wait" for input from other members when sending message values to each other. In other words, there is no waiting time required for each member when computing and releasing values to others. This attribute is referred to as "non-interactive," which can significantly speed up the communication process. Since our protocol employs broadcast transmission, a non-interactive method, it greatly enhances the efficiency of communication.

(3) *Constant-round feature with low computation cost on each group member side* The number of communication rounds is one of the main concerns for practical applications where the cardinality of group participants involved is considerable (Hu et al. 2019). It is critical to have fixed constant rounds in GKA protocols to secure these applications. About the difference of GKA protocols with constant-round and the GKA protocols with linear or logarithmic rounds. We observe that in the kind of GKA protocols without constant-round, computation overhead of the members are reduced remarkably at the price of enhancing the communication rounds. But the round efficiency of those constant-round GKA protocols undoubtedly resulted in computational cost at the group member side in linear or logarithmic increasing when the cardinality of group members rising. In our proposed GKA protocol, it is easy to observe that the proposed GKA is a constant-round protocol since the number of communication rounds where group members exchange their contributions is independent of the cardinality of group members. That is, the computational overhead at each group member's end does not increase linearly or logarithmically with the total number of group members. This is because each member always blends his/her secret input with two paired shared keys before transmitting the message value. This implies that the computation of this value is independent of the total number of group members. Hence, our constant-round protocol achieves genuinely low computational overhead.

(4) *Lightweight encryption method* Symmetric key encryption, which involves each pair of users sharing a symmetric key, ensures confidentiality. However, it encounters significant challenges in key distribution and management, leading to substantial communication and storage costs (Roy and Bhattacharya 2022). In contrast, public-key encryption offers confidentiality, authenticity, and non-repudiation but incurs high computational costs due to large modulus and modular exponentiation operations, such as a minimum modulus size of 1024 bits for RSA (Rivest et al. 1978) encryption. To address these issues, researchers have designed optimized key establishment protocols (Yang et al. 2023; Bai et al. 2022) based on bilinear mappings and complexity assumptions, requiring operations such as modular exponentiation, pairing, and scalar multiplication. Due to concerns about the computational security of the PKC scheme, scholars have recently constructed some lattice-based GKA schemes, which are not yet practical due to the high computational complexity. For example, GKA scheme constructed based on the LWE problem (Wang et al. 2022) generally only encrypts one bit at a time, and the ciphertext is composed of exponential matrix units or vector units. The conventional calculation between ciphertext bits and bits consumes a lot of time complexity and space complexity.

Compared to the high computational costs associated with public-key and lattice-based operations, methods based on bivariate polynomials not only provide authentication and information-theoretic security but also incur lower computational costs. Such methods are very efficient in offering authentication when compared to symmetric key distribution, which involves significant communication overhead. Moreover, a unique aspect of our group key establishment is the use of addition operations as the primary computational approach, truly achieving a lightweight computation and communication footprint.

In summary, the proposed scheme is lightweight, non-interactive, constant-round and computation-efficient. Table 2 presents the comparison between our scheme and the latest group key establishment proposals. It can be observed that the performance of our scheme is optimal. It has the advantages in storage, computation and communication cost. Specific analysis is as follows.

Storage cost

The storage requirement for each group member is determined by the bit length of the parameters and secret materials produced upon the complete execution of the protocol. In our scheme, each user will be assigned a token $(s_i(y), s_i(x))$ when registering with MRC, where $s_i(y)$ is $h-1$ degree, and $s_i(x)$ is $t-1$ degree. Consequently, each user is required to store $t+h$ coefficients,

Table 2 Comparison with latest related protocols

	Yang et al. (2023)	Bai et al. (2022)	Wang et al. (2022)	Roy et al. (2022)	Ours
Include membership authentication	No	Yes	No	Yes	Yes
Need additional membership authentication and shared keys distribution	Yes	Yes	Yes	Yes	No
Computations for encryption and decryption	Public-key-based Bilinear pairing	Public-key-based Rabin cryptosystem	Lattice-based LWE	Symmetric key encryption/decryption	Asymmetric bivariate polynomial, addition operation
Non-interactive and constant-round protocol with low computation cost on each group member side	No	No	No	No	Yes

which collectively occupy $(t+h)\log_2 p$ bits of memory. Here p represents a modulus significantly smaller than that of public key algorithms.

Computation cost

Since this protocol only involves two types of entities, the trusted center and the users, the computational overhead incurred by the users can be regarded as the computational cost of the protocol. Based on the Horner's rule (Knuth 1981b), the calculation of a polynomial of degree $t-1$ is equivalent to $t-1$ multiplications and t additions. During the authentication phase, each member calculates $(m-1)$ pairs of keys $k_{i,j} = s_{vi}(x_{vj}) = F(x_{vi}, x_{vj})$ shared with other members in the group, which involves $(m-1)$ polynomial computations. Then, each member executes m hash functions to authenticate his identity to other members and verify $(m-1)$ other members. During the group key negotiation phase, each member combines their secret input with the keys shared with their neighbors using the addition operation and performs encryption on the resulting value. Then, based on the received broadcast messages, each member generates the group key through addition operation and verifies the key using a hash function.

Compared to the majority of existing security protocols, our scheme exhibits significantly lower computational complexity. Additionally, no matter how many users participate in the current group session, it will not affect the computational cost of members. As demonstrated in the aforementioned computation process, users only need the keys shared with their two neighbors in the group ring to recover the group key.

Communication cost

All communications during the Authentication stage are transmitted via broadcasting. A total of m integers r_i and $m(m-1)$ responses are transmitted during this process, where $i = 1, 2, \cdots, m$. The Group Key Agreement phase involves the transmission of m integers l_i, $m(m-1)$ ciphertexts, and m hash values.

The communication overhead of the presented scheme is evaluated by the bit length of the transmitted messages. These messages are obtained through modulo calculations based on polynomials, which effectively reduces the communication overhead. Furthermore, in scenarios with a substantial number of group members, the number of session rounds plays a crucial role in determining the communication complexity. Based on this, our protocol guarantees a fixed number of rounds for key negotiation, so as to achieve lightweight computational overhead for the user.

In summary, our protocol is non-interactive and lightweight, which can reduce the computing and communication burden of users while ensuring security.

Conclusion

We presented a new and lightweight construction of ring-neighbor-based user authentication and group key distribution for IoD. This protocol provides the identity verification of member and group key negotiation simultaneously, while realizing lightweight computational overhead for users. Specifically, no matter how many users participate in the current group session, it will not affect the computational cost of members. Additionally, it is a non-interactive proposal that employs broadcasting for data transmission. The comprehensive security analysis substantiates that this proposal is secure and satisfies all defined security requirements. Moreover, we conducted a performance analysis of the presented protocol, and the findings demonstrated its superior lightweight and efficient nature. Hence, our group secret key agreement scheme is absolutely attractive to the IoD environment.

Acknowledgements
Not applicable.

Author contributions
All authors contributed equally to this work, including writing and revising the paper Lightweight Ring-neighbor-based User Authentication and Group-key Agreement for Internet of Drones.

Funding
This work was partially supported by the National Natural Science Foundation of China (Grants Nos. 62172181, 62272189, 62072133), the Fundamental Research Funds for the Central Universities (No. CCNU19TS019), the Research Planning Project of National Language Committee (No. YB135-40) and the Research Initiation Project of Zhejiang Lab (No. 2022PD0AC02).

Availability of data and materials
The data used to support the findings of this study are included within the article

Declarations

Consent for publication
All authors consent to the publication of the manuscript.

Competing interests
The authors declare that they have no conflict of interest.

Received: 26 February 2024 Accepted: 19 April 2024
Published online: 18 August 2024

References

Abualigah L, Diabat A, Sumari P et al (2021) Applications, deployments, and integration of internet of drones (IoD): a review. IEEE Sens J 21(22):25532–25546
Badshah A, Abbas G, Waqas M et al (2024) USAF-IoD: ultralightweight and secure authenticated key agreement framework for internet of Drones environment. IEEE Trans Veh Technol
Bai L, Hsu C, Harn L et al (2022) A practical lightweight anonymous authentication and key establishment scheme for resource-asymmetric smart environments. IEEE Trans Dependable and Secure Comput
Boneh D, Lynn B, Shacham H (2001) Short signatures from the Weil pairing. In: Advances in cryptology—ASIACRYPT 2001: 7th international conference on the theory and application of cryptology and information security gold coast, Proceedings 7. Springer Berlin Heidelberg, pp 514–532
Burmester M, Desmedt Y (1994) A secure and efficient conference key distribution system. In: Advances in cryptology—EUROCRYPT'94: workshop on the theory and application of cryptographic techniques Perugia, Proceedings 13. Springer Berlin Heidelberg, p 199
Cheng Y, Agrawal Y (2005) A improved key distribution mechanism for large-scale hierarchical wireless sensor networks. J Ad Hoc Netw 5(1):35–48
Cho G, Cho J, Hyun S et al (2020) SENTINEL: a secure and efficient authentication framework for unmanned aerial vehicles. Appl Sci 10(9):3149
Chor B, Goldwasser S, Micali S, Awerbuch B (1985) Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Proceedings of the 26th IEEE symposium on the foundations of computer science, Oregon, pp 383–395
Cramer R, Damgard I, Dziembowski S, Hirt M, Rabin T (1999) Efficient multiparty computations secure against an adaptive adversary. In: Proceedings of 18th annual IACR EUROCRYPT, Prague, LNCS, Springer, vol 1592, pp 311–326
Cui J, Liu Y, Nallanathan A (2020) Multi-agent reinforcement learning-based resource allocation for UAV networks. IEEE Trans Wirel Commun 19(2):729–743
Derhab A, Cheikhrouhou O, Allouch A et al (2023) Internet of drones security: taxonomies, open issues, and future directions. Veh Commun 39:100552
Desmedt Y, Frankel Y (1991) Shared generation of authenticators and signatures. In: Advances in cryptology-crypto'91, pp 457–569
Diffie W, Hellman M (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654
Gope P, Sikdar B (2020) An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. IEEE Trans Veh Technol 69(11):13621–13630
Gupta L, Jain R, Vaszkun G (2015) Survey of important issues in UAV communication networks. IEEE Commun Surv Tutor 18(2):1123–1152
Harn L, Lin C (2010) Authenticated group key transfer protocol based on secret sharing. IEEE Trans Comput 59(6):842–846
Hsu C, Harn L, Xia Z et al (2021) Non-interactive integrated membership authentication and group arithmetic computation output for 5G sensor networks. IET Commun 15(2):328–336
Hsu C, Harn L, Xia Z et al (2023a) Construction of lightweight authenticated joint arithmetic computation for 5G IoT networks. Comput J 66(1):208–220
Hsu C, Xia Z, Cheng T et al (2023) Extremely lightweight constant-round membership-authenticated group key establishment for resource-constrained smart environments toward 5G. Comput J bxad023
Hsu C, Xia Z, Harn L et al. (2023) Ideal dynamic threshold multi-secret data sharing in smart environments for sustainable cities. Inf Sci 119488
Hu X, Wu Y, Lu Z (2019) A survey of group key agreement protocols with constant rounds. ACM Comput Surv 52(3):1–32
Hussain S, Chaudhry SA, Alomari OA et al (2021) Amassing the security: an ECC-based authentication scheme for internet of drones. IEEE Syst J 15(3):4431–4438
Joux A (2000) A one round protocol for tripartite Diffie–Hellman. In: Algorithmic number theory: 4th international symposium, ANTS-IV Leiden, Proceedings 4. Springer Berlin Heidelberg, pp 385–393
Katz J, Koo C, Kumaresan R (2008) Improved the round complexity of VSS in point-to-point networks. In: Proceedings of ICALP '08, Part II, LNCS. Springer, vol 5126, pp 499–510
Knuth DE (1981a) The art of computer programming, semi-numerical algorithms, vol II. Addison Wesley, Reading
Knuth DE (1981b) The art of computer programming, semi-numerical algorithms, vol II. Addison Wesley, Reading
Kumaresan R, Patra A, Rangan CP (2010) The round complexity of verifiable secret sharing: the statistical case. In: Advances in cryptology—ASIACRYPT 2010, LNCS, Springer, vol 6477, pp 431–447
Laih CS, Lee JY, Harn L (1989) A new threshold scheme and its application in designing the conference key distribution cryptosystem. Inf Process Lett 32(3):95–99
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
Pu C, Wall A, Choo KKR et al (2022) A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment. IEEE Internet Things J 9(12):9918–9933
Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
Roy P K, Bhattacharya A (2022) A group key-based lightweight Mutual Authentication and Key Agreement (MAKA) protocol for multi-server environment. J Supercomput 1–28
Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
Sharma P, Purushothama BR (2022) BP-MGKM: an efficient multi-group key management scheme based on bivariate polynomial. Comput Netw 216:109244
Srinivas J, Das AK, Kumar N et al (2019) TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. IEEE Trans Veh Technol 68(7):6903–6916
Tanveer M, Kumar N, Hassan MM (2021) RAMP-IoD: a robust authenticated key management protocol for the Internet of Drones. IEEE Internet Things J 9(2):1339–1353
Tian Y, Yuan J, Song H (2019) Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. J Inf Secur Appl 48:102354
Wang Z, Yang Z, Li F (2022) A two rounds dynamic authenticated group key agreement protocol based on LWE. J Syst Architect 133:102756
Yang Z, Wang Z, Qiu F et al (2023) A group key agreement protocol based on ecdh and short signature. J Inf Secur Appl 72:103388
Zhang Y, He D, Li L et al (2020) A lightweight authentication and key agreement scheme for Internet of Drones. Comput Commun 154:455–464

Publisher's Note