frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 14 June 2023
DOI 10.3389/fphy.2023.1210777

Check for updates

OPEN ACCESS

EDITED BY
Bo Rong,
Communications Research Centre Canada (CRC), Canada

REVIEWED BY
Meet Kumari,
Chandigarh University, India
Zeeshan Asghar,
Prince Sultan University, Saudi Arabia
Sajid Anwar,
Institute of Management Sciences, Pakistan

*CORRESPONDENCE
Min Li,
limintomato@163.com

RECEIVED 23 April 2023
ACCEPTED 24 May 2023
PUBLISHED 14 June 2023

CITATION
Miao J, Wang Z, Xue X, Wang M, Lv J and Li M (2023), Lightweight and secure D2D group communication for wireless IoT. *Front. Phys.* 11:1210777.
doi: 10.3389/fphy.2023.1210777

COPYRIGHT
© 2023 Miao, Wang, Xue, Wang, Lv and Li. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Lightweight and secure D2D group communication for wireless IoT

Junfeng Miao[1], Zhaoshun Wang[1], Xingsi Xue[2], Mei Wang[3], Jianhui Lv[4] and Min Li[5]*

[1]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China, [2]Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fujian University of Technology, Fuzhou, China, [3]School of Cyber Science and Technology, Shandong University, Qingdao, China, [4]Pengcheng Lab, Shenzhen, China, [5]China Industrial Control Systems Cyber Emergency Response Team, Beijing, China

In recent years, wirless Internet of Things (IoT) technology has developed rapidly, and the reuse of spectrum resources, network efficiency, and the diversity of multi-communication scenarios have brought great challenges to the existing Internet of Things. And Device to Device (D2D) communication technology in 5th Generation Mobile Communication Technology (5G) has good application prospects in these aspects. Therefore, the combination with D2D can well solve the needs in the wirless Internet of things. However, safe and effective communication has become an urgent problem to be solved. In this paper, this paper proposes a D2D group communication protocol for wireless IoT in 5G. In this protocol, the Chinese remainder theorem is introduced into the protocol design, and a secure and efficient group authentication scheme is constructed based on secret sharing and Chebyshev Polynomials. The formal security proof using Burrows Abadi Needham (BAN) logic and informal security analysis show that our proposed protocol meets the security requirements. Through performance analysis, compared with other related schemes, this scheme not only provides better security, but also has obvious advantages in computation and communication efficiency.

KEYWORDS

authentication, communication, Device to Device, security, wireless IoT

1 Introduction

With the continuous development of technology, the connotation and concept of the wirless IoT are constantly deepening, and the extension is also constantly expanding [1]. To this day, wirless IoT has initially possessed the characteristics of intelligent terminal interconnection, open platform services, and wide network coverage, and is widely used in various fields such as transportation, agriculture, healthcare, education, and finance. As a major scene of today's communication, mobile communication is formulating 5G to obtain a greater transmission rate [2]. D2D communication which is a traffic offloading technology can directly communicate between neighboring devices, and reduce the burden of base stations carrying network traffic [3]. D2D communication technology, as a 5G key technology, reuses the resources, communicates directly between devices and has the ability to reduce the base station load, lower communication delay, improve the spectrum efficiency of cellular communication system, and adapt to more complex communication environment [4]. And it expands network range and places that cannot be covered by the network. In practical application, D2D communication not only provides traffic unloading technology, but also is used to build the network, and provides relevant location services, content sharing, etc [5].

1.1 Significance and motivation

In view of the conflict between explosive growth of smart devices and scarce spectrum resources, many scholars have tried to solve this contradiction through spectrum resource redistribution, but in fact it is difficult to achieve [6]. Therefore, the combination of wirless IoT technology and 5G network can well solve their business needs [7]. Corresponding to the communication of massive devices, this is the application scenario of 5G D2D communication. In this way, the communication timeliness of resource limited IoT devices can be improved [8]. However, wireless networks are open and heterogeneous, so that they are vulnerable to various security attacks. Attackers can disrupt user communication security through eavesdropping, interception, tampering, and other methods, steal user privacy data, and seriously threaten IoT communication security [9]. In addition, the computing and storage resources of IoT devices are limited, and complex cryptographic primitives cannot be used to protect their security. The devices are vulnerable to attacks and destruction, thereby leaking stored private data [10]. Due to the above reasons, the D2D communication security challenge in the 5G Internet of Things is more critical and more difficult to solve. Therefore, this paper proposes a new protocol for wirless IoT in 5G. The features are as follows:

1) The D2D group communication protocol based on secret sharing is designed for wirless IoT. The Chinese remainder theorem is introduced into the protocol, and a group communication scheme is constructed based on secret sharing technology and Chebyshev polynomials.
2) Formal security verification and analysis using BAN logic show that our proposed protocol meets security requirements. Informal security analysis proves the safety of the protocol.
3) Compared with the existing protocol, our protocol has low the computation and communication overhead.

The rest is organized. Section 2 and Section 3 organize related work and preliminaries. Our proposed group authentication protocol is introduced in Section 4. Section 5 and Section 6 carried out security proof and performance analysis respectively. Section 7 is the conclusion.

2 Related work

Recently, more and more scholars have begun to focus on D2D secure communication. Here we introduce the point-to-point D2D communication and the D2D group communication respectively.

First, we introduce the point-to-point D2D communication. Alam et al. [11] designed a scheme based on XOR operations. However, the key based on XOR operations could be easily extracted, so this scheme could not guarantee secure D2D communication. Shen et al. [12] designed a scheme through WiFi direct connection, which ensured secure key distribution through Diffie-Hellman key exchange mechanism. However, this

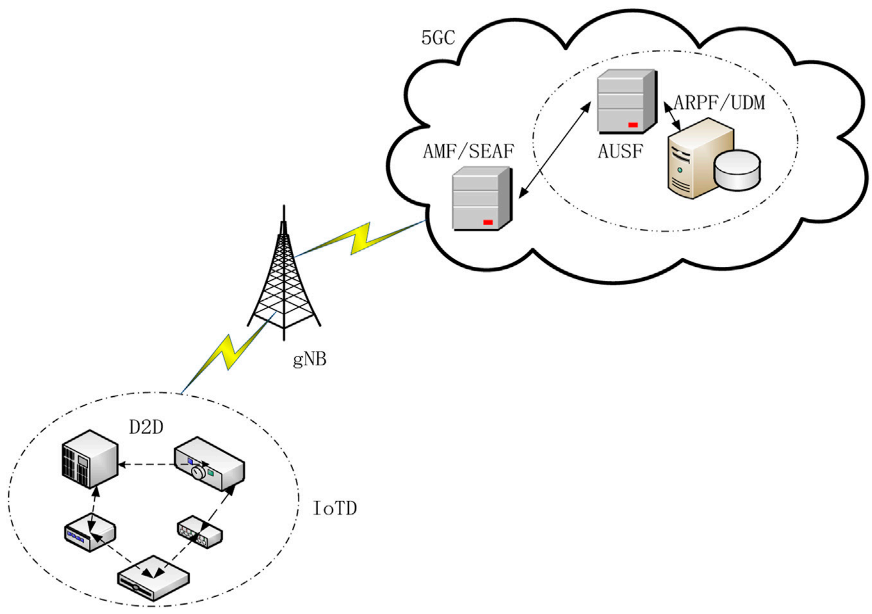

FIGURE 1
System model.

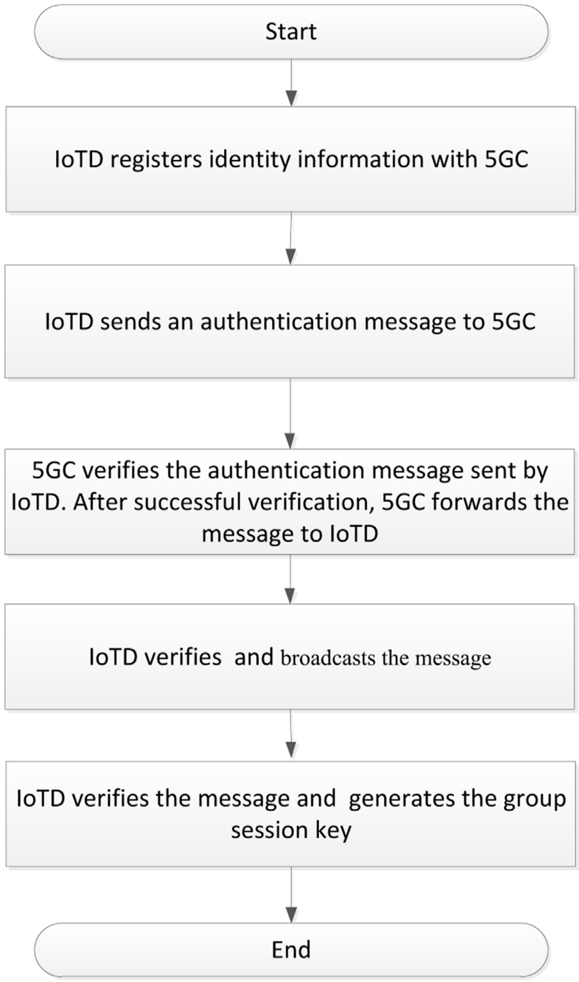

FIGURE 2
Flow chart.

scheme did not realize real mutual authentication process, and was vulnerable to impersonation attacks. Zhang et al. [13] proposed a protocol, which realized mutual authentication and secure data transmission by means of base stations. However, the excessive participation of the base station leaded to the limitations. Hsu et al. [14] proposed a D2D group communication protocol to achieve anonymity. But this protocol was only for communication between two users. Zhang et al. [15] designed a D2D communication transmission protocol based on certificateless generalized signcryption technology. This protocol could protect sensitive information and was suitable for mobile medical systems. However, this protocol could not be applied to batch verification. Man et al. [16] proposed a secure device discovery and data transmission for 5G D2D devices. It used the associated data authentication encryption. The scheme was computationally light, could be used in any resource-constrained 5G device, and it can withstand a variety of active and passive protocol attacks. However, this scheme provided one-to-one scenario communication. Wang et al. [17] proposed a protocol that could be authenticated in roaming scenarios. Pham et al. [18] proposed a privacy protection protocol. The protocol protected the privacy of related devices and realized the secure communication between devices. However, the computation overhead of this scheme was large. Gaba et al. [19] proposed a key exchange algorithm. The protocol could carry out D2D communication in WiFi direct environment and had strong resistance. Moreover, the above schemes are based on one-to-one communication mode and are not suitable for group communication.

Then, we introduce the D2D group communication. Wang et al. [20] proposed a dynamic group key protocol. It realized secure communication. Since the users of this protocol did not directly participate in the communication with the base station, it was easy to cause internal attacks in the protocol. Mustafa et al. [21] proposed a group key agreement scheme suitable in the medical Internet of Things. This scheme used secret sharing to distribute keys. But this scheme could not achieve dynamic group member management. When the members changed, the forward and backward security of the group could not be guaranteed. Shang et al. [22] proposed a protocol based on certificateless public key encryption. This scheme provided secure and anonymous communication, but this scheme required each group device to verify all signatures in the group. Sun et al. [23] proposed a unified and efficient authentication mechanism for heterogeneous D2D terminals based on unpaired creditless batch signature, prefix encryption of identity and Chinese

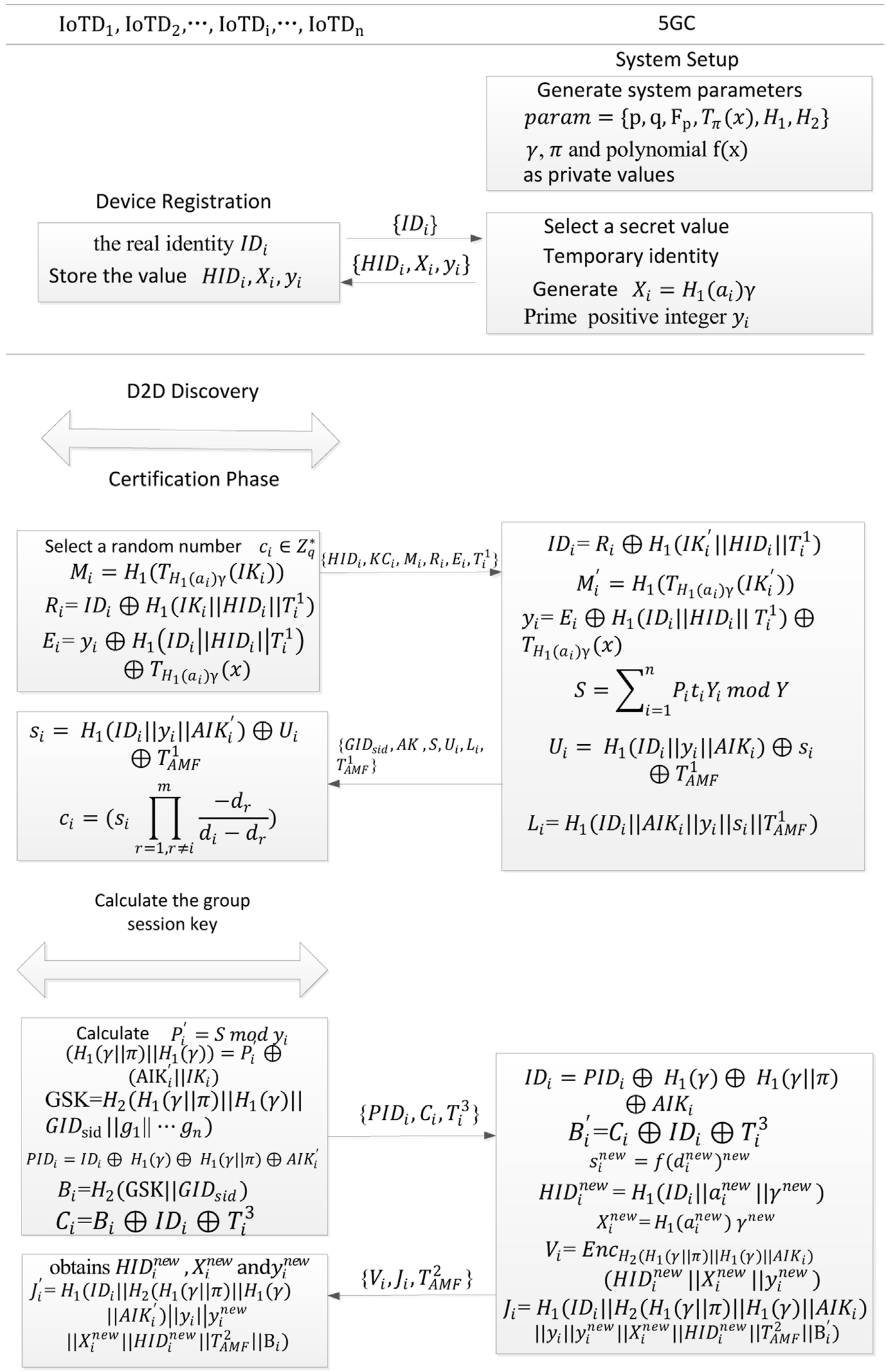

FIGURE 3
Authentication process of the proposed protocol.

remainder theorem. Hsu et al. [24] introduced a group-anonymity and accountability mechanism to assist D2D communication authentication and key agreement. The mechanism included two authentication methods, both of which can realize communication. Wang et al. [25] proposed an authentication protocol. It used hash and identity signature. This protocol could be used for privacy protection of D2D communication. However [24, 25], required more overhead.

3 Preliminaries

3.1 System model

The system model adopted in this paper is shown in Figure 1; [11–15, 20–22], which includes gNB, 5G core network, and Internet of Things device (IoTD). The gNB is the infrastructure connecting the core network and device. 5G core network is mainly composed of access and mobility management function (AMF), security anchor function (SEAF), authentication server function (AUSF), authentication credential repository and processing function (ARPF), and unified data management (UDM) [8]. IoTD is an Internet of Things device that needs D2D communication. It is assumed that a group of IoTDs is within the coverage of the same gNB. In our system model, as the registration center of IoTD, ARPF/UDM is mainly responsible for the information registration of IoTD. According to the diameter protocol [26] formulated by 3GPP organization, since the communication of 5G core network nodes is transmitted by using the wired channel between backbone networks, it is reasonable to believe that the communication channel between ARPF/UDM and AMF/SEAF is safe. In order to reduce the bandwidth consumption and communication delay, after the Internet of Things device is registered through ARPF/UDM, it sends the relevant registration information to AMF through the secure channel. AMF acts as a server to complete the authentication with the Internet of Things device.

3.2 Threat model

In the communication, because it is an open wireless channel, an attacker can monitor the channel without worrying about eavesdropping being discovered, and at the same time, the intercepted data can be used for traffic analysis. In addition, attackers can also construct D2D masquerading nodes and interfere with network security authentication and key agreement. The scene characteristics of this communication are similar to the Dolev-Yao model [27]. Therefore, we define that the attacker in this scenario has similar attack capabilities to the attacker in the Dolev-Yao model. The attacker can monitor, intercept, and store all the conversations between devices, establish a connection with the device by constructing a disguised node and perform security authentication and key agreement protocols, and can replay intercepted messages.

3.3 Security requirements

The protocol needs to meet the following requirements to ensure the security of the protocol [16–18, 24, 25].

1) Mutual authentication: in order to prevent attackers from interfering with the data flow process, the identity of the IoTD is determined through mutual authentication [28–30].
2) Session key agreement: the IoTD generates a session key through session key agreement and uses the session key to encrypt data, thereby ensuring the security of data transmission.
3) Identity anonymity: in the D2D communication process, the security of the IoTD identity must always be guaranteed.
4) Resist attacks: the protocol proposed in this paper should be able to resist all kinds of active and passive attacks [31–33].

3.4 Chebyshev polynomials

The definition of n-order Chebyshev polynomial is shown in the following equation [34]:

$$T_n(x) = \cos(\mathrm{n}\arccos(\mathrm{x})) \tag{1}$$

The recurrence relation of Chebyshev polynomials is shown in the following equation:

$$T_n(x) = (2\mathrm{x}T_{n-1}(\mathrm{x}) - T_{n-2}(\mathrm{x})) \tag{2}$$

Where: $x \in [-1, 1], n \in [2, +\infty), T_0(x) = 1, T_1(x) = x$.

Chebyshev polynomials have semigroup propertie: $T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x)\, mod\, p$, r and s are two positive integers, p is a large prime number and $x \in [-1, 1]$. And Zhang [35] proved that the semigroup propertie in real number fields (−∞, +∞) is still valid

Definition 1. chaotic map-based computational Diffie Hellman problem (CCDH problem): given a Chebyshev polynomial $T_n(x)$, $x \in (-\infty, +\infty)$ and two multiple recursive values $T_r(x)$ and $T_s(x)$ are known, in which r and s are two positive integers.The probability that the enemy calculates $T_{rs}(x)$ in the probability polynomial time is negligible [36].

3.5 Chinese remainder theorem

The Chinese remainder theorem can solve any system of Congruence Equations to obtain the same solution [37]. The theorem is introduced as follows.

Suppose there are coprime positive integers $z_1, z_2, \cdots, z_k$ and positive integers $v_1, v_2, \cdots, v_k$, M is the product of $m_i, i = 1, 2, \cdots k$. Then equation system (3) has a unique solution. The unique solution is calculated as shown in Eq. 4

$$\begin{cases} X \equiv v_1 (mod\, z_1) \\ X \equiv v_2 (mod\, z_2) \\ \vdots \\ X \equiv v_k (mod\, z_k) \end{cases} \tag{3}$$

$$X \equiv v_1 M_1 M_1' + v_2 M_2 M_2' + \cdots + v_k M_k M_k' (mod\, M) \tag{4}$$

Where: $M_i = M/z_i (i = 1, 2, \cdots, k)\, and\, M_i'$ is an integer solution satisfying $M_i M_i' \equiv 1 (mod\, z_i)(i = 1, 2, \cdots, k)$.

3.6 Secret sharing algorithm

The secret sharing algorithm [38] divides the secret value s into n secret shares through relevant algorithms and distributes them to n users for sharing, and each user saves one secret share. If users want to recover the shared secret value, they only need any t or more users to provide their own secret share, and the secret value will be reconstructed. It mainly includes secret share distribution and secret reconstruction.

1) Secret share distribution

The distributor selects any finite field F_p and selects a random polynomial of order t − 1 in the finite field.

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} mod\, p \tag{5}$$

TABLE 1 symbols.

Notations	Definitions
AMF	Access and mobility management function
$IoTD_i$	Internet of things device
$f(x)$	Polynomial
F_p	Finite field
$H_i(\cdot)$	A one-way secure hash function
ID_i	The real identity
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation
T_i	The timestamp
s_i	The secret share
HID_i	The temporary identity
π	The system master key
GID_{sid}	The group identity
GSK	the group session key

Where p is a large prime number, the secret value $D = f(0) = a_0$. Then it randomly generates n different integers x_i and calculates the corresponding $f(x_i)$. Then it sends $(x_i, f(x_i))$ to n users safely.

2) Secret reconstruction

Suppose a total of m users participate in secret reconstruction, and the secret value is calculated by formula (6). If the reconstructed secret value satisfies $D' = D$, the secret reconstruction is successful. On the contrary, when the equation is not tenable or the number of participating users is less than t, the secret reconstruction fails.

$$D' = \sum_{i=1}^{m} f(x_i) \prod_{r=1, r \neq j}^{m} \frac{-x_r}{x_j - x_r} mod\ p \quad (6)$$

4 Proposed scheme

Based on [11–25], this paper proposes a lightweight and secure D2D group authentication protocol. This section describes flow chart and the protocol process in Figures 2, 3; Table 1 lists the symbols used in the protocol.

4.1 System setup

At this stage, ARPF/UDM chooses two relatively prime large prime numbers p and q. Then ARPF/UDM selects the anti-collision hash function H_1: $\{0,1\}^* \to Z_q^*$, H_2: $\{0,1\}^* \times \{0,1\}^* \to Z_q^*$. ARPF/UDM continues to randomly select a value $\gamma \in F_p$ as the secret authentication message, and ARPF/UDM selects a polynomial $f(x) = b_0 + b_1 x + ... + b_{t-1} x^{t-1} mod\ p$ which satisfies $b_0 = H(\gamma)$, $b_0, \cdots, b_{t-1} \in F_p$. Finally, ARPF/UDM selects a secret value $\pi \in Z_q^*$ as the master key, discloses the system parameters {p, q, F_p, $T_\pi(x)$, H_1, H_2}, and saves γ, π and polynomial $f(x)$ as private values. At the same time, ARPF/UDM sends the generated information to AMF safely.

4.2 IoTD registration

1) $IoTD_i$ sends the real identity ID_i to ARPF/UDM securely.
2) After receiving the message, ARPF/UDM randomly selects a value $a_i \in Z_q^*$, generates the user pseudonym information $HID_i = H_1(ID_i \| a_i \| \gamma)$. Then, ARPF/UDM allocates different positive integer parameters d_i for the registered devices and calculates the respective shares $s_i = f(d_i)$. It stores (ID_i, a_i, s_i) in the database and generates $X_i = H_1(a_i)\gamma$. Then, ARPF/UDM allocates the mutually prime positive integer y_i for different devices and sends the message $\{HID_i, X_i, y_i\}$ to $IoTD_i$ through the secure channel. At the same time, ARPF/UDM sends the saved registration information to AMF safely, where d_i is the public parameter.

4.3 Device discovery and authentication phase

Here, we assume that n devices communicate with each other through the D2D discovery process [27]. At this time, the devices need to verify their identity through AMF.

1) $IoTD_i$ first randomly selects a value $c_i \in Z_q^*$ and the timestamp T_i^1, calculates $KC_i = T_{c_i}(x)$, $IK_i = T_{c_i}(T_\pi(x))$, $R_i = ID_i \oplus H_1(IK_i || HID_i || T_i^1)$, $E_i = y_i \oplus H_1(ID_i || HID_i || T_i^1) \oplus T_{H_1(a_i)\gamma}(x)$, $M_i = H_1(T_{H_1(a_i)\gamma}(IK_i))$ and sends the message $\{HID_i, KC_i, M_i, R_i, E_i, T_i^1\}$ to AMF
2) AMF sets a time timer to wait for n devices to be received. If the information of all devices is received, the authentication continues, otherwise, the authentication process is terminated. AMF checks whether the received timestamp T_i^1 is correct. If the verification passes, it calculates $IK_i' = T_\pi(T_{c_i}(x)) = T_{\pi c_i}(x)$, $ID_i = R_i \oplus H_1(IK_i' || HID_i || T_i^1)$ to get the real identity ID_i, and obtain a_i by querying the database. Then AMF calculates $M_i' = H_1(T_{H_1(a_i)\gamma}(IK_i'))$ and compares M_i and M_i'. If equal, AMF generates a group identity GID_{sid}, and a random value v_i, selects the timestamp T_{AMF}^1, calculates $y_i = E_i \oplus H_1(ID_i || HID_i || T_i^1) \oplus T_{H_1(a_i)\gamma}(x)$, $AK_i = T_{v_i}(x)$, $AIK_i = T_{v_i}(T_{c_i}(x)) = T_{v_i c_i}(x)$, $P_i = (AIK_i \| IK_i') \oplus (H_1(\gamma \| \pi) \| H_1(\gamma))$, $Y = \prod_{i=1}^{n} y_i, Y_i = Y / y_i, Y_i t_i \equiv 1 (mod\ y_i)$, $S = \sum_{i=1}^{n} P_i t_i Y_i mod\ Y$, $U_i = H_1(ID_i || y_i || AIK_i) \oplus s_i \oplus T_{AMF}^1$, $L_i = H_1(ID_i \| AIK_i \| y_i \| s_i \| T_{AMF}^1)$, and sends a message $\{GID_{sid}, AK_i, S, U_i, L_i, T_{AMF}^1\}$ to $IoTD_i$.
3) After receiving the message, $IoTD_i$ first checks whether T_{AMF}^1 is correct. If not, the authentication is terminated, otherwise the authentication continues. Firstly, $IoTD_i$ calculates $AIK_i' = T_{c_i v_i}(x)$, $s_i = H_1(ID_i || y_i || AIK_i') \oplus U_i \oplus T_{AMF}^1$, obtains the secret share s_i, and calculates the random component $c_i = (s_i \prod_{r=1, r \neq j}^{m} \frac{-d_r}{d_j - d_r})$ mod p. $IoTD_i$ calculates $L_i' = H_1(ID_i \| AIK_i' \| y_i \| s_i \| T_{AMF}^1)$. If L_i' and L_i are equal, $IoTD_i$ authenticates AMF.

At this time, if the verification is passed, then the devices start mutual authentication and group session key negotiation. If the verification fails, the verification is terminated.

1) $IoTD_i$ randomly selects a value $g_i \in Z_q^*$, the timestamp T_i^2 and calculates $P_i' = S \, mod \, y_i$, $(H_1(\gamma\|\pi)\|H_1(\gamma)) = P_i' \oplus (AIK_i'\|IK_i)$, $N_i = c_i \oplus H_1(\gamma\|\pi)$, $Z_i = c_i \oplus g_i \oplus T_i^2$. Finally, $IoTD_i$ broadcasts the message $\{GID_{sid}, N_i, Z_i, T_i^2\}$.
2) When $IoTD_i$ receives messages from other devices, $IoTD_i$ first checks whether T_i^2 is correct. If not, the authentication is terminated, otherwise the authentication continues. $IoTD_i$ calculates $(c_1, \cdots c_n)$ and $(g_1, \cdots g_n)$ through the stored $H_1(\gamma\|\pi)$. Then, $IoTD_i$ calculates $H_1(\gamma)' = (\sum_{j=1}^{n} c_j mod \, p) \bmod q$ and compares $H_1(\gamma)'$ and $H_1(\gamma)$. If equal, the group device identity is verified. $IoTD_i$ selects the timestamp T_i^3 and calculates the group session key $GSK = H_2(H_1(\gamma||\pi)\|H_1(\gamma)\|GID_{sid}\|g_1 \cdots g_n)$, $PID_i = ID_i \oplus H_1(\gamma) \oplus H_1(\gamma\|\pi) \oplus AIK_i'$, $B_i = H_2(GSK\|GID_{sid})$, $C_i = B_i \oplus ID_i \oplus T_i^3$. Finally, $IoTD_i$ sends the message $\{PID_i, C_i, T_i^3\}$to AMF.
3) After receiving the message, AMF checks whether the information of n devices is received. If the information of all devices is received, the authentication continues; otherwise, the authentication process is terminated. AMF checks whether the received timestamp T_i^3 is correct. If the verification passes, AMF first calculates $ID_i = PID_i \oplus H_1(\gamma) \oplus H_1(\gamma\|\pi) \oplus AIK_i$, $B_i' = C_i \oplus ID_i \oplus T_i^3$ and compares all the values of B_i'. If equal, it proves that the generated group session keys are equal. At this time, AMF selects the timestamp T_{AMF}^2, the values γ^{new}, , a new polynomial $f(x)^{new}$ which satisfies $b_0^{new} = H_1(\gamma^{new})$, and the value a_i^{new}.Then, AMF selects positive integer parameters d_i^{new}, calculates $s_i^{new} = f(d_i^{new})^{new}$ and the pseudonym information $HID_i^{new} = H_1(ID_i||a_i^{new}||\gamma^{new})$, and updates $(ID_i, a_i^{new}, s_i^{new})$ in the database. AMF generates the registration values $X_i^{new} = H_1(a_i^{new})\gamma^{new}$ and y_i^{new}, and calculates the encryption value $V_i = Enc_{H_2(H_1(\gamma)\|H_1(\gamma\|\pi)\|AIK_i)}(HID_i^{new}||X_i^{new}||y_i^{new})$ and the value $J_i = H_1(ID_i\|H_2(H_1(\gamma||\pi)\|H_1(\gamma)\|AIK_i)\|y_i\|y_i^{new}\|X_i^{new}\| HID_i^{new}||T_{AMF}^2||B_i')$. Then, AMF sends the message $\{V_i, J_i, T_{AMF}^2\}$ to $IoTD_i$.
4) When $IoTD_i$ receives the message, it first checks whether T_{AMF}^2 is correct. If not, the authentication is terminated; otherwise, the authentication continues. Then, it obtains HID_i^{new}, X_i^{new} and y_i^{new} by decrypting the message using $H_2(H_1(\gamma)\| H_1(\gamma\|\pi)\|AIK_i')$, calculates $J_i' = H_1(ID_i\|H_2(H_1(\gamma||\pi)\|H_1(\gamma)\|AIK_i')\|y_i\|y_i^{new}\|X_i^{new}\|HID_i^{new}||T_{AMF}^2||B_i)$ and compares whether J_i and J_i' are equal. If they are equal, the values stored by the device are updated to $(HID_i^{new}, X_i^{new}, y_i^{new})$. Finally, the group devices communicate through the group session key.

5 Security evaluation

5.1 Proof of security

This section uses BAN logic [39] to formally analyze the proposed protocol, and theoretically prove the safety. The logic rules and symbols are shown in Table 2. Here, we only prove the mutual authentication and key negotiation of IoTD.

1) Protocol idealization

$$M_1: IoTD_i \rightarrow IoTD_j: \ <GID_{sid}, c_i, g_i>_{H_1(\gamma\|\pi)}$$

$$M_2: IoTD_j \rightarrow IoTD_i: \ <GID_{sid}, c_j, g_j>_{H_1(\gamma\|\pi)}$$

2) Protocol goal

$$G_1: IoTD_i \mid\equiv \left(IoTD_i \overset{GSK}{\rightarrow} IoTD_j\right)$$

$$G_2: IoTD_j \mid\equiv \left(IoTD_j \overset{GSK}{\rightarrow} IoTD_i\right)$$

$$G_3: IoTD_i \mid\equiv IoTD_j \mid\equiv \left(IoTD_j \overset{GSK}{\rightarrow} IoTD_i\right)$$

$$G_4: IoTD_j \mid\equiv IoTD_i \mid\equiv \left(IoTD_i \overset{GSK}{\rightarrow} IoTD_j\right)$$

3) Initial hypothesis

$$A_1: IoTD_i \mid\equiv \left(IoTD_i \overset{H_1(\gamma\|\pi)}{\rightarrow} IoTD_i\right)$$

$$A_2: IoTD_j \mid\equiv \left(IoTD_j \overset{H_1(\gamma\|\pi)}{\rightarrow} IoTD_i\right)$$

$$A_3: IoTD_i \mid\equiv \left(IoTD_i \overset{H_1(\gamma\|\pi)}{\rightarrow} IoTD_i\right)$$

$$A_4: IoTD_j \mid\equiv \left(IoTD_j \overset{H_1(\gamma\|\pi)}{\rightarrow} IoTD_i\right)$$

$$A_5: IoTD_i \mid\equiv \#\left(H_1\left(\gamma\|\pi\right)\right)$$

$$A_6: IoTD_i \mid\equiv \#(H_1(\gamma))$$

$$A_7: IoTD_i \mid\equiv \#\left(g_j\right)$$

$$A_8: IoTD_j \mid\equiv \#\left(H_1\left(\gamma\|\pi\right)\right)$$

$$A_9: IoTD_j \mid\equiv \#(H_1(\gamma))$$

$$A_{10}: IoTD_j \mid\equiv \#(g_i)$$

$$A_{11}: IoTD_j \mid\equiv IoTD_i \mid\Rightarrow <GID_{sid}, c_i, g_i>$$

$$A_{12}: IoTD_j \mid\equiv IoTD_i \mid\Rightarrow \left(IoTD_i \overset{GSK}{\rightarrow} IoTD_j\right)$$

$$A_{13}: IoTD_i \mid\equiv IoTD_j \mid\Rightarrow <GID_{sid}, c_j, g_j>$$

$$A_{14}: IoTD_i \mid\equiv IoTD_j \mid\Rightarrow \left(IoTD_i \overset{GSK}{\rightarrow} IoTD_j\right)$$

4) Proof of protocol

The security proof of this scheme is as follows:
From the message M_1, it can be obtained that:

$$R_1: IoTD_j \triangleleft <GID_{sid}, c_i, g_i>_{H_1(\gamma\|\pi)}$$

From R_1, A_2 and the message meaning rule, we can get:

$$R_2: IoTD_j \mid\equiv IoTD_i \mid\sim <GID_{sid}, c_i, g_i>$$

From R_2, A_{10} and nonce verification rule, we can get:

$$R_3: IoTD_j \mid\equiv IoTD_i \mid\equiv \ <GID_{sid}, c_i, g_i>$$

From R_3, A_{11} and the jurisdiction rule, we can get:

TABLE 2 BAN logic rules and symbols.

Contruct	Explanation
X,Y	Parameter
P,Q	Communication party
K	Key
$P \lhd X$	P receives a message containing X
$P \mid\sim X$	P sends a message containing X
$P \mid\equiv X$	P believes X
$P \overset{K}{\rightarrow} Q$	P and Q share secret K
$< X >_Y$	X contains the secret Y
$P \Rightarrow X$	P has the right to decide whether X is right or not
Message meaning rule	$\frac{P \mid\equiv P \overset{K}{\rightarrow} Q, P \lhd < X >_Y}{P \mid\equiv Q \mid\sim X}$
Belief rule	$\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X,Y)}$
Nonce verification rule	$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$
Arbitration rule	$\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\sim X}{P \mid\equiv X}$

$$R_5: IoTD_j \Big| \equiv \ < GID_{sid}, c_i, g_i >$$

Given R_5, A_2, A_4, A_8 , A_9 and A_{10}, we can get

$$R_6: IoTD_j \mid \equiv IoTD_i \mid \equiv \left(IoTD_j \overset{GSK}{\rightarrow} IoTD_i \right)$$

From R_6, A_{12} and the jurisdiction rule, we can get:

$$R_7: IoTD_j \Big| \equiv \left(IoTD_j \overset{GSK}{\rightarrow} IoTD_i \right)$$

According to the message M_2, we can get:

$$R_8: IoTD_i \lhd < GID_{sid}, c_j, g_j >_{H_1(\gamma \| \pi)}$$

According to R_8, A_1 and the message meaning rule, we can get:

$$R_9: IoTD_i \Big| \equiv IoTD_j \Big| \sim < GID_{sid}, c_j, g_j >$$

From R_9, A_7 and the nonce verification rule, we can get:

$$R_{10}: IoTD_i \Big| \equiv IoTD_j \Big| \equiv \ < GID_{sid}, c_j, g_j >$$

According to R_{10}, A_{13} and the jurisdiction rule, we can get:

$$R_{11}: IoTD_i \Big| \equiv \ < GID_{sid}, c_j, g_j >$$

From R_{11}, A_1 A_3, A_5, A_6 and A_7, we can get:

$$R_{12}: IoTD_i \mid \equiv IoTD_j \mid \equiv \left(IoTD_j \overset{GSK}{\rightarrow} IoTD_i \right)$$

Given R_{12}, A_{14} and the jurisdiction rule, we can get:

$$R_{13}: IoTD_i \Big| \equiv \left(IoTD_j \overset{GSK}{\rightarrow} IoTD_i \right)$$

Through R_6, R_7, R_{12} and R_{13}, we can see that our scheme reaches the goals.

5.2 Security analysis

This section uses informal security analysis to prove that the proposed authentication protocol can support a variety of security attributes and effectively resist known security attacks.

Identity Anonymity Protection. In this scheme, the user registers by using a temporary identity $HID_i = H_1(ID_i \| a_i \| \gamma)$ during the registration stage. It can only get the true identity through the secret

TABLE 3 Security comparison.

Functionality	[22]	[16]	[17]	[24]	[25]	[18]	Our scheme
Identity anonymity	✓	✓	✓	✓	✓	✓	✓
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓
Session Key Negotiation	✓	✓	✓	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓	✓	✓	✓
MitM attack	✓	✓	✓	✗	✗	✓	✓
Counterfeit attack	✓	✓	✓	✓	✓	✓	✓
PFS	✓	✓	✗	✗	✓	✓	✓
Batch Verification	✗	✗	✗	✗	✗	✗	✓

TABLE 4 Computation overhead.

Protocol	Computation overhead	Total execution time
[22]	$7n\ T_{ECC} + 4n\ T_H$	2.923n
[23]	$(5n+2)\ T_{ECC} + 7n\ T_H + 2nT_{EN} + (n+1)T_{DE}$	2.2n + 0.857
Our scheme	$10nT_{CCM} + 18nT_H + nT_{LI} + nT_{EN} + nT_{DE}$	1.152n

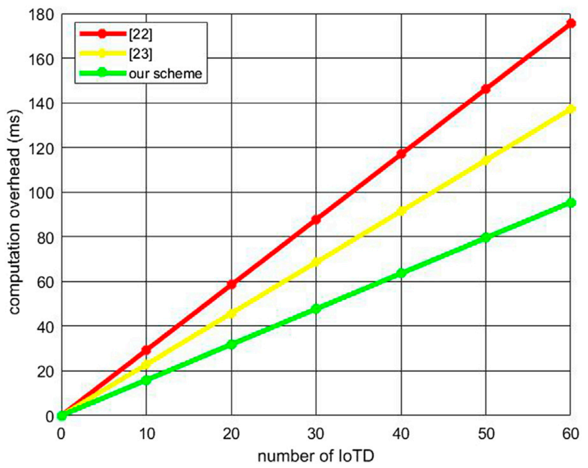

FIGURE 4
Compution overhead.

value $T_{c_i\pi}(x)$ generated by the Chebyshev Polynomials. Even if the attacker obtains temporary identity and tracks the target user, it cannot eavesdrop the behavior of the user after the temporary identity expires. And because the temporary identity is constantly updated, it is impossible for an attacker to accurately associate the temporary identity with the real identity. Therefore, the user's privacy and security can be guaranteed.

Mutual Authentication. In the scheme, the device generates the authentication value M_i through the Chebyshev Polynomials, and the AMF completes the authentication with the device by verifying the authentication value M_i. AMF generates the hash value $L_i^{'}$ through the Chebyshev Polynomials, and the device completes the authentication with the device by verifying the hash value $L_i^{'}$. The device calculates the Lagrangian component c_i through the secret sharing algorithm. By recovering the secret value $H_1(\gamma)$, the device can authenticate a set of device identities

Resist Counterfeiting Attacks. In this scheme, Chebyshev Polynomials is used to generate the verification value M_i to ensure the correctness of the message. If an attacker fakes a device, it will generate a corresponding fake message and send it to AMF. However, the message can be determined to be correct only through verification.

Resist Replay Attacks. In this scheme, the timestamp T_i is used to resist replay attacks. Each session request in the protocol is marked with a timestamp, which ensures that the attacker cannot send the same session request message.

Resisting MitM Attacks. During the execution of the protocol, the attacker may eavesdrop on the communication information $\{HID_i, KC_i, M_i, R_i, E_i, T_i^1\}$ between the device and the AMF and tamper with it. AMF needs to detect whether the information has been modified. If attacker modifies the value of M_i, AMF cannot recover the correct value of M_i, and thus cannot pass the device's identity authentication. In addition, if the attacker modifies the values of L_i, the device cannot successfully authenticate the identity of the AMF.

Perfect Forward Secrecy. In this scheme, $IoTD_i$ calculates the group session key GSK $= H_2(H_1(\gamma\|\pi), H_1(\gamma), GID_{\text{sid}}, g_1, \cdots g_n)$. $H_1(\gamma\|\pi), H_1(\gamma)$ and g_i are all secret values. Therefore, only the corresponding device can have the group session key. The group session key negotiated each time is a randomly generated, and the subsequent group session key cannot be calculated.

TABLE 5 Communication overhead.

Protocol	Communication overhead
[22]	$928n^2 + 352n$
[23]	1536n+1504
Our scheme	$416n^2 + 2368n$

5.3 Security comparison

To prove the security of the protocol, the research work with similar functions in recent years is selected for comparison. Table 3 shows the comparison results of security attributes and functions with those in the same type of protocols. The proposed protocol can meet all the security attributes in the table, while other authentication protocols could not meet.

6 Performance analysis

This section will analyze the computation overhead and communication overhead. In addition, this section will also compare the proposed protocol with the research work of [22, 23].

6.1 Computation overhead

In order to quantify the calculation time of each algorithm, through simulation on 64-bit Windows 10 system, we tested the calculation time of ecc-based scalar multiplication T_{ECC}, hash operation T_H, chaotic map operation T_{CCM} and lagrange interpolation operation T_{LI}, symmetric encryption T_{EN} and decryption T_{DE}. The result of our test is T_{ECC} = 0.413 ms, T_H = 0.008 ms, T_{CCM} = 0.138 ms, T_{LI} = 0.011 ms, T_{EN} = 0.024 ms, T_{DE} = 0.031 ms. The above protocols all have XOR operations and string connection operation, but compared with the calculation time of other operations, the calculation time of these two operations is basically negligible. Table 4 compares the calculation overhead of relevant schemes. In Figure 4, compared with other solutions, the advantages of our proposed scheme will become more obvious as IoTD increases.

6.2 Communication overhead

The communication overhead considered in this paper mainly comes from device authentication. Assume that the length of ECC algorithm, identity information, timestamp, hash value and random number are respectively 256, 128, 32, 128, 64 bits. Both chebyshev polynomial and lagrangian interpolation are 160 and 128 bits. The calculation results of relevant communication

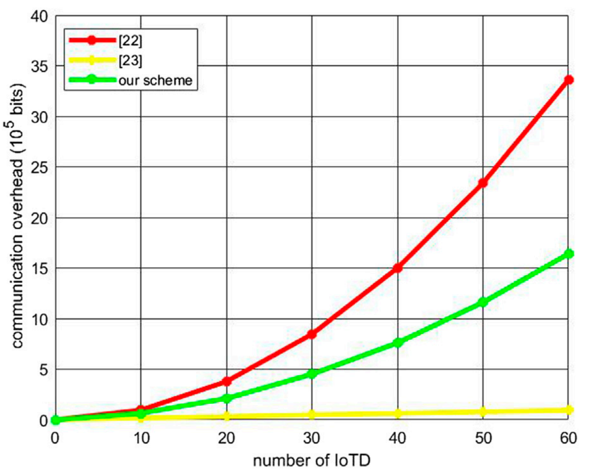

FIGURE 5
Communication overhead.

overhead in this paper are shown in Table 5 and Figure 5. From the analysis in Figure 5, it can be seen that because the scheme [23] is aimed at a one-to-many scenario, the communication overhead is small. As shown in the figure, compared with [22], the proposed scheme has less communication overhead. And as the number of IoTD increases, the advantages become more obvious.

7 Conclusion

Due to the openness of wireless communication environment and the large number of IoT equipment nodes, security and efficiency are the key factors for the development of wireless IoT. In addition, D2D communication technology in 5G is a resource reuse technology, and the terminal equipment can communicate directly without passing through the base station. Therefore, the combination of Internet of things technology and 5G network can well solve their business needs. Currently, their combination leads to more complex environment and more security challenges. Therefore, we propose a D2D group communication protocol for wirless IoT in 5G. This protocol not only realizes identity privacy protection and group authentication, but also can resist malicious attacks, so as to ensure the security of D2D communication in wireless IoT. Compared with other D2D communication related schemes, this scheme can achieve more security objectives and availability in complex communication scenarios. According to BAN logic proof and Informal security analysis, it can be seen that our scheme meets the security requirements required in this paper. Finally, through the analysis of communication overhead and computation overhead, we can see that our scheme has better performance advantages. In the future, we plan to introduce blockchain and physical unclonable function to design a more lightweight and secure group authentication protocol for wirless IoT.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

JM: study conception and administration. JM, ML, and ZW: methodology and validation. XX and MW: experimental work and manuscript drafting. XX and JL: manuscript review and editing. All authors contributed to the article and approved the submitted version.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Medaglia AS. *An overview of privacy and security issues in the Internet of things*. Berlin, Germany: The Internet of Things (2010). p. 389–95.

2. Shen X. Device-to-device communication in 5G cellular networks. *IEEE Netw* (2015) 29(2):2–3. doi:10.1109/mnet.2015.7064895

3. Asadi A, Wang Q, Mancuso V. A survey on device-to-device communication in cellular networks. *Commun Surv Tutorials* (2014) 16(4):1801–19. doi:10.1109/comst.2014.2319555

4. Doppler K, Rinne M, Wijting C, Ribeiro CB, Hugl K. Device-to-device communication as an underlay to lte-advanced networks. *Mod Sci Tech Telecommunications* (2010) 47(12):42–9. doi:10.1109/mcom.2009.5350367

5. Haus M, Waqas M, Ding AY, Li Y, Tarkoma S, Ott J. Security and privacy in device-to-device (D2D) communication: A review. *IEEE Commun Surv Tutorials* (2017) 19(2):1054–79. doi:10.1109/comst.2017.2649687

6. Saqlain J. *IoT and 5G: History evolution and its architecture their compatibility and future*. Helsinki, Finland: Subtitle Metropolia University of Applied Sciences (2018).

7. Li S, Li DX, Zhao S. 5G internet of things: A survey. *J Ind Inf Integration* (2018) 10:1–9. doi:10.1016/j.jii.2018.01.005

8. Seok B, Sicato J, Erzhena T, Xuan C, Pan Y, Park JH. Secure D2D communication for 5G IoT network based on lightweight cryptography. *Appl Sci* (2019) 10(1):217. doi:10.3390/app10010217

9. Chien HY. Two-level-composite-hashing facilitating highly efficient anonymous IoT and D2D authentication. *Electronics* (2021) 10(7):789. doi:10.3390/electronics10070789

10. Fang H, Qi A, Wang X. Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement. *IEEE Netw* (2020) 34(3):24–9. doi:10.1109/mnet.011.1900276

11. Alam M, Du Y, Rodriguez J, Abd-Alhameed RA. Secure device-to-device communication in lte-a. *IEEE Commun Mag* (2014) 52(4):66–73. doi:10.1109/mcom.2014.6807948

12. Shen W, Hong W, Cao X, Bo Y, Shila DM, Yu C. Secure key establishment for device-to-device communications. In: proceedings of the 2014 IEEE Global Communications Conference; December 2014; Austin, TX, USA. IEEE.

13. Zhang A, Chen J, Hu RQ, Yi Q. Seds: Secure data sharing strategy for d2d communication in lte-advanced networks. *IEEE Trans Vehicular Tech* (2016) 65(4):2659–72. doi:10.1109/tvt.2015.2416002

14. Hsu RH, Lee J. Group anonymous d2d communication with end-to-end security in lte-a. In: Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS); September 2015; Florence, Italy. IEEE. p. 451–9.

15. Zhang A, Lei W, Ye X, Lin X. Light-weight and robust security-aware d2d-assist data transmission protocol for mobile health systems. *IEEE Trans Inf Forensics Security* (2017) 12(3):662–75. doi:10.1109/tifs.2016.2631950

16. Man CC, Ma M. A lightweight traceable D2D authentication and key agreement scheme in 5G cellular networks. *Comput Electr Eng* (2021) 95(4):107375. doi:10.1016/j.compeleceng.2021.107375

17. Wang M, Yan Z, Niemi V. Uaka-d2d: Universal authentication and key agreement protocol in d2d communications. *Mobile Networks Appl* (2017) 22(3):510–25. doi:10.1007/s11036-017-0870-5

18. Pham C, Dang TK. A lightweight authentication protocol for D2D-enabled IoT systems with privacy. *Pervasive Mobile Comput* (2021) 74:101399. doi:10.1016/j.pmcj.2021.101399

19. Gaba GS, KumarKim GTH, Monga H, Kumar P. Secure device-to-device communications for 5G enabled internet of things applications. *Computer Communications,nol.* (2021) 169(4):114–28. doi:10.1016/j.comcom.2021.01.010

20. Wang L, Tian Y, Zhang D, Lu Y. Constant-round authenticated and dynamic group key agreement protocol for d2d group communications. *Inf Sci* (2019) 503:61–71. doi:10.1016/j.ins.2019.06.067

21. Mustafa U, Philip N. Group-based key exchange for medical iot device-to-device communication (d2d) combining secret sharing and physical layer key exchange. In: Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3); January 2019; London, UK.

22. Shang Z, Ma M, Li X. A secure group-oriented device-todevice authentication protocol for 5g wireless networks. *IEEE Trans Wireless Commun* (2020) 99:7021–32. doi:10.1109/twc.2020.3007702

23. Sun Y, Cao J, Ma M, Zhang Y, Niu B. Eapddba: Effcient anonymity proximity device discovery and batch authentication mechanism for massive d2d communication devices in 3gpp 5g hetnet. *IEEE Trans Dependable Secure Comput* (2020) 99.

24. Hsu RH, Lee J, Quek T, Chen JC. Graad: Group anonymous and accountable d2d communication in mobile networks. *IEEE Trans Inf Forensics Security* (2017) 13(2):449–64. doi:10.1109/tifs.2017.2756567

25. Wang M, Yan Z. Privacy-preserving authentication and key agreement protocols for d2d group communications. *IEEE Trans Ind Inform* (2017) 14:3637–47. doi:10.1109/tii.2017.2778090

26. 3rd generation partnership project(3gpp)ts33.501-f10, "*Tech Specification Group Serv Syst Aspects," Security architecture procedures 5G Syst*, 2018.

27. Dolev D, Yao CC. On the security of public key protocols,Symposium on Foundations of Computer Science. In: Proceedings of the 22nd Annual Symposium on Foundations of Computer Science (sfcs 1981); October 1981; Nashville, TN, USA. IEEE.

28. Nour B, Sharif K, Li F, Wang Y. Security and privacy challenges in information-centric wireless internet of things networks. *IEEE Security & Privacy* (2019) 18(2):35–45. doi:10.1109/msec.2019.2925337

29. Asghar Z, Ali N, Waqas M, Nazeer M, Khan WA. Locomotion of an efficient biomechanical sperm through viscoelastic medium. *Biomech Model Mechanobiology* (2020) 19:2271–84. doi:10.1007/s10237-020-01338-z

30. Asghar Z, Ali N, Javid K, Waqas M, Khan WA. Dynamical interaction effects on soft-bodied organisms in a multi-sinusoidal passage. *The Eur Phys J Plus* (2021) 136:693–17. doi:10.1140/epjp/s13360-021-01669-5

31. Jan S, Musa S, Ali T, Nauman M, Anwar S, Ali Tanveer T, et al. Integrity verification and behavioral classification of a large dataset applications pertaining smart OS via blockchain and generative models. *Expert Syst* (2021) 38(4):e12611. doi:10.1111/exsy.12611

32. Ali T, Khan Y, Ali T, Faizullah S, Alghamdi T, Anwar S. An automated permission selection framework for android platform. *J Grid Comput* (2020) 18:547–61. doi:10.1007/s10723-018-9455-1

33. Anwar S, Al-Obeidat F, Tubaishat A, Din S, Ahmad A, Khan FA, et al. Countering malicious URLs in internet of things using a knowledge-based approach and a simulated expert. *IEEE Internet Things J* (2019) 7(5):4497–504. doi:10.1109/jiot.2019.2954919

34. Qiu S, Wang D, Xu G, Kumari S. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. *IEEE Trans Dependable Secure Comput* (2020) 19(2):1338–1351. doi:10.1109/TDSC.2020.3022797

35. Zhang L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos Solitons & Fractals* (2008) 37(3):669–74. doi:10.1016/j.chaos.2006.09.047

36. RoyChatterjeeDas SSAK, Chattopadhyay S, Kumari S, Jo M. Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. *IEEE Internet Things J* (2018) 5(4):2884–95. doi:10.1109/jiot.2017.2714179

37. Zhang J, Cui J, Zhong H, Chen Z, Liu L PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans Dependable Secure Comput* (2019) 18. doi:10.1109/TDSC.2019.2904274

38. Fuyou M, Yan X, Xingfu W, Badawy M Randomized component and its application to (t,m,n) group oriented secret sharing. *IEEE Trans Inf Forensics Security* (2017) 10(5):889–99.

39. Burrows M, Needham MAM. A Logic of authentication. *Proc R Soc Lond* (1989) 426:233–71.