Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 6086686, 10 pages
https://doi.org/10.1155/2023/6086686

Research Article

Security Authentication Protocol for Massive Machine Type Communication in 5G Networks

Junfeng Miao,[1] **Zhaoshun Wang**,[1] **Mei Wang**,[2] **Xiao Feng**,[3,4] **Nan Xiao**,[1] **and Xiaoxue Sun**[1]

[1]*The School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijjing 100083, China*
[2]*Shandong University, Shandong 250100, China*
[3]*Beijing University of Posts and Telecommunications, Beijing 100876, China*
[4]*State Grid Information Telecommunication Group Co.Ltd, Beijing 102211, China*

Correspondence should be addressed to Xiao Feng; fengxiao@bupt.edu.cn

Received 5 July 2022; Revised 29 September 2022; Accepted 24 November 2022; Published 6 April 2023

Academic Editor: Chenglu Jin

As one of the three major applications of 5G, massive machine type communication (mMTC) is mainly oriented to network access scenarios for massive devices. mMTC focuses on solving the problem that traditional mobile communication cannot well support the Internet of Things and vertical industry applications. According to the current 3GPP standard, these massive devices still use the traditional authentication process to realize mutual authentication with 5G core network, which brings a lot of communication and computing overhead. In addition, privacy protection will also be threatened in the authentication process. In order to alleviate the signaling congestion during authentication and solve the insecurity in authentication, this paper proposes a group authentication scheme for mMTC. Due to the characteristics of low power consumption and massive connection, the scheme mainly adopts lightweight encryption operation to avoid the computational burden of equipment and server. We verify the security of our scheme by using BAN logic to formally analyze the scheme. Then, through informal analysis, our proposed scheme can not only avoid signaling blocking and provide mutual authentication but also resist various possible attacks. Through performance evaluation, it is proved that our scheme has better efficiency.

1. Introduction

With the deepening of 5G technology research, ITU-R formally defined massive machine type communication (mMTC) as one of the three major 5G application scenarios in 2015 [1]. With its huge advantages over 4G in performance indicators such as peak rate, air interface delay, and spectrum resources, 5G can meet hundreds of millions of massive IoT terminal network performance requirements, promote the deep integration of 5G and IoT, and form a mMTC business scenario [2]. From the concept definition of mMTC, hundreds of millions of terminal devices are deployed and applied to the needs of massive data acquisition and transmission [3]. Massive connections and small amount of data are one of the main characteristics of the typical mMTC mode. At the same time, it has the advantages of 5G network high speed, low delay, and other network performance advantages [4].

In the mMTC business scenario, a large number of terminal devices, 5G key technologies, etc., meet the needs of digital and diversified business in terms of coverage, number of devices, and network performance [5]. At the same time, it also brings network security challenges to the mMTC business scenario. The mMTC business scenario introduces 5G key technologies such as virtualization and network slicing to drive the mMTC business scenario network to a virtualized and service-oriented transition. At the same time, in the ubiquitous connection scenario, a large number of diversified terminals are easy to be used by attacks, and they lead to the threat of network attacks [6].

As a typical application scenario under the 5G Internet of Things architecture, mMTC has become the focus of many researchers and the cornerstone of building a global Internet of Things to realize the interconnection of all things. mMTC is mainly aimed at the Internet of Things

aiming at sensing and data acquisition. Its goal is simply to enable more machine type communication user equipment to connect to the network. The Third Generation Partnership Project (3GPP) defines the secure access process of mMTC device [7, 8]. However, it also faces many problems. Firstly, there are too many information of header transmitted between MTC device and base station in the process of random access, resulting in low data transmission efficiency. Secondly, the number of MTC devices is much larger than the number of time-frequency resources that the system can provide. The serious mismatch between the two will lead to serious equipment access collision and increase the access delay of MTC devices and excessive access energy consumption. Therefore, it is necessary to reduce the signaling interaction in the random-access process and the average delay in the access process and then improve the utilization efficiency of time-frequency resources and the data transmission efficiency of MTC device. From LTE network to 5G networks, the number of users increases exponentially. But in mMTC communication scenario, the secure access scheme still adopts 3GPP standard authentication protocol and key agreement (EAP-AKA) [9]. Therefore, when the mMTC device roams to the 5G network, serious signaling congestion and security issues may occur [10]. The inspiration of this paper is based on [11–17], which proposes a lightweight security authentication protocol based on Barrel Shifter Physical Unclonable Function (BS-PUF) for mMTC in 5G network. The protocol allows the service network to authenticate a group of devices at the same time, so as to reduce the number of signaling transmission and communication delay through the home network. The main contributions of this paper are as follows:

(1) Under the background that 5G networks have a large number of MTC devices, in order to reduce the computation overhead and communication delay, we aggregate the authentication messages on leader MTC into a message and send it to the server for authentication, which improves the authentication efficiency

(2) We propose a lightweight security authentication scheme. Our scheme is based on lightweight encryption primitives

(3) Here, we first use BAN logic to verify the correctness and safety of the scheme. Then, we use informal security analysis to analyze the related security requirements achieved by our scheme and compare it with the security functions of other related schemes later

(4) Finally, in the performance evaluation, we analyze that our scheme has less computation overhead and communication overhead. Therefore, our scheme has good security and efficiency in the process of mMTC device authentication

The remaining chapters of our article are listed below. In Chapter 2, we review related research work. In Chapter 3, we mainly introduce the relevant knowledge of the scheme. In Chapter 4, we mainly describe our proposed scheme in detail. In Chapter 5, we prove and analyze the security of the scheme. In Chapter 6, we evaluated the performance of the solution. Finally, in Chapter 7, we summarize the work of the full text.

2. Related Work

So far, many researchers have proposed a lot of research on group MTC authentication in LTE networks. With the continuous development and popularization of 5G network, many scholars also put forward the research on group MTC authentication for 5G network.

In [18], Lai et al. proposed a lightweight group authentication protocol based on aggregated messages in LTE networks. This protocol performed group authentication on MTC devices, reduced the overhead of identity verification, and effectively avoided signaling congestion in the network. Cao et al. [19] proposed a group-based access authentication scheme using aggregated signature technology. This scheme could enable a large number of MTC devices to be authenticated by the network and establish corresponding session keys, respectively. Zhang et al. [20] proposed a group-based security authentication protocol in roaming scenarios. The protocol had a dynamic group key generation and update method, and it also avoided the blockage caused by a large number of MTC devices. Cao et al. [21] proposed an efficient group-based anonymous handover protocol. The protocol could adapt to roaming scenarios in LTE-A networks and could effectively reduce signaling costs and communication costs and protect user privacy. Li et al. [22] proposed an identity verification and key agreement scheme based on a secret sharing scheme in MTC scenarios. This scheme realized distributed authentication and dynamically updated access strategy. Cao et al. [23] proposed a secure and efficient authentication scheme based on multisignature and aggregated message authentication code technology. This solution could implement a simple authentication process and switch between different scenarios and had relatively good security. These schemes were mainly for LTE networks.

Cao et al. [11] proposed a group-based handover authentication and reauthentication protocol in 5G networks. This protocol was suitable for mMTC devices roaming to a new network, and the signaling overhead and bandwidth consumption were less than other protocols.

Basudan [12] proposed a lightweight and efficient mMTC group authentication protocol in 5G networks. The protocol was based on bilinear mapping and aggregation without certificates and realized mutual authentication, session keys, and confidentiality. Cao et al. [13] proposed a secure and efficient authentication scheme for a large number of devices in 5G networks. This scheme could not only resist a large number of protocol attacks but also could update group members and realize privacy protection. Lai et al. [9] proposed a group-based secure lightweight authentication and key protocol for machine-to-machine communication. The scheme could resist various attacks and provide the required security requirements. Cao et al. [14] proposed a lightweight and secure access authentication

protocol based on extended chaotic mapping. This protocol was aimed at two types of equipment. One was ordinary user equipment, and the other was mMTC equipment. And the protocol implemented functions such as mutual authentication and anonymity protection. These schemes were mainly for 5G networks, but some schemes had large computation and communication overhead.

3. Preliminaries

3.1. System Model. As shown in Figure 1, the system model mainly includes 5G access network and 5G core network [4, 14, 24].

The 5G access network is mainly composed of MTC devices and wireless networks. The wireless network includes 5G next-generation radio access network (NG-RAN) and non-3GPP access network, which provide with data network access and communication services for devices. In 5G core network, access and mobility management function (AMF) can provide all functions related to users and control plane session management and can authenticate through security anchor function (SEAF). Authentication Server Function (AUSF) and Unified Data Management (UDM) provide authentication and user data management services for users. When connecting to the network through NG-RAN, the user authenticates with AUSF through SEAF/AMF. When connecting to the network through non-3GPP access network, the user establishes a security association through IKEv2 (Internet Key Exchange Protocol version 2) in the non-3GPP access interworking function (N3IWF) and then performs the authentication process through AMF/AUSF. In addition, 5G core network also provides session management function (SMF) and user plane function (UPF).

3.2. Security Model. The protocol security analysis method mainly focuses on whether there are loopholes in protocol interaction, that is, the Dolev-Yao model [25]. In the Dolev-Yao model, Dolev and Yao believe that the knowledge and capabilities of protocol attackers cannot be ignored in protocol security certification. The specific capabilities are as follows:

(1) The attacker can control the whole communication channel

(2) Attackers can establish connections with devices and execute security authentication and key agreement protocols by constructing masquerade nodes

(3) Attackers can eavesdrop, store, forge, modify, and replay messages transmitted on the channel

3.3. Security Requirements. In order to eliminate possible security threats and ensure that mMTC devices can communicate securely, the authentication protocol we designed should meet the following security goals:

(1) *Identity Authentication*. The communication entities authenticate each other to ensure the legitimacy of the authentication entities

(2) *Session Key Security*. The communication entity negotiates the secure session key, and the attacker cannot obtain the session key

(3) *Identity Anonymity and Unlinkability*. In the whole authentication process, the user identity information must be hidden, and the attacker cannot associate its identity information with the public information of the channel

(4) *Forward Security*. This goal ensures that even if the session key is leaked, the previous session key cannot be calculated from the key, which is irrelevant to each other. The security of session key is guaranteed

(5) *Antiattack Ability*. The proposed scheme can resist existing protocol attacks, including replay attack and forgery attack

(6) *Avoid Authentication Signaling Congestion*. When a large number of users make access requests at the same time, it can simplify the authentication process, reduce the authentication delay, avoid signaling congestion, and finally ensure the smooth progress of the whole authentication system

3.4. Barrel Shifter Physical Unclonable Function. Physical Unclonable Function (PUF) is a group of miniature delay circuits, which extracts the differences in the chip manufacturing process to obtain a group of input and output called stimulus-response pairs. The relationship between stimulus and response is only determined by certain physical differences in the device. Due to the differences in the chip manufacturing process, it has a non-reproducible characteristic [15].

In 2018, Guo et al. [16] proposed a Barrel Shifter Physical Unclonable Function (BS-PUF) based on reversible and commutativity. It is defined as follows:

Property 1: reversible

Given a reversible keyed PUF, the value x and the key K, calculate $\mathrm{PUF}(K, x) = y \Rightarrow \mathrm{PUF}^{-1}(K, y) = x$, where PUF^{-1} is the reverse calculation on the same PUF.

Property 2: commutativity

Given two commutative PUF_1 and PUF_2, for BS-PUF, such the commutative PUF not only has logical commutativity but also physical commutativity, so $\mathrm{PUF}_1(\mathrm{PUF}_2(x)) = \mathrm{PUF}_2(\mathrm{PUF}_1(x))$ can be calculated.

4. Proposed Scheme

Based on research [11–23], this paper proposes a lightweight security authentication scheme. This solution enables the mMTC devices to communicate securely through the session key in the 5G networks. Table 1 lists the main notations used here.

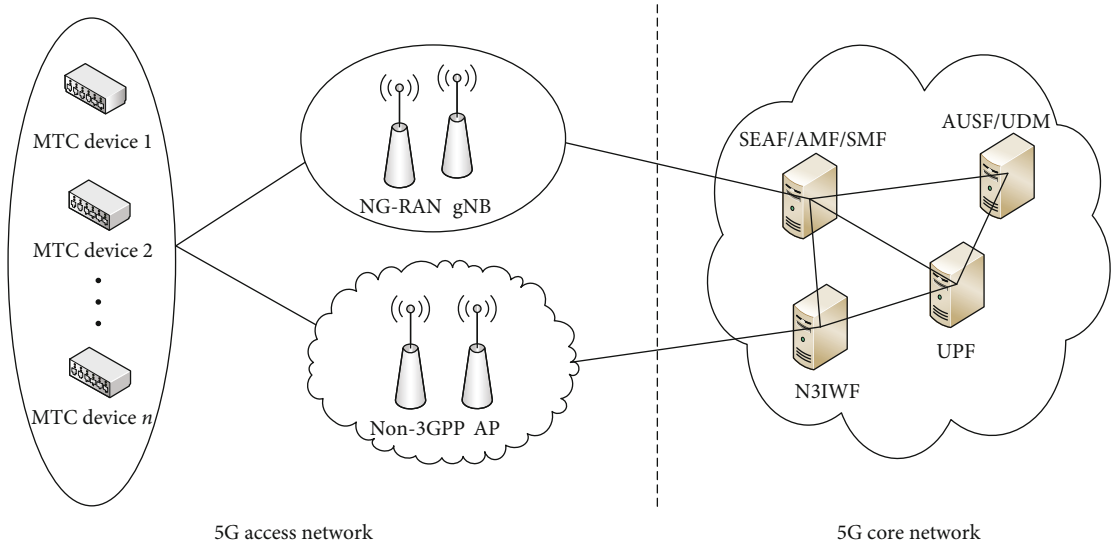

Figure 1: System model.

Table 1: Notations.

Notations	Definitions
TRC	The trusted registration center
MTC_i	Machine type communication device
AUSF/UDM	Authentication server function/unified data management
SEAF/AMF	Security anchor function/access and mobility management function
$H(\bullet)$	A one-way secure hash function
$PUF_i(\bullet)$	Physical Unclonable Function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation
T_x	The timestamp
GID	The group identity
TID_i	The temporary identity
s	The system master key
MAC_x	Message authentication code

4.1. System Setup. In order to better design the access authentication protocol for mMTC device and facilitate the security analysis of the protocol, in the scheme, it is assumed that each user device and 5GC network node can perform BS-PUF. In this initialization phase, the trusted registration center (TRC) is a trusted entity responsible for registering MTC device. TRC selects the master key $s \in Z_q^*$ and a one-way secure hash function $H: \{0,1\}^* \longrightarrow Z_q^*$. Then, TRC publishes system parameters $\{H(\bullet)\}$. Here, we merge TRC and AUSF/UDM. Each MTC device first registers with TRC and returns relevant parameters to the user device through the secure channel. According to the Diameter protocol [4] formulated by 3GPP organization, it can be seen that the communication between AUSF/UDM and SEAF/AMF uses the wired channel between backbone networks for transmission. Therefore, we believe that the communication channel between AUSF/UDM and SEAF/AMF is safe. In addition, for mMTC devices in the same range, we select a device leader MTC_n based on the functions of the mMTC device including computing capabilities and communication capabilities. As shown in Figure 2, it shows the specific authentication details of our scheme.

4.2. Registration. In the registration phase, each device MTC_i registers with the TRC through a secure channel. Firstly, MTC_i randomly selects a random value X_i, calculates $PK_{MTC_i} = PUF_{MTC_i}(X_i)$, and then sends the identity ID_i, X_i, and PK_{MTC_i} to TRC through the secure channel. When TRC receives the values sent by $MTCD_i$, it randomly selects the value e_i, calculates the temporary identity $TID_i = PUF_{TRC}(s, e_i)$, $PK_i = PUF_{TRC}(X_i)$, $A_i = H(s, e_i)$, stores (ID_i, PK_{MTC_i}) in the database, and then sends the message (TID_i, PK_i, and A_i) to $MTCD_i$ through the secure channel.

4.3. Access Authentication

(1) First, the device MTC_i in the group generates a random number X_i^{new}; calculates the secret value $K_{MTC_i} = PUF_{MTC_i}(PK_i)$, $PK_{MTC_i}^{new} = PUF_{MTC_i}(X_i^{new})$, $HID_i = A_i \oplus ID_i$, and $M_{MTC_i} = (H(A_i, ID_i)||K_{MTC_i}) \oplus (PK_{MTC_i}^{new}||X_i^{new})$; and generates a verification message $MAC_i = H(ID_i, TID_i, K_{MTC_i}, PK_{MTC_i}^{new}, X_i^{new})$. Then, MTC_i sends the message $\{TID_i, HID_i, M_{MTC_i}, MAC_i\}$ to MTC_n

(2) Upon receiving the messages sent by the group members, MTC_n performs the same operation as MTC_i. And it generates the current timestamp T_{MTC_n} and the corresponding group identity GID and calculates $TGID = GID \oplus H(A_n, ID_n, K_{MTC_n})$ and $MAC_L = H(MAC_1, MAC_2 \bullet\bullet\bullet, MAC_n, T_{MTC_n}, GID)$. Finally, MTC_n

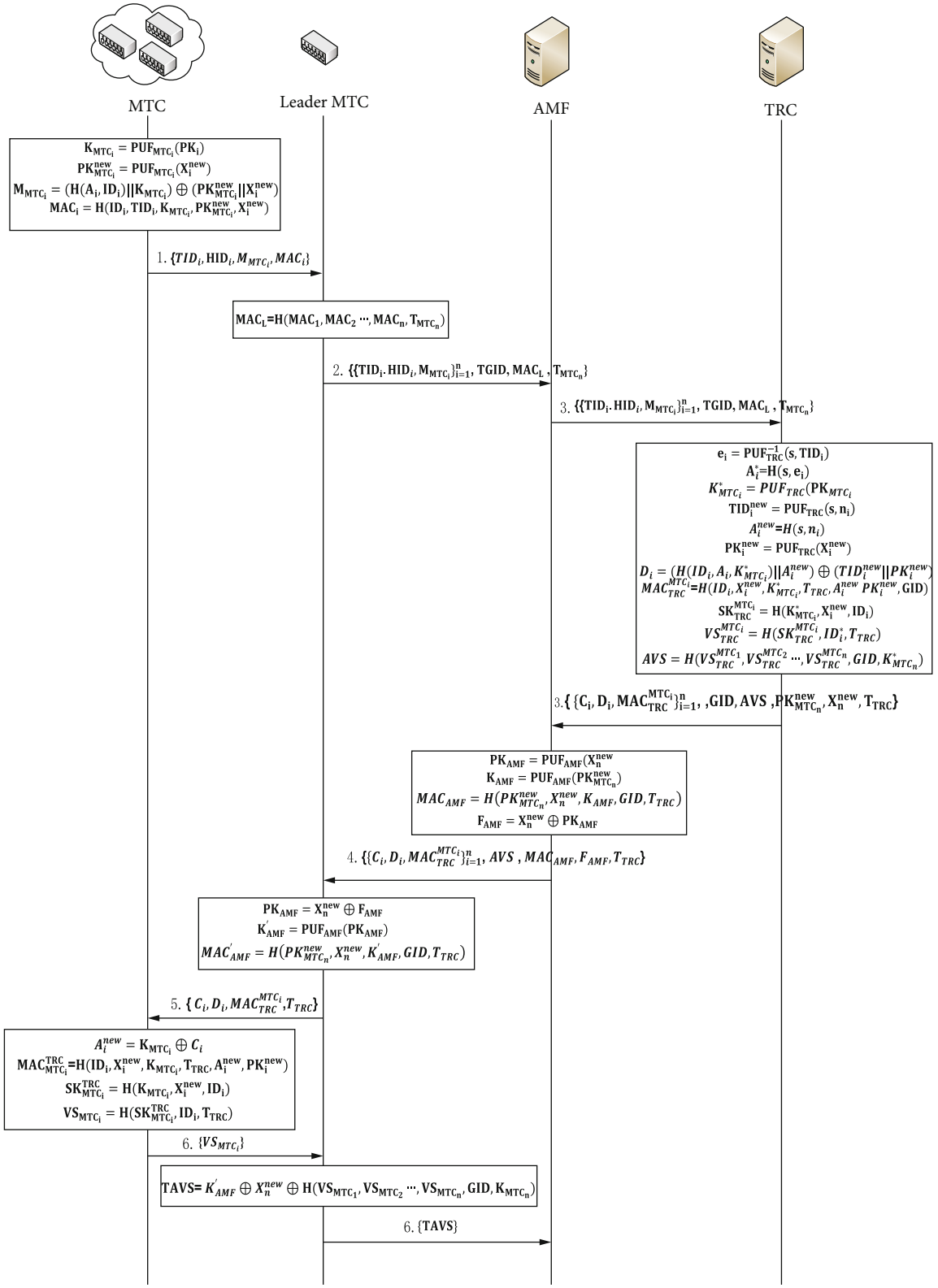

Figure 2: Authentication process of the proposed protocol.

sends the message $\{\{\mathrm{TID}_i.\mathrm{HID}_i, M_{\mathrm{MTC}_i}\}_{i=1}^{n}, \mathrm{TGID}, \mathrm{MAC}_L, T_{\mathrm{MTC}_n}\}$ to AMF

(3) On receiving the messages, AMF sends the message $\{\{\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}\}_{i=1}^{n}, \mathrm{TGID}, \mathrm{MAC}_L, T_{\mathrm{MTC}_n}\}$ to TRC

(4) When TRC receives the message from AMF, it first verifies whether the timestamp T_{MTC_n} is within the legal range. If it is within the legal scope, TRC calculates $e_i = \mathrm{PUF}_{\mathrm{TRC}}^{-1}(s, \mathrm{TID}_i)$, $A_i^* = H(s, e_i)$, and $\mathrm{ID}_i^* = A_i^* \oplus \mathrm{HID}_i$. TRC queries the database to verify whether the identity ID_i^* is legal. If the verification is legal, TRC gets $\mathrm{PK}_{\mathrm{MTC}_i}$ and calculates $K_{\mathrm{MTC}_i}^* = \mathrm{PUF}_{\mathrm{TRC}}(\mathrm{PK}_{\mathrm{MTC}_i})$, $\mathrm{GID} = \mathrm{TGID} \oplus H(A_n^*, \mathrm{ID}_n^*, K_{\mathrm{MTC}_n}^*)$, $(\mathrm{PK}_{\mathrm{MTC}_i}^{\mathrm{new}} \| X_i^{\mathrm{new}}) = (H(A_i^*, \mathrm{ID}_i^*) \| K_{\mathrm{MTC}_i}^*) \oplus M_{\mathrm{MTC}_i}$. Then, it calculates $\mathrm{MAC}_i' = H(\mathrm{ID}_i^*, \mathrm{TID}_i, K_{\mathrm{MTC}_i}^*, \mathrm{PK}_{\mathrm{MTC}_i}^{\mathrm{new}}, X_i^{\mathrm{new}})$. TRC calculates $\mathrm{MAC}_L' = H(\mathrm{MAC}_1', \mathrm{MAC}_2' \bullet\bullet\bullet, \mathrm{MAC}_n', T_{\mathrm{MTC}_n}, \mathrm{GID})$ and verifies whether MAC_L' and MAC_L are equal. If they are equal, then the group MTC devices are certified. If they are not equal, there are illegal devices in the group. TRC selects random value n_i and timestamp T_{TRC}; calculates $\mathrm{TID}_i^{\mathrm{new}} = \mathrm{PUF}_{\mathrm{TRC}}(s, n_i)$, $A_i^{\mathrm{new}} = H(s, n_i)$, $\mathrm{PK}_i^{\mathrm{new}} = \mathrm{PUF}_{\mathrm{TRC}}(X_i^{\mathrm{new}})$, $C_i = K_{\mathrm{MTC}_i}^* \oplus A_i^{\mathrm{new}}$, and $D_i = (H(\mathrm{ID}_i, \mathrm{A}_i^*, K_{\mathrm{MTC}_i}^*) \| A_i^{\mathrm{new}}) \oplus (\mathrm{TID}_i^{\mathrm{new}} \| \mathrm{PK}_i^{\mathrm{new}})$; and updates value $(\mathrm{ID}_i, \mathrm{PK}_{\mathrm{MTC}_i}^{\mathrm{new}})$, stored in the database. Then, TRC generates verification message $\mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i} = H(\mathrm{ID}_i^*, X_i^{\mathrm{new}}, K_{\mathrm{MTC}_i}^*, T_{\mathrm{TRC}}, A_i^{\mathrm{new}}, \mathrm{PK}_i^{\mathrm{new}})$ and the session key $\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i} = H(K_{\mathrm{MTC}_i}^*, X_i^{\mathrm{new}}, \mathrm{ID}_i^*)$. TRC generates verification value $\mathrm{VS}_{\mathrm{TRC}}^{\mathrm{MTC}_i} = H(\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, \mathrm{ID}_i^*, T_{\mathrm{TRC}})$ and aggregates the verification values to obtain $\mathrm{AVS} = H(\mathrm{VS}_{\mathrm{TRC}}^{\mathrm{MTC}_1}, \mathrm{VS}_{\mathrm{TRC}}^{\mathrm{MTC}_2} \bullet\bullet\bullet, \mathrm{VS}_{\mathrm{TRC}}^{\mathrm{MTC}_n}, \mathrm{GID}, K_{\mathrm{MTC}_n}^*)$. Finally, TRC sends message $\{\{C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}\}_{i=1}^{n}, \mathrm{GID}, \mathrm{AVS}, \mathrm{PK}_{\mathrm{MTC}_n}^{\mathrm{new}}, X_n^{\mathrm{new}}, T_{\mathrm{TRC}}\}$ to AMF

(5) After receiving the message sent from TRC, AMF verifies whether the timestamp T_{TRC} is within the legal range. If the verification is legal, it stores the group identity GID and AVS; calculates $\mathrm{PK}_{\mathrm{AMF}} = \mathrm{PUF}_{\mathrm{AMF}}(X_n^{\mathrm{new}})$, $K_{\mathrm{AMF}} = \mathrm{PUF}_{\mathrm{AMF}}(\mathrm{PK}_{\mathrm{MTC}_n}^{\mathrm{new}})$, $\mathrm{MAC}_{\mathrm{AMF}} = H(\mathrm{PK}_{\mathrm{MTC}_n}^{\mathrm{new}}, X_n^{\mathrm{new}}, K_{\mathrm{AMF}}, \mathrm{GID}, T_{\mathrm{TRC}})$, and $F_{\mathrm{AMF}} = X_n^{\mathrm{new}} \oplus \mathrm{PK}_{\mathrm{AMF}}$; and forwards the message $\{\{C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}\}_{i=1}^{n}, \mathrm{AVS}, \mathrm{MAC}_{\mathrm{AMF}}, F_{\mathrm{AMF}}, T_{\mathrm{TRC}}\}$ to MAC_n

(6) MAC_n receives the message sent and verifies whether the timestamp T_{TRC} is within the legal range. If the verification is legal, it calculates $\mathrm{PK}_{\mathrm{AMF}} = X_n^{\mathrm{new}} \oplus F_{\mathrm{AMF}}$, $K_{\mathrm{AMF}}' = \mathrm{PUF}_{\mathrm{MTC}_n}(\mathrm{PK}_{\mathrm{AMF}})$, and $\mathrm{MAC}_{\mathrm{AMF}}' = H(\mathrm{PK}_{\mathrm{MTC}_n}^{\mathrm{new}}, X_n^{\mathrm{new}}, K_{\mathrm{AMF}}', \mathrm{GID}, T_{\mathrm{TRC}})$. It verifies whether $\mathrm{MAC}_{\mathrm{AMF}}'$ and $\mathrm{MAC}_{\mathrm{AMF}}$ are equal. If they are equal, it verifies AMF. Then, MAC_n calculates $A_n^{\mathrm{new}} = K_{\mathrm{MTC}_n} \oplus C_n$, $(\mathrm{TID}_n^{\mathrm{new}} \| \mathrm{PK}_n^{\mathrm{new}}) = (H(\mathrm{ID}_n, A_n, K_{\mathrm{MTC}_n}) \| A_n^{\mathrm{new}}) \oplus D_n$, and $\mathrm{MAC}_{\mathrm{MTC}_n}^{\mathrm{TRC}} = H(\mathrm{ID}_n, X_n^{\mathrm{new}}, K_{\mathrm{MTC}_n}, T_{\mathrm{TRC}}, A_n^{\mathrm{new}}, \mathrm{PK}_n^{\mathrm{new}})$. If the generated value $\mathrm{MAC}_{\mathrm{MTC}_n}^{\mathrm{TRC}}$ and the received value $\mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_n}$ are equal, then it verifies the server TRC and updates the device parameters at the same time. MTC_n generates the session key $\mathrm{SK}_{\mathrm{MTC}_n}^{\mathrm{TRC}} = H(K_{\mathrm{MTC}_n}, X_n^{\mathrm{new}}, \mathrm{ID}_n)$ and the verification value $\mathrm{VS}_{\mathrm{MTC}_n} = H(\mathrm{SK}_{\mathrm{MTC}_n}^{\mathrm{TRC}}, \mathrm{ID}_n, T_{\mathrm{TRC}})$. Finally, MTC_n forwards message $\{C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, T_{\mathrm{TRC}}\}$ to MAC_i

(7) When receiving a message from MAC_n, MTC_i verifies whether the received timestamp T_{TRC} is legal. If the timestamp T_{TRC} is legal, MTC_i calculates $A_i^{\mathrm{new}} = K_{\mathrm{MTC}_i} \oplus C_i$, $(\mathrm{TID}_i^{\mathrm{new}} \| \mathrm{PK}_i^{\mathrm{new}}) = (H(\mathrm{ID}_i, A_i, K_{\mathrm{MTC}_i}) \| A_i^{\mathrm{new}}) \oplus D_i$, and $\mathrm{MAC}_{\mathrm{MTC}_i}^{\mathrm{TRC}} = H(\mathrm{ID}_i, X_i^{\mathrm{new}}, K_{\mathrm{MTC}_i}, T_{\mathrm{TRC}}, A_i^{\mathrm{new}}, \mathrm{PK}_i^{\mathrm{new}})$. If the generated value $\mathrm{MAC}_{\mathrm{MTC}_i}^{\mathrm{TRC}}$ and the received value $\mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}$ are equal, then it verifies the server TRC and updates the device parameters at the same time. MTC_i generates the session key $\mathrm{SK}_{\mathrm{MTC}_i}^{\mathrm{TRC}} = H(K_{\mathrm{MTC}_i}, X_i^{\mathrm{new}}, \mathrm{ID}_i)$ and the verification value $\mathrm{VS}_{\mathrm{MTC}_i} = H(\mathrm{SK}_{\mathrm{MTC}_i}^{\mathrm{TRC}}, \mathrm{ID}_i, T_{\mathrm{TRC}})$. Finally, the message $\{\mathrm{VS}_{\mathrm{MTC}_i}\}$ is sent to MTC_n

(8) On receiving the message sent by the group members, MTC_n calculates $\mathrm{TAVS} = K_{\mathrm{AMF}}' \oplus X_n^{\mathrm{new}} \oplus H(\mathrm{VS}_{\mathrm{MTC}_1}, \mathrm{VS}_{\mathrm{MTC}_2} \bullet\bullet\bullet, \mathrm{VS}_{\mathrm{MTC}_n}, \mathrm{GID}, K_{\mathrm{MTC}_n})$ and sends it to AMF

(9) AMF receives the message and calculates $\mathrm{AVS}^* = K_{\mathrm{AMF}} \oplus X_n^{\mathrm{new}} \oplus \mathrm{TAVS}$. Then, it compares AVS with the received AVS^*. If they are equal, the correctness of the generated session key is verified

Finally, MTC_i communicates through the session key.

5. Security Evaluation

5.1. Security Proof Based on BAN Logic

5.1.1. BAN Logic Rules. In this paper, BAN logic is used to formally analyze the proposed authentication scheme. BAN logic [26] is a formal analysis tool based on knowledge and belief.

5.1.2. Verification. Here, we formally verify our scheme. First, we idealize the scheme.

(1) The messages involved in our scheme are idealized

$\mathrm{Mes}_1 : \mathrm{MTCD_i} \longrightarrow \mathrm{TRC} : <\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i>_{K_{\mathrm{MTC}_i}}$

$\mathrm{Mes}_2 : \mathrm{TRC} \longrightarrow \mathrm{MTCD}_i : <C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, T_{\mathrm{TRC}}>_{K_{\mathrm{MTC}_i}}$

(2) Formal description of initial state

$A_1 : \mathrm{MTCD}_i| \equiv \mathrm{MTCD}_i \overset{K_{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

$A_2 : \mathrm{TRC}| \equiv \mathrm{MTCD_i} \overset{K^*_{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

$A_3 : \mathrm{TRC}| \equiv \#(X_i^{\mathrm{new}})$

$A_4 : \mathrm{TRC}| \equiv \mathrm{MTCD}_i \Rightarrow <\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i>$

$A_5 : \mathrm{TRC}| \equiv \mathrm{MTCD}_i \Rightarrow \mathrm{MTCD_i} \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

$A_6 : \mathrm{MTCD}_i| \equiv \#(T_{TRC})$

$A_7 : \mathrm{MTCD}_i| \equiv \mathrm{TRC} \Rightarrow <\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i>$

$A_8 : \mathrm{MTCD}_i| \equiv \mathrm{TRC} \Rightarrow \mathrm{MTCD}_i \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

(3) The ultimate goal of the scheme

In this section, our scheme needs to meet the following goals:

$G_1 : \mathrm{MTCD}_i| \equiv \mathrm{MTCD_i} \overset{\mathrm{SK}_{\mathrm{MTC}_i}^{\mathrm{TRC}}}{\leftrightarrow} \mathrm{TRC}$

$G_2 : \mathrm{MTCD}_i| \equiv \mathrm{TRC}| \equiv \mathrm{MTCD_i} \overset{\mathrm{SK}_{\mathrm{MTC}_i}^{\mathrm{TRC}}}{\leftrightarrow} \mathrm{TRC}$

$G_3 : \mathrm{TRC}| \equiv \mathrm{MTCD}_i \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

$G_4 : \mathrm{TRC}| \equiv \mathrm{MTCD}_i| \equiv \mathrm{MTCD_i} \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

(4) Logical reasoning

According to the message Mes_1 sent by $\mathrm{MTC_i}$ to TRC, it can be concluded that

$S_1 : \mathrm{TRC} \triangleleft <\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i>_{K_{\mathrm{MTC}_i}}$

Given S_1 and A_2, from the message meaning rule, we can get

$S_2 : \mathrm{TRC} |\equiv \mathrm{MTCD}_i| \sim \mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i$

From S_1, A_3 and the freshness rule, we can get

$S_3 : \mathrm{TRC}| \equiv \#\{\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i\}$

From S_2,S_3, and nonce verification rule, we can get

$S_4 : \mathrm{TRC}| \equiv \mathrm{MTCD}_i| \equiv \{\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i\}$

From S_4, A_4, and arbitration rules, we can get

$S_5 : \mathrm{TRC}| \equiv \{\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i\}$

Given S_5 and $\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i} = H(K^*_{\mathrm{MTC}_i}, X_i^{\mathrm{new}}, \mathrm{ID}_i)$, we can get

$S_6 : \mathrm{TRC} |\equiv \mathrm{MTCD}_i| \equiv \mathrm{MTCD_i} \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

According to S_6, A_5, and the arbitration rule, we can get

$S_7 : \mathrm{TRC}| \equiv \mathrm{MTCD}_i \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

According to the message Mes_2 sent by TRC to MTCD_i, we can get:

$S_8 : \mathrm{MTCD}_i \triangleleft <C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, T_{\mathrm{TRC}}>_{K_{\mathrm{MTC}_i}}$

Given S_8 and A_1, from the message meaning rule, we can get

$S_9 : \mathrm{MTCD}_i| \equiv \mathrm{TRC}| \sim \{C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, T_{\mathrm{TRC}}\}$

According to S_9, A_6, and the freshness rule, we can get

$S_{10} : \mathrm{MTCD}_i| \equiv \#(C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, T_{\mathrm{TRC}})$

From S_9, S_{10}, and the nonce verification rule, we can see

$S_{11} : \mathrm{MTCD}_i| \equiv \mathrm{TRC}| \equiv \{C_i, D_i, \mathrm{MAC}_{\mathrm{TRC}}^{\mathrm{MTC}_i}, T_{\mathrm{TRC}}\}$

From S_{11}, A_7, and the arbitration rule, we can get

Table 2: Computation overhead.

Protocol	Computation overhead
LPPA [13]	$(2n + 2m)T_{D/E} + (12n + 8m)T_H$
LSAA [14]	$16nT_{CM} + 4nT_{E/D} + 6nT_H$
Our scheme	$(6n + 3m)T_{\mathrm{PUF}} + (14n + 7m)T_H$

Table 3: Communication overhead.

Protocol	Leader MTC
LPPA [13]	$640n + 1280m$
LSAA [14]	$1152n + 384m$
Our scheme	$1056n - 256m$

$S_{12} : \mathrm{MTCD}_i| \equiv \{\mathrm{TID}_i, \mathrm{HID}_i, M_{\mathrm{MTC}_i}, \mathrm{MAC}_i\}$

From S_{12} and $\mathrm{SK}_{\mathrm{MTC}_i}^{\mathrm{TRC}} = H(K_{\mathrm{MTC}_i}, X_i^{\mathrm{new}}, \mathrm{ID}_i)$, we can see

$S_{13} : \mathrm{MTCD}_i| \equiv \mathrm{TRC}| \equiv \mathrm{MTCD_i} \overset{\mathrm{SK}_{\mathrm{MTC}_i}^{\mathrm{TRC}}}{\leftrightarrow} \mathrm{TRC}$

According to S_{13}, A_8, and the arbitration rule, we can get

$S_{14} : \mathrm{MTCD}_i| \equiv \mathrm{TRC} \overset{\mathrm{SK}_{\mathrm{TRC}}^{\mathrm{MTC}_i}}{\leftrightarrow} \mathrm{TRC}$

Through S_6, S_7, S_{13}, and S_{14}, we can see that our scheme reaches the goals.

5.2. Security Analysis. The security of our scheme is mainly analyzed from the aspects of identity authentication, session key security, resistance to attacks, and so on.

(1) *Identity Authentication*. In our scheme, communication entities use message authentication codes to verify their legitimacy. Because the generated message verification code includes the secret value generated by BS-PUF, the security of the verification message is guaranteed

(2) *Session Key Security*. Each MTC device negotiates a session key with the server. The corresponding session key is generated through the secret value generated by the BS-PUF and other parameters, ensuring the security of the session key

(3) *Identity Anonymity and Unlinkability*. In our scheme, each MTC device communicates with the server through pseudonym $\mathrm{TID}_i = \mathrm{PUF}_{\mathrm{TRC}}(s, e_i)$, and the real identity is encrypted as $M_{\mathrm{MTC}_i} = H_1(A_i, T_{\mathrm{MTC}_i}) \oplus \mathrm{ID}_i$. After receiving the pseudonym TID_i and M_{MTC_i}, the server obtains the real identity through calculation. Because the real identity of the device can be obtained only through the calculation of the server, the anonymity of the device is guaranteed. Because the temporary identity of each MTC device in the scheme changes and the generated messages use random numbers and time stamps, the messages transmitted in the network are different, and the attacker cannot distinguish that the two messages are sent by the same device

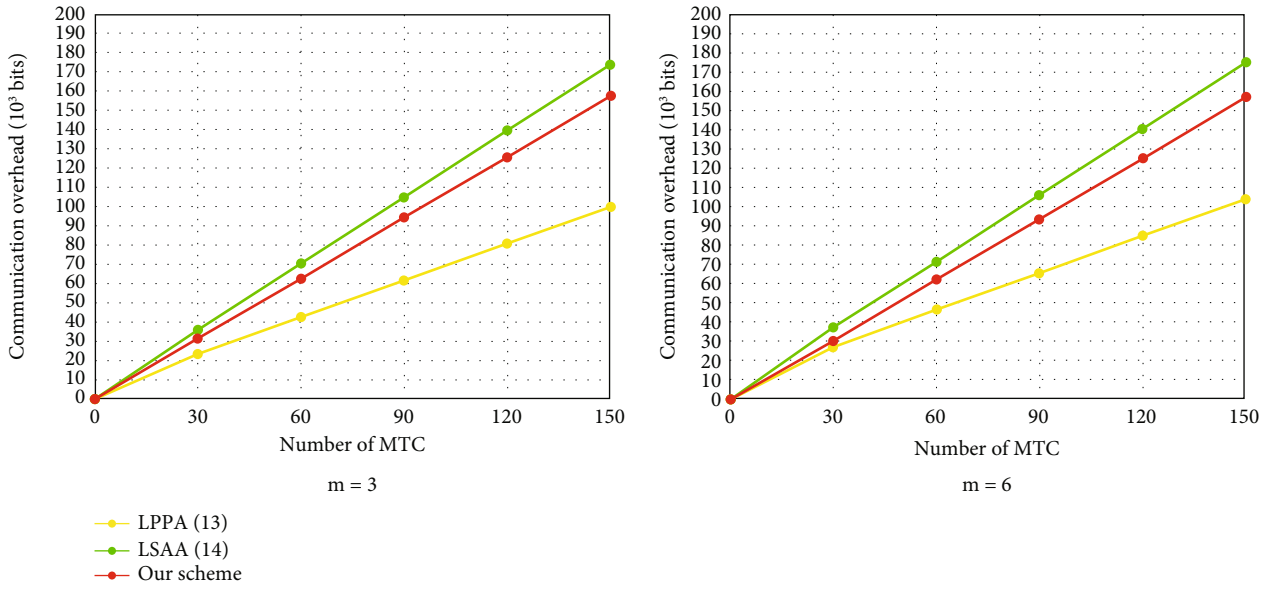

Figure 3: Communication overhead between different protocols.

(4) *Forward Security*. Each MTC device negotiates with the server to generate a corresponding session key through the secret value and random number generated. Because the secret value and random number generated for each authentication are different, the security of the session key is guaranteed. Even if the session key is leaked, it will not affect the previously generated session keys

(5) *Antiattack Ability*. In the communication process of our scheme, each MTC device ensures the freshness of messages by using time stamps, so it can effectively avoid replay attacks. In the process of message verification, our scheme uses the message authentication code. Because the message authentication code is generated by the secret value and other parameters generated, it is difficult for the attacker to generate the correct message authentication code, so it can effectively avoid man in the middle attack. In our scheme, because the real identity is encrypted, it is difficult for the attacker to extract the user identity from the message, so it is difficult to impersonate a legitimate user for communication. In the authentication process, since the secret value $K^*_{\mathrm{MTC}_i}$ can only be generated by the server, the attacker cannot generate this value for verification, so it is difficult for the attacker to impersonate the server

(6) *Avoid Authentication Signaling Congestion*. Our scheme uses aggregation message authentication technology to aggregate a group of MTC device request messages into one request message. Here, we complete the message aggregation in leader MTC, reduce the signaling computation and communication overhead, and send it to the server for authentication. Our scheme effectively simplifies the authentication process, reduces the authentication delay, and avoids signaling congestion

6. Performance Analysis

In this section, we mainly analyze the performance of our scheme from two aspects: computation overhead and communication overhead. Here, we mainly compare the schemes similar to our scheme.

6.1. Computation Overhead. By calculating the time of various encryption operations, we analyze the computation overhead of the protocol. In this paper, we omit the lightweight operations including XOR operations and concatenation operations. Here, $T_{D/E}$ represents the time to calculate symmetric encryption or decryption, T_H represents the time to calculate one-way hash, and T_{CM} represents the time to calculate an extended chaotic map. In addition, we refer to [17] to obtain $T_H \approx 1.6T_{\mathrm{PUF}}$. The computation overhead of relevant schemes is obtained, as shown in Table 2.

Therefore, we can see that our scheme has obvious advantages in terms of computation overhead.

6.2. Communication Overhead. Here, we evaluate the communication overhead of our scheme by comparing similar schemes. We define the size of different authentication messages. In this article, we refer to standards [27, 28]. Assume that the random number, hash value, and device identity size are 128 bits. The size of the time stamp is 32 bits. The size of the chaotic map is 128 bits. In the scheme of [17], we define the size of PUF to be 128 bits. According to the size of the defined message, we obtain the size of the communication overhead of the comparison schemes. Because of different schemes, the number of server entities communicating is different. Therefore, for the sake of fairness, we mainly compare the communication overhead of the group leader MTC device in Table 3.

Figure 3 shows the comparison results of different m values and changes in the number of devices. We can see that

[13] has small communication overhead, but it has security vulnerabilities. Therefore, our scheme has obvious advantages in terms of communication overhead and security.

7. Conclusion

Due to the signaling congestion and security problems encountered for mMTC communication in 5G networks, we propose a mMTC group authentication scheme. The scheme is based on lightweight encryption operation, which reduces the computational burden of equipment and server, and ensures the security of the scheme. Then, security verification of the proposed scheme is carried out through BAN logic and informal security analysis. The verification results show that our scheme has strong security in the process of encryption and authentication and can resist most known attacks. The data analysis shows that the proposed scheme has great improvement in communication overhead and computation overhead compared with the existing schemes. In the future research work, we will start to study the authentication scheme based on group signature. With the development of 5G communication technology, a more efficient scheme is designed to meet the requirements of lightweight and security.

Data Availability

The data used to support the findings of this study are included within this article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the 2020 Industrial Technology Foundation Public Service Platform Project (grant number 2020-0105-2-1).

References

[1] M. Series, "Framework and overall objectives of the future development of IMT for 2000 and beyond," ITU-R M. 2083, 2015.

[2] G. Wunder, Č. Stefanović, P. Popovski, and L. Thiele, "Compressive coded random access for massive MTC traffic in 5G systems," in *2015 49th Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2017.

[3] D. T. Wiriaatmadja and K. W. Choi, "Hybrid random access and data transmission protocol for machine-to-machine communications in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 33–46, 2015.

[4] 3rd Generation Partnership Project (3GPP)TS33.501-f10, "Technical specification group services and system aspects," Security architecture and procedures for 5G system, V.15.0.0, 2018.

[5] W. Zhan and L. Dai, "Massive random access of machine-to-machine communications in LTE networks: modeling and throughput optimization," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2771–2785, 2018.

[6] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes," *Journal of Network & Computer Applications*, vol. 101, pp. 55–82, 2018.

[7] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine- type communication," *Transactions on Emerging Telecommunications Technologies (ETT)*, vol. 26, no. 3, pp. 414–431, 2015.

[8] J. Puneet, H. Peter, and Z. Haris, "Machine type communications in 3GPP systems," *IEEE Communications Magazine*, vol. 50, no. 11, pp. 28–35, 2012.

[9] C. Lai, R. Lu, D. Zheng, H. Li, and X. Shen, "Toward secure large-scale machine-to-machine communications in 3GPP networks: challenges and solutions," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 12–19, 2015.

[10] J. Cao, M. Ma, H. Li et al., "A survey on security aspects for 3GPP 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2020.

[11] J. Cao, M. Ma, H. Li, Y. Fu, and X. Liu, "EGHR: efficient group-based handover authentication protocols for mMTC in 5G wireless networks," *Journalof Network and Computer Application*, vol. 102, pp. 1–16, 2018.

[12] S. Basudan, "LEGA: a lightweight and efficient group authentication protocol for massive machine type communication in 5G networks," *Journal of Communications and Information Networks*, vol. 5, no. 4, pp. 457–466, 2020.

[13] J. Cao, M. Ma, and H. Li, "LPPA: lightweight privacy-preservation access authentication scheme for massive devices in fifth Generation (5G) cellular networks," *International Journal of Communication Systems*, vol. 32, no. 3, article e3860, 2019.

[14] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.

[15] P. Gope, J. Lee, and T.-Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2831–2843, 2018.

[16] Y. Guo, T. Dee, and A. Tyagi, "Barrel shifter physical unclonable function based encryption," *Cryptography*, vol. 2, no. 3, p. 22, 2018.

[17] T. F. Lee and W. Y. Chen, "Lightweight fog computing-based authentication protocols using physically unclonable functions for Internet of Medical Things," *Journal of Information Security and Applications*, vol. 59, no. 4, article 102817, 2021.

[18] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 832–837, Atlanta, GA, USA, 2013.

[19] J. Cao, M. Ma, and H. Li, "GBAAM: group-based access authentication for MTC in LTE networks," *Security and Communication Networks*, vol. 8, pp. 3282–3299, 2015.

[20] Y. Zhang, J. Chen, H. Li, J. Cao, and C. Lai, "Group-based authentication and key agreement for machine-type communication," *International Journal of Grid and Utility Computing*, vol. 5, no. 2, pp. 87–95, 2014.

[21] J. Cao, H. Li, and M. Ma, "GAHAP: a group-based anonymity handover authentication protocol for MTC in LTE-A networks," in *IEEE International Conference on Communications*, London, UK, 2015.

[22] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[23] J. Cao, H. Li, M. Ma, and F. Li, "UPPGHA: uniform privacy preservation group handover authentication mechanism for mMTC in LTE-A networks," *Security and Communication Networks*, vol. 2018, Article ID 6854612, 16 pages, 2018.

[24] J. Miao, Z. Wang, X. Miao, and L. Xing, "A secure and efficient lightweight vehicle group authentication protocol in 5G networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 4079092, 12 pages, 2021.

[25] D. Dolev and A. Yao, "On the security of public-key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[26] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 23, no. 5, pp. 1–13, 1989.

[27] National Institute of Standards and Technology, "Special publication 800-57: recommendation for key management part 1: general (revision 4)," NIST.SP.800-57pt1r4, 2016.

[28] "Federal information processing standards publication digital signature standard (DSS)," FIPS PUB 186-4, 2013.