Research Article

UPPGHA: Uniform Privacy Preservation Group Handover Authentication Mechanism for mMTC in LTE-A Networks

Jin Cao ¹, Hui Li,¹ Maode Ma ², and Fenghua Li³

¹School of Cyber Engineering, State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, China

²School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

³State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Correspondence should be addressed to Jin Cao; caoj897@126.com

Received 27 July 2017; Revised 2 January 2018; Accepted 18 January 2018; Published 28 February 2018

Academic Editor: Tom Chen

Copyright © 2018 Jin Cao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Type Communication (MTC), as one of the most important wireless communication technologies in the future wireless communication, has become the new business growth point of mobile communication network. It is a key point to achieve seamless handovers within Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) for massive MTC (mMTC) devices in order to support mobility in the Long Term Evolution-Advanced (LTE-A) networks. When mMTC devices simultaneously roam from a base station to a new base station, the current handover mechanisms suggested by the Third-Generation Partnership Project (3GPP) require several handover signaling interactions, which could cause the signaling load over the access network and the core network. Besides, several distinct handover procedures are proposed for different mobility scenarios, which will increase the system complexity. In this paper, we propose a simple and secure uniform group-based handover authentication scheme for mMTC devices based on the multisignature and aggregate message authentication code (AMAC) techniques, which is to fit in with all of the mobility scenarios in the LTE-A networks. Compared with the current 3GPP standards, our scheme can achieve a simple authentication process with robust security protection including privacy preservation and thus avoid signaling congestion. The correctness of the proposed group handover authentication protocol is formally proved in the Canetti-Krawczyk (CK) model and verified based on the AVISPA and SPAN.

1. Introduction

Machine Type Communication (MTC), also known as Machine to Machine (M2M), can realize intelligent and interactive seamless connection among people, machine, and system via wireless communication technologies. The purpose of the MTC technology is to enable all of machineries and equipment networking and communication ability, which is a main way of the Internet of Things (IoT) applications. The MTC technology has been commercialized in Europe, South Korea, Japan, and so on, which are mainly used in security monitoring, mechanical services and maintenance business, public transport system, fleet management, industrial automation, city information, and so on. With a widely range of potential applications [1], it has been actively developed and enhanced by many standards forums and organizations including IEEE, ETSI, 3GPP, and 3GPP2. In

particular, 3GPP is becoming increasingly active in this area with several work items defined on MTC, especially for Long Term Evolution Release 10 named as LTE-Advanced (LTE-A) [2].

Compared with other wireless networks, the LTE-A network has a higher capacity and lower transmission delay and thus can provide higher data rate and better coverage and extensibility for the real-time mobile MTC applications. Therefore, the LTE-A network can be served as an ideal platform for the MTC technology to provide strong support for the development of MTC. However, the emergence of MTC technology has brought new challenges for the LTE-A network. Different from traditional Human to Human (H2H) terminals, the MTC devices (MDs) will lead to a variety of different requirements including lower energy consumption and better security due to its characteristics of unsupervised. In addition, the number of MTC devices is rapidly increasing,

MTC market analysis forecasts 50 billion machines are expected to use wired or wireless communication technologies by the year 2020 [3]. Moreover, the analysis results show that the number of MDs is connected to a single base station in 2020 to be anywhere from 10000 to 100000 [4]. Therefore, it will bring huge loads on wireless access networks and LTE-A core network [5] when sea of MDs concurrently connects to the LTE-A network. It is particularly acute when a large number of MDs simultaneously move away from the current base station to a new base station. For example, for a large number of goods transported on a freight train, some relevant sensor devices could be deployed in each car of goods to monitor the states of the goods in the transportation. A large number of surveillance cameras, temperature and humidity sensors, and smoke detectors could also be deployed on the train to perform different functions. A large number of monitoring and sensor terminals equipped with the people and vehicles participated in marathon, cycling, car rally game, and so on, are used to track the body functions, the performance of the vehicles, and so on. These devices need to support the real-time communication between the side of the road, other vehicles, or remote servers. In this mobility scenario, frequent handover signaling interaction not only causes the signaling load on the access network and core network, but also increases the terminal energy consumption. The current handover methods suggested by the 3GPP committee require each MD independently to execute the same handover authentication process as the common User Equipment (UE) [6], which results in several security vulnerabilities described as follows:

- (i) The current handover mechanisms need several rounds of signaling interaction [7, 8] and complex handover key management mechanism [9–11], which are not suitable for a group of energy limited MDs to achieve seamless handovers in mobility scenarios.
- (ii) Owing to the support of many new types of base stations such as Home eNodeB (HeNB), eNB, and Relay Nodes (RNs), 3GPP committee [7, 8] has addressed distinct handover procedures for different scenarios, such as the handovers between eNBs, between HeNBs, between a HeNB and an eNB, and the inter-MME handovers when the base stations are managed by different MMEs, which will increase the overall system complexity.
- (iii) Since some base stations such as HeNB and RNs can be easily owned by third parties, a robust mutual authentication between MDs and base stations is required in handover process to withstand several protocol attacks such as impersonation attacks, Man-in-the-Middle (MitM) attacks, and replay attacks [12–15].
- (iv) Due to lack of user identity and location privacy preservation, an attacker can easily trace a special MD's movement locus. Therefore, a fast and secure privacy preservation handover authentication scheme for a large number of MDs is required to ensure the continuity of MTC applications in the LTE-A networks.

In this paper, taking the advantage of the novel multisignature and AMAC techniques, we propose a new uniform privacy preservation group handover authentication protocol for mMTC within E-UTRAN in LTE-A networks (UPPGHA), which can be applied to all of mobility scenarios in LTE-A networks. Compared with the current 3GPP standards and other related schemes, our scheme can not only largely reduce the signaling cost and thus avoid network congestions, but also provide robust security and privacy protection. By the scheme, a mass of MDs is initialized to form a MTC group and choose a group leader [16]. When the MTC group moves to the coverage of the target eNB (eNB₂), the eNB₂ can simultaneously authenticate the MTC group by checking the multisignature and AMAC generated by the group leader on behalf of all the group members and derives a distinct session key for each MD.

Our contributions made in this paper can be summarized up as follows:

- (1) We proposed a simple handover authentication process to achieve mutual authentication and key agreement between multiple MDs and the target eNB simultaneously.
- (2) By our solution, the network congestion incurred by frequent handover for mass of MDs can be avoided in the LTE-A networks.
- (3) The proposed scheme not only has been formally validated by both the CK model and the formal verification tool AVISPA and SPAN to show its security against various malicious attacks, but also can provide robust security protection including privacy preservation and traceability.

Compared with the conference version [17] which merely provides mutual authentications and key agreements between mMTC devices and eNB and does not give the detailed security analysis and performance evaluation, we not only identify a few distinctive security requirements in group handover authentication protocol and achieve the identity privacy preservation and traceability in new design, but also formally verify the proposed new protocol by employing the CK model and formal verification tool AVISPA and SPAN and analyze in detail the performance of our proposed protocol compared with the newest works in terms of signaling cost, communication cost and computational cost. In addition, we still give the performance analysis under unknown attacks and point out that our new scheme outperforms other schemes even if there are some unknown attacks.

The reminder of this paper is organized as follows. In Sections 2 and 3, we review the related work and introduce the MTC network architecture, respectively. In Section 4, the proposed scheme is presented in detail. The security analysis and the performance evaluation on our scheme are presented in Sections 5 and 6. Finally, we drew the conclusion of the paper in Section 7.

2. Related Works

Until now, there are only few research works on the handover authentication process for a large number of devices in

FIGURE 1: MTC network architecture.

wireless networks [18–21]. 3GPP TR 33.868 [6] has proposed a MD grouping method for congestion avoidance. By this method, a huge number of MDs can construct a MTC group to handle easily. It is very suitable for mass of MDs in mobility scenarios in the LTE-A networks. However, it is only applied to the communications between MDs and the MTC server without consideration of handover security in the current 3GPP standard.

Fu et al. [18] have proposed a new group-based handover authentication scheme with privacy protection in the mobile WiMAX network. By the scheme, a lot of UEs can form a handover group. By performing a handover authentication process, the target base station (TBS) acquires all the details of the handover group member's security context from the serving base stations (SBS) when the first UE of the same handover group moves to the TBS. Then, the TBS can directly authenticate the rest of the UEs in the same handover group without the Extensible Authentication Protocol (EAP) and Security Context Transfer phases. Thus, the scheme can reduce the handover signaling cost in the mobile WiMAX networks. However, the scheme in [18] incurs the authentication traffic between BSs, which is not fit in with the LTE-A networks due to the lack of direct interface between the eNBs and the HeNBs in the intra-MME handover and inter-MME handover processes.

Lai et al. [19] have proposed a secure and efficient group roaming scheme for MTC between 3GPP and WiMAX networks. By adopting the certificateless aggregate signature technique, the MME/ASN-GW can simultaneously trust a large number of MDs in the handover process and obtains an independent session key with each MD. Thus, the scheme can largely reduce the signaling cost and provide robust security protection. However, it is designed for 3GPP-WiMAX interworking architecture, which is not feasible for the LTE-A network. In addition, the scheme brings a lot of computational costs due to the pairing operations.

For inter-E-UTRAN group mobility, the group-based anonymity handover authentication scheme is proposed in [20]. By the scheme in [20], when the first MTC device in the

MTC handover group leaves from the current eNB to the target eNB, the current eNB or the current MME transmits all of the handover group members' security contexts to the target eNB or the MME controlling the target eNB. Then, the target eNB can authenticate the rest of the MTC devices in the MTC handover group locally. However, this scheme still incurs a lot of signaling cost and communication cost and inherits the vulnerabilities of security context transfer (SCT) mechanism. In addition, it cannot achieve the mutual authentication and the traceability of MDs. Subsequently, Kong et al. present a secure handover session key management mechanism for a group on-board UEs via mobile relay in LTE-A networks [21]. By the scheme in [21], each on-board UE generates the session key with the connected Donor eNB (DeNB) and sends the encrypted session key by using the MME's public key to the mobile relay node (MRN). Then the MRN employs the proxy reencryption mechanism to reencrypt the encrypted session key and sends the reencrypted result to the DeNB. Finally, the DeNB decrypts the session key with its private key without contacting the MME. This scheme can achieve forward and backward key separations and withstand collusion between the MRN and the DeNB. However, it brings a lot of computational costs due to the use of pairing operations and cannot achieve the mutual authentication between the MRN and the DeNB.

3. Preliminary

3.1. MTC Network Architecture. As shown in Figure 1, a large number of MDs can communicate with the MTC server via the LTE-A network domain in the MTC network architecture. The LTE-A network allows the following two types of connections to the MTC server(s): the MTC server located within the operator domain with the control by the LTE-A network and the MTC server outside the operator domain without the control by the LTE-A network. The LTE-A network domain consists of the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet Core (EPC). The EPC is comprised of a MME and a

Serving Gateway (SGW) and a Packet Data Network Gateway (PDN GW) together with a Home Subscriber Server (HSS). The E-UTRAN consists of several types of base stations including eNodeB (eNB), Home eNodeB (HeNB), and Relay Node (RN). HeNB is a low-power access point and is typically installed by a subscriber in the residence or a small office to improve the indoor coverage. It can connect to the EPC with S1 interface over the Internet via a broadband backhaul. Each eNB or HeNB can communicate with another with an X2 interface and can access to the MMEs/S-GWs with a S1 interface. E-UTRAN also supports relaying by having a Relay Node (RN) wirelessly connect to an eNB serving the RN, known as Donor eNB (DeNB). The DeNB provides X2 and S1 proxy functionality between the RN and other eNBs or MME/S-GWs, respectively. Similar to the common UE, there are mainly three different mobility scenarios when a large number of MDs move from a HeNB/RN/eNB to a new HeNB/RN/eNB, including the handovers between two MMEs (called inter-MME handover), the handovers between an eNB/RN/HeNB and another base station, both of which are managed by the same MME without an X2 interface (called intra-MME handover), and the handovers between an eNB/RN/HeNB and another base station with an X2 interface (called X2-based handover) [7, 8]. Since the current handover mechanisms suggested by 3GPP committee [7, 8] need several signaling interactions, they result in the severe signaling congestions in the E-UTRAN and the EPC when a huge number of MDs handover to the new eNB concurrently. In addition, different mobility scenarios need to execute the distinct handover processes, which may increase the overall system complexity.

3.2. Multisignature and Aggregate Message Authentication Code. In 1983, the multisignature scheme was firstly proposed by Itakura and Nakamura [22], in which a lot of signers can cooperate to sign the same message and any verifier can verify the validity of the multisignature. Subsequently, Hwang and Lee [23] proposed a novel ElGamal-like multisignature scheme using self-certified public keys. By this scheme, the self-certified approach has been adopted to provide more secrecy against the active and impersonation attacks compared with identity-based and certificate-based approach. The analysis result shows that the scheme [23] can provide robust security protection with ideal efficiency.

Katz and Lindell [24] firstly proposed the notion of aggregate message authentication codes (AMACs), in which multiple MAC tags generated by different senders on multiple different messages can be aggregated into a shorter tag and only the recipient who shares a distinct key with each sender can verify the validity of the aggregate tag.

3.3. Canetti-Krawczyk (CK) Model. The CK model is a famous model for proving the security of authentication and key agreement protocols [25]. It captures a large class of practical attacks and desirable security properties, such as the impersonation attack and man-in-the-middle attack. In CK model, there is an adversary $\mathcal{A}$ who has been completely controlled over the network and tries to break the privacy of the session key or the authentication of the players. The

security of the protocol in CK model is completed by a game between the $\mathcal{A}$ and the user. $\mathcal{A}$ can get access to the sessions and interact with them via the queries. There are the following queries that $\mathcal{A}$ can perform:

- (i) *Corrupt* (U): $\mathcal{A}$ can get the private key of a user using this query.
- (ii) *Session key reveal* (U_i, U_j): this query returns the session key between U_i and U_j .
- (iii) *Session state reveal* (U_i, U_j): this query returns all the internal state information of U_i associated with a particular session s with U_j .
- (iv) *Hash* (x): given a value x to this query, a random value is output. All of the queries and the answers of Hash are stored in a list.
- (v) *Test* (U_i): this query aims at capturing the privacy of the session key. After several queries, $\mathcal{A}$ should choose a session as the test session. The query is answered as follows: one flips a coin b ; if $b = 1$ it outputs the session key to $\mathcal{A}$; if $b = 0$, it outputs a random value to $\mathcal{A}$. This query can be issued only to a session where the session key, session state, and corrupt queries have not been requested and it can be issued only once.

In order to simplify the construction and proof of key agreement protocols, two adversarial models are defined in CK model: the unauthenticated adversarial model (UM) and the authenticated adversarial model (AM). The UM corresponds to the real world where the adversary completely controls the network in use and may modify or create messages from any party to any other party. The AM is an ideal version of the UM where the adversary can choose whether or not to deliver a message, but if a message is delivered, it must have been created by the honest users without alteration. In this way, authentication mechanisms can be separated from key agreement mechanisms by proving the key agreement secure in the AM and then applying an authenticator to the key agreement messages so that the new protocol is secure in the UM.

Definition 1. A key agreement protocol π is called SK-secure if the following properties are hold for any adversary $\mathcal{A}$ in the AM: (1) protocol π satisfies the property that if two uncorrupted parties complete matching sessions and then both of them output the same key; (2) the probability that $\mathcal{A}$ correctly guesses the bit b is no more than $1/2$ plus a negligible fraction in the security parameter.

Theorem 2. Let π be a SK-secure key agreement protocol in the AM, and let C be a secure authenticator which translates messages in the AM into messages in the UM. Then, $\pi' = C(\pi)$ is a SK-secure key agreement protocol in the UM [25].

4. Proposed Scheme: UPPGHA

Before the proposed scheme is described, we firstly give some basic assumptions for our scheme. We consider the MTC mobility scenarios, such as a large number of surveillance

TABLE 1: Definition of notations of our scheme.

Notation	Definition
p, q	Two k -bit primes
g	A generator with the maximal order in Z_N^*
$H()$	A secure hash function $H : \{0, 1\}^* \rightarrow Z_N^*$
$H_1()$	A secure hash function $H_1 : Z_N^* \times Z_N^* \rightarrow Z_N^*$
ID_i/TID_i	Node i 's private identity and temporal identity
d/PK	Private/public key of KGC, $e \times d \equiv 1 \pmod{\phi(N)}$ and $PK = (N, e)$
$GID/TGID/GPK$	MTC group's group identity/temporal group identity/group temporal public key
SK_i/PK_i	Private/public key of node i
RN_i, r_i	Random number
K_{ASME_i}	Session key between node i and HSS/MME
$(\cdot)_{K_{ASME_i}}$	Encrypted results using K_{ASME_i}
K_i	Session key between node i and eNB ₂

cameras, temperature, and humidity sensors, and smoke detectors are deployed on the train to perform different functions, where massive of MDs travel through the same eNBs at the same train or vehicles and can form a MTC group in device initialization process. MDs support multiple communication technologies both mobile broadband technology such as mobile WiMAX and WCDMA/LTE/LTE-A, and local area networking technology including Bluetooth, ZigBee, and UWB, and other coming technologies such as power line communications (PLC) [26]. Due to the merits of low power, high capacity, broadcast, and robust security, ZigBee technology has been widely used in IoTs or sensor networks. In this paper, it is assumed that MDs support both the LTE-A and ZigBee communication.

In this section, we propose a new uniform privacy preservation group handover authentication mechanism (UPPGHA) when the MTC group moves from the source eNB/RN/HeNB to the target eNB/RN/HeNB. By our scheme, the HeNBs, the eNBs, and the RNs are collectively referred to as the eNBs. In fact, the proposed scheme is to achieve the following four security goals:

- (1) *Mutual authentication*: to mutually authenticate the MTC group and the target eNB simultaneously after a handover with low signaling cost and communication cost.
- (2) *Session key agreement*: to derive a secure session key between each MD in the MTC group and the target eNB, respectively, after the successful authentication.
- (3) *Identity privacy preservation*: to achieve MD' identity and location anonymity and unlinkability in group handover authentication process. User anonymity means that the identities of MDs and the group identity should be hidden and the attacker cannot disclose real identities of MDs even if the eNB has been compromised. Unlinkability means that even if several different communication session messages between the same MD and eNB have been collected, the MD should still not be traceable and linkable.

- (4) *Traceability*: to reveal the MD's real identity and trace the MD by the HSS under the controversial scenarios.

Our scheme starts with the initial authentication phase for preparing a handover. Then, the MTC group and the target eNB implement the uniform privacy preservation group handover authentication phase to achieve the above four goals. In the uniform privacy preservation group handover authentication phase, the target eNB can authenticate the whole MTC group simultaneously based on the novel techniques, multisignature, and aggregate message authentication code (AMAC). The specific process is described in detail as follows. The notations used in the scheme are defined in Table 1.

4.1. Initial Authentication Phase. In this phase, a MTC group will be constructed by a mass of MTC devices (MDs) and an identity of the MTC group, GID, will be embedded into MDs in the device initialization process according to the specification made by 3GPP committee [16]. The same MTC group will exist in the same area and/or have the same MTC features and/or belong to the same MTC user. A group leader of the group MD_{leader} will be also chosen in device initialization process based on the communication capability, communication link quality, storage status, and battery status of each MD. When each MD in the MTC group registers to the network, it performs an initial full authentication process with a MME and HSS and then obtains its private key and self-verified public key from Key Generate Center (KGC). The eNBs have the same function as the MDs to obtain these private keys and self-verified public keys after expiration time. The KGC can be integrated with the HSS, which has preestablished secure channels with the HSS by using the network domain security (NDS)/IP [27]. This phase can be described as follows. Here, KGC computes $N = pq$ where p and q are two random secret prime integers and constructs the key pair (e, d) satisfying $e \times d \equiv 1 \pmod{\phi(N)}$. Then, it selects a generator g with the maximal order in the Z_N^* and two Hash functions $H : \{0, 1\}^* \rightarrow Z_N^*$ and $H_1 : Z_N^* \times Z_N^* \rightarrow Z_N^*$. Finally, it publishes the master public key $PK = (N, e)$

TABLE 2: Identity list for MTC group.

Group ID	Group temporal ID	Group temporal public key	Group member ID/group member temporal ID		
			ID _{MD₁}	...	ID _{MD_n}
GID	TGID ₁ /RN ₁	GPk ₁	TID _{MD₁} ¹ /RN _{MD₁} ¹	...	TID _{MD_n} ¹ /RN _{MD_n} ¹
	TGID ₂ /RN ₂	GPk ₂	TID _{MD₁} ² /RN _{MD₁} ²	...	TID _{MD_n} ² /RN _{MD_n} ²
	⋮	⋮	⋮	⋮	⋮
	TGID _m /RN _m	GPk _m	TID _{MD₁} ^m /RN _{MD₁} ^m	...	TID _{MD_n} ^m /RN _{MD_n} ^m

and the system parameters (H, H_1) and keeps the master secret key d secret.

Let $MD_1, \dots, MD_n$ be the MTC group members; each MD_i executes the following procedure when it first registers to the network.

4.1.1. $MD_i \rightarrow HSS/KGC : (ID_{MD_i}, GID, X_i)_{K_{ASME_i}}$. It is assumed that the Evolved Packet System Authentication and Key Agreement (EPS-AKA) [9] is implemented in the initial full authentication process. After the AKA, according to the scheme in [23], MD_i chooses a random number $x_i \in Z_N$ as his secret key $SK_{MD_i} = x_i$ and computes $X_i = g^{-x_i} \bmod N$. Then, it sends the private/public key request message with its identity ID_{MD_i} , group ID GID , and X_i encrypted by the session key K_{ASME_i} between MD_i and the HSS/KGC to the HSS/KGC via the MME. Here the session key K_{ASME_i} is derived between MD_i and the HSS/KGC after the AKA.

4.1.2. $HSS/KGC \rightarrow MD_i : (\{GPk_j, TGID_j, TID_{MD_i}^j\}_{j=1 \dots m})_{K_{ASME_i}}$. After the receipt of the private/public key request message from each MD_i , the HSS/KGC executes the following operations for MD_i :

- (1) Choose m random numbers $\{RN_j\}_{j=1 \dots m}$ and then calculate a set of unlinkable temporal group identities $TGID_j = GID \oplus H(RN_j^d)$ when the first MD in the MTC group registers to the network.
- (2) Choose m random numbers $\{RN_{MD_i}^j\}_{j=1 \dots m}$ and then calculate a set of unlinkable temporal identities $TID_{MD_i}^j = ID_{MD_i} \oplus H((RN_{MD_i}^j)^d \parallel TGID_j)_{j=1 \dots m}$ for MD_i .
- (3) Calculate $PK_{MD_i}^j = (X_i^{H(X_i)} - TID_{MD_i}^j)^d \bmod N$ ($j = 1 \dots m$) as MD_i 's temporal public keys.
- (4) When all of the private/public key request messages from all individuals MD_i in the MTC group have been received, the HSS/KGC computes the set of group temporal public key $GPk_j = ((\prod_{i=1}^n X_i^{RN_j \cdot H(X_i)}) - TGID_j)^d \bmod N$ for each temporal group identity $(TGID_j)$. Then, the $(\{GPk_j, TGID_j, TID_{MD_i}^j\}_{j=1 \dots m})$ encrypted by the K_{ASME_i} is sent to each MD_i . In addition, the HSS/KGC establishes and stores an identity list for MTC group as shown in Table 2 in its database.

Each eNB executes the same procedure as that of the MD_i in the initial full authentication phase unavoidable.

After the eNB is verified successfully, the eNB chooses a random key $x_{eNB} \in Z_N$ as his secret key $SK_{eNB} = x_{eNB}$ and computes $X_{eNB} = g^{-x_{eNB}} \bmod N$ and then sends ID_{eNB}, X_{eNB} to the HSS/KGC, which are encapsulated in the last message of Internet Key Exchange Protocol Version 1 (IKEv1) or IKEv2-based [27] device authentication and sent to the corresponding eNB securely. After the receipt of the message including ID_{eNB} and X_{eNB} , the HSS/KGC derives the eNB's public key $PK_{eNB} = (X_{eNB}^{H(X_{eNB})} - ID_{eNB})^d \bmod N$ and sends it to the eNB securely.

In our proposed scheme, all of public keys in our proposed scheme are generated and maintained by HSS/KGC. Once the suspicion of the validity of the public key, MD or eNB can directly send the public key verification request message to the HSS/KGC to request to determine the validity of the public key.

4.2. Uniform Privacy Preservation Group Handover Authentication Phase. In this phase, the group handover authentication for all of MDs in the MTC group is accomplished when the MTC group moves away from the source eNB (eNB_1) to the target eNB (eNB_2) simultaneously. In order to ensure that the whole MTC group securely hands over to the same eNB_2 , we take the advantage of the multisignature scheme [23] and the AMAC scheme [24] to achieve the mutual authentication and key agreement between the MTC group and the eNB_2 . As shown in Figure 2, it works as follows. Here let $TID_T^j = \langle TID_{MD_1}^j, \dots, TID_{MD_n}^j \rangle$.

Step 1. When the MTC group moves into the coverage of the eNB_2 , each MD_i executes the following procedure:

- (1) Choose a random number $r_i \in Z_N^*$ and compute $R_i = g^{r_i} \bmod N$, then pick an unused temporal identity $TID_{MD_i}^j$ and corresponding temporal group identity $TGID_j$, and broadcast $R_i, TID_{MD_i}^j$, and $TGID_j$ to other $n - 1$ MDs in the MTC group including the group leader (MD_{leader}). Note that this step can be preexecuted before the MTC group hands off to the eNB_2 .
- (2) Upon the receipt of all of R_j from other $n - 1$ MDs, compute $R_T = \prod_{j=1}^n R_j$ and $C = H(R_T \parallel TID_T^j \parallel TGID_j \parallel NAI_{eNB_2})$, then calculate $S_i = r_i + SK_{MD_i} \times RN_j \times H(X_i) \times C$, and send $(TID_{MD_i}^j, TGID_j, NAI_{eNB_2}, R_i, S_i)$ to the MD_{leader} , where NAI_{eNB_2} is Network Access Identifier of eNB_2 .

FIGURE 2: Uniform privacy preservation group handover authentication phase.

Step 2. Upon the receipt of all of $(\text{TID}_{\text{MD}_i}^j, \text{TGID}_j, \text{NAI}_{\text{eNB}_2}, R_i, S_i)$, the MD_{leader} computes $S_{\text{MD}} = \sum_{j=1}^n S_j$ and sends the authentication request message with $(R_1, \dots, R_n, \text{TID}_T^j, \text{TGID}_j, \text{NAI}_{\text{eNB}_2}, S_{\text{MD}}, \text{GPK}_j)$ to the eNB₂.

Step 3. Upon the receipt of the authentication request message from the MD_{leader}, the eNB₂ works as follows:

- (1) Check if $\text{NAI}_{\text{eNB}_2}$ is valid and then verify $g^{S_{\text{MD}}} \times (\text{GPK}_j^e + \text{TGID}_j)^C \equiv R_T$ by computing $R_T = \prod_{j=1}^n R_j$ and $C = H_1(R_T \parallel \text{TID}_T^j \parallel \text{TGID}_j \parallel \text{NAI}_{\text{eNB}_2})$. If the verification succeeds, the eNB₂ authenticates the whole MTC group and jumps to (2). Otherwise, it sends an authentication failure message to the MD_{leader}.
- (2) Choose a new random number $r_{\text{eNB}_2} \in Z_N^*$ and compute $R_{\text{eNB}_2} = g^{r_{\text{eNB}_2}} \bmod N$ and then calculate $S_{\text{eNB}_2} = r_{\text{eNB}_2} + \text{SK}_{\text{eNB}_2} \times H(X_{\text{eNB}_2}) \times H(R_{\text{eNB}_2} \parallel \text{ID}_{\text{eNB}_2})$.
- (3) Send the authentication response message with $(R_{\text{eNB}_2}, \text{ID}_{\text{eNB}_2}, S_{\text{eNB}_2}, \text{PK}_{\text{eNB}_2})$ to the MD_{leader}. Then compute the session key $K_{\text{MD}_i} = H(R_i^{r_{\text{eNB}_2}})$ for each MD_i in the MTC group to guarantee the subsequent communication.

Step 4. After the authentication response message from the eNB₂, the MD_{leader} broadcasts this message to other MDs in the MTC group.

Step 5. Upon the receipt of the message from the MD_{leader}, each MD_i executes the following process:

- (1) Check $g^{S_{\text{eNB}_2}} \times (\text{PK}_{\text{eNB}_2}^e + \text{ID}_{\text{eNB}_2})^{H(R_{\text{eNB}_2} \parallel \text{ID}_{\text{eNB}_2})} \equiv R_{\text{eNB}_2}$. If the verification succeeds, the MD_i trusts the eNB₂ and jumps to (2). Otherwise, it sends an authentication failure message to the eNB₂ via the MD_{leader}.
- (2) Compute the session key $K_{\text{MD}_i} = H(R_i^{r_{\text{eNB}_2}})$ and $\text{MAC}_i = H_1(K_{\text{MD}_i}, R_i)$.
- (3) Finally, send the MAC_i to the MD_{leader} to confirm the K_{MD_i} agreement.

Step 6. Upon the receipt of all of MAC_i from the MTC group, the MD_{leader} derives $\text{MAC} = \text{MAC}_1 \oplus \text{MAC}_2 \oplus \dots \oplus \text{MAC}_n$ and sends it to eNB₂.

Step 7. After the receiving the MAC, the eNB₂ verifies MAC. If the verification succeeds, the eNB₂ confirms K_{MD_i} agreement with each MD_i.

4.3. Identity Tracking Phase. In order to track the MTC group, after the eNB₂ trusts the MTC group, it transmits the temporal identities $\{\text{TID}_{\text{MD}_i}^j\}_{i=1 \dots n}$ and the temporal group identity TGID_j' to the HSS/KGC via the MME. Upon the receipt of the message, the HSS/KGC searches its database to find the corresponding RN_j and executes the following

operations to obtain the real group identity of the MTC group.

$$\begin{aligned} \text{TGID}'_j \oplus H(\text{RN}_j^d) &= \text{GID} \oplus H(\text{RN}_j^d) \oplus H(\text{RN}_j^d) \\ &= \text{GID}. \end{aligned} \quad (1)$$

Once the GID has been derived, the MTC group will be tracked and determined by the HSS/KGC. If the HSS/KGC needs to further know real identity of each MD in the MTC group, it can find related $\text{RN}_{\text{MD}_i}^j$ and calculate

$$\begin{aligned} &\text{TID}_{\text{MD}_i}^j \oplus H(\text{TGID}'_j \parallel (\text{RN}_{\text{MD}_i}^j)^d) \\ &= \text{ID}_{\text{MD}_i} \oplus H(\text{TGID}'_j \parallel (\text{RN}_{\text{MD}_i}^j)^d) \\ &\oplus H(\text{TGID}'_j \parallel (\text{RN}_{\text{MD}_i}^j)^d) = \text{ID}_{\text{MD}_i}. \end{aligned} \quad (2)$$

5. Security Evaluation

In this section, the formal security analysis in CK model and the formal verification tool AVISPA and SPAN are conducted to show that our proposed protocols can work correctly to achieve robust security properties.

5.1. Security Analysis

Multi-Decisional Diffie-Hellman (M-DDH) Problem [28]. Define a Multi-Diffie-Hellman (M-DH) and a Random Multi-Diffie-Hellman (RM-DH) distributions of size n as $\text{M-DH}_n = \{(\{g^{x_i}\}), \{g^{x_i x_j}\} \mid x_1, \dots, x_n \in_R Z_q\}$ and $\text{RM-DH}_n = \{(\{g^{x_i}\}), \{g^{r_{j,k}}\} \mid x_i, r_{j,k} \in_R Z_q, 1 \leq j < k \leq n\}$. An polynomial time adversary cannot distinguish whether a tuple is from M-DH_n or from RM-DH_n with a probability higher than a negligible value.

Our scheme satisfies the following security properties.

Mutual Authentication and Key Agreement in CK Model. In our proposed UPPGHA, the HSS/KGC can ensure a mutual authentication between the MTC group and the eNB_2 based on the technique of multisignature and ElGamal signature. To be authenticated by the eNB_2 , each MD in the MTC group generates the signature S_i by using its private key, and then the multisignature is obtained by summing all the signatures from the MTC group, which will be verified by the use of the self-verified group public key GPK generated by the HSS and the HSS's private key. After performing the mutual authentication, each MD and eNB_2 negotiate a distinct session key using the DH algorithm based on the Discrete Logarithm Problem (DLP) to protect the communication over air interface between the eNB_2 and each MD in the MTC group. Moreover, the AMAC technique is applied to guarantee the session key agreement between each MD and eNB_2 .

Actually, as shown in the UPPGHA, our trick is employing a signature scheme to authenticate the random value $R_i = g^{r_i}$ and $R_{\text{eNB}_2} = g^{r_{\text{eNB}_2}}$. Then employing this signature (authenticator), we can transform a protocol which is SK-secure in the AM into a protocol which is SK-secure in

the UM. Based on this idea, we divide the proof of the authentication and key agreement into two parts. Firstly, we prove that the adversary in the AM cannot correctly guess the bit b in the *test* session with the property no more than $1/2$ plus a negligible fraction. Secondly, we use a secure signature-based authenticator to transform the protocol in the AM to a secure protocol in UM.

Theorem 3. *The UPPGHA protocol without a signature-based authenticator is SK-secure in the AM provided that M-DDH problem is hard and H is a random oracle.*

Proof. In the AM, each MD_i sends its random value $R_i = g^{r_i}$ to the $\text{MD}_{\text{leader}}$ and then the $\text{MD}_{\text{leader}}$ transmits these R_i to the eNB_2 . Then, eNB_2 send a random value R_{eNB_2} to each MD. After that the session key between eNB_2 and each MD_i is computed as $K = H(g^{r_i r_{\text{eNB}_2}})$. We assume that a polynomial time adversary $\mathcal{A}$ can guess the output of a *test session* query with a nonnegligible advantage ϵ in the AM (correctly computed the session key), that is, $\Pr[\mathcal{A} \text{ succeeds}] = 1/2 + \epsilon$, then we can solve the M-DDH problem.

We simulate the protocol for the adversary and make use of $\mathcal{A}$ to solve the M-DDH problem. Suppose there are n MDs and an eNB_2 in the communication and the s th session of MDs and eNB_2 are expressed as $\Pi_{\text{MD}_i, \text{eNB}_2}^s$ and $\Pi_{\text{eNB}_2, \text{MD}_i}^s$. We can answer all of the queries asked by $\mathcal{A}$ since we initialize all of the participants. The proof is in the random oracle model which means the output of the Hash function is random. In the simulation, all of the Hash value must be obtained from a Hash query. So if $\mathcal{A}$ can win the game and correctly guess the bit b in the test session, he needs to compute the session key between MD_i and eNB_2 and ask the Hash query with these values ($K = H(g^{r_i r_{\text{eNB}_2}})$). Firstly, we exclude the collisions on the transcripts ($(R_i = g^{r_i}, R_{\text{eNB}_2} = g^{r_{\text{eNB}_2}})$) since if a collision occurs $\mathcal{A}$ can get the session by the *corrupt* query. According to the birthday paradox, we can bound the probability by $q_s^2/2^l$ where q_s^2 denotes the number of sessions and l is the security parameter. We then continue to simulate the protocol. We choose a bit b , if $b = 1$ we choose a tuple $(g^{x_i}, g^{x_i x_j})$ from M-DH set. Otherwise, we randomly choose a tuple $(g^{x_i}, g^{r_{j,k}})$ from RM-DH set. Then, we choose one session as the test session and imbed these g^{x_i} into the protocol instead of the values in $\Pi_{\text{MD}_i, \text{eNB}_2}^s$ and $\Pi_{\text{eNB}_2, \text{MD}_i}^s$. If $\mathcal{A}$ performs the *test* query, then a value chosen from M-DH or RM-DH will be returned. Suppose that the test session $\mathcal{A}$ is exactly the session we chose, the probability of this event is $1/q_s^2$. As aforementioned, if $\mathcal{A}$ succeeds in guessing b in the test session and then he must have computed the DH value $g^{x_i x_j}$ from g^{x_i} and g^{x_j} . In such case, we can solve the M-DDH problem either. So the probability of solving the M-DDH is $(1/(q_s^2 \cdot q_h)) \cdot \Pr[\mathcal{A} \text{ succeeds}]$ where q_h denotes the number of the Hash queries (we need to check which Hash query $\mathcal{A}$ was asked in the *test session* from one of q_h queries). Actually, as we know the probability of solving M-DDH problem is a negligible value [28]. Here we denote this probability as ϵ . Then we can obtain $\Pr[\mathcal{A} \text{ succeeds}] \leq 1/2 + q_s^2/2^l + \epsilon/(q_s^2 \cdot q_h)$, where $q_s^2/2^l + \epsilon/(q_s^2 \cdot q_h)$ is a negligible value. So we conclude Theorem 3. $\square$

The security of the UPPGHA protocol in the AM is proved, then we show the signature-based authenticator is a secure authenticator. As shown in [23], the signature scheme we used is based on factorization (FAC) and discrete logarithm (DL) assumptions. Under the integer factorization and DL assumptions, the signature proposed in [23] is a secure signature. So using this authenticator we can conclude that the proposed protocol is SK-secure in the UM.

Replay Attack Resistance. Our proposed UPPGHA can withstand the replay attack by the use of the random numbers (r_i and r_{eNB_2}). Whenever the MTC group moves into the coverage of the eNB_2 , both of the random numbers are updated on each MD and the eNB_2 . Thus, all session keys are freshly obtained based on these values to resist against this type of attacks.

Impersonation Attack and Man-in-the-Middle (MitM) Attack Resistance. Since the session keys are established based on the DH problem by our scheme, a MitM adversary could not derive the session keys by the use of the public values from the communication channel between each MD_i and the eNB_2 . It is infeasible to forge a valid multisignature and an ElGamal signature to deceive eNB_2 or each MD_i without the secret keys of eNB_2 or each MD_i . Therefore, our scheme can not be exposed to the impersonation attacks. Furthermore, taking the advantage of the multisignature, all of MDs in the MTC group sign the same message including the same temporal group identity TGID and all of group member's temporal identities, and the MD_{leader} can validate the signatures from the group members. Thus, other legal MDs who do not belong the MTC group can not masquerade the MTC group members to deceive the eNB_2 or the EPC by signing the same message.

Insider Attack and DoS Attack Resistance. By our proposed UPPGHA, each MD in the MTC group derives a distinct session key with the eNB_2 . Without the correct secret random values r_i of the MD_i , any other MDs in the MTC group can not obtain the legal session key K_{MD_i} of the MD_i and thus can not masquerade the MD_i to deceive the eNB_2 or the EPC. Therefore, our scheme can defend the insider attack by the MTC group members. In addition, the MD_{leader} can authenticate each MD_i by verifying the signature S_i for the same message from MD_i , and thus any attacker can not make DoS attacks to the eNB and the EPC by computing a lot of invalid signatures.

Identity Privacy Preservation. By our proposed UPPGHA, the set of temporal identities of a MD, temporal group identities and temporal group public keys are derived instead of the real identities and transmitted securely to each MD in initial full authentication phase. Since the temporal identity of each MD and the temporal group identity are generated by using the unknown random number, any attacker or eNB s cannot reveal the MD's real identity and real group identity. In addition, a new temporal identity of each MD and a new temporal group identity are selected and used in each group handover authentication process; any adversary cannot link

the temporal identities by eavesdropping the communication channel between the MTC group and eNB_2 . Furthermore, the temporal group public key GPk_j is generated by using the random number and temporal group identity and is updated in each group handover authentication process; any adversary cannot derive the value $\prod_{i=1}^n X_i$. Thus, anyone except the HSS/KGC cannot trace the MTC groups movement trail.

Traceability. Under dispute scenarios, the HSS/KGC can reveal the real identity of the MTC group according to the temporal identity by using the stored random number and its privacy key. Therefore, once a signature is in dispute or other controversial incidents happen, the HSS/KGC who had assigned temporal identities to the real identity of the MTC group is able to trace the MTC group.

Signaling Congestion Resistance. By our scheme, the signaling congestion can be avoided in terms of low signaling overhead and fast verification. On the one hand, a large number of handover request messages from the MTC group will be aggregated into a single request message by a group leader and then the single handover request message is sent to the eNB_2 . In addition, the eNB_2 only calculates a signature and sends it to the group leader via a single signaling message. Moreover, our scheme provides a simple authentication process only with 3-handshake between the MD_{leader} and the eNB_2 without contacting any other third party such as MME and HSS. Thus, it can largely reduce the signaling cost and thus avoid the signaling overload. On the other hand, the eNB_2 can simultaneously authenticate a group of MDs by adopting the technique of the multisignature and AMAC and quickly create the session keys with the MTC group. Therefore, it can alleviate the burden of the eNB_2 and ensure the QoS requirement of the MTC users without the restriction of handover requests.

We also give a security comparison between our scheme and other similar handover authentication protocols in Table 3.

5.2. AVISPA and SPAN. Due to the openness of the wireless communication channel, the intruder can intercept and store the messages on the channel, replay old messages, analyze and modify messages as far as it knows the required keys, and send any new messages that it composed to whoever at its will, impersonating other agents. This type of attack is commonly regarded as Dolev-Yao (DY) attack. In this paper, we examine various security properties of the proposed scheme by the AVISPA [29] and the SPAN [30], which analyze protocols under the assumptions of perfect cryptography, and the communication channel is under the control of a DY intruder. The AVISPA employs the High-Level Protocol Specification Language (HLPSSL) to specify the security protocols and their security properties and utilizes four back-end tools to check the security of protocols, which include On-the-Fly Model-Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). In addition, SPAN provides a graphical user interface for the protocol designer to easily interact with AVISPA capabilities.

TABLE 3: Security comparison.

Protocols	[7, 8]	[18]	[19]	[20]	[21]	Our scheme
Mutual authentication	×	✓	✓	×	×	✓
Key agreement	✓	✓	✓	✓	✓	✓
Replay attack resistance	×	✓	✓	✓	✓	✓
Impersonation attack resistance	×	✓	✓	✓	×	✓
Man-in-the-middle attack resistance	×	✓	✓	✓	×	✓
Insider attack and DoS attack resistance	-	✓	✓	✓	✓	✓
Identity privacy preservation	×	✓	×	✓	×	✓
Traceability	×	×	×	×	×	✓
Signaling congestion resistance	×	×	✓	×	×	✓

FIGURE 3: The state transition relations of our model.

Since multiple MDs can independently achieve the authentication and derive its session key with the eNB, there is no communication between them except that the group leader. In order to simplify the analysis, our scheme includes three roles MD_1 , MD_g (i.e., MD_{leader}), and eNB and five messages which are described as follows:

- (1) ACCESS REQ: $MD_1 \rightarrow MD_g : (ID_{MD_1}, GID, ID_{eNB_2}, R_1, S_1)$
- (2) AGGREGATION REQ: $MD_g \rightarrow eNB : (ID_{MD_1}, ID_{MD_g}, GID, ID_{eNB}, R_1, R_g, S_{MD}, GPK)$
- (3) ACCESS RES: $eNB \rightarrow MD_g, MD_g \rightarrow MD_1 : (ID_{eNB}, R_{eNB}, S_{eNB}, PK_{eNB})$
- (4) ACCESS REP: $MD_1 \rightarrow MD_g : MAC_1$
- (5) AGGREGATION REP: $MD_g \rightarrow eNB : MAC$

HLPSL has a formal semantics based on Lamport's Temporal Logic of Actions (TLA) [31], which is a state-of-the-art model analyzer that enumerates the reachable states in a finite-state model and checks that invariance properties hold in each of these states. Due to the limited space, we only give the state transition relations of three roles in our model as shown in Figure 3, where we neglect the specific formal description of our scheme.

By our scheme, our security goals are to achieve the mutual authentication between the MTC group and the eNB and security session key establishment between each MD and

the eNB. As shown in Algorithm 1, we specify the security goals of our proposed scheme using AVISPA.

Finally, we employ the OFMC and CL-AtSe to verify that the proposed scheme maintains its security objectives even under various attacks. The outputs of the model checking results by using SPAN in OFMC and CL-AtSe are shown in Figures 4 and 5, respectively. According to Figures 4 and 5, we can conclude that our scheme can achieve the security goals and withstand various attacks including MitM attacks, impersonation attacks, and replay attacks under the test of AVISPA and SPAN using the OFMC back-end and CL-AtSe back-end.

6. Performance Evaluation

In this section, we firstly analyze the performance of the proposed UPPGHA by comparing it with the current LTE-A handover mechanisms in [7, 8] and other related schemes [18–21] in terms of the signaling cost, the communication cost, and the computational cost. Then, we evaluate the situation when there are some attacks in execution of protocols. It is assumed that there are n MDs in the MTC group.

6.1. Signaling Cost. On the signaling cost, we mainly evaluate our scheme by comparing with the schemes [7, 8, 18–21] in terms of the number of signaling messages. According to distinct mobility scenarios, the LTE-A handover mechanisms [7, 8] and the GAHAP [20] can be divided into three different

```

goal
secrecy_of sec_md1_kme1, sec_enb_kme1 %$K_{MD1}$ is secret between MD1 and eNB
secrecy_of sec_mdg_kme2, sec_enb_kme2 %$K_{MDg}$ is secret between MDg and eNB
authentication_on s_md1 %eNB authenticates MD1 by verifying $S_{1}$
authentication_on s_enb1%MD1 authenticates eNB by verifying $S_{\{eNB\}}$
authentication_on s_mdg %eNB authenticates MDg by verifying $S_{\{leader\}}$
authentication_on s_enb2% MDg authenticates eNB by verifying $S_{\{eNB\}}$
end goal

```

ALGORITHM 1: Analysis goals of the model.

TABLE 4: Comparison of related schemes.

Related schemes	Signaling cost	Communication cost
X2-based HO [7, 8]	$5n$	$(3b + 2\delta)n$
Intra-MME HO [7, 8]	$7n$	$(4 - b)n$
Inter-MME HO [7, 8]	$8n$	$(4 - b + \eta)n$
X2-based HO [20]	$3n + 2$	$3bn + 2\delta$
Intra-MME HO [20]	$3n + 4$	$3bn + 4$
Inter-MME HO [20]	$3n + 5$	$3bn + 4 + \eta$
[18]	$4(n - 1) + 5$	$4nb + \delta$
[19]	$n + 9$	$(n + 1)a + 4$
[21]	$6n$	$2na + 2nb + 2n\delta$
Our scheme	$2n + 4$	$(2n + 1)a + 3b$

FIGURE 4: Results reported by the OFMC back-end in SPAN.

FIGURE 5: Results reported by the ATSE back-end in SPAN.

handover processes, X2-based handover (HO), intra-MME HO, and inter-MME HO, respectively. For the scheme in [18], when the first MD moves into the coverage of the target eNB, the source eNB contacts with the target eNB and transmits all of security context information for the MTC group to the target eNB, and then the target eNB can directly perform the mutual authentication with other group members only with two-handshake without the involvement of the source eNB. For the scheme in [19], taking the advantage of broadcasting and aggregation to design the signaling message, the number of signaling messages for the group is only $(n + 9)$ for the roaming phase. For the scheme in [21], due to the use of proxy

mechanism, when on-board UEs hand off the target DeNB, the target DeNB can directly obtain the session key with the UEs without the involvement of the MME. According to the number of signaling messages, we obtain a comparison of the signaling cost shown as the second row of Table 4. Since both the signaling cost and the communication cost of the scheme in [20] are much better than these in the LTE-A handover mechanisms [7, 8], which has been given in the scheme in [20], Figure 6 only shows the analysis results for the signaling cost with the increasing of the number of MDs by comparing our scheme with the schemes in [18–21]. According to the Figure 6, the signaling cost of each handover process by our scheme is much better than that

TABLE 5: Comparison of computational cost.

	Each device	The eNB (or the MME)
[19]	$5T_{\text{mul}} = 7.685$	$4nT_{\text{mul}} + 3T_{\text{pair}} = 1.9n + 48.966$
[21]	$4T_{\text{exp}} + 2T_{\text{pair}} = 83.544$	$n(3T_{\text{exp}} + 2T_{\text{pair}}) = 34.219n$
Our scheme	$5T_{\text{exp}} = 8.49$	$(n + 4)T_{\text{exp}} = 0.525n + 2.1$

FIGURE 6: Comparison of the number of signaling messages.

by the schemes in [18, 20, 21], while the scheme in [19] has better performance on the signaling cost than our scheme. However, the scheme in [19] is used to the vertical handover process for 3GPP-WiMAX interworking architecture, which is not feasible to the horizontal handover within E-UTRAN in LTE-A networks. In addition, there is no confirmation message from the MDs to the MME in the scheme in [19]. In such case the MME cannot determine whether the MD has completed the handover authentication process and obtained the session key, which may incur DoS attacks to the network. Thus, based on an overall consideration of efficiency and security, our scheme has a good performance on the signaling cost compared with other schemes.

6.2. Communication Overhead. On the communication overhead, let the transmission cost incurred by delivering an authentication packet between the MME and the MD be one unit, the cost between the MDs and the group leader be a unit, the cost between the MD and the eNB be b unit, the cost between the eNBs be δ unit, and the cost between MMEs be η unit, respectively. Since the MME locates far away from the eNB, the cost b unit is in the range $0 < b < 1/2$. Generally, the costs δ and η are also lower than 1 unit. In addition, since the distance between MDs is not more than 100 meters, the cost a unit is far less than 1 unit. In fact, the distance between MDs and that between MMEs in the EPC are relatively fixed, while the distance between eNBs and that between the MD and the eNB change greatly due to the different deployment of the eNBs. In order to facilitate analysis, we set $a = 0.005$ and

$\eta = 0.1$. The comparison of the communication cost has been shown as the third row of Table 4. Figure 7 shows the analysis results for the communication cost. From the Figure 7, the communication cost of our scheme is much lower than that of the schemes in [18, 20, 21], which is similar to that of the scheme in [19].

6.3. Computational Cost. In this section, we analyze the computational cost of our scheme by comparing with the scheme in [19] and the scheme in [21]. We only consider the cost of the following operations including a modular exponentiation T_{exp} , a point multiplication T_{mul} , and a pairing operation T_{pair} , while other operations such as point addition and one-way Hash function will be ignored. According to the time costs of the primitive cryptography operations presented by the scheme in [10], the comparison of the computational cost in the reference schemes is shown in Table 5. According to the Table 5, the computational cost of each MD by our scheme is much less than that by the scheme in [21], which is slightly larger than that by the scheme [19]. That is because the operation cost of modular exponentiation adopted by our scheme is slightly greater than that of point multiplication used by the scheme in [19]. Figure 8 shows the analysis results for the computational cost of the MME or the eNB. From the Figure 8, the computational overhead of the eNB by our scheme is much less than that by the scheme in [19] and the scheme in [21] with the increase of MDs.

6.4. Performance Analysis under Unknown Attacks. Our scheme can withstand several known attacks described in detail above, which cannot impact on the execution of our protocol. However, when there are unknown attacks or uncertain attacks, and we do not determine when or whether the unknown/uncertain attacks occur in execution of protocol, our scheme may be interrupted. In this section, we will evaluate this situation. Since we have no idea when or whether the unknown attacks happen in the execution of the protocol, step where the unknown attack happens is completely random; that is, the probability of unknown attack happened in i step is $p = 1/n_{\text{sig}}$, where n_{sig} is the total number of the signaling messages in one execution of protocol. Owing to the space limitations, we elaborate the communication overhead of our scheme under unknown attacks compared with other related schemes, and other performance evaluations under unknown attacks are similar to that of the communication overhead. Here, an impact ratio IR is defined to evaluate the impact degree of communication overhead under attacks for one success execution of protocol. In addition, we define two parameters: co_i represents the total communication overhead before the attack happens in i step and co_{total} shows that the total communication overhead for

FIGURE 7: Comparison of communication cost.

one success execution of protocol with no attack. The impact ratio IR is shown as follows:

$$IR = \frac{p \times \sum_{i=1}^{n_{sig}} (1/n_{sig}) co_i + (1-p) \times co_{total}}{(1-p) \times co_{total}}. \quad (3)$$

The comparison of IR for related schemes is given in Table 6. Figure 9 shows the analysis result of the influence rate (IR) of the one authentication process of existing schemes. According to Figure 9, the impact degree of our scheme is similar to the scheme in [18], which is much less than that of other schemes. In addition, our scheme can simultaneously achieve the authentication for a group of MDs in one success execution of protocol while the LTE schemes [7, 8], the scheme in [18], the scheme in [20], and the scheme in [21] can only provide one-by-one authentication. Therefore, our

scheme outperforms other schemes even if there are some unknown attacks.

7. Conclusion and Future Work

In the mobile MTC applications supported by the LTE-A networks, frequent handover signaling interaction not only causes the signaling load on the access network and core network, but also increases the terminal energy consumption. When a good deal of MTC devices simultaneously roams from a base station to a new base station, it is particularly serious. In this paper, we have proposed a simple and secure uniform group-based handover authentication scheme for a large number of MTC devices based on the multisignature and AMAC techniques, which is to fit in with all of the mobility scenarios in the LTE-A networks. Our analysis

TABLE 6: Comparison of related schemes.

Related schemes	IR on communication cost
X2-based HO [7, 8]	$\frac{(p/5)(8b + 7\delta)}{(1 - p) \times (3b + 2\delta)} + 1$
Intra-MME HO [7, 8]	$\frac{(p/7)(18 - 8b)}{(1 - p) \times (4 - b)} + 1$
Inter-MME HO [7, 8]	$\frac{(p/8)(18 - 8b + 6\eta)}{(1 - p) \times (4 - b + \eta)} + 1$
X2-based HO [20]	$\frac{(p/(3n + 2))((9n(n - 1)/2 + 8)b + (2n + 5)\delta)}{(1 - p) \times (3bn + 2\delta)} + 1$
Intra-MME HO [20]	$\frac{(p/(3n + 4))((9n^2/2 - 17n/2 - 4)b + 4n + 14)}{(1 - p) \times (3bn + 4)} + 1$
Inter-MME HO [20]	$\frac{(p/(3n + 5))((9n^2/2 - 17n/2 - 4)b + (n + 5)\eta + 4n + 15)}{(1 - p) \times (3bn + 4 + \eta)} + 1$
[18]	$\frac{(p/(4(n - 1) + 5))((10n + 34)b + 16\delta)}{(1 - p) \times (4nb + \delta)} + 1$
[19]	$\frac{(p/(n + 9))((6n + 8)a + 26)}{(1 - p) \times ((n + 1)a + 4)} + 1$
[21]	$\frac{(p/6)(5b + 11\delta + 5a)}{(1 - p) \times (2b + 2a + 2\delta)} + 1$
Our scheme	$\frac{(p/(2n + 4))((7n + 3)a + 10b)}{(1 - p) \times ((2n + 1)a + 3b)} + 1$

FIGURE 8: Comparison of the computational cost of the eNB by our scheme.

results show that our scheme can not only provide a simple authentication process with robust security protection, but also largely reduce the signaling costs and communication costs and thus avoid signaling congestion.

Since the next generation networks (5G) will be designed to meet stringent latency, high connection density, and high concurrent access requirements, the design of the security and efficient access and handover authentication for massive devices in LTE-A cellular networks and future 5G is the key challenge to achieve future cellular applications security. In our future work, we will consider more practical access and handover authentication mechanism in LTE-A/5G networks

based on symmetric cryptography for massive devices with resource limited under the scenarios that they belong to the same group and there is no correlation, respectively.

Abbreviations

3GPP:	Third-Generation Partnership Project
MTC:	Machine Type Communication
M2M:	Machine to Machine
mMTC:	Massive MTC
LTE-A:	Long Term Evolution-Advanced
UE:	User Equipment
MD:	MTC device
MD _{leader} :	MTC group leader
AMAC:	Aggregate message authentication code
EPC:	Evolved Packet Core
E-UTRAN:	Evolved-Universal Terrestrial Radio Access Network
MME:	Mobility Management Entity
S-GW:	Serving Gateway
PDN GW:	Packet Data Network Gateway
RN:	Relay Node
UM/AM:	Unauthenticated/authenticated adversarial model
HSS:	Home Subscriber Server
eNB/HeNB:	eNodeB/Home eNB
EPS-AKA:	Evolved Packet System Authentication and Key Agreement
PLC:	Power line communication
KGC:	Key Generate Center
NDS:	Network domain security
AVISPA:	Automated Validation of Internet Security Protocols and Applications
SPAN:	ANimator for AVISPA

FIGURE 9: Comparison of IR on communication cost.

HLPSL: High-Level Protocol Specification Language
 OFMC: On-the-Fly Model-Checker
 CL-AtSe: Constraint-Logic-based Attack Searcher
 SATMC: SAT-based Model-Checker
 TA4SP: Tree Automata based on Automatic Approximations for the Analysis of Security Protocol.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by National Key R&D Program of China (2016YFB0800703), the National Natural Science Foundation of China (nos. 61772404 and U1401251), the

Natural Scientific Basic Research Program Funded by Shaanxi Province of China (2017JM6029), and China 111 Project (no. B16037).

References

- [1] 3rd Generation Partnership Project, "Technical Specification Group Radio Access Network; Study on RAN Improvements for Machine-type Communications (Rel 11)," Tech. Rep., 2011, 3GPP TR 37.868 V12.0.0.
- [2] I. F. Akyildiz, D. M. Gutierrez-Esteviz, R. Balakrishnan, and E. Chavarria-Reyes, "LTE-advanced and the evolution to beyond 4G (B4G) systems," *Physical Communication*, vol. 10, pp. 31–60, 2014.
- [3] N. Nikaein and S. Krea, "Latency for Real-Time Machine-to-Machine Communication in LTE-Based System Architecture," in *Proceedings of Sustainable Wireless Technologies Wireless Conference*, pp. 1–6, 2011.

- [4] A. Zanella, M. Zorzi, A. F. Dos Santos et al., "M2M massive wireless access: challenges, research issues, and ways forward," in *Proceedings of the IEEE Globecom Workshops (GC Wkshps '13)*, pp. 151–156, USA, December 2013.
- [5] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 1017–1022, Anaheim, Calif, USA, December 2012.
- [6] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Security Aspects of Machine-Type Communications (Rel 12)," Tech. Rep., 2014, 3GPP TR 33.868 V12.1.0.
- [7] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Rel 14)," Tech. Rep., 2016, 3GPP TS 23.401 V14.0.0.
- [8] 3rd Generation Partnership Project, "Technical Specification Group Radio Access Network," Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; (Rel 13), 2016, 3GPP TS 36.300 V13.4.0.
- [9] 3rd Generation Partnership Project, "Technical Specification Group Service and System Aspects," 3GPP System Architecture Evolution (SAE); Security architecture (Rel 13), 2016, 3GPP TS 33.401 V13.3.0.
- [10] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Computer Networks*, vol. 56, no. 8, pp. 2119–2131, 2012.
- [11] D. Forsberg, "LTE key management analysis with session keys context," *Computer Communications*, vol. 33, no. 16, pp. 1907–1915, 2010.
- [12] 3rd Generation Partnership Project, "Technical Specification Group Service and System Aspects," Security of H(e)NB; (Rel 8), 2009, 3GPP TR 33.820 V8.3.0.
- [13] C.-K. Han, H.-K. Choi, and I.-H. Kim, "Building femtocell more secure with improved proxy signature," in *Proceedings of the 2009 IEEE Global Telecommunications Conference, GLOBECOM 2009*, USA, December 2009.
- [14] H. Nicanfar, J. Hajipour, F. Agharebparast, P. TalebiFard, and V. C. M. Leung, "Privacy-preserving handover mechanism in 4G," in *Proceedings of the 1st IEEE International Conference on Communications and Network Security, CNS 2013*, pp. 373–374, USA, October 2013.
- [15] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.
- [16] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Service Requirements for Machine-Type Communications (MTC) (Rel 13), 3GPP TS 22.368 V13.1.0, Dec. 2014.
- [17] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 7246–7251, UK, June 2015.
- [18] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, "A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1744–1747, 2012.
- [19] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 1011–1016, Australia, June 2014.
- [20] J. Cao, H. Li, and M. Ma, "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks," in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 3020–3025, UK, June 2015.
- [21] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 29–39, 2017.
- [22] K. Itakura and K. Nakamura, "A public-key cryptosystem suitable for digital multisignatures," *NEC Research and Development*, vol. 71, pp. 1–8, 1983.
- [23] S.-J. Hwang and Y.-H. Lee, "Repairing ElGamal-like multi-signature schemes using self-certified public keys," *Applied Mathematics and Computation*, vol. 156, no. 1, pp. 73–83, 2004.
- [24] J. Katz and A. Y. Lindell, "Aggregate Message Authentication Codes," in *Topics in Cryptology CT-RSA*, pp. 155–169, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.
- [25] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology EUROCRYPT*, vol. 2045 of *Lecture Notes in Comput. Sci.*, pp. 453–474, Springer, Berlin, 2001.
- [26] K.-R. Jung, A. Park, and S. Lee, "Machine-Type-Communication (MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network," *Communications in Computer and Information Science*, vol. 78, pp. 167–178, 2010.
- [27] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security (NDS); IP network layer security (Rel 13), 3GPP TS 33.210 V13.0.0, Dec. 2015.
- [28] E. Bresson, O. Chevassut, and D. Pointcheval, "Dynamic group Diffie-Hellman key exchange under standard assumptions," in *Advances in Cryptology—EUROCRYPT*, vol. 2332 of *Lecture Notes in Comput. Sci.*, pp. 321–336, Springer, Berlin, 2002.
- [29] AVISPA v1.1 User Manual, 2006.
- [30] Y. Glouche, T. Genet, O. Heen, and O. Courtay, "A Security Protocol Animator Tool for AVISPA," *ARTIST2 Workshop on Security Specification and Verification of Embedded Systems*, 2006.
- [31] L. Lamport, "Specifying Systems," in *The TLA+ Language and Tools for Hardware and Software Engineers*, Addison-Wesley Publishing Company, 2002.