An efficient anonymous group handover authentication protocol for MTC devices for 5G networks

Xiaobei Yan, and *Maode* Ma*

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

Abstract. Machine Type Communication (MTC) has been emerging for a wide range of applications and services for the Internet of Things (IoT). In some scenarios, a large group of MTC devices (MTCDs) may enter the communication coverage of a new target base station simultaneously. However, the current handover mechanism specified by the Third Generation Partnership Project (3GPP) incur high signalling overhead over the access network and the core network for such scenario. Moreover, other existing solutions have several security problems in terms of failure of key forward secrecy (KFS) and lack of mutual authentication. In this paper, we propose an efficient authentication protocol for a group of MTCDs in all handover scenarios. By the proposal, the messages of two MTCDs are concatenated and sent by an authenticated group member to reduce the signalling cost. The proposed protocol has been analysed on its security functionality to show its ability to preserve user privacy and resist from major typical malicious attacks. It can be expected that the proposed scheme is applicable to all kinds of group mobility scenarios such as a platoon of vehicles or a high-speed train. The performance evaluation demonstrates that the proposed protocol is efficient in terms of computational and signalling cost.

Keywords: Group handover authentication, MTCD, 5G, Privacy-preserving.

1 Introduction

Machine-type communication (MTC), also regarded as machine to machine (M2M) communication, is evolving to be an essential component of 5G wireless networks. MTC devices (MTCDs) communicate between a device and another entity in the network. The MTC will be popular in the scenarios such as health care services, fleet management, smart grid, and so on.[1] In some mobility scenarios, MTCDs are moving in groups from the serving base station to a new base station. It is referred as a group handover, which can be frequently observed in high-speed trains, platoon of vehicles or buses. A handover authentication process is initiated for every single MTCD to authenticate it with the network.

* Corresponding author: emdma@ntu.edu.sg

However, a group handover authentication has not been carefully considered by the current standard. The current 5th Generation (5G) standard specified by the third Generation Partnership Project (3GPP) published in April 2020 holds some problems in terms of high signalling overhead and security weaknesses when a group of MTCDs handover simultaneously. According to the 3GPP standard, a handover has been categorized into a Xn based intra-Access and Mobility Management Function (AMF) handover, a N2 based intra-AMF handover and a N2 based inter-AMF handover. It is disclosed in [2] that there are some weaknesses in the Xn handover authentication process including failure of key forward secrecy (KFS), vulnerability to Denial of Service (DoS) attacks and lack of mutual authentication between a MTCD and its target gNodeB (t-gNB). Moreover, an attacker can obtain the MTCDs' privacy information such as its moving pattern. And both N2 and Xn handovers could incur severe signalling overloads to a MTCD group. Thus, to design a secure and efficient group handover authentication protocol is a critical and important issue to support secure MTCs.

Unfortunately, existing research work has weaknesses in terms of security or efficiency. The authors in [1][3] have presented a secure context transmission (SCT)-based scheme, by which the source gNodeB (s-gNB) transmits the security contexts of all the group members when the first user equipment (UE) enters the communication coverage of the target gNodeB (t-gNB). The SCT scheme may cause key leakage because the session keys of the group members who leave the group after the first UE enters the area are still sending to t-gNB. The SCT scheme in [1] has failed key forward secrecy (KFS) and lack of mutual authentication. The SCT scheme in [3] has used the elliptic curve cryptography (ECC) which can incur high computational overheads. The authors in [4]-[8] have used the aggregated information to authenticate group members. The group leader aggregates message authentication codes (MACs) of all group members or signatures and sends the aggregated information to the network. In general, there are three weaknesses for the aggregation. The first one is the vulnerability to DoS attacks. The aggregated information can be successfully verified only if all members are legal. An attacker can send false aggregated information and make entire group verification fail deliberately. Second, lots of computations are needed at the leader's side. And the authentication of the leader has been ignored by some schemes. Third, the delays to the UEs who enter the new coverage area first is high because they have to wait for the calculations and message exchanges of the entire group over. The solution in [4] suffers from the key escrow problem and has a high computational cost because of the modular exponentiation algorithm used. The solution in [5] has a lower computation overhead, while it cannot support a dynamic change of group members. And it also has some security problems such as lack of authentication for the control mobile relay nodes, failed KFS/Key backward secrecy (KBS) and failure to preserve the privacy of the UEs. The solution in [6] has proposed a universal protocol for N2 and Xn handovers. But it also has a high computation overhead because of the ECC and the proxy signature used. The authors in [7] have proposed 2 schemes for different security requirements. However, it is only suitable for fixed-trajectory movements. The solution in [8] has a high computation overhead due to the use of the modular exponentiation algorithm.

It is clear that most of the solutions have used the algorithms with a high computational complexity for the resource-constrained devices. The security and privacy of the MTCDs have not been well protected. To overcome all the above problems, we propose a symmetric encryption-based protocol, which is named as efficient anonymous group handover authentication (EAGHA) scheme for massive MTCDs. It holds the following outstanding features: 1) The protocol can achieve all security properties while preserving the architecture of the 3GPP standard. 2) The signalling congestion can be avoided by allowing the authenticated group member to send and receive messages for the subsequent 2 members who need to be authenticated. It can also avoid a high overhead at the group leader and high

delays to the UEs who handover first. 3) The proposed protocol can resist DoS attacks and possible key leakage. 4) The identity of each MTCD is hidden by using a temporary ID (TID), which does not require the public key encryption. 5) The proposed protocol has a much lower delay compared to other existing schemes.

The organization of the rest of the paper is as follows: Section 2 illustrates the system model and threat model under the study. Section 3 details the proposed scheme. Section 4 presents the security analysis on the protocol. Section 5 shows the results of the performances evaluation. Section 6 is the conclusion of the paper.

2 System model

2.1 System model

This section introduces the system model of the 5G security architecture and the corresponding attack model. As shown in Fig. 1, the system architecture of the 5G core network and access network includes several types of devices such as AMF, Authentication Server Function (AUSF) and Authentication credential Repository and Processing Function (ARPF). During a handover process, a MTCD may hand over within an AMF, or to a different AMF. The handover using Xn interface within an AMF is called Xn-based intra-AMF handover. The handover using N2 interface within the same AMF is called N2-based intra-AMF handover. The handover between different AMFs is called N2-based inter-AMF handover. They all have been specified by the 3GPP Technical Specification TS 33.501 R16. By the specification, the handover involves three entities including MTCD, gNB, and AMF [9]. By the specification, the scope of possible t-gNBs has not been specified. In general, in a cellular network, a cell controlled by a gNB is surrounded by 6 neighbouring cells, which have been defined as neighbours of the gNB. During a handover, a MTCD can only hand over to one of the 6 neighbouring gNBs of the s-gNB. In this paper, all three types of handover scenarios will be considered.

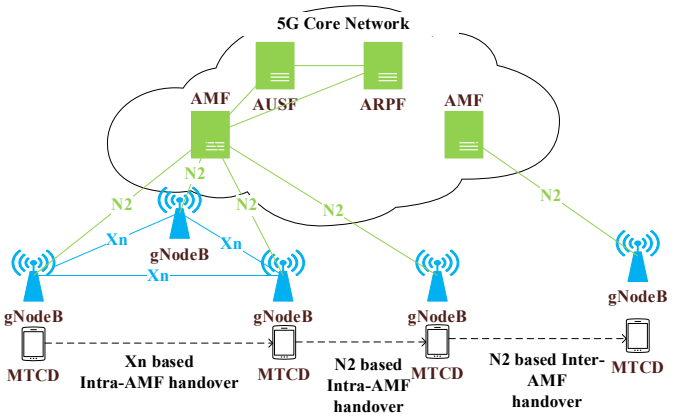

Fig. 1. System model of 5G network with different types of handovers.

2.2 Attack model

The attack model to the network under the study is the Dolev-Yao model, which is commonly used to present security vulnerabilities in various wireless networks. By the Dolev-Yao intruder model, the intruder could overhear, intercept, analyse, or manipulate messages on

communication channel. Besides, due to the failure of the KFS in the Xn handover specified by the standard, the attacker who knows a session key may launch eavesdropping attacks or message modification attacks until a new session key is derived. Moreover, impersonation attacks or false base-station attacks could be launched due to the lack of mutual authentication between a MTCD and t-gNB in the Xn handover process. DoS attacks can also be launched by an illegal gNB who transmits lots of much smaller next-hop chaining counter (NCC) values to the MTCD. A NCC value holds an initial value of zero and increases one at a time. And an attacker may obtain a user's identity to track the user by analysing the message exchanged.

3 The EAGHA scheme

In this section, we describe the proposed EAGHA in detail to show its ability to overcome the security weaknesses and avoid signalling congestion in the existing 5G handover protocols.

3.1 Motivation of the proposal

From the literature survey, the existing group handover authentication schemes including the group handover authentication specified by the 3GPP standard have various shortcomings. They either have security vulnerabilities or are inefficient in terms of latency. The protocols which aggregate user's information to authenticate UEs are vulnerable to DoS attacks. They can also incur extra latency to the UEs who enter the new coverage area first. The protocols, by which a group leader is selected to produce the aggregated information, will introduce high overheads at the leader. Based on these considerations, the EAGHA is proposed for MTCDs to mitigate the above-mentioned shortcomings. The EAGHA scheme aims to achieve various security attributes including privacy preserving, mutual authentication, perfect KFS, and resistance to a variety of malicious attacks.

3.2 Details of the proposed solution

The notations of the EAGHA scheme with their definitions are listed in Table 1. The proposed EAGHA scheme consists of three phases: i) initial authentication, ii) handover preparation, and iii) handover authentication. The first phase enables the mutual authentication for the MTCDs with the network. The second phase works before a handover happens. The third phase starts when the first MTCD enters the communication area of the t-gNB. The details of the EAGHA scheme are presented in Fig. 2. Before a handover, each gNB has a pre-shared key pair (s_i, d_i) allocated by the AMF. Only the AMF and the gNBs share the key. The AMF can renew the key through a N2 interface before a handover if needed. Also, it is assumed the AMF and the connection between AMFs and gNBs are secure.

Table 1. Notations and definition of the proposed protocol.

Notation	Definition
K_{AMF}	Access key at AMF/UE
s_i, d_i	Pre-shared keys of gNB i
K_{tempi}	One time session key of UE/t-gNB
θ	NH value encrypted with subkey s and AES key d
$\mathrm{K_{gNB}}/\ K^*_{gNB}$	Old/new session key of UE/gNB
MAC	Message authentication code
$H(\cdot)$	Hash function
$ARFCN-DL$	Absolute radio frequency channel number-down link of gNB

PCI	Physical cell identity
t	Timestamp
GK	Group Key

3.2.1 Initial authentication

In this phase, the MTCDs, the AMF, the AUSF and the ARPF will execute the 5G authentication and key agreement protocol (5G-AKA) specified by the 3GPP standard. Keying materials that could be used between the MTCDs and the serving network are provided in the subsequent procedures.

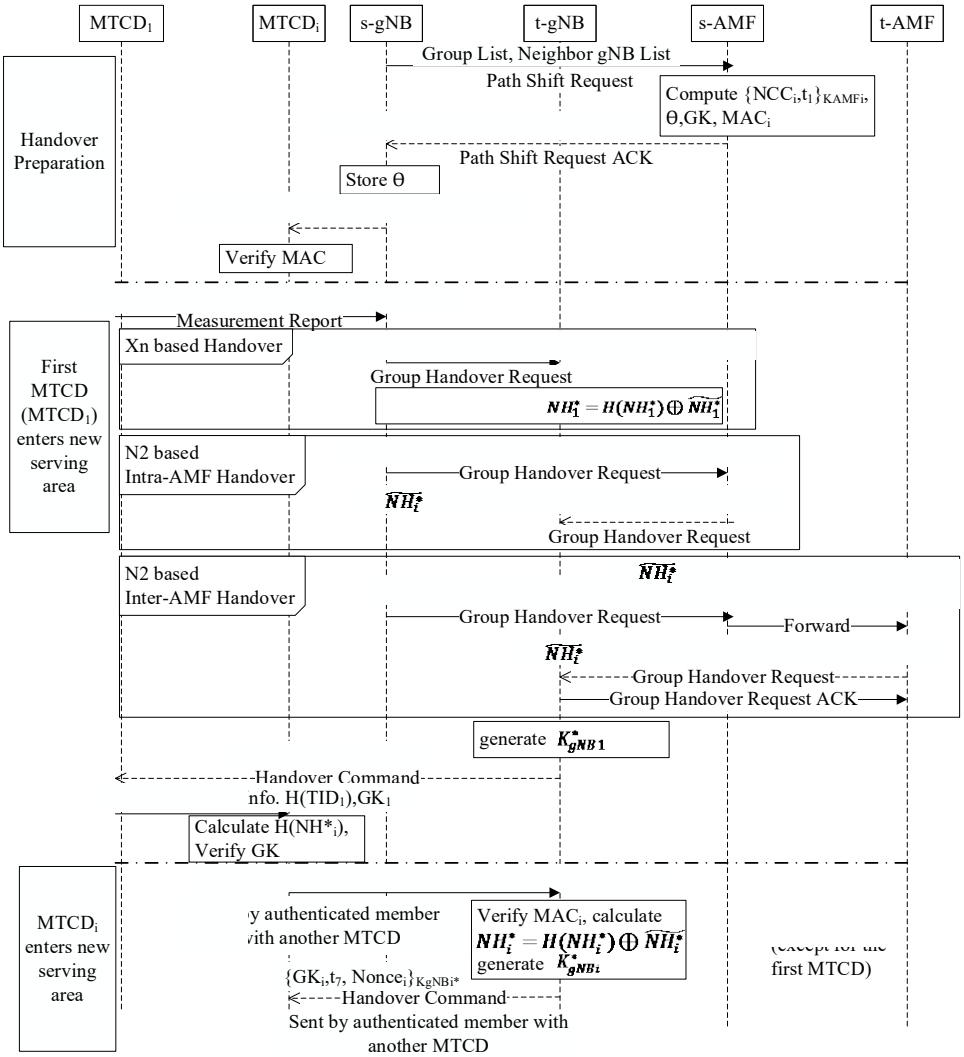

Fig. 2. The Proposed EAGHA.

3.2.2 Group handover preparation

This phase works before a handover. The keying materials are prepared in this phase. The operations are described below:

Step 1: After the previous handover, a group path shift request message will be sent by s-gNB, where s-gNB reports its neighbourhood list to the s-AMF.

Step 2: This step happens depend on status of pre-shared keys. If the criteria for key renewal are met, the AMF should renew the pre-shared keys for the gNBs and compute the new session key between two neighbouring gNBs by $K_{(sgnb,tgnb)} = H(s_i \,||s_j)$ and sends them to the corresponding gNBs.

Step 3: First, the AMF encrypts the next hop parameters (NHs) and temp session keys K_{temp} of all group members in θ. Different from the encryption scheme in [10], which is vulnerable to the plaintext attacks, by the proposed scheme, the AMF encrypts the group NHs and K_{temp} in following steps: For all allocated pre-shared subkeys of neighbouring gNBs $s_1, \dots, s_6$, AMF computes $\sigma = \prod_{i=1}^{6} s_i$, $x_i = \frac{\sigma}{s_i}, y_i = x_i^{-1}\, mod\, s_i$, and $\theta = \sum_{i=1}^{6}[y_i * \left(K_{tempi}||\widetilde{NH_i^*}\right)_{d_i}]\, mod\, \sigma$ to encrypt the NH value and K_{tempi} for all group members, where θ is encrypted information, $||$ is concatenate operation. $\widetilde{NH_i^*} = H(NH_i^*) + NH_i^*$, $\left(\widetilde{NH_i}^*\right)_{d_i}$ is encrypted $\widetilde{NH_i^*}$ by key d_i using Advanced Encryption Standard (AES). $\widetilde{NH_i}$ can prevent t-gNB from knowing the NH value of the MTCD who leaves the group. K_{tempi} will be used as session key between the MTCD and the t-gNB. The AMF computes $TID_i = H(SUPI_i \| K_{AMFi} \| K_{tempi})$, $GK = H(\sum_{i=1}^{n} H(TID_i))$ and generates $MAC_i = H(GK||K_{tempi}||NCC_i||K_{AMFi})$ and sends $TID_i, GK, \theta, \left\{K_{tempi}, NCC, t\right\}_{K_{AMFi}}, MAC_i, t$ to s-gNB.

Step 4: S-gNB checks the freshness of the timestamp, stores θ, and sends $\left\{GK, \theta, \left\{K_{tempi}, NCC, t\right\}_{K_{AMFi}}, MAC_i\right\}_{K_{gNBi}}$ to all the MTCDs in the group.

Step 5: The MTCD decrypts the message and verifies the MAC. If the verification fails, the MTCD declines the connection.

3.2.3 Group handover authentication

It happens when the first MTCD ($MTCD_1$) enters the t-gNB coverage area.

Step 1: $MTCD_1$ calculates $H(NH_1^*)$ and generates a nonce and a timestamp and sends the encrypted message $\left\{TID_1, t, H(NH_1^*), \{t, Nonce_1\}_{KgNB1*}\right\}_{KgNB1}$ to the s-gNB.

For a Xn based Handover, the process jumps to *step 2*. For a N2 based Intra-AMF Handover, the process jumps to *step 3*. For a N2 based Inter-AMF Handover, the process jumps to *step 4*.

Step 2: The s-gNB decrypts the message and sends $\left\{\theta, t, TID_i, H(NH_1^*), \{t, Nonce_1\}_{KgNB1*}\right\}_{K_{(sgnb,tgnb)}}$ to the t-gNB. The t-gNB uses its pre-shared keys (s_t, d_t) to decrypt θ by $(\theta \bmod s_t)_{d_t}$ to obtain temporary session keys K_{tempi} with the MTCDs. Then it calculates NH_1^* by $NH_1^* = H(NH_1^*) \oplus \widetilde{NH_1^*}$.

Step 3.a The s-gNB decrypts the message received from $MTCD_1$ and forwards $\{t, TID_1, \{t, Nonce\}_{KgNB1*}\}$ in the group handover request message to source-AMF (s-AMF).

3.b The AMF sends $\{\widetilde{NH_i^*}, TID_i, t, K_{tempi}, \{t, Nonce_1\}_{KgNB1*}\}$ (i= 1,…,n) in the group handover request message to the t-gNB.

Step 4.a The s-gNB decrypts the message from $MTCD_1$ and forwards $\{t, TID_1, \{t, Nonce_1\}_{KgNB1*}\}$ in the group handover request message to the s-AMF.

4.b The s-AMF sends $\{\widehat{NH_i^*}, TID_i, t, K_{tempi}, group\ security\ context, \{t, Nonce_1\}_{KgNB1*}\}$ (i=1,…,n) in one of the group handover request message to the target AMF (t-AMF). The group security context includes the session keys used with the MTCDs.

4.c The t-AMF sends $\{\widehat{NH_i^*}, TID_i, t, NH_1^*, K_{tempi}, \{t, Nonce_1\}_{KgNB1*}\}$ (i=1,…,n) in one group handover request message to the t-gNB. The t-gNB sends an acknowledgement (ACK) message back to the t-AMF.

Step 5: The t-gNB calculates its session key with $MTCD_1$ K_{gNB1}^* using the formula stated in [9]. i.e., $K_{gNB*} = KDF(NH\|PCI\|ARFCN-DL)$ and sends $\{GK_1, Nonce_1, t\}_{KgNB1*}$ to $MTCD_1$, where GK_1 is the partial group key for $MTCD_1$ calculated by $GK_i = \sum_{k=1\ldots n}^{k\neq i} H(TID_k)$. After this step, the mutual authentication between the $MTCD_1$ and the t-gNB is successful.

Step 6: The *MTCD1* broadcasts t-gNB's information, $H(TID_1)$ *and* GK_1 to all group members. The subsequent 2 members who enter the new area verify the $MTCD_1$ by calculating if $H(H(TID_1) + GK_1) = GK$. If equals, the subsequent 2 members send $\{MAC_i, TID_i, t, H(NH_i^*), \{t, Nonce_i\}_{KgNBi*}\}_{Ktempi}$ to $MTCD_1$, where the MAC is the hash of the message and K_{tempi}. The $MTCD_1$ concatenates two messages into one message and sends it to the t-gNB. If the waiting time for these 2 members to find an authenticated member exceeds a preset value, they should send the message to the t-gNB directly.

Step 7: The t-gNB decrypts the message using K_{tempi} and verifies the MACs. It derives the NH value by $H(NH_i^*) \oplus \widehat{NH_i^*}$ and generates K_{gNBi}^*. Finally, the t-gNB sends $\{GK_i, t_7, Nonce_i\}_{KgNBi}*$ of the two members to $MTCD_1$, which sends the messages to the corresponding members, respectively. The two members verify the equality of the received nonce with the one they have sent before. If equals, the authentication is success. And each of the two members will help another 2 unauthenticated members to upload and download the messages, following the same procedure as $MTCD_1$.

4 Security analysis

In this section, the security properties of EAGHA are analysed.

Anonymity and Unlinkability: By the proposed scheme, the temp identity TID is used to achieve the anonymity. The real identity of a MTCD (SUPI) is concealed with K_{AMF} and K_{temp} using hash function. The real identity of a user will only be known to the AMF and be changed in every handover. Besides, with the use of the nonces in each message, it is hard to decide whether two messages are computed by the same group members. Thus, this scheme can achieve the anonymity and unlinkability.

Mutual Authentication: By the EAGHA scheme, the MTCDs authenticates t-gNB by the temporary session key K_{temp}, *H(NH)* and K_{gNB}. Only legitimate t-gNB can obtain K_{temp} to decrypt the message and calculate the NH to derive the session key K_{gNB}. The MTCD can determine if correct keys have been used by comparing the nonce with the one it has sent before. Similarly, the gNB authenticates the MTCD by determining if the same correct keys have been used and verifying TID. Therefore, mutual authentication between MTCDs and t-gNB can be achieved.

Ability against DoS Attacks: By the original 3GPP scheme, an attacker may launch DoS attacks by impersonating a legal gNB and send lots of fake NCC values to the UE to sabotage the key derivation process. And by the schemes using the aggregated MAC or signature, an attacker may launch DoS attacks by sending the false information to make the verification of the aggregated information for the entire group fail. By the EAGHA scheme, a MAC value

is added to ensure the NCC's integrity without aggregating any messages. Therefore, the DoS attacks cannot proceed.

Ability against Impersonation/False Base-station: It is possible for an illegal gNB to impersonate a legal gNB to setup illegal communication with the MTCDs. By the EAGHA scheme, a MTCD is able to tell if NCC and K_{temp} have been modified by verifying the MAC, which is only calculable by the AMF and the MTCD who knows K_{AMF}. Moreover, only the legal gNB can receive new pre-shared key from the AMF, which is also updated periodically. Without a valid pre-shared key, the false gNB cannot derive session key K_{gNB*} The MTCD can authenticate the gNB by determining if the correct pre-shared key is used and if the gNB has modified the NCC and K_{temp} value. Therefore, the false base-station attacks and the impersonation attacks can be prevented.

Ability against Man-in-the-Middle (MitM) Attacks: By the EAGHA scheme, an adversary cannot masquerade as a legitimate t-gNB to deceive MTCDs because temporary session keys K_{temp} have been established between them by the AMF. As the communication between AMF and gNBs are considered as safe, and a MAC of K_{temp} has been generated with K_{AMF} and sent to MTCDs. An adversary cannot obtain or modify the temporary session keys and therefore cannot setup communication with MTCDs.

Ability against Replay Attacks: By the EAGHA scheme, timestamps and nonces are employed in each message, which is also encrypted with the session key. Thus, each message will be completely different and cannot be understood by the adversary without a session key. Then, replay attacks can be avoided.

5 Performance evaluation

In this section, the performance of the proposed scheme has been evaluated with the comparison of the performance of other schemes. It includes the evaluation of computational cost and signalling cost. It is assumed that all AES keys including NH are 256 bits, MAC is 160 bits, hash, nonce, TID and the pre-shared key (s, d) are 128 bits, timestamp is 32 bits and NCC is 3 bits.

5.1 Signaling cost

The signalling cost of the proposed scheme has been evaluated to compare with that of the 5G standard specified by 3GPP [9] in terms of the number of signalling messages for *n* MTCDs. The results of the signalling overheads have been shown in Table 2.

Table 2. Signalling overhead for n MTCDs.

	Xn-based Handover	Intra-AMF Handover	Inter-AMF Handover
5G	5n	7n	8n
EAGHA	n+2	n+3	n+5

According to Table 2, the signalling cost of each of the handover scenarios by proposed scheme is much less than that by 3GPP 5G schemes [9].

5.2 Computational cost

To evaluate the computational overhead, according to the testing data of the cryptography operations in [7], the point addition operation T_{PA} for a MTCD and a gNB are 2.53μs, 1.39μs respectively. The point multiplication operation T_{PM} for a MTCD and a gNB are 960μs, 500μs respectively. The modular exponentiation operation T_E for a MTCD and a gNB are 1890 μs, 1000 μs respectively. The symmetric encryption/decryption operation T_A for a

MTCD and a gNB are 2.26μs, 1.05μs respectively. And the hash operation T_H for a MTCD and a gNB are 2.38μs, 1.21μs respectively. We ignore xor, multiplication and arithmetic operation. The computational cost of the EAGHA is compared with that of 5G standard specified by 3GPP [9] and the scheme SRGH [6]. The results for different schemes are shown in Table 3.

Table 3. Computational overhead for n MTCDs.

Scheme	T_{UE}	T_{gNB}	T_{UE} (μs)	T_{gNB} (μs)
5G	$4T_H n$	$2T_H n$	$9.52n$	$2.42n$
SRGH	$5(T_{PM} + T_H)(n+1) - 2T_{PM}$	$5(T_{PM} + T_H)(n+1)$	$4810n + 2892$	$2510n + 2510$
EAGHA	$(3T_H + 3T_A)n - 2T_H$	$(2T_H + 3T_A)n - T_H$	$13.92n - 4.76$	$5.57n - 1.21$

Finally, the robustness of schemes is evaluated. Unknown attacks have been introduced to each of the systems. When facing the unknown attacks, an authentication process could be forced to stop and restarts. It is assumed that at each step of the authentication, the probability of a unknown attack appearing is even. In the simulation, the total time is the total authentication time for *n* group members, which equals to the communication delay with the computational delay. The results of the simulation are shown in Fig. 3.

It is clearly shown that with the increase of the unknown attacks, the time costs by both handover authentication schemes increase. The proposed scheme has a better performance in terms of the total time costs over that of the SRGH scheme, while it has a similar performance as that of 3GPP 5G.

6 Conclusion

In this paper, we have proposed a novel scheme to enhance the security functionality and reduce signalling overheads of the scheme of the 3GPP standard by pre-distributing keys and message concatenation. It has been analysed to hold the ability to resist DoS attacks, impersonation /false base- station attacks with perfect KFS and preserve user's privacy. The performance evaluation has shown that the EAGHA scheme has a much lower delay than other existing schemes. Compared to 3GPP standard, the signalling overhead has been greatly reduced. Thus, it meets the requirements when a group of devices in high-speed moving scenarios while avoiding the signalling congestion.

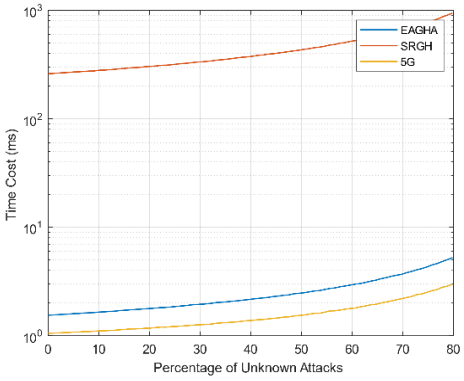

Fig. 3. Comparison of time cost.

References

1. J. Cao, H. Li and M. Ma, "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks," 2015 IEEE International Conference on Communications (ICC), 2015, pp. 3020-3025, doi: 10.1109/ICC.2015.7248787.
2. A. Sharma, A. Jain and I. Sharma, "Exposing the Security Weaknesses of Fifth Generation Handover Communication," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6.
3. Fu A, Zhang G, Zhang Y, Zhu Z., "GHAP: an efficient group-based handover authentication mechanism for IEEE 802.16m networks", in Wireless personal communications, 2013;70(4): pp.1793-1810.
4. J. Cao, H. Li, M. Ma and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," 2015 IEEE International Conference on Communications (ICC), 2015, pp. 7246-7251, doi: 10.1109/ICC.2015.7249483.
5. J. Cao, M. Ma and H. Li, "G2RHA: Group-to-Route Handover Authentication Scheme for Mobile Relays in LTE-A High-Speed Rail Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 9689-9701, Nov. 2017.
6. Gupta, S., Parne, B. L., & Chaudhari, N. S., "SRGH: A secure and robust group‐based handover AKA protocol for MTC in LTE‐A networks", in International Journal of Communication Systems, 32(8), e3934.
7. R. Ma, J. Cao, D. Feng, H. Li and S. He, "FTGPHA: Fixed-Trajectory Group Pre-Handover Authentication Mechanism for Mobile Relays in 5G High-Speed Rail Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 2126-2140, Feb. 2020.
8. Z. Haddad, A. Alsharif, A. Sherif and M. Mahmoud, "Privacy-Preserving Intra-MME Group Handover via MRN in LTE-A Networks for Repeated Trips," 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 2017, pp. 1-5.
9. 3GPP TS 33.501 V16.1.0. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 16)". Valbonne: 3PP Support Office, 2019.
10. Davida, George I., David L. Wells, and John B. Kam. "A database encryption system with subkeys." in ACM Transactions on Database Systems (TODS) 6.2 (1981) pp.312-328.