American Journal of Engineering Research (AJER) 2017
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-2, pp-181-192
www.ajer.org
Research Paper Open Access

SEGHAS: A Secure & Efficient Group-Based Handover Authentication Scheme for Machine -to- Machine Communication in LTE-A Network

Ali Saqib[1], Jianye Song[2],Alassane Coulibaly[3] , Mukhtar Abdirahman[4]
School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China

ABSTRACT: *Machine to Machine Communication has been proved as the vital entity with its inherent and real-time network applications in the LTE-A network. Machine-to-Machine (M2M) or Machine Type Communication (MTC) is also becoming the milestone in the era of new technologies for the future mobile communication. With the real-time network applications, MTC has drawn tremendous attention in the short span of time. MTC is a mean source of communication between devices, core network without intervention of the third party. With the rapid growing and usage of MTC devices, the threat of breach in security is also increasing, while security is the paramount issue in M2M communication. When we talk about a huge number of MTC devices request all together for the register to the desired network, whereas individual device has to complete its authentication procedure over the network. The procedure of access authentication of a huge number of devices at a time which could suffer from a severe signaling congestion and reluctant to provide a robust security mechanism for the MTC devices over the LTE-A Network. To come up with these issues, we propose a secure and efficient group-based handover authentication scheme (SEGHAS) which is capable of achieving all the security mechanism with less communication and computation cost, fast handover, avoiding the signaling congestion and also preventing from unauthorized user access in M2M Communication in LTE-A Network. Furthermore, by using the Pro-Verif tool for network testing and authentication against malicious attacks, while concluding the results it is shown that our scheme is best fit in terms of computation and signaling overhead.*

Index Terms *—Security, Group-Based Handover, M2M, LTE-A*

I. INTRODUCTION

Machine Type Communication (MTC) is also known as Machine to Machine (M2M) communication. Nowadays, the era of advanced technologies, such as smartphones, smart grid, smart metering etc, has shown that there is a growing trend to rely on these new technologies to generate and support for the progress. Society is clearly ready to trust on these advanced communication systems to face today's concerns on new technologies. MTC is becoming evolutionary in the new generation communication system, it has gained more ascendancy by the standardization with 3rd generation partnership project (3GPP). Furthermore, with the capacity of higher data rate, lower access latency and satisfactory coverage as compared to another wireless access networks, LTE-A network can achieve the desired goals in enhancing MTC devices and its applications [1]. M2M is an emerging technology and has gained tremendous attention in big sectors e.g., mobile networks, research entities, health, industrial automation, fleet management and so on [2]. MTC is a special type of data communication which is quite different from Human to Human (H2H) intervention [3].

In addition, with the rapid usage & growing number of MTC devices, according to hypothesized data that the average sum of MTC devices will be 1000 times larger than that of smart devices/User Equipment (UEs) [4]. According to the analysis results show that the number of MTCDs connected to a single base station in 2020 to be anywhere from 10000 to 100000 [5]. However, increasing numbers of the MTC devices, the threat of breach in security is also increasing, while security is the most important issue in the M2M communication. When these large number MTC devices instantaneously move from one base station/source (eNB) to new (eNB) /target base station to get the full access and authentication towards the core network, causing a severe signal overhead. However, each device is prone to perform access confirmation process with the network. The authentication and the security of these group of smart deviceslead to acute signaling congestion and refuse to provide robust security mechanism over the LTE-A network. Consequently, network declines to provide better services for the MTC devices. Rendering to 3GPP standards, all MTC devices send a request to accomplish the same verification with the same device such as the common UE [6]. Moreover, during the mobility of a group of

MTCs, it is utmost required to accomplish a secure, fast and efficient handover is a key concern in the LTE-A network need to be solved.

The contributions in this paper have been summarized up as follows:

1) We proposed a secure and an efficient handover authentication scheme to form a group of MTC devices during mobility, which can reduce the ultimate cause of the signal congestion in the LTE-A network. 2) The proposed scheme has a secure mechanism which is useful for all group based handover scenarios in the LTE-A networks to achieve the desired results regarding latency in the handover authentication process. 3) By the scheme network crowding can be avoided by using fewer data packets when compared with computation and communication cost with other LTE schemes. 4) Our proposed scheme can enhance fast handover and prevent from unauthorized user access in LTE-A Network. While network efficiency and confidentiality during handover can be enhanced also.

II. RELATED WORK

The mobility of MTC devices in the traditional authentication protocols, e.g., (EPS-AKA) [18], has a bulge of signal overhead, leading to handover authentication because of performing a full AKA with the home authentication server, respectively. During the handover authentication, the system should ensure that the data is exchanged without any modification and shield against some malicious attacks such as masquerade, Man-in-the-Middle (MITM) and replay attacks [7]. In that case, the security methods become vital in M2M communication in LTE-A network. Key generation in [8], this paper analyzes the switching key management mechanism of LTE-A network and points out that different key derivation methods will increase the complexity of the system. The source eNodeB can link the current key and the related parameters, and at the same time, the system will select the horizontal key derivation method, but this key management mechanism still has some shortcomings [9]. In [17], it is pointed out that the horizontal key derivation method lacks the forward security, because an attacker can obtain future session keys from the current session key and some public parameters and the vertical key derivation is only limited by two hops forward security, a unified switching scheme based on proxy signature for LTE network is proposed. The scheme can resist desynchronization attacks, but also ensures forward security, but cannot realize privacy protection [10] and [11] analyzed that the handover process of the LTE network cannot resist the desynchronization attack. The malicious eNB may disturb the update of the Next Hop Chaining Counter (NCC) values, and the NCC is the vertical key derivation scheme. If the NCC value of the UE and the target eNodeB is not synchronized, the system will abandon the use of the vertical key derivation method and use the horizontal key derivation method. As a result, the future session key will be leaked further.

Until now, there are many group based handover authentication schemes have been presented, however, they still have some vulnerabilities to improve the robust security mechanism. To deal with such vulnerabilities, there are a lot of group based schemes have been proposed in [12], [13], [16]. By using these schemes, the communication cost can be reduced to some extent during the initial authentication process. Specifically, they still prompt to consider the mobility procedure of a large number of devices. C. Lai et al [7] haveprojected a secure roaming scheme for M2M and Worldwide Interoperability for Microwave Access (WIMAX) network. However, the scheme is planned for the WIMAX network, but it does not meet the architecture of MTC in LTE-A network and carries a lot of computational overhead because of extra pairing. In [10], the location and information identity protection areatstake, where an attacker can manipulate the data because location confidentiality is plain. Fu.et al. [14] propose a scheme with privacy protection in the WiMAX network. According to the scheme, MTC devices form a group handover at target side during the mobility. Furthermore, the Service base station (SBS) transmits all the secure handover information of the group to the target base station (TBS). By the scheme rest of TBS in the same group handover can bypass the secure information directly without communicating with other SBS. The scheme is best fit to reduce signaling handover overhead in WIMAX network. Though the scheme can reduce the signaling overhead, but it has some vulnerabilities during bulge of authentication to the SBS, which is not suitable for MTC in LTE-A network because of thedirect intervention with the base stations and HeNBs in the Intra-inter MME handover process. Cao et al. [15] scheme for a number of MTCs to access and authenticate in LTE-A network. In the scheme, all MTC devices send an aggregate signature through the group leader, which is performed by each MTC device and send to the MME. However, the communication cost in the scheme is still high, because of using the elliptic curve and bilinear pairing algorithm.

The reminder of this paper is formed as follows: Section III represents the preliminary of MTC network architecture. Section IV describes the proposed scheme in detail. In Section V, we present the security analysis and the performance evaluation of our scheme are. Finally, Section VI contains the conclusion.

III. MTC NETWORK ARCHITECTURE IN LTE-A NETWORK

The backbone of the LTE-A network architecture consists of (E-UTRAN), Evolved Packet Core (EPC) and Radio Link Interface. The E-UTRAN is in charge of MTC devices and base stations (eNBs), while the MTC devices (MTCDs) are interconnected with the eNBs through the EPC. The EPC is consist of MME, HSS, S-GW and Packet Data Network Gateway (PDN GW). The MME and S-GW play the key role in managing the signal flow and MTCD data amenities. HSS is responsible for handle MTC and prone to authentication information of MTCDs to the MME for the validation. The E-UTRAN contains access points (APs) and two types of base stations, (eNB) and (HeNB). Moreover, HeNB is a low-power terminal point used for indoor coverage, such as small office/residence area to boost up the signal quality which is interconnected with EPC via S1 interface. However, X2 interface is responsible for connecting eNB, HeNB and MMEs/SGWs with S1 interface. According to the current handover specifications suggested by 3GPP committee in [16] need several signaling interactions, they lead to the severe signaling overhead in the E-UTRAN and the EPC, during the mobility of mass of MTCDs handover to the new eNB simultaneously. Specifically, different mobility scenarios need to execute the dissimilar handover procedures, which may cause to increase the overall system complexity. Such as the mobility of both X2-based handovers, intra-Mobility Management Entity (intra-MME) handover it is also called (horizontal handover), inter-MME handovers called (vertical handover) and relevant handover scenarios.

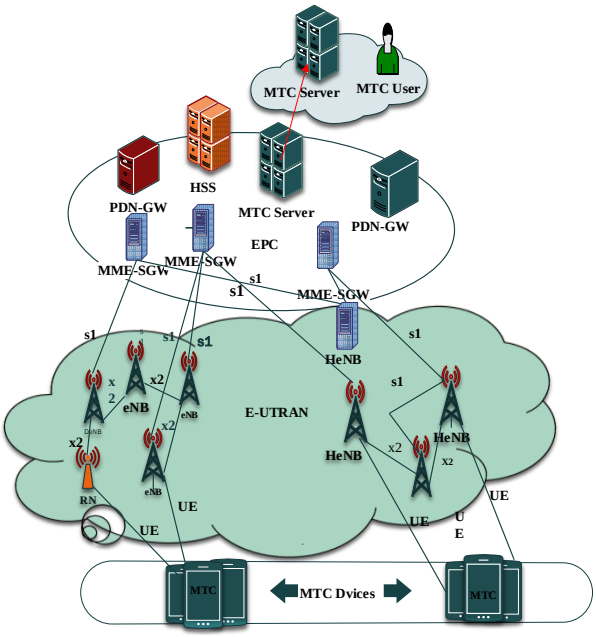

Figure 1. MTC Architecture in LTE-A Network

In addition, all the MTCDs are connected and controlled by the MTC server, these devices can be accessed inside or out of the network operator. When an MTCD try to connect with the LTE-A network via MTC server which is controlled by MTC users and MTC servers. By enabling the MTCDs and MTC server to communicate with LTE-A network need to authenticate the MTCDs before connecting to the servers.

IV. THE PROPOSED SCHEME

In this section, the design of our protocol is described. This section is divided into three phases: an initial authentication phase, MTCD mutual authentication phase, and group-based handover authentication phase. The acronyms and their meaning used in proposed scheme are mentioned in table I.

Table I: Notations and Acronyms

Notation	***Meaning***
r_X	The randomly generated number by x
ID_X	The identity of x
$MTCD_{G1-i}$	The*i*-th identity of MTCD in G1 handover group
$ID^{j}_{MTCD_{G1-i}}$	The *j*-th pseudonym of the*i*-th MTCD in G1 handover group
GK_i	The group key of the temporary*i*-th handover group
GTK_i	The group temporary key of the*i*-th handover group

MAC_X	Message authentication code computed by x
MAC_{Gi}	Message authentication code computed by $MTCD_{leader}$ in G1
$AUTN_X$	The validation of token generated by x
$H()$	A Secure Message authentication function
$KDF()$	A Key generation function

4.1An Initial Authentication Phase

In this phase, each MTC device in implements the initial authentication process when access to the LTE-A network. HSS randomly chooses a *k*-bit prime number *q* and construct, an additive and multiplicative cyclic groups G_1, G_2 of order *q*, a generator *P* in G_1, an admissible pair of the group $e: G_1 \times G_1 \to G_2$ and one-way key derivation function $f: G \to \{0,1\}^*$. Finally, HSS broadcasts $\{q, G_1, G_2, P, e\}$, assystem parameters. During the device authentication phase, when an individual MTCD sends the request for the access of LTE/LTE-A networks, HSS validate the authenticity of MTCDs. Then, HSS computes a series of unrelated pseudo- identities/Pseudonym $\{ID^1_{MTCD_i}, ID^2_{MTCD_i}, \cdots\}$ instead of revealing the MTCD's real identity (ID_{MTCD_i}) as follows [14].

1) HSS generates N random numbers $R_j \in Z_P^*$, *j*=1, 2, …, N;

2)Calculates N pseudonym

$ID^j_{MTCD_i} = ID_{MTCD_i} \oplus H_1(R_j \cdot PK)$, *j*=1, 2, ..., N, where $\oplus$ is an Exclusive-OR (XOR) operation. After successful access authentication register of MTCD to the LTE-A network, the system sends all $ID^j_{MTCD_i}$ back to the corresponding MTCD securely by using the secure channel assigned between the MTCD and the HSS.

The mechanism to form MTCD group, based on pre-set method such asapplication within the same region and MTCD with the same MTC service constrained. It is necessary to mention that group of MTCDs can be a single MTC user may be launched at the same time and move forward to the same location/direction, which can form a group of MTCDs in the MTCD initial authentication process. By the use of some grouping techniques can construct the handover group of MTCD, however, grouping techniques are outside the scope of this paper. Meanwhile, some recent and efficient group-based schemes have been proposed in this paper and they can be used in our scheme by making some modifications. To form a group of MTCDs, the HSS provides a group identity (ID_{Gi}), and a group private key (GK_{Gi}) for the individual MTC handover group.

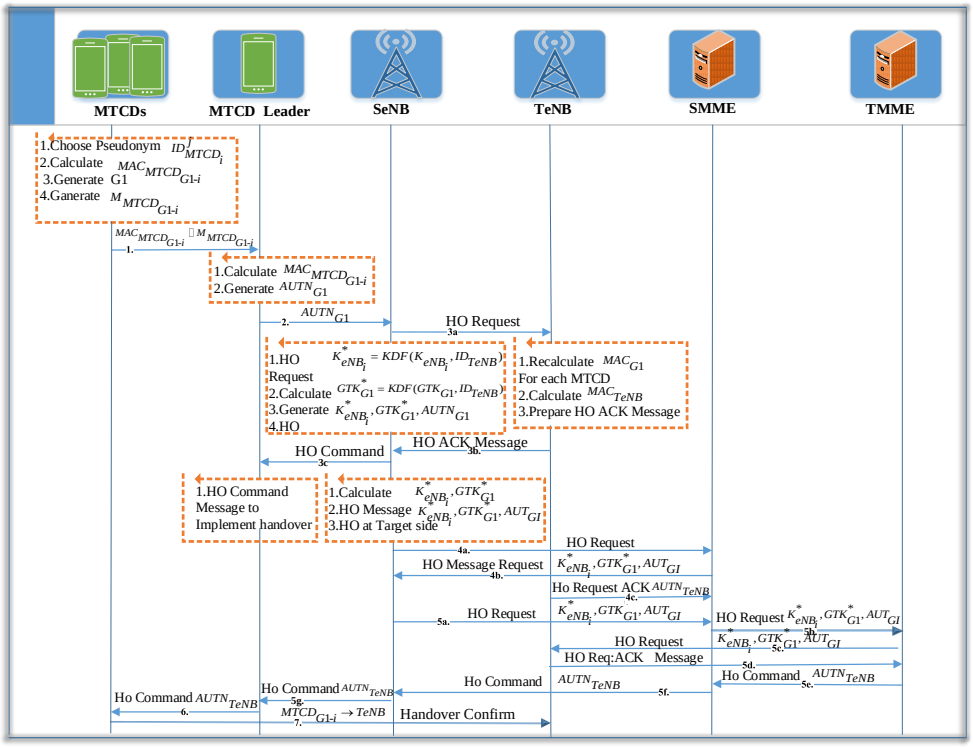

Figure 2. group-based handover authentication process

4.2 Mutual authentication phase

After completing the registration of MTCDs to the network, MTCDs form a group based on a certain principle, as defined G1. In this phase, group verification for all of the MTCD in the MTC handover group take into the consideration when performs the authentication process during initial group handover access authentication to the LTE-A network. Here we mention that we can not only put the standard of EPS AKA process [18], but also aid the group based handover access authentication processes proposed in [12], [13], [14], [15] to attain the initial access authentication process between the MTC handover group and the MME. Moreover, when MTC handover group successfully attains the access authentication, each $^{MTCD}_{G1\text{-}i}$ and the HSS generate a shared secret key $K_{ASME}^{MTCD_{G1-i}}$, and then the HSS transmits the $K_{ASME}^{MTCD_{G1-i}}$ to the MME. In the response of $K_{ASME}^{MTCD_{G1-i}}$, the MME aggregates the session key $K_{eNB_i} = KDF(K_{ASME}^{MTCD_{G1-i}} \| ID_{MME} \| ID_{SeNB} \| ID_{MTCD_{G1-i}})$ between the $MTCD_{G1-i}$ and the source base station or eNB (SeNB). And the group key (GK_{G1}) has been sent to MME in the mutual authentication phase. Subsequently, MME computes $GTK_{G1} = KDF(GK_{G1} \| ID_{SeNB})$ and sends GTK_{G1} and K_{eNB_i} ($1 \le i \le n$) to SeNB. At the same time, every $MTCD_{G1-i}$ computes the same process as K_{eNB_i} and GTK_{G1}. However, $\|$ represents a message concatenation operation.

4.3 Group-Based Handover Authentication Phase

The group based handover authentication of all theMTCDs take into the consideration throughout the mobility scenario from Source base station($SeNB$) to the target base station ($TeNB$) at the same time. Note that we will select a group leader ($MTCD_{leader}$) who has same functions as an MTCD. The $MTCD_{leader}$ can be formed for all MTC members in the G1 group, based on computing power, an efficient communication capacity, better storage capacity and large batterypower capacity. In this phase, the handover authentication process for all MTC members in the group handover G1 is accomplished during the mobility from the SeNB to the target eNB (TeNB) simultaneously. The rest of this process is defined in detail as follows.

Step 1. $MTCD_{G1-i} \rightarrow MTCD_{leader}$: ($MAC_{MTCD_{G1-i}} \| M_{MTCD_{G1-i}}$)

MTC devices (MTCDs) starts group authentication when they simultaneously move from connected eNB to the coverage of the TeNB, MTCDs request to handover into TeNB simultaneously. First, every $MTCD_{G1-i}$ computes new $K^*_{eNB_i} = KDF(K_{eNB_i}, ID_{TeNB})$,then calculates the relevant message authentication codes $MAC_{MTCD_{G1-i}} = H(K^*_{eNB_i} \| ID^j_{MTCD_{G1-i}} \| ID_{G1} \| r_{MTCD_{G1-i}} \cdot P)$ and verify the generated codes with its own validation message $M_{MTCD_{G1-i}} = (ID^j_{MTCD_{G1-i}} \| ID_{G1} \| r_{MTCD_{G1-i}} \cdot P)$. Finally, the group of MTCDs send their own authentication message $MAC_{MTCD_{G1-i}}$ and $M_{MTCD_{G1-i}}$ to the $MTCD_{leader}$ in G1 handover group.

Step 2. Measurement Report ($AUTN_{G1}$)

When $MTCD_{leader}$ receives all $MAC_{MTCD_{G1-i}}$ and $M_{MTCD_{G1-i}}$ from the G1 handover group, then equates an aggregated message authentication code $MAC_{G1}=MAC_{MTCD_{G1-1}} \oplus MAC_{MTCD_{G1-2}} \oplus ... \oplus MAC_{MTCD_{G1-n}}$, and creates a valid token for an authentication $AUTN_{G1}=(M_{MTCD_{G1-1}} \| M_{MTCD_{G1-2}} \| .. \| M_{MTCD_{G1-n}} \| MAC_{G1})$. Then $MTCD_{leader}$ sends a measurement report message which includes $AUTN_{G1}$ to the SeNB.

Upon receipt of the measurement report, the SeNB implements the subsequent processes for the different mobility and handover scenarios.

①X2-based Handover: This process occurs between SeNB and TeNB Without changing of the MME and Serving Gateway then process switch to the step 3.

②Intra-MME Handover. This handover procedure is very similar using the X2 interface, except the intervention of the MME in relaying the handover signaling between the SeNB and TeNB. If the intra-MME handover occurs between eNBs, which are managed by the same MME without the involvement of an X2 interface, the process switch to the next Step.

③Inter-MME Handover. This scenario is similar to the previous one, except the Source and the Target eNBs are operated by the different MMEs, this kind of handover happens throughout the eNBs. When this process happens, then process switch to the Step 5.

Step 3.

3a. $SeNB \rightarrow TeNB$: HO_Request Message ($K^*_{eNB_i} \| GTK^*_{G1} \| AUTN_{G1}$)

When SeNB receives the handover (HO) message, the SeNB computes a new session key $K^*_{eNB_i} = KDF(K_{eNB_i}, ID_{TeNB})$ of each $MTCD_{G1-i}$ in the MTC handover group. And the SeNB also computes a new group temporary key $GTK^*_{G1}=KDF(GTK_{G1}, ID_{TeNB})$. Finally, the SeNB sends an HO request to the TeNB, which includes all the necessary parameters of the $K^*_{eNB_i}$ for the entire group of MTC handover, GTK^*_{G1} and $AUTN_{G1}$.

3b. $TeNB \rightarrow SeNB$: Acknowledgement of HO_Request ($AUTN_{TeNB}$)

In response to the HO request message, the TeNB first recalculates MAC_{G1}' according to step 1, 2 and related verification vector contained in $AUTN_{G1}$. Then the TeNB checks whether MAC_{G1}' is equal to MAC_{G1} in order to make sure, whether every $MTCD_{G1-i}$ is legal or not. If both are not equal, TeNB simply sends a prompt message of request failure to all MTCDs in the G1 group. Otherwise, the TeNB computes an authentication message codes $MAC_{TeNB} = H(GTK^*_{G1} \| ID_{TeNB} \| r_{TeNB} \cdot P)$ and generates $AUTN_{TeNB} = (ID_{TeNB} \| r_{TeNB} \cdot P \| MAC_{TeNB})$. Finally, the TeNB sends the acknowledgment of the handover request message, including the parameters of $AUTN_{TeNB}$ to the SeNB for the confirmation of HO. Furthermore, SeNB also computes the new session key $K^{**}_{eNB_i}=KDF(K^*_{eNB_i} \| r_{TeNB} \cdot (r_{MTCD_{G1-i}} \cdot P))$ for each $MTCD_{G1-i}$.

3c. $SeNB \rightarrow MTCD_{leader}$: HO _Command ($AUTN_{TeNB}$)

After receiving the HO request acknowledgment message, the SeNB sends an HOcommand message to the $MTCD_{leader}$ for the implementation of HO. Next, the SeNB issues the handover command message in response to handover acknowledgment, then process jumps to next Step. Otherwise, SeNB discards it.

Step 4.

4a. $SeNB \rightarrow SMME$: HO_ Request ($K^*_{eNB_i} \| GTK^*_{G1} \| AUTN_{G1}$)

When SeNB receives the message from $MTCD_{leader}$, the process jumps to the next step, where SeNB computes $K^*_{eNB_i}$ and GTK^*_{G1} which is similar to step 3a. Next, the SeNB sends a message to comply with HO request to the SMME. Upon receiving the message, SMME formulates the HO at the target side, which is consist of $K^*_{eNB_i}$, GTK^*_{G1} and $AUTN_{G1}$.

4b. $SMME \rightarrow TeNB$: HO_Request ($K^{*+}_{eNB_i} \| GTK^*_{G1} \| AUTN_{G1}$)

In response to the HO request message from SeNB, the SMME calculates the new $K^{*+}_{eNB_i} = KDF(K^{MTCD_{G1-i}}_{ASME} \| K^*_{eNB_i})$ which is received from $K^*_{eNB_i}$ for the individual $MTCD_{G1-i}$ in the MTC handover group. Moreover, the SMME creates a new message HO message and sends to the TeNB. When TeNB receives the corresponding message from SMME to prepare the HO including, $K^{*+}_{eNB_i}$, GTK^*_{G1} and $AUTN_{G1}$ for the whole group of MTCD handover.

4c. $TeNB \rightarrow SMME$: HO_ Request Acknowledgement ($AUTN_{TeNB}$)

The TeNB comply with the HO request message and recalculates MAC_{G1}' according to step 1, 2and parameters for the authentication vector contained in $AUTN_{G1}$. Then the TeNB checks whether MAC_{G1}' is equal to MAC_{G1} in order to make sure that whether every $MTCD_{G1-i}$ is legal or not, If not the TeNB sends a prompt messageof requestfailure to all MTCDs contained in the G1 group. Otherwise, the TeNB computes new message for the authentication codes $MAC_{TeNB}=H(GTK^*_{G1} \| ID_{TeNB} \| r_{TeNB} \cdot P)$ and generates $AUTN_{TeNB}=(ID_{TeNB} \| r_{TeNB} \cdot P \| MAC_{TeNB})$. Lastly, the TeNB sends the HO request acknowledgment message which consists of $AUTN_{TeNB}$ to the SeNB to validate the HO and calculates a new session key $K^{**}_{eNB_i}=KDF(K^{*+}_{eNB_i} \| r_{TeNB} \cdot (r_{MTCD_{G1-i}} \cdot P))$ for each $MTCD_{G1-i}$.

4d-4e. $SMME \rightarrow SeNB$, $SeNB \rightarrow MTCD_{leader}$: HO_Command ($AUTN_{TeNB}$)

In response to the HO request acknowledgment message from SeNB, the SMME sends the command message for the handover which includes $AUTN_{TeNB}$ to the $MTCD_{leader}$ via a secure channel to the SeNB to implement the HO. Next, the process switches to Step 6 for the further steps.

Step 5.

5a. $SeNB \rightarrow SMME$: HO_Request ($K^{*}_{eNB_i} \| GTK^{*}_{G1} \| AUTN_{G1}$)

This process is similar as described in Step 4a.

5b. $SMME \rightarrow TMME$: HO_Request ($K^{*+}_{eNB_i} \| GTK^{*}_{G1} \| AUTN_{G1}$)

Upon receipt of HO request message, the SMME computes $K^{*+}_{eNB_i}$, the process is similar to**Step** 4b. Then, the SMME forwards the handover request message to the target MME (TMME).

5c. $TMME \rightarrow TeNB$: HO_ Request ($K^{*+}_{eNB_i} \| GTK^{*}_{G1} \| AUTN_{G1}$)

When TMME receives HO request message, then forwards the corresponding message to the TMME.

5d. $TeNB \rightarrow TMME$: HO_ Request Acknowledgement ($AUTN_{TeNB}$)

This process is same as we have mentioned in the Step **4c**, upon receive of the message, the TeNB sends a message for the completion of the HO request acknowledgment at the TMME side. However, the TMME includes $AUTN_{TeNB}$ and it also calculates $K^{**}_{eNB_i}$.

5e-5g. $TMME \rightarrow SMME$, $SMME \rightarrow SeNB$, $SeNB \rightarrow MTCD_{leader}$: HO_Command ($AUTN_{TeNB}$)

The TMME sends HO command message in response to the acknowledgment of HO request message. The corresponding message carries $AUTN_{TeNB}$ to the $MTCD_{leader}$ via the SMME and SeNB to implement the HO. Next, the process switches again to Step 6.

Step 6. $MTCD_{leader} \rightarrow MTCD_{G1-i}$: HO_Command ($AUTN_{TeNB}$)

When $MTCD_{leader}$ receives $AUTN_{TeNB}$, it forwards $AUTN_{TeNB}$ to all group members in G1 by sending the broadcast message.

Step 7. $MTCD_{G1-i} \rightarrow TeNB$: HO_Confirmation

Each $MTCD_{G1-i}$ will recalculate $MAC_{TeNB}=H(GTK^{*}_{G1} \| ID_{TeNB} \| r_{TeNB} \cdot P)$ and also confirms that whether MAC_{TeNB}' equals to MAC_{TeNB} or not which arepresented in $AUTN_{MME}$. If both MAC_{TeNB}' are not equal, the TeNB sends a prompt message of request failure to authorize the MTCD in the group. Otherwise, every $MTCD_{G1-i}$ derives the new session key $K^{**}_{eNB_i} = KDF(K^{*}_{eNB_i} \| r_{MTCD_{G1-i}} \cdot (r_{TeNB} \cdot P))$. Finally, each $MTCD_{G1-i}$ sends HO confirmation message to the TeNB to complete the HO. Additionally, the session key $K^{**}_{eNB_i}$ creates a channel forthe subsequent secure communication between each MTCD and TeNB. In conclusion, the full handover authentication of MTCDs in the group is completed.

V. SECURITY ANALYSIS

We investigate the robustness of our proposed scheme in this section. By the security and formal verification analysis using Pro-Verify tool against highly vicious network attacks which leads to network instability and vulnerability. The proposed scheme can meet the security challenges against well-known attacks in the LTE-A network.

5.1 Analysis by Security Aspects

1) *Secure Mutual Authentication:* In our scheme, MTCD and MME can achieve a robust and secure mutual authentication through the EPS-AKA protocol or the scheme [10]. However, at the end of this phase, the session key $K^{MTCD_{G1-i}}_{ASME}$ is used to enable a secure channel for the communication between individual MTCD and MME accordingly. Furthermore, the MME computes the K_{eNB_i} and GTK_{G1}, after sends them to the SeNB for the next process. In group-based handover authentication phase, we use aggregate message authentication codes (AMAC) and the keys K_{eNB_i} for the validation between TeNB and MTCDs in the G1group.Furthermore, every MTCD in G1 first uses K_{eNB_i} to compute $K^{*}_{eNB_i}$ which is used by the TeNB and individual MTC member in the handover group. Then each MTCD computes, and send them to the

$MTCD_{leader}$. After receipt of the $MAC_{MTCD_{G1-i}}$ $MTCD_{leader}$ computes MAC_{G1} by aggregating all $MAC_{MTCD_{G1-i}}$ in the G1.Only the legitimate $MAC_{MTCD_{G1-i}}$ can aggregate the signature, if the invalid $MAC_{MTCD_{G1-i}}$ exists in the MAC_{G1}, is considered as null and void. As we have described in the step 3b (section 2.3), TeNB can confirm the MAC_{G1} , confined in $AUTN_{G1}$ by enabling the key of $K^{*}_{eNB_i}$ to recalculate, to filter some illegitimate MTCDs. Furthermore, TeNB also calculates MAC_{TeNB} by using the group temporary key GTK_{G1}, which is proved to be a shield against illegal access of the MTCDs in the group. In step 7 (in subsection 2.3), as we can see, each MTCD recalculates $MAC_{TeNB}{}'$ by using GTK_{G1}. Consequently, every MTCD and TeNB achieve mutual authentication.

2) *Resistance Against Replay Attack:* Replay attacks can be prevented by adding random numbers or timestamps to messages. In our scheme, $MTCD_{G1-i}$ and TeNB generate the random numbers $r_{MTCD_{G1-i}}$, and r_{TeNB} for the authentication parameters. Since randomly generated numbers are used differently in every iteration of the verification process. In the case of vandalism of the values, the masquerader still cannot copy or overwrite the messages by using these same values in a new authentication process. Thus, it is difficult for the masquerader to accomplish a replay attack, due to the fact all of the values are synchronized freshly derived and primarily based on these values to resist against replay assaults.

3) *Secure Anonymity protection:* By the use of a pseudonymin each handover authentication process, $MTCD_i$ randomly selects an unlikable pseudo-identities $ID^{j}_{MTCD_i}=ID_{MTCD_i}\oplus H_1(R_j \cdot PK)$. By this $MTCD_i$ can constantly change its pseudo-identity to generate $MAC_{MTCD_{G1-i}}$, therefore, it makes sure that the real identities of every MTCD should be secret to achieve the anonymity from normal message receivers. On the other hand, though an attacker succeeds to get the numerous pseudo-identities of the desired MTCD, it is far difficult for the adversary to get related data/information from those pseudonyms. Consequently, only HSS/AuC is in charge of trace the actual identity of $MTCD_i$ by calculating $ID^{j}_{MTCD_i} \oplus H_1(R_j \cdot PK) = \{ID_{MTCD_i} \oplus H_1(R_j \cdot PK)\} \oplus H_1(R_j \cdot PK) = ID_{MTCD_i} \oplus \{H_1(R_j \cdot PK)$. Thus, our proposed scheme also provides MTCD traceability (i.e., provisional privacy preserving traceability) which is proving to be a shield against numerous privacy preserving attacks by the malicious MTCD.

4) *Resistance to Impersonation Attack:* When a masquerader tries to impersonate the MTCD of a group to illegally access the network. Hence, He/She cannot forge the real identity, MAC_{MTCD_i} and authentic MAC_{MTCD_i} .However, they also do not know the session key $K_{ASME}^{MTCD_{G1-i}}$. The TeNB confirms the valid key by verifying MAC_{G1}. Even if an MTCD member of handover group tries to impersonate another group member's $K^{**}_{eNB_i}$ key, it cannot because of the pseudonym. Meanwhile, when an adversary impersonates TeNB, it cannot personify or generate a legitimate group temporary key GTK^{*}_{G1}, without a valid MAC_{TeNB}. MTCD can distinguish it by confirming the MAC_{TeNB} . However, the session keys $K^{**}_{eNB_i} = KDF(K^{*}_{eNB_i} \| r_{MTCD_{G1-i}} \cdot (r_{TeNB} \cdot P))$ are dynamically generated from the secret values, K_{eNB_i} and. By our scheme, we can secure from Man-in-the-Middle (MitM) attack and resist an adversary from obtaining the session keys by using the public values from communication channel between each MTCD and the eNBs.

5) *Resistance to Man-in-the-middle(MITM) Attack:* In our scheme due to severity and the intricacy of the elliptic curve algorithm, an adversary cannot forge and evaluate $r_{MTCD_{G1-i}}, r_{TeNB} \cdot P$ according to the intricacy of $r_{MTCD_{G1-i}}$ and $r_{TeNB} \cdot P$ .Thought, he/she can get full access to all exchange messages over the communication channels, in spite of that, our scheme can resist the vulnerable attack like MitM. On the other hand, SEGHAS generates a new session key $K^{**}_{eNB_i}$ at target side, which performs the function to scramble payloads between MTCDs in G1 handover and TeNB. Hence, $K^{**}_{eNB_i}$ can thwart communication from being eavesdropped and modified.

6) *Authentication Signaling overhead resistance:* The signal congestion and authentication in our proposed scheme conceivably reduced. In an effort to avoid authentication and signaling overhead, a vast quantity of access request messages $^{MAC}MTCD_{G1-i}$ from a G1 handover group are sent to $MTCD_{leader}$, where all messages are aggregated into a single message .As a result, $MTCD_{leader}$ just sends a single message to TeNB without sending extra messages. Therefore, SEGHAS can be proved to reduce the authentication of signaling overhead from eNBs at a large extent. Additionally, by using aggregation technique, the TeNB can verify all MTCDs in G1 simultaneously. By the scheme, a crowd of signaling flow can be reduced to the large extent. With the help of AMAC technique, the TeNB can verify a group of MTCDs. Hence, it can ease the signal congestion of the TeNB and safeguard the security of MTCD group without any hindrance of the handover requirements. And the bulge in the process of message authentication request from the MTCDs in the G1 will be sum up in a single message, then perform handover by single message to the TeNB.

5.2 Discussion

Table II shows the evaluation of the security aspects; from which we can conclude that our scheme is more secure and efficient than the other three schemes.

Table: II Comparison of Security Aspects

Comparison of Security Aspects	*Cao J [17]*	*EPS-AKA 18]*	*Haddad Z [19]*	*Our Scheme*
Privacy Protection	N	N	N	Y
Resistance to Replay Attack	Y	N	Y	Y
Mutual Authentication	Y	Y	N	Y
Resistance to Impersonation Attack	Y	N	Y	Y
Resistance to MitM Attack	Y	N	Y	Y
Authentication Signaling Congestion Avoidance	N	N	N	Y
Authentication a group of devices Simultaneously	N	N	N	Y

5.3Security Analysis by Using Pro-Verif Tool

Security is the paramount issue in the LTE-A network. By using the Pro-Verif tool we analysis the security attributes and the robustness of our scheme. The formal specification of Pro-Verif tool [20] is accomplished to measure the robustness of security protocols in our scheme, such as authentication of MTCDs, confidentiality of user identities and the secrecy of session keys. We run the Pro-Verif tool to get the experimental results on Intel(R) Core i5-3470 CPU @ 3.20GHZ (4 CPUs) system.

Firstly, after completing the registration process to the network, MTCDs form a group based on certain principles as defined in G1 to attain the initial authentication process between MTC handover group and MME. We describe the further steps as follows:

1) According to the results, the event new kasme: is used for shared key generated by MTC and HSS and MME aggregates the shared key and session key between i-th MTCD and SeNB.

2) Event bit-string: Authenticates the GK and GTKG1 to the MME.

3) Term query event: All MTCD devices perform handover authentication process in the group handover G1 during mobility from SeNB to the TeNB simultaneously.

4) Query inj-event(termTeNB): This event describes that all MTCDs performs group based handover at the target side.

5) Event term bit-string: Authenticates GTKG1 and G1 handover group.

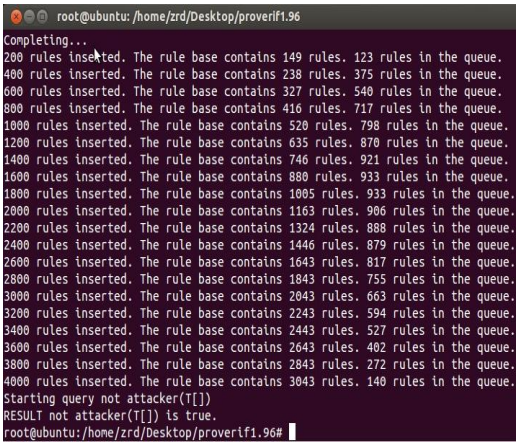

Figure 3. Mutual Authentications of MTCDs

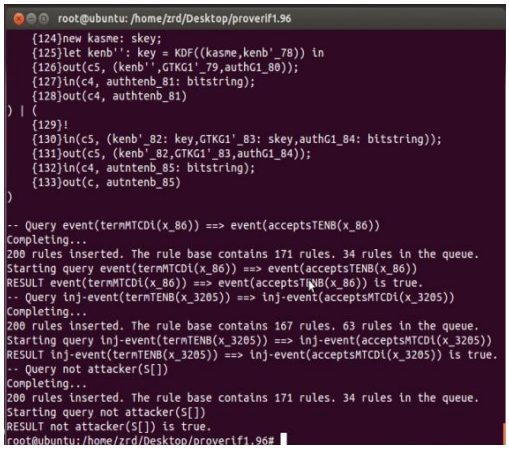

Figure 4. MTCDs Confidentiality

The formal verification using Pro-Verif tool, the verification results are shown in figure 3 and 4. In figure 3 we can see that event(termMTCDi(x_86)) ==> event (accepts TeNB(x_86)) and inj-event (termTeNB(x_3205)) ==>inj-event (accepts MTCDi(x_3205)) both queries are true. We can assume that the verification results are successful and secure group based handover authentication between MTCDs in G1 and TeNB.

Secondly, to ensure the verification and secrecy of the session key ($\kappa_{ASME}^{MTCD_{G1-i}}$) to encrypt the message [s]. The purpose of the use of session knows whether the adversary tries to eavesdrop the message. In figure 4 we can see that the query Result, not attacker (T []) in the figure is true, it means there is no adversary attack to eavesdrop the message.

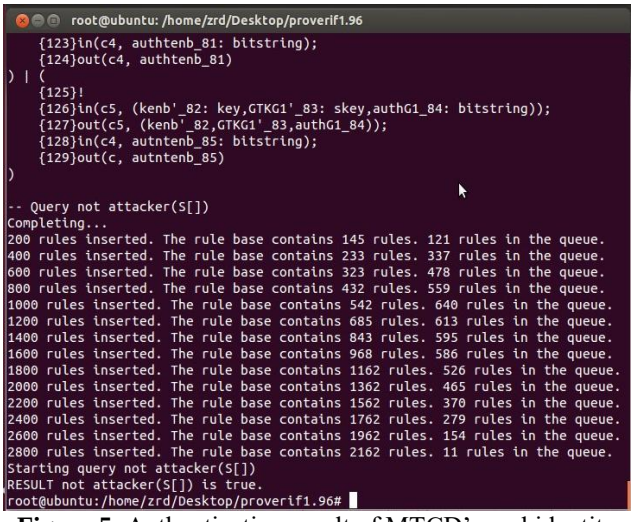

Figure 5. Authentication result of MTCD's real identity

Finally, in order to verify the confidentiality and secrecy of the MTCD's real identity, it is not easy to evaluate that whether or not the real identity is being attacked by the adversary. Thus, instead of real identity, we use session key for the encryption of messages. In figure 5 we have shown that result, not attacker (s []) is true. The result shows that no attacker can temper with the real identity. Meanwhile, even if the masquerader gets successful in getting a pseudonym, he/she does not know the real identity of the MTCD. Hence, we can use the pseudonym to achieve the security against malicious attacks. In concluding remarks, we can say that using formal verification by the Pro-Verif tool in our scheme, we can achieve the secure and efficient group based handover authentication between MTCDs in the G1.

5.3. Performance Evaluation

In this section, we analyze the performance of our proposed scheme by comparing with the current LTE-A group based handover scenario in [17], [19] in contrast of signaling cost, communication cost, and computational cost. We assume that n number of MTCDs perform the mobility from SeNB to the TeNB at the same time. In contrast, we have compared our scheme with the current LTE-A handover mechanism according

to the number of signaling messages. By comparing signaling cost with existing schemes is illustrated in table III and Figure 6,7. Moreover, the signaling cost as compare to current LTE-A schemes in [17], [19] is far better than in our scheme, according to the handover process.

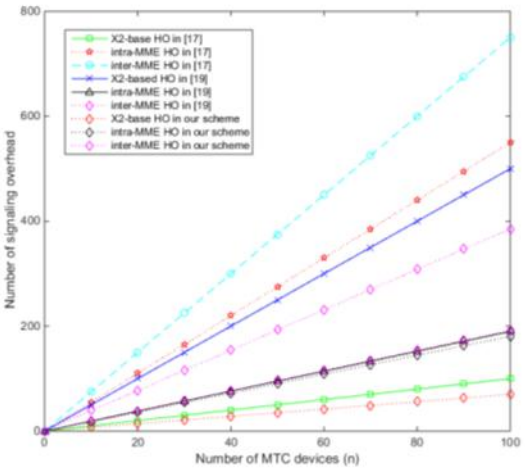

Figure 6. Signaling Cost

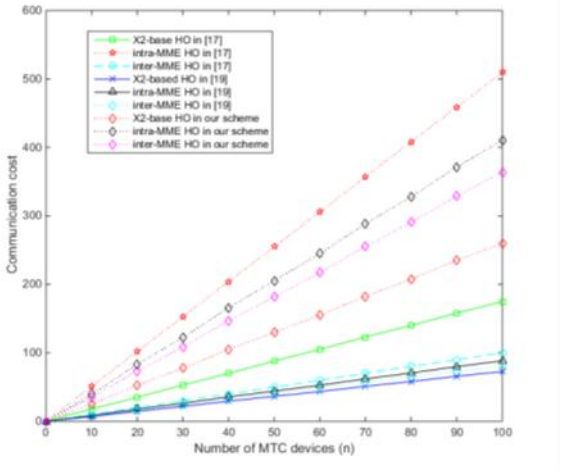

Figure7. Communication Cost

On the other hand, we assume that the communication cost between MME and eNBs can be one unit. However, the cost between MTCD and eNB represents the e cost between eNBs represents δ and MME represents η cost correspondingly. Meanwhile, the range of MME is far away from the eNB, we set the average cost of the MME as e between the range from $0 < e < 1$. Specifically, the costs of δ and η is comparatively lower than 1. The comparison of communication cost and signaling compared with current LTE-A schemes [17], [19], has been shown in the fig.6,7 and table III.

Table: III Comparison with LTE-A Schemes

HO Scenario	***Signaling Cost***		***Communication Cost***	
	LTE-A Schemes [17] ,[19]	Our Scheme	LTE-A Schemes [17] ,[19]	Our Scheme
Intra-MME HO	$9\eta, 6\eta$	$3\eta + 5$	$5e + 5\delta = \eta$	$3e\eta + 5\delta$
Inter-MME HO	$6\eta, 8\eta$	$3\eta + 6$	$4e + 7\delta = \eta$	$3e\eta + 6\delta$
X2-Based HO	$5\eta, 7\eta$	$3\eta + 3$	$3e + 2\delta = \eta$	$3e\eta + 2\delta$

We evaluate the data as the cost between MTCD and eNB is $e = \delta = 0.6$ a unit, however, the cost between MME and eNB is $\eta = \delta = 0.4$ a unit, which is lower than 1.The performance and analysis results show that communication cost and signaling cost in our scheme is far better than the LTE-A schemes. Moreover, the comparison of computational overhead with LTE-A schemes is large in our scheme than that of LTE-A. In contrast, our scheme has an advantage of pseudo-identity, avoidance over signaling congestion, user anonymity, fast handover and so on, while LTE-A schemes are a lack of it.

VI. CONCLUSION

MTC is becoming an evolutionary in the new generation of mobile communication system, it has gained more ascendancy in short span of time by the standardization with 3GPP in the LTE-A networks. Though, there is still need to achieve some challenging task in terms of security and the authentication of the mass of MTCDs during the mobility scenario. The authentication of these mass of MTCDs leads to severe signaling congestion over the LTE-A and core network. In this paper, we have proposed a secure and efficient group based handover authentication for M2M in LTE-A network. Our proposed scheme can simultaneously authenticate the group handover of MTCDs by using AMAC technique, it is also vulnerable to security threats, such as MitM and impersonation attacks by using the Pro-Verif tool. The analysis and performance results show that our scheme attains tremendous results in reducing the communication cost and signaling cost over the LTE-A and core networks.

REFERENCES

[1] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on RAN Improvements for Machine-type Communications (Rel 11), 3GPP TR 37.868 V12.0.0, Sept. 2011.

[2] I. F. Akyildiz, D. M. Gutierrez-Estevez, R. Balakrishnan, E. Chavarria Reyes, LTE-Advanced and the evolutionto Beyond 4G (B4G) systems, Physical Communication, Vol. 10, pp.31-60, Mar. 2014.

[3] Cao, Jin, et al. "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks." Communications (ICC), 2015 IEEE International Conference on. IEEE, 2015.

[4] Z.M. Fadlullah, M.M Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, Toward intelligent machine-to-machine communications in smart grid, IEEE Communications Magazine, Vol.49, No.4, pp.60-65, Apr. 2011.

[5] Cao, Jin, Hui Li, and Maode Ma. "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks." Communications (ICC), 2015 IEEE International Conference on. IEEE, 2015.

[6] Jin, C. A. O., and L. I. Hui. "Handover authentication between different types of eNBs in LTEnetworks." The Journal of China Universities of Posts and Telecommunications 20.2 (2013): 106-112.

[7] C. Lai, H. Li, R. Lu, R. Jiang, X. Shen," SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," 2014 IEEE International Conference on Communications (ICC), Jun. 2014, pp.1011-1016.

[8] Forsberg, D., 2010. LTE key management analysis with session keys context. Computer Communications, 33(16), pp.1907-1915.

[9] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (EUTRAN) access (Rel 13), 3GPP TS 23.401 V14.1.0, Dec. 2014.

[10] Cao, J., Ma, M., Li, H., Zhang, Y., & Luo, Z. (2014). A survey on security aspects for LTE and LTE-A networks. IEEE Communications Surveys & Tutorials, 16(1), 283-302.

[11] Han C, Choi H. Security Analysis of Handover Key Management in 4G LTE/SAE Networks[J]. IEEE Transactions on Mobile Com puting, 2014, 13（2）: 457-468.

[12] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects of Machine-Type Communications (Rel 12), 3GPP TR 33.868 V12.1.0

[13] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (EUTRAN) access (Rel 13), 3GPP TS 23.401 V13.1.0, Dec. 2014.

[14] Fu A, Zhang Y, Zhu Z, et al. An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network. Computers & Security 2012; 31(6):741–749.

[15] Cao J, Ma M, Li H. A group-based authentication and key agreement for MTC in LTE networks. In Proc.IEEE GLOBECOM'12. Anaheim: America, 2012; 1017–1022

[16] Lai, Chengzhe, et al. "A novel group access authentication and key agreement protocol for machine-type communication." Transactions on emerging telecommunications technologies 26.3 (2015): 414-431.

[17] Cao J, Li H, Ma M, et al. A simple and robust handover authentication between HeNB and eNB in LTE networks[J]. Computer Net works, 2012, 56（8）: 2119-2131.

[18] 3rd generation partnership project; technical specification group services and system aspects; service requirements for the evolved packet system (EPS); (release 13); 3GPP TS 22.278 V13.2.0, Aug. 2014.

[19] Haddad, Zaher, et al. "Secure and efficient uniform handover scheme for LTE-A networks." Wireless Communications and Networking Conference (WCNC), 2016 IEEE. IEEE, 2016.

[20] Blanchet B, "ProVerif: cryptographic protocol verifier in the formal model", URL http://prosecco.gforge.inria.fr/personal/bblanche/proverif/.