A Group-based Security Protocol for Machine Type Communications in LTE-Advanced

Daesung Choi
Computer Science and Engineering
Sungkyunkwan University
dschoi@hit.skku.edu

Sungdae Hong
Computer Science and Engineering
Sungkyunkwan University
sdhong@hit.skku.edu

Hyoung-Kee Choi*
Computer Science and Engineering
Sungkyunkwan University
meosery@skku.edu

***Abstract*—We propose Authentication and Key Agreement (AKA) for Machine Type Communications (MTC) in LTE-Advanced. This protocol is based on an idea of grouping devices so that it would reduce signaling congestion in the access network and overload on the single authentication server. We verified that this protocol is designed to be secure against many attacks by using a software verification tool. Furthermore, performance evaluation suggests that this protocol is efficient with respect to authentication overhead and handover delay.**

I. Introduction

The Machine Type Communications (MTC) enables millions of MTC devices to communicate with each other [1]. We expect that this new technology will realize new applications that are not feasible through human-to-human (H2H) communication. We propose, as part of a security remedy, a group-based authentication and key agreement that operates by leveraging group information to authenticate a number of devices in a group efficiently and effectively without any needs of excessive authentication signaling.

II. Proposed Protocol

Evolved Packet System (EPS)-Authentication and Key Agreement (AKA) is a security protocol for authentication and key management in 4G LTE-Advanced. When a group of n MTC devices authenticate themselves to a core network simultaneous authentication of individual MTC devices can burden signaling on the network. Its efficiency drops significantly because of repetitive invocation of costly authentication signaling.

A. System Initialization Phase

MTC devices belonging to the same MTC user or sited in the same area can easily be grouped for management, control, and charging operations [2]. The Home Subscriber Server (HSS) first generates a unique group key GK per group and identifies a group by International Mobile Group Identity (IMGI). Next, the HSS builds a binary tree and MTC devices are located in a leaf node as shown in Fig. 1. Each node in the tree has a different secret value $SECRET_i$. Two hash functions HR and HL, respectively, are used to derive secret values of left and right children from a parent's secret value. Hence, one can always derive all secret values of descendent nodes if one know the nodes' secret value. A member located in the leaf node knows all secret values in the tree except for those restricted secret values. The restricted secret values (RS) of nodes are located in the upward path to a root from its own node. For instance, the restricted values $member_4$ in Fig. 1 are

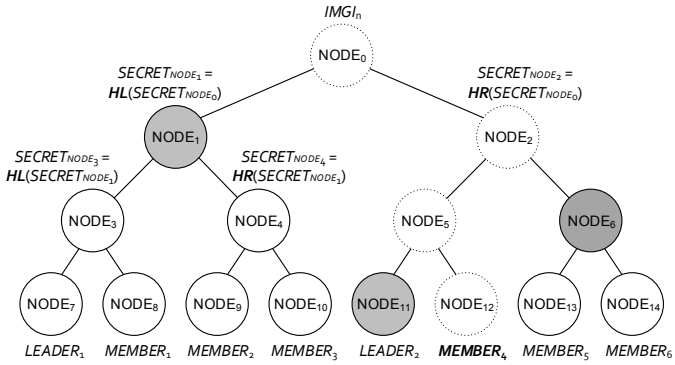

Fig. 1. An illustration of binary tree to manage the secret keys. Secret values of nodes with dotted lines are restricted to member$_4$.

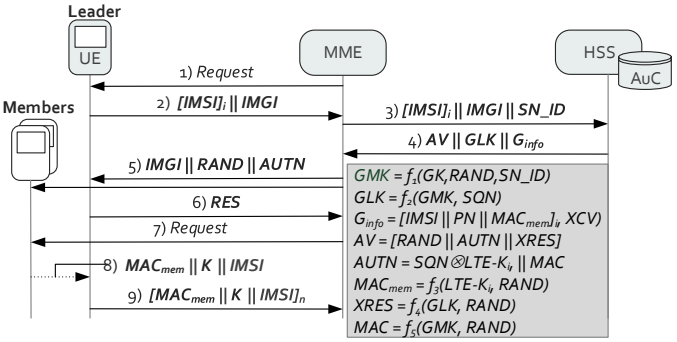

Fig. 2. Nine messages for the group-based mutual authentication between MTC devices and the core network.

$SECRET_{NODE_{12}}$, $SECRET_{NODE_5}$, $SECRET_{NODE_2}$ and $SECRET_{NODE_0}$. Finally, $IMGI$, GK, RS, HR, HL, one hash function H, and different positive prime number PN_i are stored in Universal Integrated Circuit Card (UICC) of MTC device by the service provider.

B. Mutual Authentication Phase

By our design, a set of leaders are included among members to represent the group to the core network. In order to avoid collisions as a result of multiple initiations at the same time, leaders are instructed to wait for a random amount of time before they can send the first message. If any leaders hears the first message sent by another leader the hearing leader postpones sending until the current procedure is complete with success.

The chosen leader and the HSS authenticate mutually as shown in Fig. 2. The leader sends the second message including their own identity, members' identity $[IMSI]_i$ and group identity $IMGI$ to the Mobility Management Entity

* Hyoung-Kee Choi is a corresponding author.

(MME), where $1 \le i \le n$. The MME adds its own identity $SN - ID$ and passes to the HSS. The HSS checks the third message first. Next, it generates a random number $RAND$ and sequence number SQN and computes three parameters: authentication vector AV, group information G_{Info} and group leader key GLK. Then, it includes three parameters in the fourth message and sends to the MME. The MME sends the fifth message to the MTC devices via a broadcast channel in the LTE downlink channel.

All group members should overhear this broadcasting message. Each member can locally compute group master key GMK and the leader can compute GLK using their own authentication key $LTE - K_i$. The leader and members can authenticate the network's legitimacy via the message authentication code MAC and leader sends the sixth message to the MME. The MME authenticates the leader if response value RES and expected response value $XRES$ are the same and sends the seventh message to authenticate members. Member i computes $K = KDF(GMK \oplus LTE - K_i)$ and $MAC_{Mem} = KDF(LTE - K_i, RAND)$ and sends the eighth message to the leader. The leader collects the eighth message from members in the group and sends the ninth message to the MME. The MME first validate the members' legitimacy via the MAC_{Mem}. If members are normal, it computes confirmation value $CV = K_1 mod PN_1 = K_2 mod PN_2 = \cdots = K_i mod PN_i$ and authenticates if XCV equals to CV.

C. Group Key Update and Session Key Agreement Phase

Once mutual authentication is successful, the HSS assigns the MME to a leaf node in the tree and sends a joining message to the MME. This joining message contains the MME's position in the tree and is encrypted with GMK. The MME sends this joining message to the group member by broadcasting. All members in the group and the HSS locally extract the MME's $SECRET_i$ and update the group key using an equation $GK' = H(GK \oplus SECRET_i)$. When a group changes an anchor point of MME due to mobility the old MME simply leaves the group. The HSS updates the structure of the tree to reflect the change caused by the old MME's departure and joins new MME to an unoccupied leaf node in the tree. All members update the group key using old MME's $SECRET_i$.

The MME and each member locally compute common $SECRET_i$ within its own RS and extract the session key $SK = H(SECRET_k \oplus \cdots \oplus SECRET_i)$, where $1 \le k \le i$.

III. Evaluation

Firstly, we verify the security of our proposed protocol by using the ProVerif [3]. We only consider verification procedure between MTC devices and the MME. This is because (1) communication between the MME and the HSS is secure, (2) authentication procedure and session key agreement are proceeded between MTC devices and the MME. The verification results inform us that authentication of leader (or member) to MME and authentication of MME to leader (or member) hold. In addition, the attacker has not been able to obtain the secret value.

Next, we evaluate the authentication overhead in terms of communication cost and computation delay by the network programming. We conducted the experiments with Crypto++ library and JavaCard development kit to measure the elapsed time of cryptographic operations. We compared the authentication overhead of proposed protocol with EPS-AKA as shown in Fig. 3. When the number of MTC devices was one hundred, the authentication overhead of our proposed protocol was about 24.5 percent lower than the EPS-AKA.

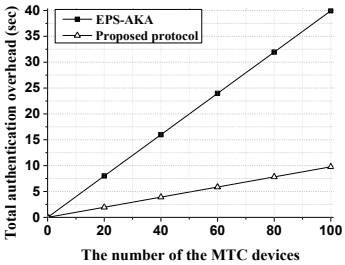

Fig. 3. Comparison of total authentication overhead between proposed protocol and EPS-AKA.

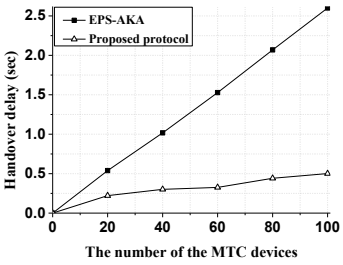

Fig. 4. Comparison of handover delay between proposed protocol and EPS-AKA.

Further, we simulate the handover delay by using the Network Simulator-3 (NS-3) version 3.16 [6] with LTE module [7]. We ran the simulation 1,000 times and excluded the 5% of ceiling value and minimum value (i.e., 50 times) to reduce the consequences that outliers might affect. We measured the handover delay by calculating $t_{target-end} - t_{source-start}$ at every handover, where $t_{target-end}$ is the time instance of the handover confirm message being received at the target eNB, and $t_{source-start}$ indicates that the measurement report is enqueued at the MTC device's queue. We assume that the leader can send the security context of members to the source eNB, and the target eNB can send the handover message to members by broadcasting. As shown in Fig. 4, the handover delay of our proposed protocol was about 19.3 percent lower than the EPS-AKA when the number of MTC devices was one hundred.

IV. Conclusion

We have proposed a secure and efficient group-based authentication protocol. Software verification by using ProVerif has shown that proposed protocol is secure against a variety of attacks. In addition, the performance evaluation in terms of authentication overhead and handover delay also shows that proposed protocol is more efficient than EPS-AKA.

References

[1] 3GPP TR 22.868 ver. 8.0.0, "Study on Facilitating Machine to Machine Communications in 3GPP Systems (Release 8)," May 2007.

[2] 3GPP TR 33.868 ver. 0.8.0, "Security aspects of Machine-Type Communications (Release 11)," May 2012.

[3] ProVerif, *available at* http://prosecco.gforge.inria.fr/personal/bblanche/proverif/

[4] The Network Simulator (NS-3), *available at* http://www.nsnam.org

[5] G. Prio, N. Baldo and M. Miozzo, "An LTE module for the ns-3 network simulator," International ICST Conference on Simulation Tools and Techniques (SIMUTools), Mar. 2011.