Toward Secure Large-Scale Machine-to-Machine Communications in 3GPP Networks: Challenges and Solutions

Supporting a massive number of machine-to-machine (M2M) communications devices has been considered an essential requirement for mobile operators. Meanwhile, cyber security is of paramount importance in M2M as all applications involving M2M cannot be widely accepted without security guarantee.

Chengzhe Lai, Rongxing Lu, Dong Zheng, Hui Li, and Xuemin (Sherman) Shen

Abstract

With trillions of machines connecting to mobile communication networks to provide a wide variety of applications, supporting a massive number of machine-to-machine (M2M) communications devices has been considered an essential requirement for mobile operators. Meanwhile, cyber security is of paramount importance in M2M as all applications involving M2M cannot be widely accepted without security guarantees. In this article we focus on the standardization activities of 3GPP, especially group-based security for large-scale M2M communications in 3GPP networks. We first introduce the main components of the machine-type communication (MTC) security architecture. Then we discuss several major challenges for group-oriented secure M2M communications in 3GPP systems, i.e. authentication signalling congestion and overload, and group message protection. Specifically, we identify the performance issues of authentication signalling congestion and overload in no/low mobility scenarios, and propose three group access authentication and key agreement protocols. Moreover, several 3GPP candidate solutions for group message protection are introduced. Finally, we present key issues and research directions related to group-based secure M2M communications, including security, privacy, and efficiency in mobility scenarios of MTC, and flexible and efficient group key management.

COMMUNICATIONS STANDARDS

Introduction

Machine-to-machine (M2M) communications is an emerging technology empowering full mechanical automation (e.g. in the smart grid, smart transportation, smart city, etc.), and its rapid development is changing our living styles vigorously [1]. M2M technology is drawing overwhelming attention in the standardization and industry areas. Many standards forums and organizations, including the Institute of Electrical and Electronics Engineers (IEEE), the European Telecommunications Standards Institute (ETSI), the Third Generation Partnership Project (3GPP), the China Communications Standards Association (CCSA), oneM2M, etc., have engaged in M2M standard development.

To take full advantage of the opportunities created by a global M2M market over cellular networks, 3GPP[1] has initiated their working groups to facilitate such applications through various releases of their standards [2]. So far, much research effort has focused on the MTC, such as subscription control and network congestion/overload control [3], potential issues on the air interface, including physical layer transmissions, the random access procedure, and radio resource allocation supporting the most critical QoS provisioning [4], mobility management [5], green, reliability, and security of M2M communications [6], etc. As a cutting edge technology for next generation communications, M2M communications is undergoing rapid development and inspiring numerous applications. However, all applications involving M2M cannot be widely accepted without security guarantees. In addition, to support large-scale M2M communications, the 3GPP mobile operator must accommodate its network to support a large number of MTC devices. Therefore, achieving secure large-scale machine-to-machine networking will be a challenge issue in the near future.

In this article we cover some of the standardization activities of 3GPP, focusing especially on the problem of group-based security for large-scale M2M communications in 3GPP networks. First, to address the problems of authentication signaling congestion and overload, we define three types of performance issues in no/low mobility scenarios. Then we propose three group access authentication and key agreement protocols for M2M in 3GPP networks to address them. Second, to solve the key issues in the group based feature (i.e. group based messaging, group based charging optimizations, group based policy control, and group based addressing and identifiers, etc.), several candidate solutions of group message protection are given from the 3GPP point of view.

The remainder of this article is organized as follows. We present the main components of the MTC security architecture. We then discuss several major challenges for group-oriented secure M2M communications in 3GPP systems, i.e. authentication signalling congestion and overload, and group message protection. Furthermore, we introduce new solutions to congestion and overload control for authentication signalling, and provide a summary of the solutions, agreed within 3GPP SA2, for group message protection. Finally, we present potential research directions and conclude the article.

Security Architecture

Figure 1 [7] shows the security architecture for MTC connecting to the 3GPP evolved universal terrestrial radio access network (E-UTRAN) via the LTE-Uu interface. The security architec-

Chengzhe Lai and Dong Zheng are with Xi'an University of Posts and Telecommunications, Xidian University, and Chinese Academy of Sciences.

Rongxing Lu is with Nanyang Technological University.

Hui Li is with Xidian University.

Xuemin (Sherman) Shen is with University of Waterloo.

[1] In 3GPP standards, M2M communications is also named machine-type communication (MTC).

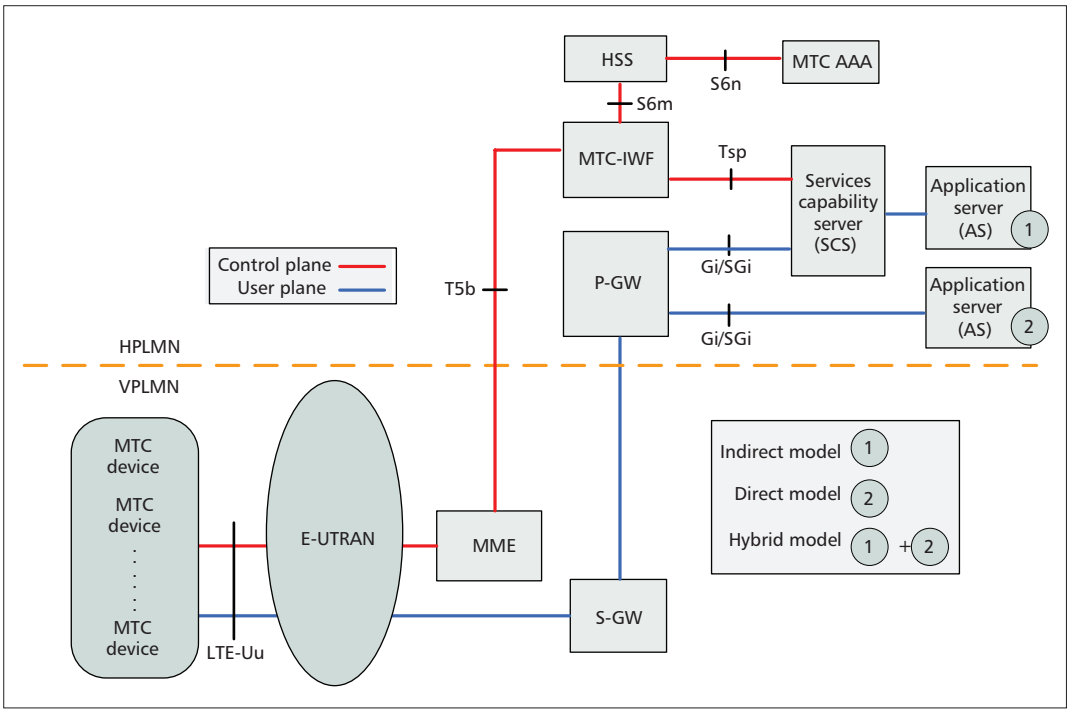

Figure 1. 3GPP security architecture for MTC.

To support large-scale M2M communications, the 3GPP mobile operator has to accommodate its network to support a large number of MTC devices. Therefore, achieving secure large-scale machine-to-machine networking is a challenge issue in the near future.

ture is considered in the roaming scenario, which includes the roaming network domain, i.e. the visited public land mobile network (VPLMN), and the home network domain, i.e. the home public land mobile network (HPLMN).

Table 1 summarizes the functions and descriptions of security related components and reference points of the MTC in this article. The main security related components and reference points of the MTC are introduced as follows.

Network Elements

Home Subscriber Server (HSS): Besides original functions (e.g. authentication and authorization), HSS supporting device triggering mainly supports the following functionalities:

- Stores and provides to MTC-IWF (and optionally to MTC-AAA) the mapping/lookup of the E.164 MSISDN (i.e. the mobile subscriber international ISDN/PSTN number) or external identifier(s) to IMSI (i.e. international mobile subscriber identity) and subscription information used by MTC-IWF for device triggering.
- Mapping of the E.164 MSISDN or external identifiers to IMSI.
- HSS stored "routing information" including serving node information if available for the MTC device (e.g. serving the MME identifier).
- Determines if an SCS is allowed to send a device trigger to a particular MTC device.
- Provides to MTC-AAA the mapping between IMSI and external identifier(s).

MTC Accounting, Authorization, and Authentication (MTC-AAA): To support translation of the IMSI to external identifier(s) at the network egress, an AAA function (MTC-AAA) is used in the HPLMN. The MTC-AAA may be deployed to return the external identifier(s) based on IMSI. Alternatively the MTC-AAA may be deployed as a RADIUS/diameter proxy between the packet data network gateway (P-GW) and the AAA server in the external packet data network (PDN).

MTC Interworking Function (MTC-IWF): The MTC-IWF is the functional entity that hides the internal network topology and relays/translates signaling protocols used over Tsp to invoke specific functionality in the public land mobile network (PLMN) (e.g. control plane device triggering). An MTC-IWF could be a stand-alone network element or a functional entity of another network element and always reside in the HPLMN.

Services Capability Server (SCS): The SCS connects to the 3GPP network via the MTC-IWF in the HPLMN to communicate with the MTC device. The SCS offers capabilities for use by one or multiple MTC applications. An MTC device can host one or multiple MTC applications. The corresponding MTC applications in the external network are hosted on one or multiple application servers (ASs).

Reference Points

The SCS provides an application programming interface (API) to allow different ASs to use the capabilities of the SCS.[2] Tsp is a 3GPP standardized interface to facilitate value-added services motivated by MTC (e.g. control plane device triggering) and provided by an SCS. The T5b interface is intended to provide optimized paths for device trigger delivery and possibly other services (e.g. small data service) to the MTC device. T5b was not standardized in 3GPP Rel-11. The S6m interface is used by the MTC-IWF to interrogate the HSS for mapping an MSISDN or external identifier to the IMSI, retrieving serving node information, and authorizing a device trigger to a particular MTC device. The S6n is an inter-

[2] The interface between SCS and AS is not standardized by 3GPP, but other standards development organizations (SDOs) such as the European Telecommunications Standards Institute (ETSI) Technical Committee on Machine-to-Machine Communications (TC M2M) are expected to standardize APIs.

Network elements	Function
HSS	Main database containing subscription-related information, which is used for authentication, authorization, and supporting device triggering.
MME	The mobility management entity for all mobility related functions and performing the authentication on behalf of the 3GPP core network.
MTC-IWF	The functional entity that hides the internal network topology and relays/translates security related signaling protocols, e.g. generates group key, encrypts, and signs the group message.
SCS	The entity connects to the 3GPP network via the MTC-IWF in the HPLMN to communicate with the MTC device, e.g. makes group message request.
MTC-AAA	The entity that supports translation of the IMSI to external identifier(s) at the network egress, or plays a "RADIUS/diameter proxy" role between the P-GW and the AAA server.
Reference points	**Description**
Tsp	Reference point used by an SCS to communicate with the MTC-IWF related control plane signaling.
T5b	Reference point used between the MTC-IWF and the serving MME.
S6m	Reference point used by the MTC-IWF to interrogate the HSS.
S6n	Reference point used by the MTC-AAA to interrogate the HSS.

Table 1. Summarizing table of security related network elements and reference points.

face between MTC-AAA and HSS to interrogate HSS for mapping IMSI to external identifier(s) and vice versa at the network egress.

Group-Oriented Secure M2M Communications

There exist several major challenges for group-oriented secure M2M communications in 3GPP systems, including: How to control authentication signalling congestion and overload when a large number of MTC devices want to securely access the 3GPP core network? How to securely and effectively protect group message distribution for the one-to-many or many-to-many communication paradigms?

Challenge 1: Congestion and Overload Control for Authentication Signalling

An MTC group is formed when a group of MTC devices are in the same area and/or have the same MTC features attributed and/or belong to the same MTC user. The MTC group should be identified uniquely across 3GPP networks. When a group of MTC devices want to access the network, they may send their access authentication requests toward the core network successively over a short period of time, or even at the same time, leading to congestion in the different nodes of the network, across the communication path. According to 3GPP TS 22.368 [8], the congestion could happen at different locations, as shown in Fig. 2.

Radio Network Congestion: Radio network congestion because of mass concurrent access authentication requests takes place in some MTC applications. One of the typical applications is tbridge monitoring with a mass of sensors. When a train passes through the bridge, all the sensors may access the network and transmit monitoring data almost simultaneously. The same thing happens in hydrology monitoring during times of heavy rain and in building monitoring when intruders break in. The network should be optimized to enable a mass of MTC devices in a particular area to access the network and transmit data almost simultaneously.

Core Network Congestion: Authentication signalling congestion in the core network is caused by a high number of MTC devices trying almost simultaneously:

- To attach to the network.
- To activate/modify/deactivate a connection.

In a 3GPP system supporting MTC applications, such an overload of the network can be caused by, for example, many mobile payment terminals that become active on a national holiday or by high numbers of metering devices becoming active almost simultaneously after a period of power outage. Also, some MTC applications generate recurring data transmissions at precisely synchronous time intervals (e.g. precisely every hour or half hour). Preferably, the 3GPP system provides the ability to the network operator and MTC user to spread the resulting peaks in the signalling traffic.

To support M2M communications, the 3GPP mobile operator must accommodate their network to support a large number of MTC devices, which can overload network resources and introduce congestion in the network at both the data and control planes. In fact, congestion may occur due to simultaneous authentication signalling messages from MTC devices. Unfortunately, the recent authentication and key agreement (AKA) protocols dedicated to the 3GPP evolved packet system (EPS), known as EPS-AKA [9], or for non-3GPP access networks (e.g. WLAN or WiMAX), known as EAP-AKA [10], cannot provide a group authentication mechanism. If a large number of MTC devices in a group need to access the network almost simultaneously, the traditional authentication protocols (e.g. EPS-AKA or EAP-AKA) will suffer from high signalling overhead, leading to authentication signaling congestion and decreasing the quality of service (QoS) of the network, because every device must perform a full AKA authentication procedure with the HSS, respectively. Because the traditional AKA protocols are not suitable for large-scale M2M communications, we consider designing new group-based access authentication and key agreement protocols.

Our Proposed Solution: Group-Based Access Authentication and Key Agreement

To facilitate system optimization, 3GPP defines a low mobility feature in M2M communications, which is suitable for MTC devices that do not move, move infrequently, or move only within a certain area. This feature enables the network operator to be able to simplify and reduce the frequency of mobility management procedures.

In such no/low mobility scenarios, the following three types of performance issues (PIs) are shown:

PI1: In some applications, a group of MTC devices may want to access the network and send their access authentication requests toward the core network successively over a short period of time. In such a case, if every device still performs a full authentication and key agreement (AKA) procedure with the HSS, the authentication signaling in the network increases. Meanwhile, the overload of HSS will increase because of frequently acquiring authentication vectors (AVs). Moreover, when these devices roam in a visiting domain, which is far from their home domain, the communication may suffer from high network access latency until the completion of authentication procedures by all MTC devices in the same group.

PI2: In some applications, the capabilities of each MTC device, such as computation, battery, and storage, are enough to support a public key cryptosystem. When a group of MTC devices want to access the network and send their access authentication requests toward the core network simultaneously, if every device still performs a full authentication and key agreement (AKA) procedure with the HSS, besides PI1, the authentication signalling congestion occurs at the HSS, MME, and evolved node B (eNB).

PI3: In some applications, a group of MTC devices may want to access the network and send their access authentication requests toward the core network simultaneously. Besides PI2, the capabilities of each MTC device, such as computation, battery and storage, are not enough to support a public key system and thus the symmetric key cryptosystem needs to be applied.

Accordingly, we present three group access authentication and key agreement protocols: GAAKA-1, GAAKA-2, and GAAKA-3.

GAAKA-1: First, the MTC devices form groups based on certain principles (e.g. they belong to the same application, are located within the same region, etc.), then the supplier provides a group identity (ID_{Gi}) and a group key (GK_i) to each group for authentication [11]. When a group of MTC devices want to access the network successively over a short period of time, the first device performs a full AKA procedure and obtains a group temporary key (GTK) for all of the group members. Then the remaining devices in the group only need to perform a simplified AKA procedure with the MME locally without interacting with the HSS. Therefore, the authentication signaling between the MME and the HSS can decrease. Meanwhile, the overload of HSS will decrease as well. Especially when these devices roam in a visiting domain, the performance can be optimized significantly.

GAAKA-2: Similarly, the MTC devices form groups based on certain principles (e.g. they belong to the same application, are located within the same region, etc.), and then the identities of MTC groups (ID_{Gi}) are assigned to each group. Meanwhile, a group leader of MTC devices in the group ($MTCD_{leader}$) will be selected in advance. When each MTC device registers with the EPC, it contacts the key generate center (KGC), provides an identifier, and then receives its private key. Only the authenticated MTC devices can obtain the private keys from the KGC. The KGC can be integrated with the HSS, which has pre-established secure channels with the MME by using the NDS/IP security mechanism. By adopting the certificateless aggregate signature techniques [12], the $MTCD_{leader}$ can collect all signatures of members in the same group and aggregate them to a new signature SIG_{agg}. Then the $MTCD_{leader}$ sends SIG_{agg} to the network, and all members in the group can be authenticated at the same time. Moreover, the independent session key can be negotiated between the core network and each MTC device. Therefore, GAAKA-2 can significantly relieve authentication signalling congestion occurring at the HSS, MME, and eNB.

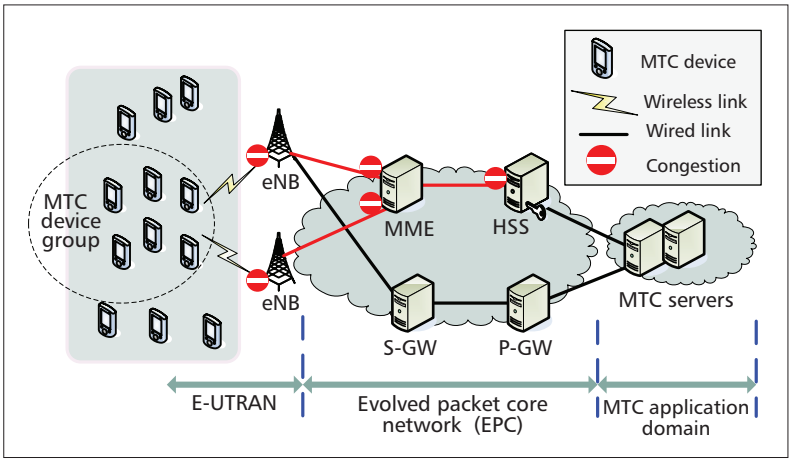

Figure 2. Authentication signalling congestion

GAAKA-3: Constrained by the computation, battery, and storage capabilities of the MTC device, GAAKA-2 may not be suitable for resource-constrained devices due to applying the public key system (e.g. certificateless aggregate signature techniques). Therefore, GAAKA-3 can be proposed by adopting the aggregate message authentication code (AMAC) techniques [13]. Similar to GAAKA-1, the supplier provides a group identity (ID_{Gi}) and a group key (GK_i) to each group for authentication. Each MTC device has a pre-shared secret key (K_{Gi-j}) with HSS when it is first registered in HSS. Meanwhile, a group leader of MTC devices in the group ($MTCD_{leader}$) will be selected in advance. Then the $MTCD_{leader}$ can collect all message authentication codes ($MAC_{indiv}s$) of members in the same group and aggregate them to a new message authentication parameter MAC_{agg}. Then, the $MTCD_{leader}$ sends MAC_{agg} to the network and all members in the group can be authenticated at the same time. Moreover, the independent session key can be negotiated between the core network and each MTC device. Therefore, GAAKA-3 cannot only relieve authentication signalling congestion occurring at the HSS, MME, and eNB, but also is suitable for resource-constrained devices. However, different from GAAKA-2, GAAKA-3 requires two additional authentication signalling exchanges between the MME and HSS.

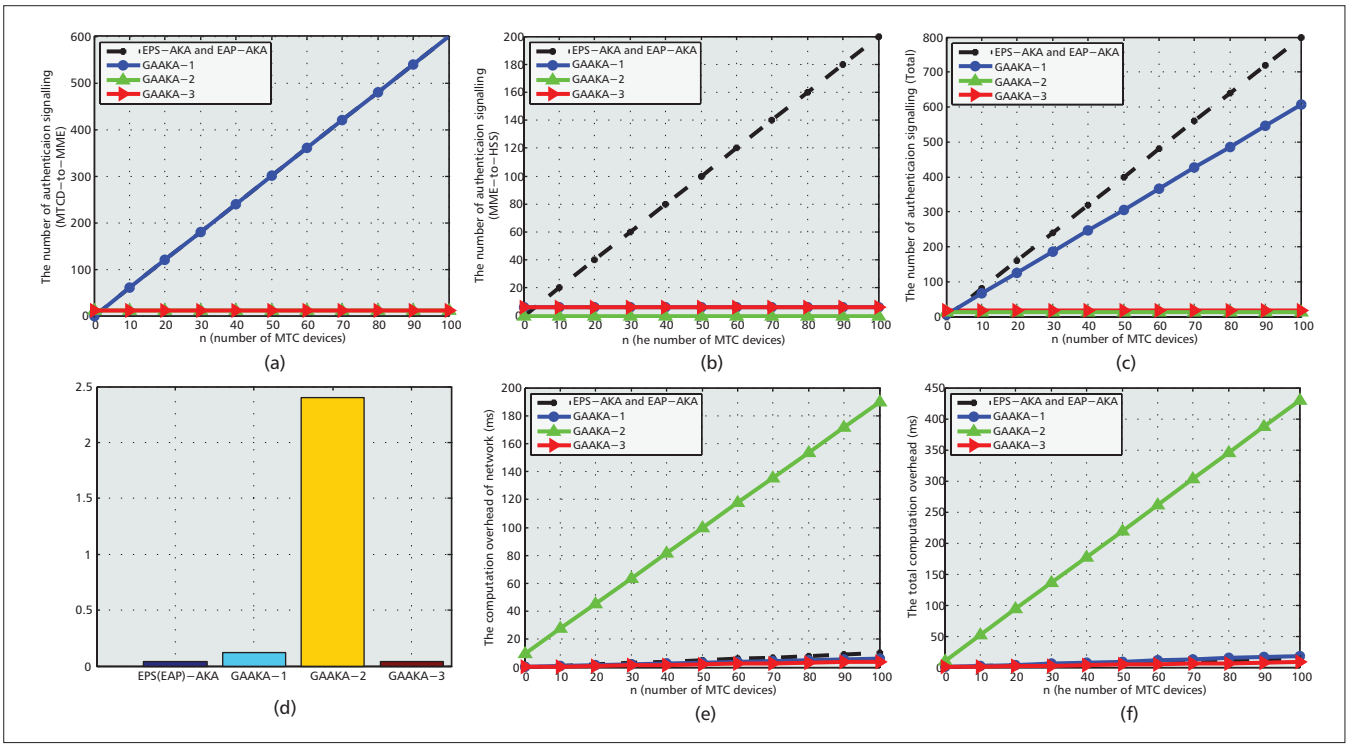

Figure 3. Performance comparison, (a–c): comparison of the authentication signalling; (d–f): comparison of the computation overhead (ms): a) authentication signalling between MTC device and MME (MTCD-to-MME); b) authentication signalling between MME and HSS (MME-to-HSS); c) total authentication signalling; d) computation overhead of each MTC device; e) computation overhead of network; and f) total computation overhead.

Analysis and Evaluation

We assume that there are n MTC devices forming m groups, obviously, $n > m$. We fix m, and plot Fig. 3. According to Fig. 3, we can see that the signalling of GAAKA-2 and GAAKA-3 do not change with n, and only depend on m; therefore, the authentication signalling incurred by GAAKA-1, 2, 3 are much less than that of EPS-AKA/EAP-AKA. Due to the use of symmetric cryptography (the hash operation T_{hash} takes 0.02 milliseconds (ms)), computation overheads of EPS-AKA/EAP-AKA, GAAKA-1 and GAAKA-3 are fairly small. Thus, we mainly consider the cost of the following operations, including a point multiplication T_{mul}, a pairing operation T_{pair}, and a map to point hash operation T_{mtp}. Generally, T_{mtp} takes the same time as T_{mul} ($= 0.6ms$) and $T_{pair} = 4.5ms$. The cost of XOR can be negligible. Therefore, we can see that GAAKA-1 and GAAKA-3 are more efficient than GAAKA-2 in computation, and are close to EPS-AKA/EAP-AKA.

Finally, a comprehensive comparison of design goals among several authentication and key agreement protocols is given in Table 2. We can find that except for GAAKA-2, other protocols are all designed based on the symmetric cryptosystem. Therefore, the computation overhead of GAAKA-2 is larger than that of other protocols. In addition, compared to the existing standard protocols, our proposed protocols have enhanced security properties, including privacy preservation, resistance to redirection attack, and resistance to MITM attack. Most importantly, different from the existing standard protocols, our proposed protocols support group access authentication, and can efficiently control authentication signalling congestion and overload.

Challenge 2: Group Message Protection for Secure M2M Communications

Recently, 3GPP SA2 has been working on the group based feature that includes the following key issues [14]: group based messaging, group based charging optimizations, group based policy control, group based addressing and identifiers, etc. To provide secure M2M group communications, 3GPP SA2 is currently considering the mechanism to distribute a group message from an SCS to those members of an MTC group located in a particular geographic area. According to the current architecture and solutions, MTC-IWF receives a group message from the SCS and forwards it to the target group of MTC devices. As group based messaging can significantly reduce the overhead of network resources, the corresponding session key establishment mechanism should be required to protect the group messages, which can be divided into two cases:

- For the MTC devices in one group, each device may need to communicate with the core network individually so an independent session key for each device may be needed.
- For the MTC devices in one group, the core network may need to distribute the same message (e.g. a trigger request) to those members of one MTC group as a same group session key is needed.

The first case has been discussed above, and we focus on the group message protection issue in this section.

If the broadcast message for a particular MTC group is not protected, then private information related to the particular group is revealed. Therefore, a mechanism should be provided to protect the confidentiality of the group message broadcasted for a particular group. However, confidentiality protection is subject to regional regulatory requirements. Group based messaging would be more prone to tampering and fake triggering attacks, if there is no integrity and replay protection provided by the core network or by the SCS. With a group message, multiple MTC devices can be triggered. Therefore, an unauthorized group message may cause a much more severe problem compared to what a trigger to a single MTC device can cause. Therefore, 3GPP has defined the following security requirements for group based messaging:

- The MTC-IWF should verify if the SCS is authorized to send a group message to a given MTC group.
- The core network should be able to distinguish a group message from other messages.
- The group messages that are distributed to the group of MTC devices should be integrity protected, replay protected, and confidentiality protected.
- Local group ID should not to be exposed to an entity that is located outside the 3GPP network, including the SCS, which is outside the 3GPP network as well.

	EPS-AKA [9]	EAP-AKA [10]	GAAKA-1	GAAKA-2	GAAKA-3
TOC	Symmetric	Symmetric	Symmetric	Asymmetric	Symmetric
FTS	Yes	Yes	Yes	No	Yes
PPR	Weak	Weak	Normal	Strong	Normal
RRA	No	No	Yes	Yes	Yes
RMA	No	No	Yes	Yes	Yes
CAH	No	No	Yes	Yes	Yes
CAM	No	No	No	Yes	Yes
CAE	No	No	No	Yes	Yes
CON	Large	Large	Medium	Small	Small
COM	Small	Small	Small	Large	Small
SGA	No	No	Yes	Yes	Yes

TOC: type of cryptosystem; FTS: follow the standard; PPR: privacy preservation; RRA: resistance to redirection attack; RMA: resistance to MITM attack; CAH: congestion avoidance at HSS; CAM: congestion avoidance at MME; CAE: congestion avoidance at eNB; CON: communication overhead of the core network; COM: computation overhead of MTC device; SGA: support group authentication.

Table 2. Comparison of design goals among the authentication and key agreement protocols.

Candidate Solutions from 3GPP

According to the corresponding security requirements, the 3GPP has proposed the following candidate solutions for secure group based messaging.

Application layer based protection: Security protection applied at the MTC application layer is a straightforward solution. However, the network should trust the SCS and assure/ensure that the SCS protects the group message and MTC application if the MTC device verifies it. In this case, if the security is not applied in the application layer, then there can be attacks on the network. The SCS should apply encryption, signature, and replay protection to the group message. The MTC application on the MTC device should verify the source of the group message and ensure the integrity of the received group message. The MTC device should discard the group message if it is not signed and replay protected by the SCS.

Network based protection for cell broadcast: In network based protection, the MTC-IWF generates the keys for group message protection and protects the group message. Figure 4 [14] shows the message sequence and describes the mechanism.

1. The MTC-IWF creates the group and generates the group encryption key for encrypting the group message. The MTC-IWF uses the public key infrastructure (PKI) for signing the group message, and symmetric key (Gkey) is used for encryption/decryption of the group messages.
2. The MTC-IWF updates the HSS with the public key and the encryption key for a particular group with the group ID. The HSS maintains/maps the group based feature subscription details along with the MTC device subscription data.
3. During individual authentication, the MME fetches subscription data from the HSS. If the MTC device is subscribed for group based features, then the subscription data contains the group based feature information (GID, encryption key, public key, and the key index).
4. After successful authentication, the MME passes the group keys to the MTC device. The MME protects the keys using the non-access stratum (NAS) security context.
5. When the SCS wants to send the group message, it provides the group message over the Tsp interface.
6. The MTC-IWF protects the group message based on the group ID received from the SCS or from the HSS.
7. The MTC-IWF sends the protected group messages to the selected cell broadcast center (CBC). The protected group message includes the key ID and the algorithm ID used for protection.

Multimedia broadcast multicast service (MBMS) based method: MBMS security can provide a shared key for transferring data. Thus it can be used to protect the group message transferred from one MTC application server/MTC SCS to multiple MTC devices in the group when the MTC devices use shared secret keys for transferring. Otherwise, when all MTC devices in one group need to be authenticated together, or the MTC device wants to communicate with the MTC application server/MTC SCS/network individually, or MTC devices want to send uplink data, the current MBMS security solution cannot be applied.

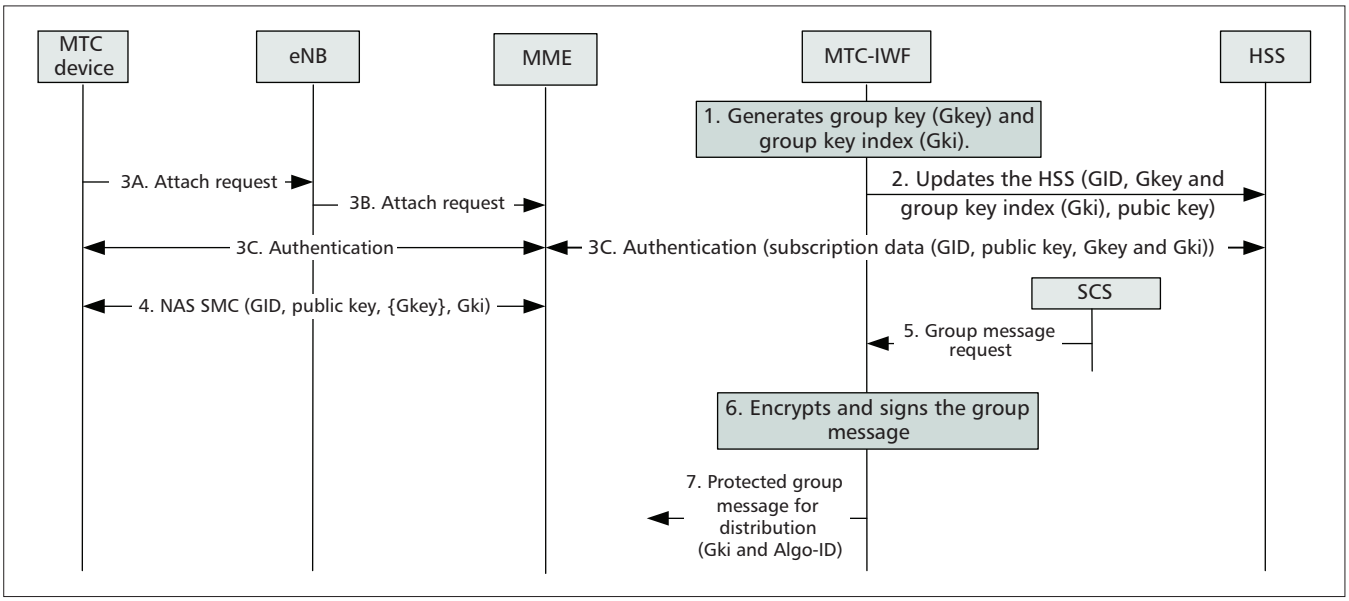

Figure 4. Network based protection for cell broadcast.

Research Challenges

In this section we present key issues and research directions related to group-based secure M2M communications.

Security, Privacy and Efficiency in Mobility Scenarios of MTC

To facilitate system optimization, the 3GPP defines a low mobility feature in M2M communications, which is suitable for MTC devices that do not move, move infrequently, or move only within a certain area. This feature enables the network operator to simplify and reduce the frequency of mobility management procedures. However, a tremendous number of Internet of Things (IoT) applications in M2M communications, such as fleet management or logistics management, have group-based behavior and high/frequent mobility. Therefore, new requirements for secure mobility management should be put forward. First, to reduce the computation and communication overhead during the move, MTC devices can form temporary groups based on the similarity of their mobility patterns at the location database. However, those MTC devices may not have a pre-established trust relationship and need to establish a temporary group without revealing group member information (i.e. privacy). This is difficult but desirable. Traditional schemes are based on a hierarchical tree, and any network entity that wants to set up a group needs to know the keys of the other group members. Therefore, some emerging cryptographic techniques, e.g. attribute-based cryptography, private set intersection, etc., can be considered to design a privacy-preserving group establishment scheme. In addition, when the MTC groups want to access the network, the new group-based access authentication and key agreement protocols should be studied due to introducing the high/frequent mobility scenario. To this end, fast group-based handover authentication protocols must be proposed.

Flexible and Efficient Group Key Management

3GPP SA2 has pointed out that group key management for application layer based protection is within the scope of 3GPP. Consequently, further research effort should be focused on addressing group key distribution. Generally, group key management schemes fall into two categories:

- Designed for large-scale (e.g. MTC message multicast) groups [15], with a one-to-many communication paradigm. Most of these schemes are centralized key distribution schemes that rely on a single fixed key server to generate and distribute keys to the group.
- Designed to support medium size tightly coupled dynamic peer groups, with a many-to-many communication paradigm.

It is worth noting that the two cases coexist in M2M communications. A group of MTC devices can access the core network to receive the same group message from the SCS, and can also communicate with each other to exchange massages. Therefore, designing a flexible and efficient group key management scheme for hybrid machine-to-machine networking is a desirable and challenging issue. However, traditional centralized key management is not well-suited for dynamic group communication systems, i.e. network partitions or faults may occur randomly. On one hand, the issues with centralized trust and single point of failure/attack should be avoided, and the requirements for strong security properties such as forward and backward secrecy, key independence, etc., should be fulfilled. On the other hand, to improve efficiency, new schemes should significantly reduce memory and computation overhead for each group member (i.e. suitable for a resource-constrained MTC device), efficiently deal with massive membership change by minimizing re-keying messages, and be efficient and very scalable for large-size MTC groups.

Conclusion

In this article we have investigated group-based security for large-scale M2M communications in 3GPP networks.

We first introduced the network elements and reference points of the MTC security architecture. We then identified three types of performance issues for authentication signalling congestion and overload in no/low mobility scenarios, and proposed three group access authentication and key agreement protocols to address them. Moreover, we provided several 3GPP candidate solutions for group message protection. Finally, we proposed future research directions with respect to group-based secure M2M communications. The research work should be useful for both mobile operators and MTC users.

Acknowledgments

We thank the anonymous reviewers for their valuable comments. This work is financially supported by the National Natural Science Foundation of China Research Grant (61272037, 61472472, 61402366, 61502386), the International Science and Technology Cooperation and Exchange Plan in Shaanxi Province of China (2015KW-010), and the Natural Science Basic Research Plan in Shaanxi Province of China (2015JQ6236).

References

[1] M. Chen, *et al.*, "A Survey of Recent Developments in Home M2M Networks," *IEEE Commun. Surveys Tut.*, vol. 16, no. 1, pp. 98–114, 2013.

[2] F. Ghavimi and H. Chen, "M2M Communications in 3GPP LTE/LTE-A Networks: Architectures, Service Requirements, Challenges and Applications," *IEEE Commun. Surveys Tut.*, 2014.

[3] T. Taleb and A. Kunz, "Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 178–184, 2012.

[4] S. Lien, K. Chen, and Y. Lin, "Toward Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 66–74, 2011.

[5] H. Fu, *et al.*, "Group Mobility Management for Large-Scale Machine-to-Machine Mobile Networking," *IEEE Trans. Veh. Technol.*, 2014.

[6] R. Lu, *et al.*, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 28–35, 2011.

[7] 3GPP TS 23.682 V13.0.0, Architecture Enhancements to Facilitate Communications with Packet Data Networks and Applications, Dec. 2014.

[8] 3GPP TS 22.368 V13.0.0, Service Requirements for Machine-Type Communications (MTC); Stage 1, Jun. 2014.

[9] 3GPP TS 33.401 V12.5.0, 3GPP System Architecture Evolution (SAE); Security Architecture, Sep. 2012.

[10] 3GPP TS 33.402 V12.5.0, 3GPP System Architecture Evolution (SAE); Security Aspects of Non-3GPP Accesses, Dec. 2014.

[11] C. Lai, *et al.*, "SE-AKA: A Secure and Efficient Group Authentication and Key Agreement Protocol for LTE Networks," *Computer Networks*, vol. 57, no. 17, pp. 3492–3510, 2013.

[12] C. Lai, *et al.*, "SEGR: A Secure and Efficient Group Roaming Scheme for Machine to Machine Communications between 3GPP and WiMAX Networks," in *Proc. IEEE ICC 2014*, pp. 1011–1016.

[13] ——, "LGTH: A Lightweight Group Authentication Protocol for Machine-Type Communication in LTE Networks," in *Proc. IEEE GLOBECOM 2013*, pp. 832–837.

[14] 3GPP TR 33.868 V12.1.0, Study on Security Aspects of Machine-Type Communications (MTC) and Other Mobile Data Applications Communications Enhancements, Jun. 2014.

[15] H. Zhang, *et al.*, "Optimal DoS Attack Scheduling in Wireless Networked Control System," *IEEE Trans. Control Syst. Technol.*, to appear.

Biographies

Chengzhe Lai [M'15] (lcz.xidian@gmail.com) received a B.S degree in information security from Xi'an University of Posts and Telecommunications in 2008, and a Ph.D. degree from Xidian University in 2014. He was a visiting Ph.D. student with the Broadband Communications Research (BBCR) Group, University of Waterloo from 2012 to 2014. At present he is with the School of Telecommunication and Information Engineering, Xian University of Posts and Telecommunications, and with the National Engineering Laboratory for Wireless Security, Xian, China. He is also a visiting researcher at the State Key Laboratory of Integrated Services Networks and State Key Laboratory of Information Security. His research interests include wireless network security, privacy preservation, and M2M communications security.

Rongxing Lu [S'09, M'11, SM'15] (rxlu@ntu.edu.sg) received a Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006, and a Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2012. He is currently an assistant professor with the Division of Communication Engineering, School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, and trusted computing.

Hui Li [M'10] (lihui@mail.xidian.edu.cn) received his B.Sc. degree from Fudan University in 1990, and M.A.Sc. and Ph.D. degrees from Xidian University in 1993 and 1998, respectively. He is a professor with the School of Telecommunications Engineering, Xidian University, Xian, China. In 2009 he was with the Department of ECE, University of Waterloo as a visiting scholar. His research interests are in the areas of cryptography, security of cloud computing, wireless network security, information theory, and network coding. He is the co-author of two books. He served as TPC co-chair of ISPEC 2009 and IAS 2009, and general co-chair of e-forensic 2010, ProvSec 2011, and ISC 2011.

Dong Zheng (zhengdong@xupt.edu.cn) received an M.S. degree in mathematics from Shaanxi Normal University, Xian, China, in 1988, and a Ph.D. degree in communication engineering from Xidian University, Xian, in 1999. He was a postdoctoral fellow in the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China, from 1999 to 2001, and a research fellow at Hong Kong University, Hong Kong, in 2002. He was a professor in the School of Information Security Engineering, Shanghai Jiao Tong University. He is also with the State Key Laboratory of Integrated Service Networks, Xidian University. He is currently a professor in the School of Telecommunication and Information Engineering, Xian University of Posts and Telecommunications, and is also connected with the National Engineering Laboratory for Wireless Security, Xian, China. His research interests include provable security and new cryptographic technology.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] (xshen@bbcr.uwaterloo.ca) received his B.Sc. degree from Dalian Maritime University, China, in 1982, and his M.Sc. and Ph.D. degrees from Rutgers University, New Jersey, in 1987 and 1990, respectively, all in electrical engineering. He is a professor and University Research Chair in the Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks. He has co-authored three books and has published more than 400 papers and book chapters in wireless communications and networks, control, and filtering. He is a former Editor-in-Chief of *IEEE Network* and served as a Technical Program Committee Co-Chair for IEEE INFOCOM 2014. He is the Chair of the IEEE ComSoc Technical Committee on Wireless Communications, and P2P Communications and Networking, and a voting member of GITC. He was a founding area editor of *IEEE Transactions on Wireless Communications*, and a guest editor for *IEEE JSAC*, *IEEE Wireless Communications*, and *IEEE Communications Magazine*. He also served as the Technical Program Committee Chair for GLOBECOM'07, Tutorial Chair for ICC'08, and Symposia Chair for ICC'10. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo, and the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada. He is a registered professional engineer of Ontario, Canada, an IEEE Fellow, a Fellow of the Engineering Institute of Canada, and a Fellow of the Canadian Academy of Engineering. He has been a ComSoc Distinguished Lecturer.

When the MTC groups want to access the network, the new group-based access authentication and key agreement protocols should be studied due to introducing the high/frequent mobility scenario. To this end, fast group-based handover authentication protocols must be proposed.