Security Issues on Machine to Machine Communications

Chengzhe Lai[1], Hui Li[1], Yueyu Zhang[1] and Jin Cao[1]
[1] Key Laboratory of Computer Networks and Information Security, Ministry of Education, School of Telecommunications Engineering, Xidian University
[e-mail: lcz.xidian@gmail.com]
*Corresponding author: Chengzhe Lai

Received September 16, 2011; revised November 14, 2011; accepted November 21, 2011; published February 28, 2012

Abstract

Machine to machine (M2M) communications is the hottest issue in the standardization and industry area, it is also defined as machine-type communication (MTC) in release 10 of the 3rd Generation Partnership Project (3GPP). Recently, most research have focused on congestion control, sensing, computing, and controlling technologies and resource management etc., but there are few studies on security aspects. In this paper, we first introduce the threats that exist in M2M system and corresponding solutions according to 3GPP. In addition, we present several new security issues including group access authentication, multiparty authentication and data authentication, and propose corresponding solutions through modifying existing authentication protocols and cryptographic algorithms, such as group authentication and key agreement protocol used to solve group access authentication of M2M, proxy signature for M2M system to tackle authentication issue among multiple entities and aggregate signature used to resolve security of small data transmission in M2M communications.

Keywords: M2M, MTC, security, authentication, signature, 3GPP

This work is supported by the National Natural Science Foundation of China grant 61102056 and the Fundamental Research Funds for the Central Universities (JY10000901025).

DOI: 10.3837/tiis.2012.02.003

1. Introduction

Machine to machine (M2M) communications [1] is the hottest issue in the standardization and industry areas, it is also defined as machine-type communication (MTC) [2] in release 10 of the 3rd Generation Partnership Project (3GPP). There are many applications made possible thanks to machine to machine communications, such as personal health monitoring, intelligent tracking and tracing in the supply chain, smart utility metering, remote control of vending machines, industrial wireless automation and ambient assisted living etc. European telecommunications standards institute (ETSI) indicates that this fast-growing sector has the potential to connect up to 50 billion machines today, and even more in the near future. The cellular M2M segment in particular is forecast to produce record growth. The primary advantage of M2M communications is that many intelligent wireless devices may act as "servers," collaboratively collecting and delivering real-time monitoring data to people. Since it does not need direct human intervention, M2M communications is fast becoming a market-changing force for the next-generation intelligent real-time networked applications [3].

Many component-level standards already exist, addressing various radio interfaces, different meshed or routed networking choices, or offering a choice of identity schemes. However, until now, little effort has been made to focus on security aspects. According to the different network structures, M2M can be divided into general M2M and 3GPP M2M, general M2M communications can generally be considered as the heterogeneous mobile ad hoc network (HetMANET). As a consequence, general M2M communications may face security challenges that can be encountered in the HetMANET [4]. In this paper, we mainly consider the security of 3GPP M2M communications. Firstly, security threats and corresponding solutions will be introduced according to 3GPP [5], including MTC device triggering, secure connection, security of small data transmission, reject message without integrity protection, MTC monitoring congestion control, external interface security, security of MTC devices/UEs configuration and restricting the USIM to specific MEs/MTC devices. Moreover, we raise several new security issues and propose corresponding solutions through modifying existing authentication protocols and cryptographic algorithms. The first is group access authentication. The authentication procedure of group communication of M2M is different from that of one to one communication [6][7][8][9][10][11][12], in order to reduce authentication cost, we must design a new group authentication and key agreement protocol for group access authentication of M2M. The second is multiparty authentication, in the scenario which MTC server is located outside of the operator domain, the connection between 3GPP core network (CN) and MTC server might be insecure, there are untrust relationships among MTC device, core network and MTC server. It is necessary to design a new kind of mutual authentication protocol between MTC device, core network and MTC server, we try to use proxy signature scheme to solve the problem [13][14][15]. The third is data authentication, since M2M communications has a "small data transmission" feature, existing authentication schemes, such as IKEv2 protocol, is not suitable for the data transmission of M2M communications, aggregate signature [16][17][18][19][20][21] is a candidate solution to resolve security issue of small data transmission for M2M.

The rest of this paper is organized as follows. In Section 2, we introduce some security threats and corresponding solutions according to 3GPP. In Section 3, we raise several new security

issues that need to be addressed and propose our solutions. Section 4 is conclusion and future work.

2. Background

2.1 Network Architecture for M2M

Key network elements defined in ETSI are shown in **Fig. 1**, consisting of the following parts.

• M2M Device

– A device capable of replying to request for data contained within those device or capable of transmitting data contained within those devices autonomously.

• M2M Area Network (Device Domain)

– Provide connectivity between M2M devices and M2M gateways (e.g. personal area network).

• M2M Gateway

– Use M2M capabilities to ensure M2M devices inter-working and interconnection to the communication network.

• M2M Communication Networks (Network Domain)

– Communications between the M2M gateway(s) and M2M application (e.g. xDSL, LTE, WiMAX, and WLAN).

• M2M Applications

– Contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.

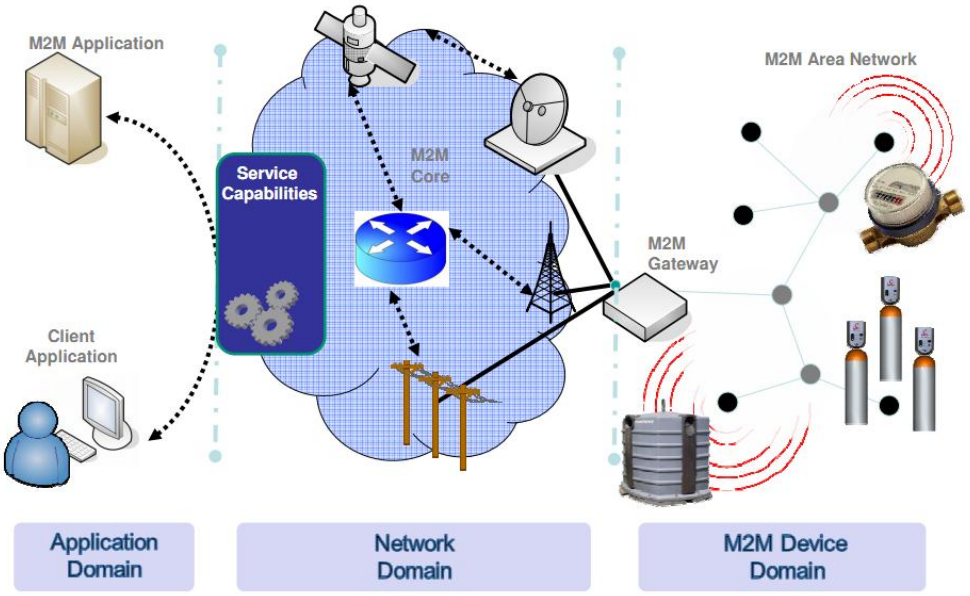

Fig. 1. Network architecture for M2M from ETSI

3GPP defines three different areas, as shown in **Fig. 2**. Security for MTC communication between the MTC device and 3GPP network can be further divided to:

(A1) Security for MTC communication between the MTC device and radio access network (RAN).

(A2) Security for MTC communication between the MTC device and non-access stratum (NAS).
(A3) Security for MTC communication between the MTC device and gateway GPRS support node (GGSN)/packet data gateway (PGW)/evolved packet data gateway (ePDG).

(B) Security for MTC communication between the 3GPP network and the MTC server/application can be further divided to:
(B1) Security for MTC communication between the MTC server and 3GPP network in indirect deployment model. This can be further divided into security aspects when the MTC server is within the 3GPP network and when it is outside the 3GPP network.
(B2) Security for MTC communication between the MTC application and 3GPP network in direct deployment model.

(C) Security for MTC communication between the MTC server/application and MTC device can be further divided to:
(C1) Security for MTC communication between the MTC server and MTC device in indirect deployment model.
(C2) Security for MTC communication between the MTC application and MTC device in direct deployment model.

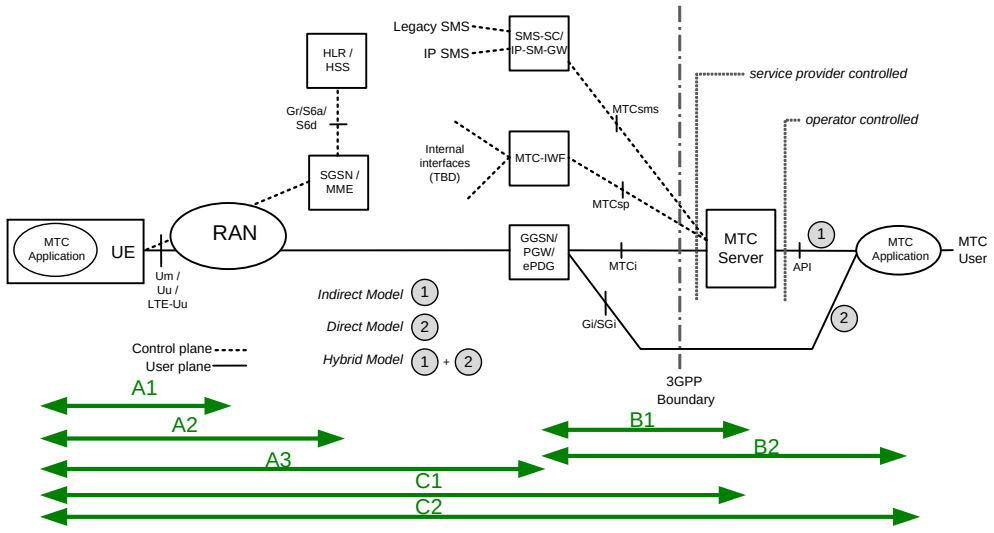

Fig. 2. Network architecture for M2M from 3GPP

2.2 Threats Analysis and Existing Solutions

2.1 MTC Device Triggering

Threats: MTC device triggering issues are defined in [2], relevant threats are as follows.

False network attack: When an MTC device is in detached state, the attacker can impersonate a network to send a trigger indication to the MTC device. Because MTC devices need to operate for a long time by using a single battery supply without recharging, false network triggering can awaken an MTC device and waste its power.
Tamper attack: The trigger indication may contain the IP (or fully qualified domain name (FQDN)) and/or TCP (or UDP) port of the application server that the MTC device has to contact. If the IP (or FQDN) and/or TCP (or UDP) port of the application server are tampered by the attacker, the MTC device may establish the packet data network (PDN) connection to the wrong MTC server or be rejected by the MTC server. MTC device is unable to communicate with the correct MTC server and it will also waste the MTC device's power consumption.
Existing solutions:
We need to consider two situations: offline MTC device and online MTC device.

For offline MTC device:

1) If the MTC device is in detached state, the MTC device should be able to validate the network identity when it receives a trigger indication.
2) If the MTC device is in detached state, the network should protect the trigger indication message by using the last security context stored in the network and the MTC device.

For online MTC device:

1) [2] has proposed a solution of MTC device triggering via non-access stratum (NAS) signaling. In this case, current mechanisms can be used to solve the security issue. After NAS SMC (confidentiality and integrity algo), NAS security is activated. All NAS signaling messages should be integrity-protected according to [12], therefore current LTE [22] security mechanisms ensure that the trigger indication is not tampered with.

2) When the MTC device is in online state, the MTC server should be able to trigger MTC device through the process of generic bootstrapping architecture (GBA) push function.

2.2 Secure Connection

The MTC feature secure connection requires a secure connection between the MTC device and MTC server.
Existing solutions:
1) GBA, as specified in [23], is used to bootstrap authentication and key agreement (AKA) for application security based on the 3GPP AKA mechanism. It can be used to establish the end-to-end security and provide different security levels based on detailed requirements.
2) GBA Push, as specified in [24], can be used for key establishing between an MTC device and an MTC server. Under system improvements to machine-type communications (SIMTC) scenario, MTC device acts as UE which generates a network application function (NAF) key derived from the bootstrap key Ks, and MTC server acts as NAF which received the NAF key from the bootstrapping server function (BSF). Then MTC device and MTC server can set up secure connection based on this shared NAF key.

2.3 Security of Small Data Transmission

The MTC feature small data transmissions requirements are defined in [25].
Threats: Small data transmission allows M2M devices to arbitrary create NAS content and

traffic. Such content will be generated by potentially hundreds of millions devices, creating an environment for a DoS attack on MME. Moreover, there may be no pre-established NAS security context in transfer data via optimised short message service (SMS) solution, thus the small data transmission can not be protected by valid security context and can be easily tampered or intercepted by the attacker. Sometimes small data is sensitive and important because it may be related to emergency event or commerce. Once it is tampered or intercepted, the consequence can be serious.

Existing solutions:

In 3GPP TR 33.868 [5], how to provide confidentiality and integrity protection for small data transfer should be further studied when there is no pre-established security context. Unfortunately, there are no proposed solutions for the security threat currently. We will try to give a method based on aggregate signature to solve the problem in the following sections.

2.4 Reject Message without Integrity Protection

Threats: In the overload situation, the mobility management (MM)/ GPRS mobility management (GMM)/ EPS mobility management (EMM) reject cause values such as "IMSI unknown in HLR"; "illegal ME"; and "PLMN not allowed" could be wrongly sent by an overloaded (V)PLMN. It's unrealistic for serving GPRS support node (SGSN)/ mobility management entity (MME) to get authentication vector from the HSS, perform a successful AKA with the MTC device, then perform the security mode command procedure for integrity protection and encryption. So the MM/GMM/EMM reject message will be sent to the MTC device without with integrity protection. If that, any false base station can fake the MM/GMM/EMM reject cause values in the reject message as a denial of service attack to the MTC devices and the network.

Existing solutions: Similarly, there are no proposed solutions for the security threat currently.

2.5 MTC Monitoring

Threats: As discussed in [2], MTC devices may be deployed in locations with high risk, there are MTC devices that should not move from an authorized location, or should only move in an authorized area. In the case of an MTC application where the MTC device should not move from an authorized location, or should only move in an authorized area (e.g. within a home), there could be security risks if the device is operated from an unauthorized location.

Existing solutions:

MTC device reports the location identifiers. Network entity (e.g. SGSN/MME) should store the pre-defined location identifier and be able to verify the location identifier by comparing these two identifiers. When the MTC device moves, a network entity (e.g. SGSN/MME) receives new location information which is reported by RAN or by the MTC device explicitly and detects if it is different from pre-configured location information. Then the network entity can confirm that the MTC device has moved to other area and will send a warning message to the MTC server, which can then take further action.

2.6 Congestion Control

Threats: When requesting access to the mobile network, a UE should provide its currently enabled indicators to the network. There exist security threats if the indicators are sent without any protection. The attackers can tamper with the low access priority indicators to the normal state to let many MTC devices connect when the network setup congestion control mechanism. The problem is serious since nowadays congestion is the most urgent issue that operators face. Vice versa, if an attacker adds a fake low access priority indicator in the request sent by normal UEs, the service of normal UEs will be maliciously degraded.

Existing solutions:

Current GSM/UMTS/LTE mechanism should be used to protect low access priority indicator.

If the UE has valid security context, the attach request and location area update (LAU)/ routing area update (RAU)/tracking area update (TAU) request should be integrity protected. However, attach request and LAU/RAU/TAU request can not be protected initially, i.e. when MTC device connects to the network for the first time, because MTC device would not have any valid security context.

Therefore, a new mechanism to protect low access priority indicator without valid security context is needed.

2.7 External Interface Security

Threats: There are two scenarios of MTC devices communication with MTC server(s) illustrated in [25], MTC server(s) controlled by the network operator or MTC server(s) not controlled by the operator. The interface between MTC server and CN may be over an insecure link. Communication between the MTC server and the CN for common and specific services (such as MTC device triggering, MTC monitoring) are carried on this insecure link. Attack on the communication between MTC server and CN may cause false activities either to the MTC server, MTC device or to the 3GPP network or privacy sensitive information such as identities may be eavesdropped, which may lead to serious problems. Detailed analysis can be found in [5].

Existing solutions:

As shown in **Fig.3**, when the MTC server is located outside the operator domain, the interface between the core network and the MTC server may be protected using mechanisms like directory name service (NDS)/IP [26]. As the MTC server is located outside the operator domain it may not be possible to mandate the use of NDS/IP but the exact protection mechanism may be based on the agreements between the 3GPP network and MTC server. Security GW could be used between the MTC server and the core network as the first point of entry into a secure operator network.

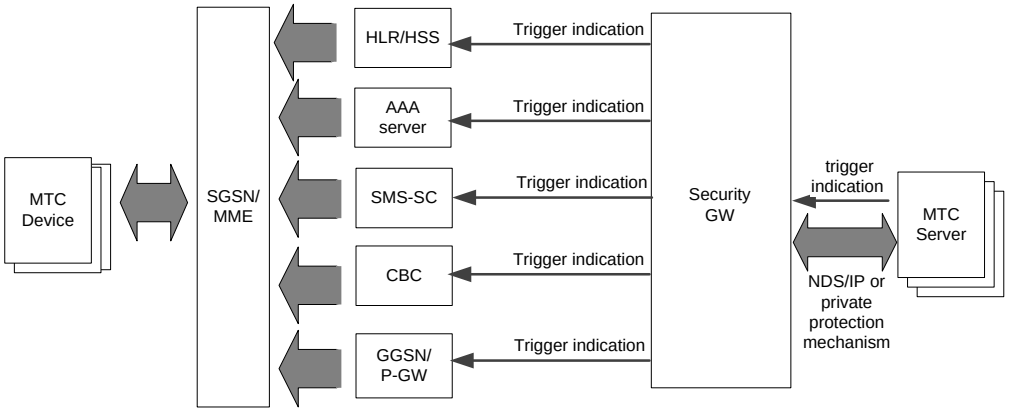

Fig.3. Security GW exists between the MTC server and the network entity

Thus the security GW can perform access control functionality to prevent the unauthorized MTC server from accessing to the core network. It can authenticate with MTC server on behalf of the 3GPP network. The NDS/IP security mechanism or private protection mechanism can protect the trigger indication sent from the MTC server to the security GW. The Security GW can be an independent node or co-located with an intermediate node (e.g. trigger GW). However, the authentication procedure between MTC server and security GW has not yet been realized. Moreover, in this case, there are untrust relationships among MTC device, core

network and MTC server, therefore, it is necessary to design a new kind of multiparty authentication protocol among them.

2.8 Security of MTC Devices/UEs Configuration

Threats: Different MTC devices configuration options were introduced in stage 2 to avoid/alleviate congestion and overload in the network, in particular to control the network access from low priority MTC devices (i.e. delay tolerant).There are two potential approaches for delivering the configuration options to the MTC devices. One approach is using open mobile alliance device management (OMA DM) and the other is using universal integrated circuit card (UICC) over-the-air (OTA) (as specified in ETSI [27][28] and 3GPP [29][30]). The OMA DM approach only applies to the terminal part of the MTC device (MTC ME). This clause details only the OMA DM approach. Without security protection, the management object will face man-in-the-middle (MitM) attack when it's provisioned to the MTC devices.

Existing solutions:

OMA DM security, as specified in [31] and [32], contains a number of options, where some are not needed for the purposes of this paper and others are required. Therefore, OMA DM security is profiled as:

-The MTC devices/UEs should have a root certificate to authenticate the DM server.
-The root certificate needs to be provided to the MTC devices/UEs in a secure manner.
The root certificate should be securely stored.
-The DM server and the MTC devices/UEs should support and use transport layer security (TLS) according to the profile specified in [33].

2.9 Restricting the USIM to Specific MEs/MTC Devices

Threats: As shown in **Fig. 4**, in some configurations, it may be necessary to restrict the access of a UICC that is dedicated to be used only with machine type modules associated with a specific billing plan. It should be possible to associate a list of UICC to a list of terminal identity such as international mobile equipment identity software version (IMEISV), so that if the UICC is used in another terminal type, the access will be refused. See the following configuration: The restriction can be enforced by a one USIM to one MTC device binding or a one USIM to many MTC device binding. It is the operator that shall be able to enforce the restriction. An attacker moves a UICC to a different device in order to use a subscription to get network access for himself, e.g. the attacker may try to insert a UICC with low data rate subscription, dedicated to MTC MEs, into a smartphone in order to download large files.

Existing solutions:

3GPP CT6 discussed and considered three UE-based mechanisms to restrict the use of UICC to specific MTC MEs, which are proposed in C6-110182:

- Secure channel pairing
- USIM application toolkit (USAT) application pairing
- Personal identification number (PIN) verification pairing

Specific mechanism and corresponding evaluations can be found in [5].

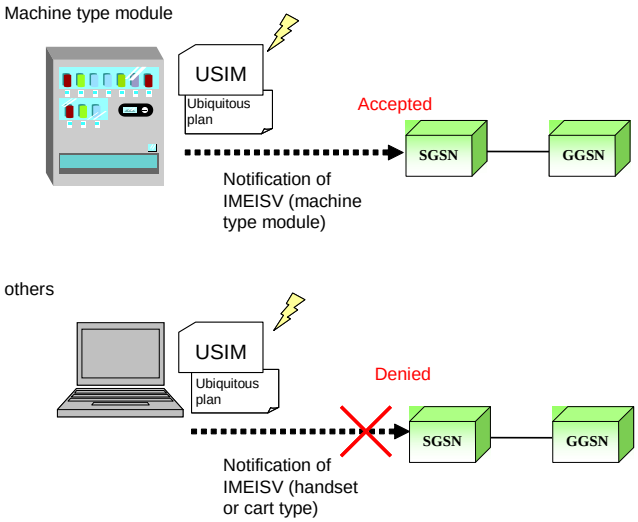

Fig. 4. Access control with billing plan

3GPP and other organizations have already started to address these security problems mentioned above. Some security issues have corresponding candidate solutions, like (1), (2), (5)-(9), however, performance evaluations of candidate solutions, such as cost and benefit trade-off analysis, are not given. Next, it is necessary to evaluate these performance indicators accurately. Others, like (3), (4), have no proper solutions currently and further research is needed. There are also some problems, such as (6), (7), have not been solved completely, and need further improvements and enhancements. In summary, there is still a lot of work to do in future. Besides security threats analysed above, several new security issues and solutions will be introduced in the next section.

3. Several New Security Issues and Our Solutions

3.1 Group Access Authentication

To the best of our knowledge, the existing network authentication systems are mainly designed for a single object, and they all need 3 or 4 rounds of interaction to realize the mutual authentication beween a user and a server. In practical applications, however, there may be a large number of users with the same properites in a network. Take an specific example of the MTC, user terminals can form a group when they are in the same region, belong to the same application or have the same behavior. The network model of group communication is illustrated in **Fig. 5**.

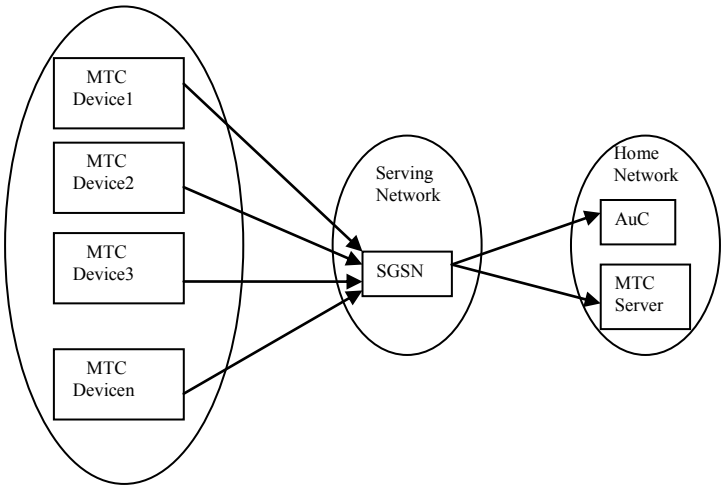

Fig. 5. Network model of group communication

In the above application, if substantial user terminals of a group access the network simultaneously, the available authentication methods suffer from network congestion and high network resources occupancy rate by increasing the network signal. In order to prevent network congestion and efficiently authenticate user terminals of a group, group authentication is introduced, which performs authentication for group units. As a kind of network authentication technology, group authentication aims to authenticate multiple or all the user at one time. In this technology, the group is assigned a unique identifier and the user terminals as a whole are authenticated. Group authentication can be fulfilled by utilizing the authentication agency or the gateway. After successful group authentication, user terminals and network side entities can share some keys. Certainly, a single user terminal and a network side entity can also obtain independent keys. Presently, the standardization work on group authentication is still in progress. A majority of standardization organizations only present security threats and requirements of group authentication, and the mechanism and procedure have not yet been developed.

In the literature, few authentication protocols of group communications have been proposed, such as an individual and group authentication model for wireless network services using dynamic key cryptography and group key management for individual and group of users and services [6], G-AKA for a group of mobile stations (MSs) roaming from the same home network (HN) to a serving network (SN) [7] and group authentication protocol for mobile networks which proposes a new architecture for authentication management and an associated authentication protocol for mobile groups and individual nodes over heterogeneous domains [8]. However, there are still no appropriate group authentication methods for MTC communications in 3GPP. On the other hand, several existing protocol, like UMTS AKA [9], UMTS X-AKA [10], UMTS T-AKA [11] and EPS AKA [12] are not suitable for group authentication. They need to be modified to apply to the group authentication of MTC. In this paper, we introduce a novel kind of group authentication and key agreement protocol, the main idea of our group authentication and key agreement protocol is as follows. We first select a leader MTC device of a group and perform a full AKA authentication procedure. In this process, the leader MTC device obtains a group of authentication vectors and a group authentication key (GAK) on behalf of other MTC devices of the group. Then the serving network (SN) is enabled to carry out mutual authentication with remaining MTC devices of the group using obtained authentication vector and GAK without intervention of the remote

home network (HN). The authentication delay can be decreased as a whole and the signaling overhead between the HN and the SN is considerably reduced. Overall authentication procedures are shown in **Fig.6** and **Fig.7**.

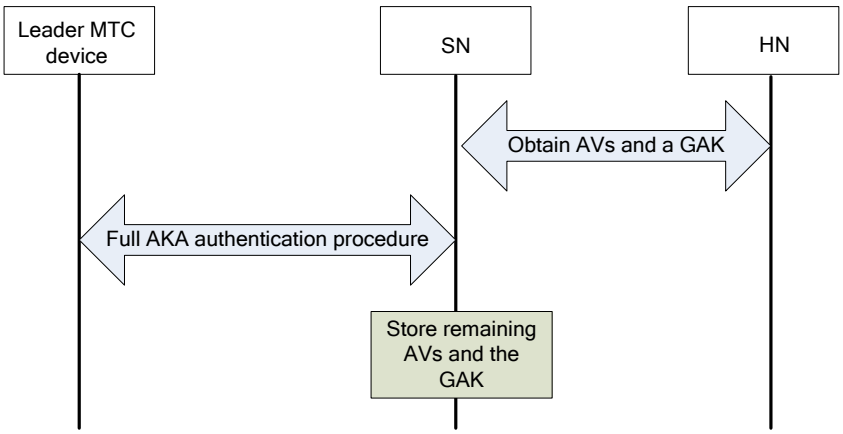

Fig. 6. The authentication procedure of leader MTC device

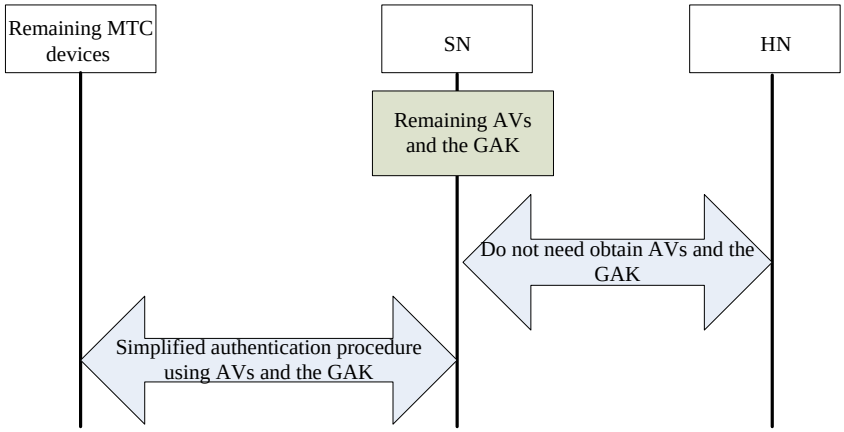

Fig. 7. The authentication procedure of remaining MTC devices

We tested our protocol using formal security verification tool known as the "automated validation of Internet security protocols and applications" (AVISPA) [34]. We only present the authentication analysis of one MTC device as an example, analysis result is shown in **Fig.8**.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  d:\SPAN\testsuite\results\lcz.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.00s
  visitedNodes: 2 nodes
  depth: 1 plies
```

Fig. 8. Results reported by the OFMC back-end

In addition, a comparison of communication cost between our scheme and original authentication protocols is made and analysis result is shown in **Fig.9**. *I* denotes communication cost improvement of our scheme over original authentication protocols. The larger *I* is, the better communication cost improvement of our scheme over original authentication protocols will be.

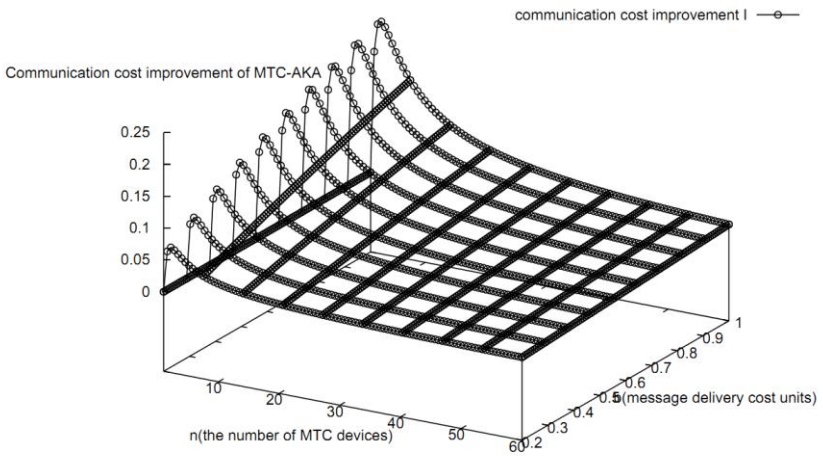

Fig. 9. Communication cost improvement *I* of our scheme over original authentication protocols

3.2 Multiparty Authentication

Actually, 3GPP considers three scenarios for MTC communications. First scenario is depicted in **Fig.10**. It shows the communication scenario with MTC devices communicating with MTC server. MTC server is located in the operator domain. Second scenario is depicted in **Fig.11**. It shows the communication scenario with MTC devices communicating with MTC server. MTC server is located outside of the operator domain. Third scenario is not considered in 3GPP specification. Therefore, we only consider the security of two types of MTC communications scenarios. In the first scenario, MTC server is located in the operator domain, thus it is regulated by the 3GPP core network, and its security is same as existing standard.

However, in the second scenario, MTC server is located outside of the operator domain, the connection between 3GPP core network and MTC server might be insecure, there are untrust relationships among MTC device, core network and MTC server. It is necessary to design a new kind of mutual authentication protocol between MTC device, core network and MTC server. In this circumstance, three contractual relationships should have been established between (1) an MTC device and its MTC server; (2) MTC device and core network; (3) MTC device's core network and its MTC server.

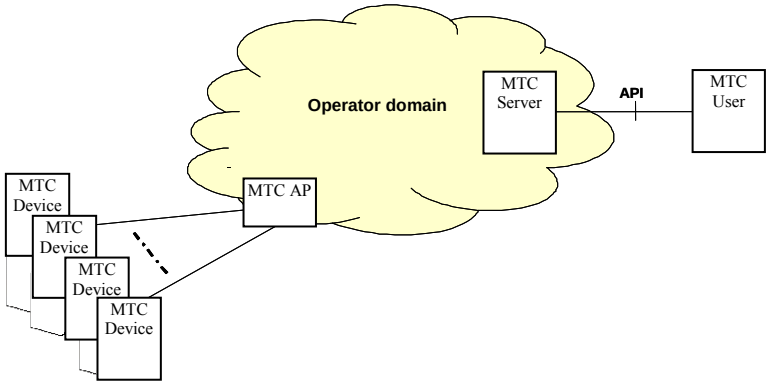

Fig.10. Communication scenario with MTC devices communicating with MTC server. MTC server is located in the operator domain

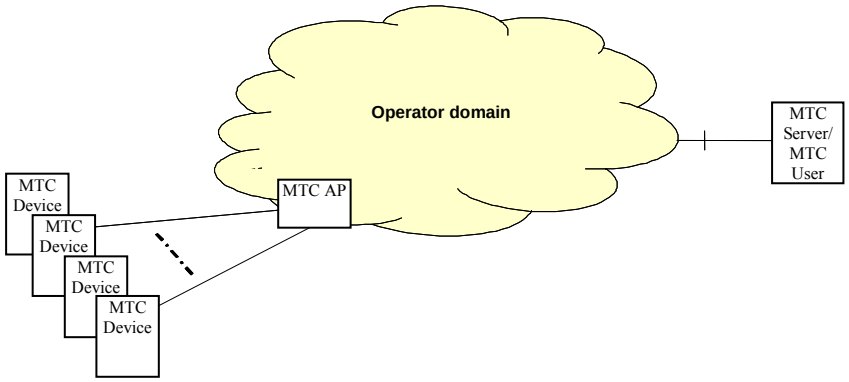

Fig.11. Communication scenario with MTC devices communicating with MTC server. MTC server is located outside the operator domain

We consider designing a mutual authentication and access control mechanism by adapting the proxy signature [13][14][15]. Firstly, MTC server and core network operator have a contractual agreement on management of MTC device by issuing proxy-signature each other. MTC server (core network operator) re-delegates its proxy-signing capability to an MTC device. At the same time, core network operator delegates its signing capability to MTC device access point (MTCAP). Hence, the MTC device authenticate the MTCAP by verifying signature from MTC device via public key of core network, while the MTCAP authenticate the MTC device by verifying signature from MTCAP via proxy-signed public key of core network operator as well as that of MTC server.

Inspired by the idea of [13], we present the mutual authentication protocol between 1) MTC device and core network (CN), 2) MTC device and MTC server, and 3) MTC device and MTCAP. As shown in **Fig. 11**, CN have a contractual relationship with MTC server. MTC server should convince MTCAP to authenticate MTC device in company with corresponding CN. Proxy signature scheme provides a method of delegating and verifying among entities. In our scheme, MTC server issues the proxy signature on behalf of CN to MTC device. The CN also issues the proxy signature on behalf of MTC server to MTC device, and its own signature to MTCAP. And then, MTCAP (MTC device) trusts MTC device (MTCAP) with proxy signature on behalf of CN and MTC server.

3.3 Data Authentication

There exists a kind of application scenario of M2M: Smart Metering, as shown in **Fig. 12**. In this scenario, a large amount of data may be sent to data center via wide area network (WAN), these data conveyed to the data center must be authenticated by data center and ensure the confidentiality and integrity. On the one hand, the security solution of small data transmission mentioned above have not been solved, it's unrealistic for MTC device to guarantee security by implementing IKEv2 [35] protocol and establish a secure tunnel, because these data are not always transmitting in the tunnel and only transmit in a certain period of time, therefore establishing an IPsec will be more expensive for small data transmission of MTC device. On the other hand, if we use general signature algorithms, it would generate a large number of costs of computation and communication, thus we need to find a kind of cryptographic algorithm to reducing computation and communication cost.

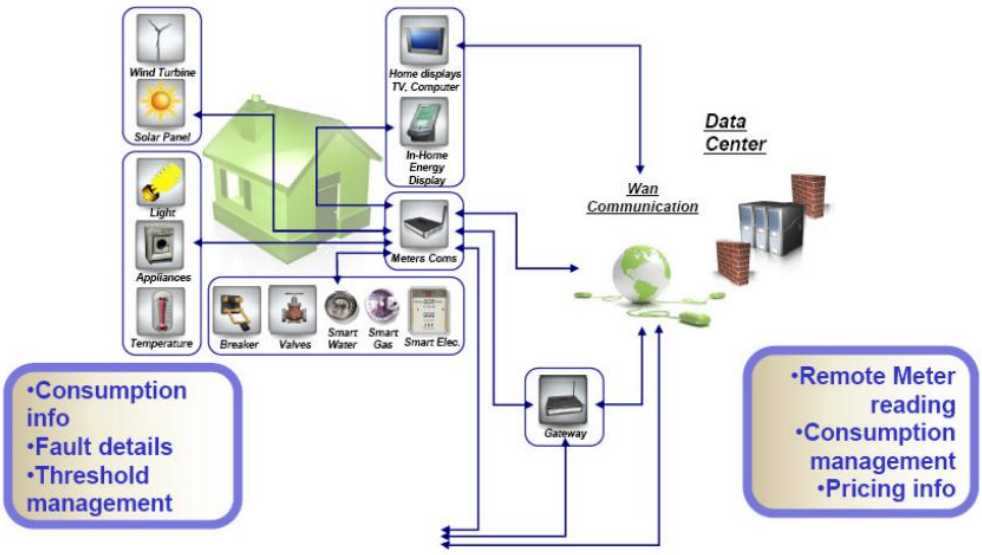

Fig.12. A kind of application scenario of M2M – Smart Metering

An aggregate signature [16][17][18][19][20][21] is one technique towards achieving this aim. In aggregate signature schemes, multiple signatures can be aggregated into a compact "aggregate signature," even if these signatures are on (many) different documents and were produced by (many) different signers. Apart from compactness, aggregate signatures have another advantage which can prevent a malicious party from removing a signature from a collection of signatures without being detected. At present, two aggregate signature schemes

exist. D. Boneh et al. [16] uses bilinear maps and supports flexible aggregation. A. Lysyanskaya et al. [17] uses a weaker assumption, certified trapdoor permutations, but it permits only sequential aggregation. Recently, an identity-based cryptography (IBC) is proposed by [20], the main idea is to simplify public-key and certificate management by using a user's "identity" as its public key. In an identity-based signature (IBS) scheme, the verifier verifies a signature by using the signer's identity and PKG's public key; the authentication information does not include any certificate or any individual public key for the signer. The main advantage of IBS is communication efficiency, since the signer does not need to send an individual public key and certificate with its signature. Therefore, constructing an "identity-based aggregate signature" (IBAS) scheme is natural. Based on the above discussion, the idea of aggregate signature is also suitable for use in small data transmission of MTC device. It can provide security services and reduce calculation and communication cost effectively.

4. Conclusion and Future Work

In this paper, we make an analysis of threats that exist in M2M system and corresponding solutions according to 3GPP. In addition, we raise several new security issues including group access authentication, multiparty authentication and data authentication, and propose our solutions through modifying existing authentication protocols and cryptographic algorithms, the first is group authentication and key agreement protocol used to solve group access authentication of M2M, the second is proxy signature for M2M system to tackle authentication issue among multiple entities and the third is aggregate signature used to resolve security of small data transmission for M2M. In future work, an in-depth research on three security issues introduced in this paper is necessary, on the other hand, due to the complexity of M2M system, more security issues need to be found and solved.

References

[1] ETSI, "Machine-to-Machine communications (M2M); M2M service requirements," *TS 102 689 V1.1.2*., 2011.
[2] 3GPP TR 23.888, "System improvements for machine-type communications," Mar.2010.
[3] S. Gilani, "The promise of M2M: How pervasive connected machines are fueling the next wirelessevolution," 2009. Article (CrossRef Link)
[4] Shao-Yu Lien, Kwang-Cheng Chen and Yonghua Lin, "Toward ubiquitous massive accesses in 3GPP machine-to-machine communications," *Communications Magazine, IEEE,* vol.49, no.4, pp.66-74, Apr.2011.Article (CrossRef Link)
[5] 3GPP TR 33.868, "Security aspects of Machine-Type communications," Jul.2011.
[6] Huy Hoang Ngo, XianpingWu, Phu Dung Le and Bala Srinivasan, "An individual and group authentication model for wireless network services," *JCIT: Journal of Convergence Information Technology*, vol.5, no.1, pp.82-94, 2010. Article (CrossRef Link)
[7] Chen Yu-Wen, Wang Jui-Tang, Chi Kuang-Hui and Tseng Chien-Chao, "Group-Based authentication and key agreement," in *Proc. of Wireless Personal Communications*, vol.61, pp.1-15, 2010. Article (CrossRef Link)
[8] Nidal Aboudagga, Jean-Jacques Quisquater and Mohamed Eltoweissy, "Group authentication protocol for mobile networks," in *Proc. of the Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications IEEE Computer Society*, 2007. Article (CrossRef Link)
[9] 3GPP TS 21.133 V4.1.0, "3G security; Security threats and requirements," 2001.

[10] Huang, C. M. and Li, J. W., "Authentication and key agreement protocol for UMTS with lowbandwidth consumption," in *Proc. of 19th IEEE international conference on advance information networking and applications,* pp.392-397, 2005. Article (CrossRef Link)
[11] Ka-Kyung Oh, Tae-You Lee, Choon-Sung Nam and Dong-Ryeol Shin, "Strong authentication and key agreement protocol in UMTS," in *Proc. of Fifth International Joint Conference on INC, IMS and IDC*, 2009. Article (CrossRef Link)
[12] 3GPP TS 33.401 V11.1.0, "3GPP System Architecture Evolution (SAE); Security architecture", Sep.2011.
[13] C. K. Han, H. K. Choi and I. H. Kim, "Building femtocell more secure with improved proxy signature," in *Proc. of IEEE GLOBE COM*, pp.1-6, Dec.2009. Article (CrossRef Link)
[14] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol.E79-A, no.9, pp.1338-1354, 1996. Article (CrossRef Link)
[15] S. Kim, S. Park and D. Won, "Proxy signatures, revisited," in *Proc. of the First International Conference on Information and Communication Security,* vol.1334, pp.223-232, 1997. Article (CrossRef Link)
[16] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," In *Proc. of Eurocrypt 2003*, vol.2656, pp.416–432, 2003.
[17] A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, "Sequential aggregate signatures from trapdoor permutations," In *Proc. of Eurocrypt 2004*, vol.9999, pp.74–90, 2004. Article (CrossRef Link)
[18] E. Mykletun, M. Narasimha and G. Tsudik, "Signature bouquets: immutability for aggregated/condensed signatures," in *Proc. of ESORICS 2004*, pp160–176, 2004. Article (CrossRef Link)
[19] T. Suzuki, Z. Ramzan, H. Fujimoto, C. Gentry, T. Nakayama and R. Jain, "A system for end-to-end authentication of adaptive multimedia content," in *Proc. of Conference on Communications and Multimedia Security*, 2004. Article (CrossRef Link)
[20] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of Crypto 1984*, vol. 196, pp.47–53, 1984. Article (CrossRef Link)
[21] Craig Gentry and Zulfikar Ramzan, "Identity-Based aggregate signatures," in *Proc. of 9th International Conference on Theory and Practice of Public-Key Cryptography*, pp. 257-273, 2006. Article (CrossRef Link)
[22] S. Sesia, I. Toufik and M. Baker*, "LTE: The UMTS Long Term Evolution"*, *John Wiley and Sons*, 2009.
[23] 3GPP TS 33.220, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)," Sep.2011.
[24] 3GPP TS 33.223, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function," Apr.2011.
[25] 3GPP TS 22.368, "Service requirements for Machine-Type Communications (MTC); Stage 1," Sep.2011.
[26] 3GPP TS 33.210, "3G security; Network Domain Security (NDS); IP network layer security," Jun.2011.
[27] ETSI, "Smart Cards; Secured packet structure for UICC based applications (Release 9)," *TS 102 225*, May.2010.
[28] ETSI, "Smart cards; Remote APDU structure for UICC based applications (Release 6)," *TS 102 226*, May.2002.
[29] 3GPP TS 31.115, "Remote APDU Structure for (U)SIM Toolkit applications," Apr.2011.
[30] 3GPP TS 31.116, "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications," Apr.2011.
[31] Open Mobile Alliance OMA-TS-DM_Protocol V1.3, "OMA Device Management Protocol". Article (CrossRef Link)
[32] Open Mobile Alliance OMA-TS-DM_Security V1.3, "Device Management Security," Article (CrossRef Link)

[33] 3GPP TS 33.310, "Network Domain Security (NDS); Authentication Framework (AF)," Sep.2011.
[34] Kaufman, C., "The Internet key exchange (IKEv2) protocol," *RFC 4306*, Dec.2005. Article (CrossRef Link)

Lai Chengzhe, received his B.S. degree in Information Security from Xi'an University of Posts and Telecommunications, China in 2008. Currently he is a PhD Candidate in the School of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, China. His current research is in wireless network security and mobility management.

Li Hui, received his B.S. degree from Fudan University in 1990, M. S. and Ph.D. degrees from xidian University in 1993 and 1998. Since June 2005, he has been the professor in the school of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, China. He is aco-author of two books. He served as technique committee co-chairs of ISPEC 2009 and IAS 2009. His research interests are in the areas of cryptography, wireless network security, information theory and network coding.

Zhang Yueyu, received his B.S. degree from xidian University in 2005, M.S. and Ph.D. degrees from xidian University in 2005 and 2008. Currently he is a Associate Professor in the School of Telecommunications Engineering. His current research is in information security and next generation mobile communication network security.

Cao Jin, received his B.S. degree in Applied Mathematics from xidian University in 2008. Currently he is a PhD Candidate in the School of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, China. His current research is in wireless network security and handover authentication .