Computer Science and Information Systems 11(3):1071–1090 DOI: 10.2298/CSIS130922065D

Pairwise and Group Key Setup Mechanism for Secure Machine-to-Machine Communication

Inshil Doh[1], Jiyoung Lim[2], Shi Li[1], and Kijoon Chae[1]

[1] Dept. of Computer and Science and Engineering,
Ewha Womans University, Seoul, Korea
isdoh1@ewha.ac.kr, lishi1116@gmail.com, kjchae@ewha.ac.kr
[2] Dept. of Computer Software,
Korean Bible University, Seoul, Korea,
jylim@bible.ac.kr

Abstract. In the ubiquitous environment, more and more devices are deployed in our daily life, and need to communicate with one another. M2M (Machine-to-Machine) communication is considered to be one of the major issues in future networks. M2M is expected to bring various benefits in wireless communications when it is interconnected with cellular networks. Considering the characteristics of cellular M2M networks, traditional security solutions are not proper to be applied to cellular M2M networks because the M2M network itself is vulnerable to various attacks. We consider security aspects for cellular M2M communications and propose a key management mechanism including the pairwise key and group key establishment. Our proposal could provide reliability and efficiency for the cellular M2M communication network in the secure manner.

Keywords: M2M, cellular M2M communication, security, pairwise key, group key

1. Introduction

A machine can communicate with another machine directly in wireless manners. The Machine-to-machine (M2M) has attracted a lot of people and industries for its ability to increase efficiency and improve productivity while reducing operating costs. It has great application areas and it can be connected with other infrastructure and brings much more powerful and efficient results. M2M devices or M2M Equipments (M2MEs) will ultimately connect to core network services through a variety of means, from direct broadband or capillary wireless networks, to wired networks.

Connectivity to these wireless and wired networks is an essential part of M2M communication networks. There is a need to be able to integrate a variety of application-specific technologies into a complete end-to-end solution to be offered by service providers [1]. The leap in technology would not be possible without the support of the wide area wireless communication infrastructure in particular cellular data networks. It is estimated that there are already tens of millions of such smart devices connected to cellular networks worldwide and within the next 3-5 years this number will grow to hundreds of millions [2, 3]. Table 1 shows various application areas in the M2M communication. Among the application areas, the cellular M2M provides the ability to connect diverse devices and applications by enabling fixed assets, such as electric meters, or mobile assets, such as fleet vehicles. The cellular M2M is the best option to connect assets over great distances using already established, robust, and proven networks. The cellular technology is effective across widely varied industries because it is easy to integrate and cost-effective to deploy [4].

Table 1. M2M Application Area [5]

Market	Description	Applications
Security	Abnormal situation detection Homeland/industiry security	Suveilance Alert
Energy	Remote collect data on flow rate, pressure, temperature	AMR (automatic meter reading)
Transport	Tracking Telematics services ITS	Fleet Management Toll payment Emergency alerts
Commerce	Monetics	E-payment Virtual wallet solution
Automotive	Adapted insurance rate Telematics services	“Pay as you drive” Remote diagnotic
Home Automation	Remote monitoring, Managing	Surveillance Energy management
Healthcare	Patients monitoring, Curing	Blood pressure check

The cellular M2M market benefited from increasing numbers of mobile network operators launching M2M service offerings as their core service market grows increasingly mature and saturated. ABI Research expects cumulative cellular M2M connections to rise to 364.5 million globally by 2016. This report discusses the market and technical trends impacting the cellular M2M connectivity services market, analyzes cellular M2M connectivity service provider strategic responses, and forecasts cellular M2M connections and revenue growth for the period from 2007 through 2016, segmented by regions, applications, and air interface standards [6, 7].

There are lots of advantages of the cellular M2M. While Ethernet or Wi-Fi only provides the local coverage, cellular networks provide the ubiquitous coverage and the global connectivity. Users are already familiar with cellular networks, and they could use M2M applications easily on proprietary platforms [8].

A cellular M2M has great applications including telematics, asset management, U-healthcare, security and so on. Its application area will be drastically expanded. The more an organization relies on information technology and the more mobile it is, the greater the risks of security breaches. The success and the expansion of M2M depend on protecting security issues such as confidentiality, integrity, and availability of the data. As in Fig.1, basically, a Machine Type Communication (MTC) device, or an M2ME can be managed by the MTC server to be used by MTC users. They can be interconnected with each other through a Mobility Management Entity (MME), a Packet Gateway (P-

GW), and a Serving Gateway (S-GW). In some cases, they can communicate directly with each other. An M2ME is easy to be lost and hard to detect the malfunction. When integrity is not guaranteed, the equipments are excluded for services. In addition, M2MEs from one server or from one M2M user should be authenticated as one group, and they need to provide the individual communication at the same time.

Our contribution is that we have newly suggested the pairwise key establishment mechanism to make the direct communication more flexible and more secure for devices in mobile environments. It is especially important because the devices are mobile and can be located in the communication range of the others. If pairwise keys need to be distributed by the eNB every time they are required, the keys could be captured by the attackers. In addition to that, pairwise keys need to be generated in more structured way for better management. We propose a pairwise key generation mechanism using the key related information which is computed and delivered by the eNB efficiently in the energy and time consumption. Our proposal includes followings.

- Key establishment between eNB and mobile M2ME
- Key establishment between a pair of M2MEs for direct communication
- Group key establishment among M2MEs for group communication: Depending on the group key generation mechanism in our previous work [9], we defined functional group keys and regional group keys based on the location or their functions.
- We further simulated our proposal to compare the energy consumption for each type of devices. We also analyzed the computation, communication, and security aspects.

The remainder of this paper is organized as follows. Section 2 describes the system architecture for our proposal. Keys required for cellular M2M communication and the pairwise key agreement and group key agreement mechanisms are explained in Section 3. Section 4 evaluates the performance and security. Finally, we conclude our paper in Section 5.

2. Related Works

The 3GPP SA3 studied in TR 33.812, "Feasibility study on remote management of USIM application on M2M equipment". Its goal is to make it possible that the network can provision the remote management of USIM and ISIM application at M2M equipments in a secure way in a 3GPP system [10]. One of the main issues in TR 33.812 is to investigate candidate security solutions and signaling procedures for provisioning and the remote management of USIM/ISIM applications at M2M equipments in a secure manner. When an M2M is connected with cellular networks, its vulnerabilities to various attacks are increased. Security vulnerabilities get more serious when M2M is adopted on the top of cellular communication technologies. As a result, the growth of cellular M2M services would be limited without providing the service security.

We have proposed the key establishment and management mechanisms in our previous work [11]. Especially, for the direct communication between two devices, we suggested key distribution by an eNB (evolved Node B). When a pair of devices need a direct communication, they request pairwise keys to the eNB, and under the cooperation of eNBs, pairwise keys are generated and distributed by the eNBs for communication between two devices. In this work, we enhanced the pairwise key establishment mechanism to provide the security for the service.

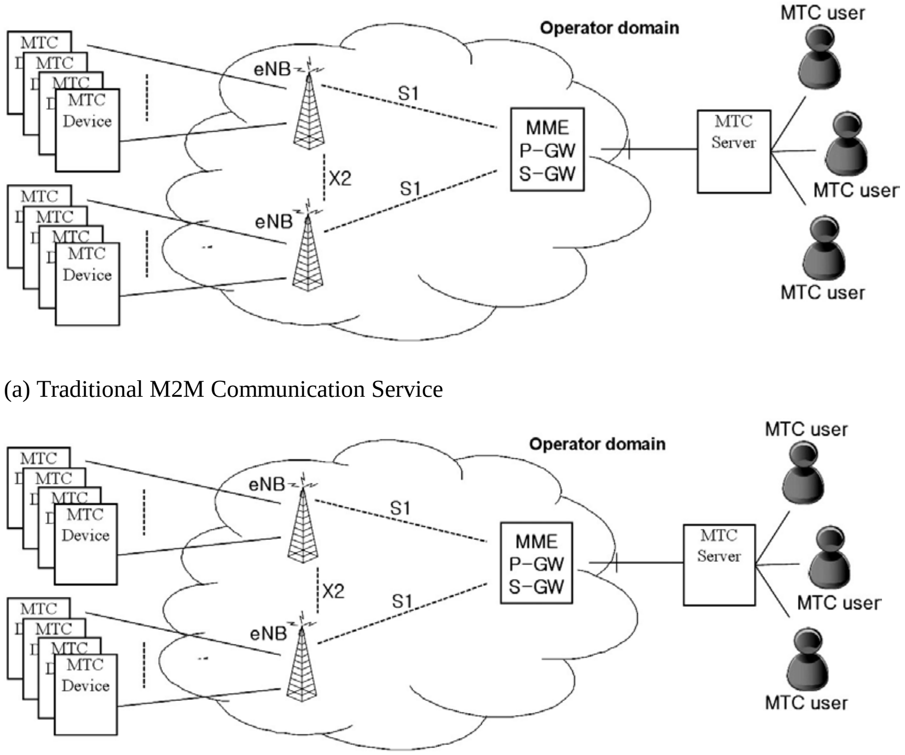
In general, group key management mechanisms can be classified into three categories. In centralized key management schemes, a group manager generates group keys and distributes the key to authenticated group members and manages the key material and lists. Blundo, C. et al. proposed a mechanism in which a server chooses a *t*-degree polynomial randomly and distributes them to neighbor nodes and the member nodes substitute the polynomial with their IDs; hence, all the nodes share one group key [12]. Wang, Y. and Ramamurthy, B. proposed four safe group communication methods [13]. Information for group key rekeying is unicasted to each node. This creates a heavy overload when group size grows. Broadcasting is proposed to solve the overhead problem. The broadcasting mechanism requires heavier overhead when groups are generated; however, rekeying cost is relatively low. Overlapping is also proposed to prevent a flooding attack. Finally, the group information pre-distribution minimizes the group generation time. A lot of researches have been done for centralized group key management. However, in mobile communication environment, parent-child relationship changes constantly because of devices movements. Even if centralized management is very stable and secure, it is not proper for adopting in mobile networks.

In distributed key management, multiple key managers generate group keys and distribute them to authentic members. Zhang, W. and Cao, G. proposed a mechanism (PCGR) that pre-distributes key related information and generates group keys [14]. When the group key rekeying is required, nodes cooperate and a new group key is computed. This scheme is applied in our proposal and will be more described in subsection 3.3. Huang, J. H. et al. proposed a level key infrastructure for multicast and group communication that uses level keys to provide an infrastructure that lowers the cost of nodes joining and leaving [15]. This scheme has a drawback in that process delay increases even when many nodes are changed. Zhu, S. et al. proposed a key management protocol for sensor network designed to support in-network processing, while at the same time restricting the security impact of a compromised node [16]. This mechanism is safer, because it uses four different kinds of keys. However, key update consumes much overhead. Adusumilli, P., Zou, X. and Ramamurthy, B. proposed a Distributed Group Key Distribution (DGKD) protocol which does not require existence of central trusted entities such as group controller or subgroup controllers [17]. Aparna, R. and Amberker, B.B. proposed a key management scheme for managing multiple groups. They uses a combination of key-based and secret share-based approach for managing the keys and showed that it is possible for members belonging to two or more groups to derive the group keys with less storage [18]. Kim, Y., Perrig, A, and Tsudik, G. investigated a novel group key agreement approach which blends key trees with Diffie--Hellman key exchange [19]. It yielded a secure protocol suite called Tree-based Group Diffie-Hellman (TGDH) that is both simple and fault-tolerant.

Contributed management mechanisms rekey the group keys through nodes' cooperation without specific key managers. Yu, Z. and Guan, Y. propose a group key management mechanism [20] in which basic matrix G and secret matrices A,B are assigned to each sensor node; each matrix is used to generate group keys among nodes in the same groups and different groups, respectively. The advantage of this mechanism is that the probability of generating group keys is high. However, when the grid size is large, much energy is wasted and when the grid size is small, group keys may not be generated.

3. System Architecture

Fig. 1 shows the M2M service infrastructure under the cellular communication environment. As in the figure, devices can communicate with one another with the help of eNBs which play the role of intervention. In this work, we basically assume that the devices can communicate directly when they are located closely enough while they move.

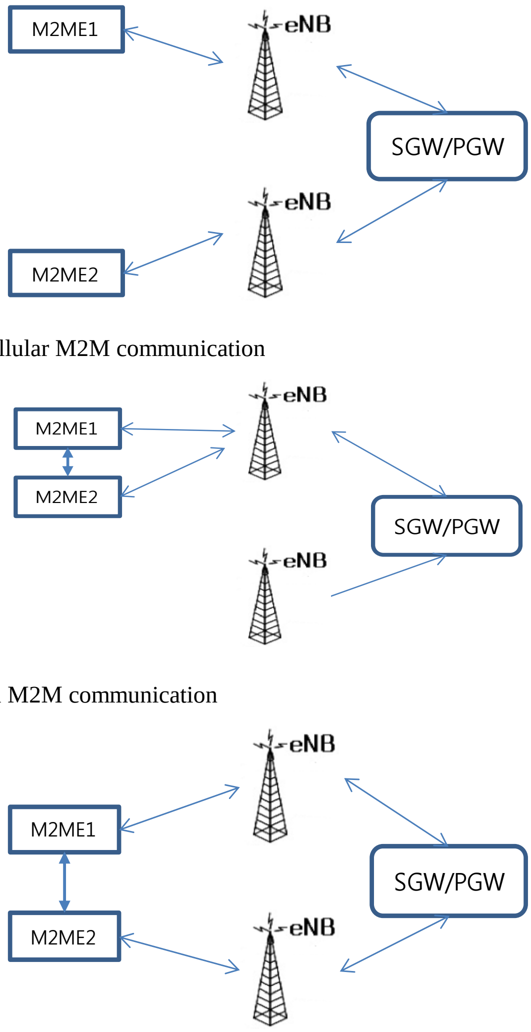


(a) Traditional M2M Communication Service

eNB: evolved Node B
P-GW: Packet Gateway
S-GW: Serving Gateway
(b) Cellular M2M Communication Service

Fig. 1. M2M Service Infrastructure

M2M devices could have high mobility. They need to communicate with other various devices while they are on the move. As in Fig. 2, a pair of M2M devices can communicate with each other when they meet and recognize that they are located in each other’s communication range. When they are enough close, they do not need the help of eNBs, but talk to each other as in (b) and (c) of Fig. 2. And for the direct communication, they need to be distributed pairwise keys for the secure connection. The pairwise keys are very important because they are the base for various security services such as confidentiality, integrity, authentication, and so on. Especially, these keys should be generated and deleted often without the breach of security in the mobile ubiquitous environment. The proper pairwise key generation mechanism should be provided.



(a) Default data cellular M2M communication

(b) Locally routed M2M communication

(c) Direct mode M2M communication

Fig. 2. Cellular M2M device communication

4. Key Establishment for M2M Communication

Various keys are required for the secure cellular M2M communication. They need to be established for data encryption, authentication, integrity, and so on. The keys required for the M2ME communication are as follows. We assume that each pair of eNBs shares pairwise keys for the secure communication among them. This assumption is reasonable because they are connected with one another in the wired infrastructure and considered relatively safe.

Pairwise Keys between an eNB and an M2ME. For the default data communication in the cellular M2M communication, an eNB and an M2ME need to share a pairwise key. In the initial stage, each M2ME belongs to specific eNB. However, they have the mobility and can meet the other devices while they are on the move. Even the devices move and communicate with other devices, the security should be provided in the reliable manner.

Pairwise Keys between M2MEs. As described in Section 2, M2MEs can communicate with each other with the help of an eNB, or they can communicate directly when they are in each other vicinity as in (b) and (c) of Fig. 2. There are a lot of devices and many instant direct connections are established and abolished. We need to support the situation with proper pairwise keys.

Functional Group Keys for M2MEs. Some M2MEs need the group communication. When it is for the functional group communication, they can share a group key. The group keys need to be managed by the Mobility Management Entity (MME) in Fig. 1, because the M2MEs are still group members even if they move from one cell to another.

Regional Group keys for M2MEs. The regional group can be formed in some region of the network field. When an M2ME moves in the region, they need to be provided the group key while they stay in the region and want to receive the data traffic of the group (Fig. 2 (b)). When they leave the region, the key is not valid anymore and the old group key needs to be rekeyed depending on the membership policy.

4.1. Key Establishment between eNB and Mobile M2ME

In our previous work [9], we have proposed the key establishment and authentication mechanism based on the USIM card for the ubiquitous healthcare system. For the cellular M2M communication, we basically assume that the USIM card and A3 and A8 algorithms are deployed in each M2ME. Based on the assumption, we can apply the initialization, key establishment, and authentication mechanism in our previous work to the cellular M2ME communication.

When an M2ME device is registered to an eNB, the ID of M2M device and a hashed key, $H(K_i)$ for the key generation are transferred to the eNB and M2ME through a secure channel. After registering the IDs of the device, the device and the eNB need to generate key chains with hash functions and A8 algorithm. The authentication processes for mobile devices to eNB is described in Fig. 3.

After getting the ID_{M2ME} and $H(K_i)$ of the M2M device, the eNB generates a nonce and encrypts it with $H(K_i)$ for the device to process A3 algorithm for authentication. After receiving and decrypting $Enc_{H(Ki)}$(nonce), the device computes A3 to generate RES_{M2ME} and sends this value back to the eNB. The eNB also computes RES_{eNB} with $H(K_i)$, nonce, and A3, and compares two values. If the eNB verifies the results are the same, authentication is completed. Then, two parties generate a hash chain and exchange the commitment values for the pairwise key generation. In this way, two parties prepare the keys for the future communication. Each computes the session key by computing A8 algorithm with the seed value from the key chain.

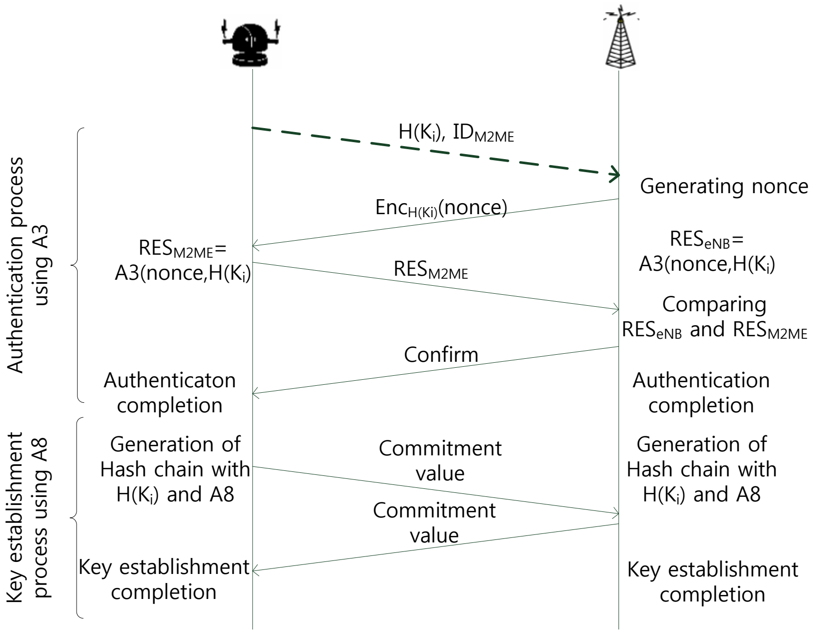

Authentication process using A3
Key establishment process using A8
H(Ki), IDM2ME
Generating nonce
EncH(Ki)(nonce)
RESM2ME= A3(nonce,H(Ki)
RESeNB= A3(nonce,H(Ki)
RESM2ME
Comparing RESeNB and RESM2ME
Confirm
Authenticaton completion
Authentication completion
Generation of Hash chain with H(Ki) and A8
Commitment value
Generation of Hash chain with H(Ki) and A8
Commitment value
Key establishment completion
Key establishment completion

Fig. 3. M2ME authentication and key generation in the cellular M2M communication system

When an M2ME moves in the cell, the eNB notifies it to an MME and receive the security information from the eNB where the M2ME has left. The information is renewed periodically for the security purpose.

4.2. Key Establishment between a Pair of M2MEs for Direct Communication

When M2MEs are communicating directly with each other, there are many advantages. Time and frequency resources can be reused and the latency can be reduced. For direct communication, pairwise keys are required for security. The pairwise key establishment processes follows on.

The eNB randomly generates an n×n grid with a set of 2^n bivariate polynomials $\Phi=\{F_i(x,y), G_i\ (x,y)\}$i=1,2,…,n as shown in Fig. 4. Each row i in the grid is associated with a polynomial $F_i(x,y)$, and each column i is associated with a polynomial $G_i(x,y)$. Each M2ME located in the eNB communication range will be randomly assigned to a unique intersection in the grid. For the M2ME at the coordinate (i, j) in the grid, (i, j) is considered as the ID of M2ME, and eNB distributes the polynomial shares of $(F_i(x,y), G_j(x,y))$ to the M2ME. In an example in Fig. 4, an M2ME (h, k) is assigned to the polynomial shares of $(F_h(x,y), G_k(x,y))$, and an M2ME (p, q) is assigned to $(F_p(x,y), G_q(x,y))$ similarly. And the polynomial shares belonging to an M2ME have two intersections with the polynomial shares belonging to the other one in the grid which are marked by stars in Fig. 4. The intersection polynomial shares are $(F_h(x,y), G_q(x,y))$ and $(F_p(x,y), G_k(x,y))$ respectively.

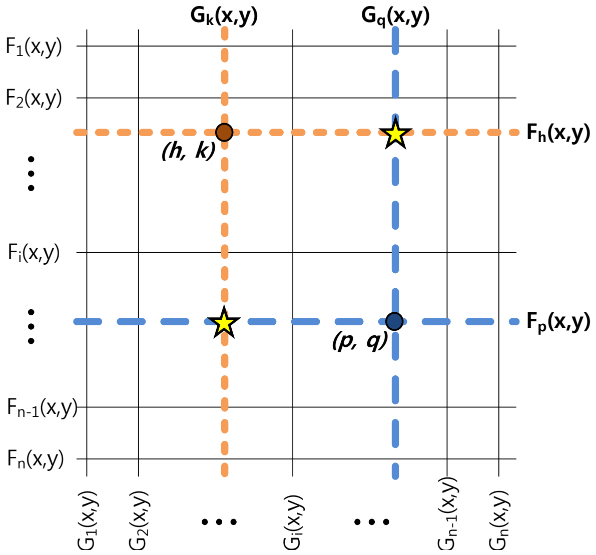


Fig. 4. Grid based key information distribution to M2MEs by eNB

When two M2MEs located in the same communication range of an eNB want to transmit secret messages to each other directly, they should encrypt the message by using pairwise keys between them. The pairwise key generation process is as follows:

– If there are two M2MEs want to communicate with each other directly, as mentioned above, the eNB will generate two points (e.g., (h,k) and (p,q)) as the ID of each M2ME in the n×n polynomial grid and distribute the IDs and the polynomial shares at the intersection of corresponding point in the grid (e.g., $\{F_h(x,y), G_k(x,y)\}$ and $\{F_p(x,y), G_q(x,y)\}$) to them respectively. As a result, the first M2ME obtains its ID(h,k) and polynomial share $\{F_h(x,y), G_k(x,y)\}$, and the second M2ME also receives its ID(p,q) and the corresponding polynomial share $\{F_p(x,y), G_q(x,y)\}$ as shown in Fig. 4.

– According to the above theory, an eNB can also find another two intersection polynomial shares in the grid as the star points shown in Fig. 4 and one polynomial share of them will be selected as the common secret information of the pairwise key. Assume that the intersection star point at the top-right corner ($F_h(x,y)$, $G_q(x,y)$) is selected here. And an eNB will inform two M2MEs of the selected polynomial part from each of them. Here, the first part $F_h(x,y)$ comes from the polynomial share of an M2ME (h,k) and the second part $G_q(x,y)$ is from an M2ME (p,q).

- By utilizing the average coordinate of two M2MEs in the grid and another bivariate polynomial e(x,y) which is pre-distributed in all components of the system, two M2MEs can generate the pairwise key between them at each side. The process can be seen in Fig. 5.

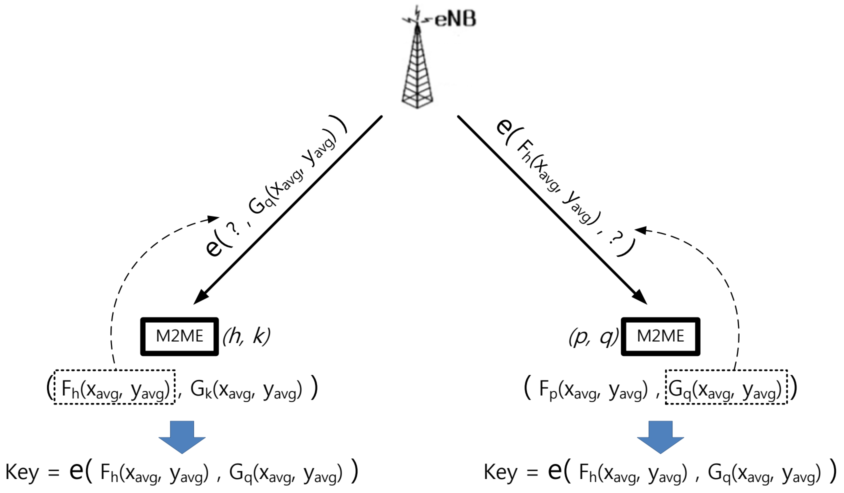

eNB
$e(? , G_q(x_{avg}, y_{avg}))$
$e(F_h(x_{avg}, y_{avg}) , ?)$
M2ME (h, k)
(p, q) M2ME
$(F_h(x_{avg}, y_{avg}) , G_k(x_{avg}, y_{avg}))$
$(F_p(x_{avg}, y_{avg}) , G_q(x_{avg}, y_{avg}))$
$Key = e(F_h(x_{avg}, y_{avg}) , G_q(x_{avg}, y_{avg}))$
$Key = e(F_h(x_{avg}, y_{avg}) , G_q(x_{avg}, y_{avg}))$

Fig. 5. Pairwise key generation process between M2MEs

An eNB replaces the variable y in the bivariate polynomial e(x, y) by the value of $G_q(x_{avg}, y_{avg})$ and transmits the result polynomial with only one unknown x to M2ME (h, k), where Gq is the polynomial selected from polynomial share of an M2ME (p, q) as mentioned above and (x_{avg}, y_{avg}) stands for the average coordinate of M2MEs (h, k) and (p, q), the calculation is as follows:

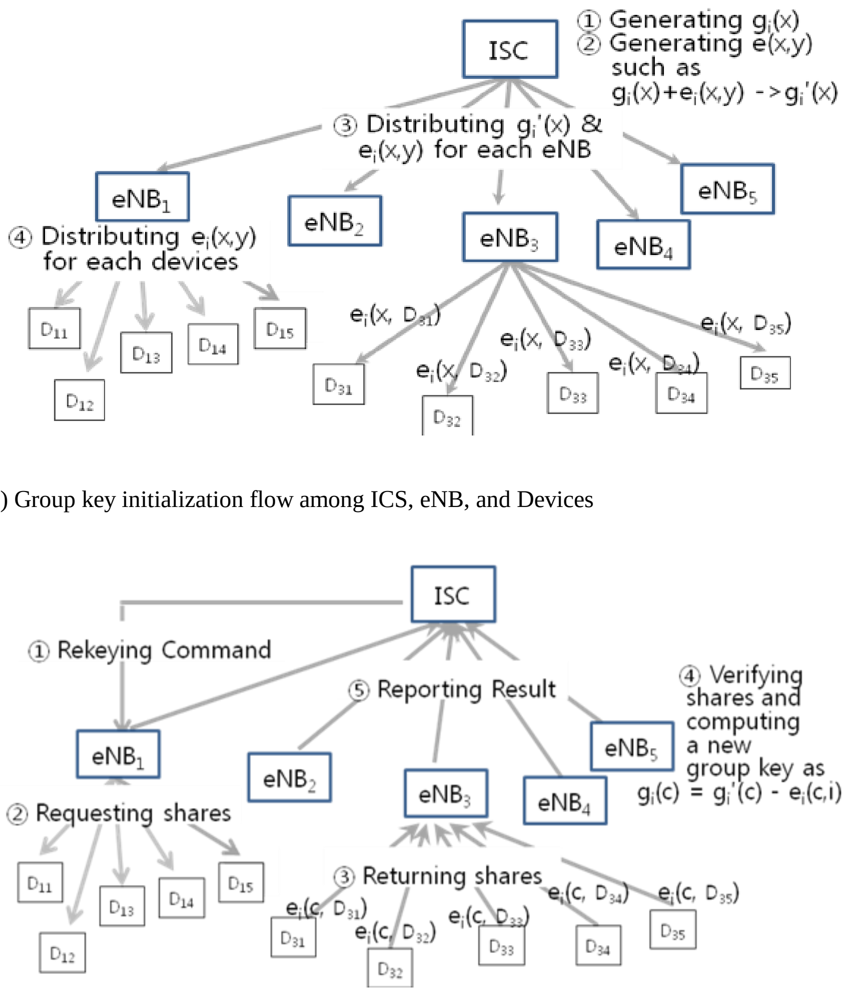
$$(x_{avg} , y_{avg}) = ((h+p)/2, (k+q)/2) \qquad (1)$$

After receiving the polynomial $e(x, G_q(x_{avg}, y_{avg}))$ with unknown x, an M2ME (h, k) replaces the variable x by the value of $F_h(x_{avg}, y_{avg})$ which is calculated by its own polynomial F_h selected in step 2 and the average coordinate of two M2MEs, then an M2ME (h, k) can obtain the pairwise key, $e(F_h(x_{avg}, y_{avg}), G_q(x_{avg}, y_{avg}))$ shared with an M2ME (p, q). For an M2ME (p, q), it can also calculate the pairwise key by operating the similar process. According to the calculation above, M2MEs (h, k) and (p, q) can generate their pairwise key as:

$$Key = e(F_h(x_{avg}, y_{avg}) , G_q(x_{avg}, y_{avg}) \qquad (2)$$

4.3. Group Key Establishment among M2MEs for Group Communication

The group based policing and addressing are required in the cellular M2M communication. The network shall enable the broadcast to a specific group of devices. In our previous work, we proposed an energy-efficient and secure channel group key establishment and rekeying management scheme for mobile IPTV services [9, 22].



(a) Group key initialization flow among ICS, eNB, and Devices

(b) Group key rekeying for all devices

Fig. 6. Group key management based on PCGR

It adopted Pre-distribution and local Collaboration-based Group Rekeying (PCGR), a group key management scheme for sensor networks [14]. We basically considered the cellular network environment where many mobile devices are provided IPTV services through eNBs and an ISP (Internet Service Provider). Because the mechanism is to generate group keys for the group communication and to rekey the group keys is can be efficiently adopted for the cellular M2M group communication. Its process is shown in Fig. 6 and here is the brief description.

- ISC generates the channel key polynomials, g(x)s for each channel and encryption polynomials e(x,y)s. ISC then distributes encryption polynomials e(x,y)s and encrypted polynomials g'(x)s to each eNB under the channel service.
- After receiving the polynomial information, the eNB distributes the shares of the encryption polynomials of its own to its member nodes and deletes the original polynomial information.
- On rekeying time, the eNB gathers computed shares from its devices to compute the new keys. When the verification of the shares from the devices is successful, the eNB computes the new group key with the shares and distributes the new group key to its members.

The details are omitted here. One more important advantage of our proposal is that we can reuse the polynomials distributed in the pairwise key setup phase to compute group keys. In the case, not only the communication overhead, but also the computation and storage overhead can be decreased.

Group keys can be classified into functional group keys and regional group keys based on the situation where they are used. They do not have any difference in the establishing or rekeying process. When nodes need any functional group communication even if they are located in physically different regions, they generate keys and share them among functional group members. The difference between functional group keys and regional group keys are shown in Fig. 7.

Functional Group Key. When the group communication is required for specific functions among M2MEs, group keys are to be established among M2MEs which accomplish the functions. In this case, M2MEs can be scattered in many cells. For example, some of the M2MEs need to provide specific data or need to play the role of relaying for other M2MEs. In this case, several designated M2MEs require group keys and even if they are mobile, memberships are not often changed. Even if the M2ME moves to another cell, an MME can manage their locations if only the M2ME maintains the group membership. When new M2MEs move in to the specific cell, the eNB of the cell notifies it to the MME and the location information is managed by the MME while the group membership and the group key are not changed. It is because the M2ME is still the functional group member even if its location is changed.

Regional Group Key. The regional group membership is related to the specific region of the network. In the regional group, the group membership could be changed depending on the policy and the mobility of the M2MEs. The ratio of M2MEs to eNB in the regional group is higher than that of functional group membership. The overhead for managing the group keys can be decreased when eNBs provide the secret share and the new group keys generated are just distributed to M2MEs by the eNBs. After generating the new regional group key, eNB distributes the new key encrypted with the old group key to each group member M2ME. When the M2ME moves out of the regional group, it is notified to the MME, and the group keys can be rekeyed according to rekeying policy. The process is as in Fig. 7.

- When an M2ME moves in the new cell and the M2ME is still in the regional group area, the eNB asks if the M2ME wants to get the group service.
- If the answer is yes, the eNB notifies this to the MME and the MME just modifies the location information without rekeying the group key because the M2ME is still the group member.
- Otherwise, eNB notifies the answer to the MME, and the MME decides if the group key should be rekeyed or not.
- If rekeying is required, the MME requests the key share to the eNBs.
- The eNB replies with the key shares.
- The MME computes the new group key, sends it back to eNBs. Finally, eNBs distribute the new group key to each member devices in each cell.

When the devices move into another cell in the regional group keying or if there is any change in their subscription, group keys need to be rekeyed right away for the security protection while a pairwise key between a pair of M2MEs keeps for certain period because they can communicate with each another again in short time difference.

5. Performance Analysis

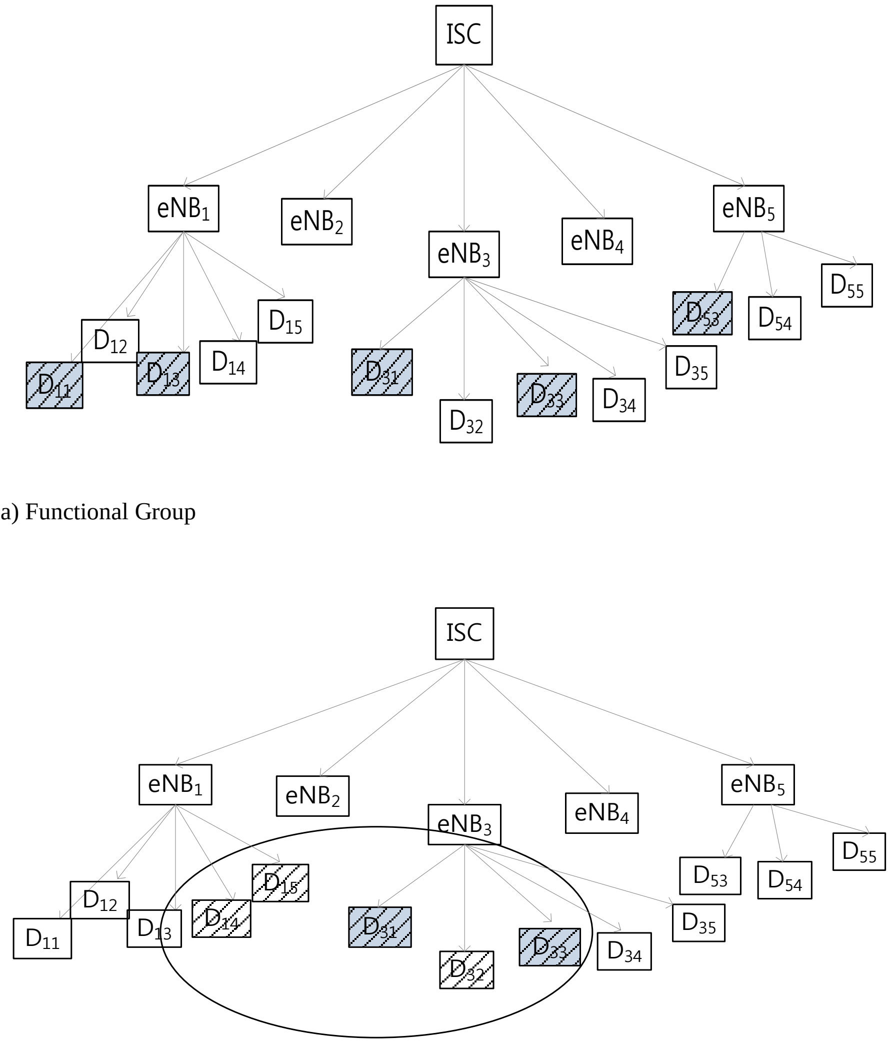
When an M2M is coupled with the cellular communication, the cellular network security mechanisms can be basically applied. To the best of our knowledge, there is no key agreement mechanism proposal for cellular M2M group communication. Even through traditional security mechanisms in cellular network can be applied, direct M2M communication has different characteristics and different security mechanisms are required. It is not possible that we compare our key agreement proposal with other mechanisms because there is no proper one to be compared. We would like to analyze our proposal to show how it is efficient. We also consider the communication, computation overhead, and security aspects for cellular M2M communications related to proposed key establishment.

5.1. Simulation Result

In Fig. 8, we can see the communication time between a pair of M2MEs. When they are located in its own communication range, they can talk to each other in direct mode. Communication time in direct mode is much shorter than the case in which they communicate passing through the eNB.

Fig. 9 shows the energy usage of M2MEs and the eNB in M2ME direct communication. Sending M2ME consumes more energy than the receiving M2ME, and of course eNB consumes basic energy for its own function as the base station, while eNB in indirect mode consumes more energy than the M2MEs because it needs to relays the data in between as in Fig. 10.

In Fig.11, we can see that key information is sent by the eNB to each M2MEs, and the receiving energy of the M2MEs increases a little, while energy consumption of eNB for sending data increases. It shows that M2MEs do not consume much energy for key information distribution.



(a) Functional Group

(b) Regional Group

Fig. 7. Two different kinds of groups for the efficient group key management

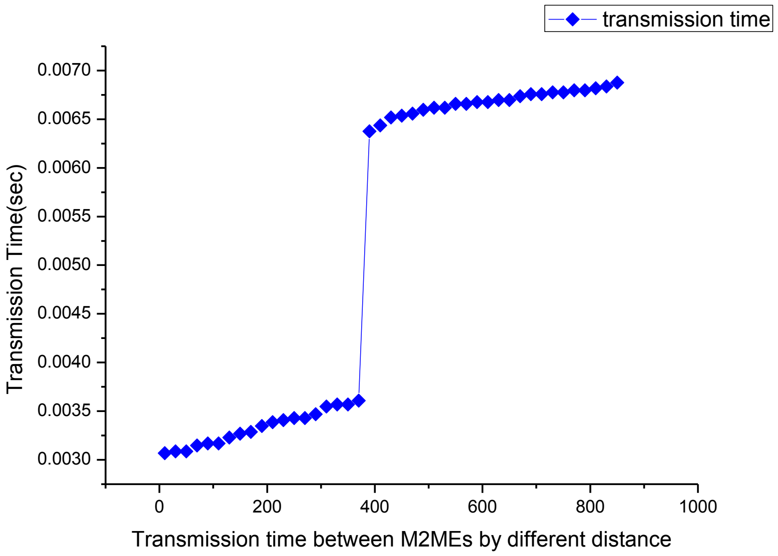


Fig. 8. Transmission time between M2MEs as a function of distance

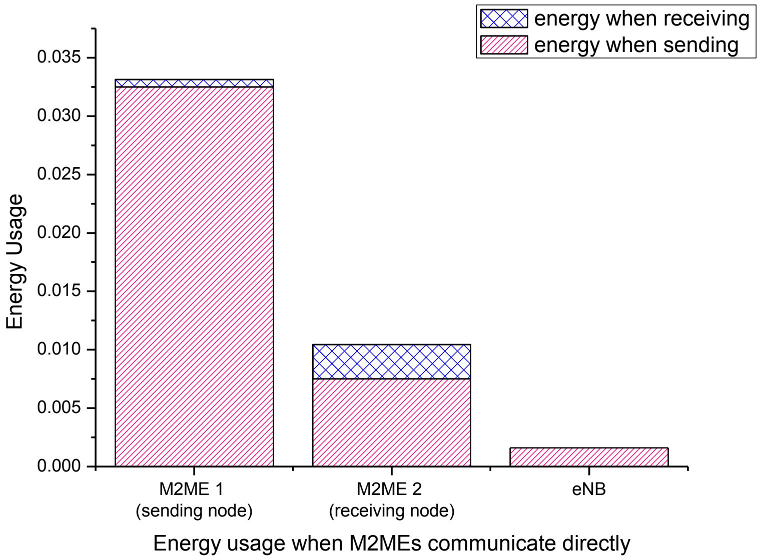


Fig. 9. Energy consumption in direct mode M2ME communication

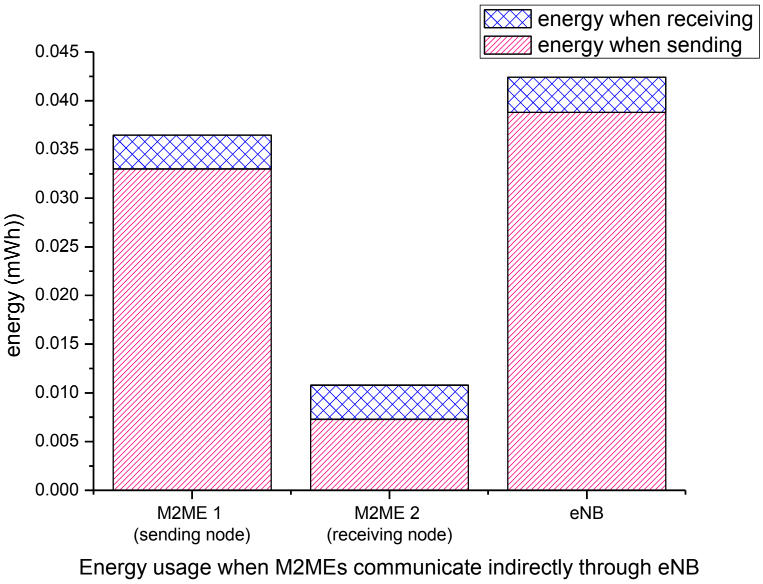


Fig. 10. Energy consumption in indirect mode M2ME communication

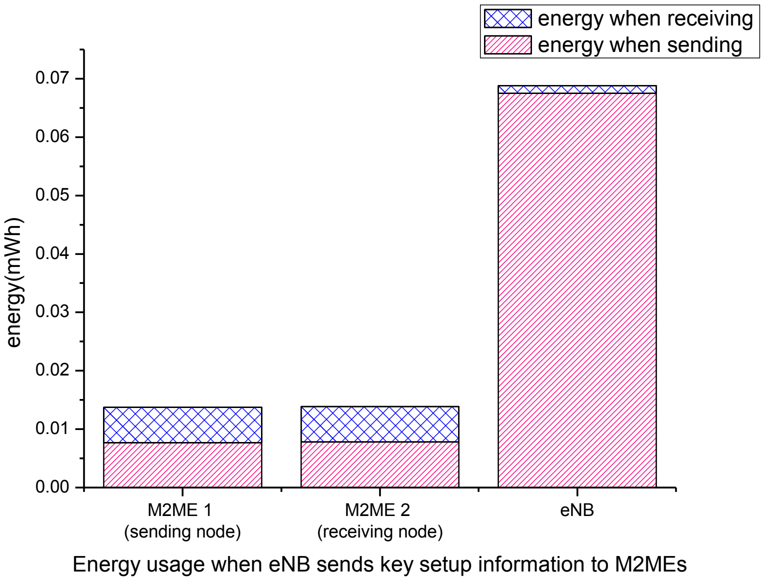


Fig. 11. Energy consumption of eNB and M2MEs for key information delivery

5.2. Communication and Computation Analysis

In our previous work [11], we have proposed key establishment and authentication mechanism based on USIM card for ubiquitous healthcare system. In the mechanism, we proposed that when direct M2M communication is required, they request key information to their own eNBs, and the eNBs generate a pairwise key between two devices through cooperation. The problem is that when more and more pairs of devices request direct communication, key generation overhead is getting heavy on the eNBs. In addition, key management is getting difficult and complicated.

In our newly proposed mechanism, all the M2MEs are pre-distributed the e(x,y) in the setup stage, and when they want to communicate with one another, they are additionally distributed two more polynomials to compute pairwise keys. With the polynomials, they can make pairwise keys with another M2ME no matter how many communication partners they may have. Because M2MEs can compute pairwise keys and communicate with one another, the overload of the eNBs is getting lighter, and the management is also very simple.

For communication overhead, the M2MEs request key shares to eNBs, and once they get two more polynomials for direct communication, they don’t need to request keys to eNBs but can calculate their own keys. When there are a lot of pairs wanting direct communication, our proposal decreases the communication overhead in great amount.

For computation and storage overhead, each M2MEs need to store three polynomials for setting up the pairwise keys. However, only coefficients are delivered and the storage required is not big. In addition, the computation is very simple, and it does not cost much for mobile M2MEs. In addition, using the polynomials distributed, group keys can be computed and the overall computation and storage overhead can be lowered further.

5.3. Security Analysis

In this subsection, we consider the security aspect of our proposal. As described in 3.2, in our proposal, there are two intersection points, and one of the points is chosen to setup the pairwise key. This increases the security level because even if some security information revealed, the attackers have 50% chance to compute the pairwise keys. Especially, periodic redistribution of polynomials makes the security level high.

Confidentiality. In cellular M2M communication, personal information such as location, account data, the content of the data can be revealed if the data are not encrypted. For encrypting the data, traffic encryption keys are used. In our work, we have proposed the pairwise key agreement between M2MEs and eNBs or between M2ME communications. We also proposed the group key establishment process for the secure group communication. Even the attackers would eavesdrop on the data using the keys properly, the confidentiality could be achieved.

Authentication. Basically, a machine needs to authenticate the other entities before their communication. In many cases, they need to mutually authenticate each other. In our proposal, by adopting the algorithms in the USIM card, the device and an eNB can mutually authenticate each other. For the communication between the devices, additional authentication process is required.

Access Control. For the devices to get the access to the network, they need a process for getting the admission. The process is out of the scope or our work. However, through the admission step in cellular network, access can be controlled by the eNBs, and basic key related information can be acquired for further security functions.

Integrity. Integrity is required for keeping data from being forged or modified by the attackers. The keys from our proposal can be used for encrypting the data and the data can be decrypted only by the receiver. If pairwise keys could be delivered by the eNB, and the eNB could be not compromised, integrity could be obtained.

Privacy. In many cases, M2MEs are deployed closely to human beings. The data can contain very personal information which is not supposed to be disclosed. These days, privacy is one of the major security issues to be protected. Privacy protection is one of our future works.

6. Conclusions

More and more M2MEs are connected to traditional infrastructures in wired or wireless environments. Especially, connection between cellular network and M2M equipment is expected to bring great impacts and the market share in the future network. When M2MEs communicate with one another in the cellular infrastructure, the possibility of security breaches is getting higher while the great deal of application services are provided. In this work, we proposed key establishment mechanisms for secure communication among entities in the cellular M2M network. The mechanism includes pairwise keys for the M2M communication and the group communication among the M2MEs. Our key agreement proposal can provide security and reliability for the cellular M2M communication.

Acknowledgments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A3019459).

References

1. Cha, I., Shah, Y., Schmidt, A. U., Leicher, A., and Meyerstein, M.: Trust in M2M communication. IEEE Vehicular Technology Magazine, Vol.4, Issue 3, pp. 69-75. (2009)
2. 3G machine-to-machine (M2M) communications: Cellular 3G, WiMAX, and municipal Wi-Fi for M2M applications. Technical report, ABI Research (2007)
3. Ryberg T.: The global wireless M2M market. Technical report, Berg Insight (2009)

4. Fledderjohn, D.: Learn Cellular M2M Basics. Field Tchnologies Online
5. M2M Technology and Services of KT, KNOM Tutorial (2011)
6. Cellular M2M Connectivity Services - Research Report by ABI Research (2012)
7. Shafiq, M. Z., Ji, L., Liu, A. X., Pang, J., and Wang J.: A First Look at Cellular Machine-to-Machine Traffic – Large Scale Measurement and characterization. SIGMETRICS'12, June pp. 11-15 (2012)
8. Dohler, M., Watteyne, T., Alonso-Zárate, J.: Machine-to-Machine: An Emerging Communication Paradigm. Mobilight 2010, MONAMI 2010, PIMRC 2010, Globecom 2010 (2010)
9. Doh, I., Lim, J., and Chung, M.: Group Key Management for Secure Mobile IPTV Service. In Proceedings of Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 352-357 (2012)
10. 3GPP TR 33.812, [Online]. Available: http://www.3gpp.org/DynaReport/33812.htm (current Jun 2014)
11. Doh, I., Lim, J., and Chae, K.: Key establishment and management for Secure Cellular Machine-to-Machine Communication. In Proceedings of the Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 579-584 (2013)
12. Blundo, C., Santis, A. D., Herzbeerg, A., Kutten, S., Vaccaro, U., and Yung, M.: Perfectly-Secure Key Distribution for Dynamic Conference. Information and Computation, Vol. 146, Issue 1, pp. 1-23 (1998)
13. Wang, Y., Ramamurthy, B., and Xue, Y.: Group Rekeying Schemes for Secure Group Communication in Wireless Sensor Networks. Proceedings of the IEEE International Conference on Communications, pp. 3419-3424 (2007)
14. Zhang, W., and Cao, G.: Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration Based Approach. IEEE Infocom 2005, Vol. 1, pp.503-514 (2005)
15. Huang, J. H., Buckingham, J., and Han, R.: A Level Key Infrastructure for Secure and Efficient Group Communication in Wireless Sensor Networks. Proceedings of The International Conference on Security and Privacy for Energing Areas in Communications Networks, pp. 249-260 (2005)
16. Zhu, S., Setia, S., and Jahodia, S.: LEAP+: Efficient Security Mechanisms for Large-Scale Disributed Sensor Networks. ACM Transactions on Sensor Networks, Vol. 2, Issue 4, pp. 500-528 (2006)
17. Adusumilli, P., Zou, X., and Ramamurthy, B.: DGKD: Distributed Group Key Distribution with Authentication Capability. Proceedings of the IEEE Workshop on Information Assurance and Security, pp. 276-293 (2005)
18. Aparna, R., and Amberker, B. B.: Key management scheme for multiple simultaneous secure group communication. Proceedings of the IEEE Internet Multimedia Services Architecture and Applications (IMSAA), pp. 1-6 (2009)
19. Kim, Y., Perrig, A., and Tsudik, G.: Tree-based group key agreement. ACM Transactions on Information and System Security (TISSEC), Vol. 7, Issue 1, pp. 60-96 (2004)
20. Yu, Z., andGuan, Y.: A Robust Group-based Key Management Scheme for Wireless Sensor Networks. Proceedings of the IEEE Communications Society 2005, Vol. 4, pp. 1915-1920 (2005)
21. Park, J., Doh, I., and Chae, K.: Security Approach for Ubiquitous Healthcare Services through Wireless Communication. In Proceedings of ACSA 2012, pp. 381-385 (2012)
22. Doh, I., Lim, J., and Chae, K.: Key Management Approach for Secure Mobile Open IPTV Service. Computer Science and Information Systems 2013, Vol. 10, pp. 843-864 (2013)

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009~2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul. Her research interests include wireless network, sensor network security, and M2M network security.

Jiyoung Lim is the corresponding author of this paper. She received the B.S. and M.S degrees in Computer Science at Ewha Womans University, Korea, in 1994 and 1996, respectively and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2001. She is currently an associate professor of Computer Software at Korean Bible University, Seoul, Korea. Her research interests include wireless/sensor network security, and M2M network security.

Shi Li received the B.S. degree in the Department of computer science and engineering from Harbin Institute of Technology, China in 2010. She is currently a Ph.D candidate in the Department of computer science and engineering at Ewha Womans University, Seoul, Korea. Her research interests include sensor network security, smart grid security and content delivery network security.

Kijoon Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D degree in Electrical and computer engineering from North Carolina State University in 1990. He is currently a professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include network security, sensor network, network protocol design and performance evaluation.

Received: *September 22, 2013*; *Accepted*: *February 18, 2014.*