A Security Mechanism for Public Warning System in LTE

Kyungjoo Suh† †and Sunghyun Choi† †
†School of Electrical & Computer Engineering and INMC, Seoul National University, Seoul, Korea
†Samsung Electronics, Suwon, Korea
Email: kjsuh@mwnl.snu.ac.kr, schoi@snu.ac.kr

Abstract—In this paper, we propose a security mechanism for Public Warning System (PWS) in Long Term Evolution (LTE) communication system. The proposed mechanism enhances the security for LTE PWS. It also includes the methods to reduce the overhead of message transfer and security key distribution compared with existing solutions.

Index Terms—3GPP, PWS, Security

I. INTRODUCTION

Long Term Evolution (LTE) is developed for high speed data communication in wireless environment and it evolves from GSM and UMTS network technology. LTE is specified in release 8 document series in 3GPP (The Third Generation Partnership Project). The LTE coexists with other previous mainstream technologies including Code Division Multiple Access (CDMA) and Wideband Code Division Multiple Access (WCDMA). CDMA is standardized mainly through The Third Generation Partnership Project 2 (3GPP2) in the USA while 3GPP in Europe standardized WCDMA. The increasing demand for capacity and speed is in line with the growth of packet data communication by using smartphones.

As more natural disasters are caused by abnormal climate in the world, the public warning mechanism becomes more important. Therefore, Public Warning System (PWS) based on mobile communication system is being introduced. On the other hand, Japan builds Earthquake Tsunami Warning System (ETWS) to issue earthquake warning. Because the warning messages of PWS or ETWS are broadcast concurrently to the group of people who are in the site of disaster, the speed is more important than security. However, recently security is considered an important feature. For example, if an unauthorized user can send warning message to the group of people in the sports stadium, people can be crushed to death while trying to be evacuated to outside simultaneously. Therefore, the PWS with security feature has been discussed in the 3GPP standardization. In this paper, we present the problems of PWS security mechanism, and propose a secure method for PWS with reduced overhead.

II. 3GPP LTE PWS

3GPP PWS requirements are reflected in 3GPP TS 22.268, which encompasses ETWS requirements in 3GPP TS 22.168 and Commercial Mobile Alert Service (CMAS) requirements. To satisfy the requirements, Cell Broadcast System (CBCS) is adopted in 3GPP TS 23.041. The public warning messages are broadcast to every receiver in a specific cell broadcast area in the form of unacknowledged Cell Broadcast System (CBS) messages [1–3]. This CBS message is delivered from a Cell Broadcast Entity (CBE) such as national agency or disaster management agency to Cell Broadcast Center (CBC). Fig. 1 presents PWS architecture for public warning message delivery. The PWS security solution has to satisfy roaming requirements. That is, in the case of roaming, the PWS supporting User Equipment (UE) has to receive the warning message from the Visited Public Land Mobile Network (VPLMN).

To protect PWS, the security mechanism with which security keys are delivered and updated through Non-Access Stratum (NAS) message is being discussed in 3GPP. Other candidate security solutions for PWS include Generic Bootstrapping Architecture (GBA) based protection, implicit certificate Public Key Infrastructure (PKI) based solution, and national PWS solution based on Universal Integrated Circuit Card (UICC) Over-The-Air (OTA). Each solution has pros and cons. If the operator deploys security solution using GBA for PWS, to support roaming, the VPLMN also should be deployed utilizing GBA. If implicit certificate PKI solution is applied for PWS, the management of certificate authority (CA) is important for the system to work properly. The hierarchy of CAs and their mapping with regions make impact on the performance. If multiple CBEs exist, the system complexity is affected by the relationship among multiple CAs and CBEs. Using the OTA, enforcing the PWS security mechanism has limitation for applicable areas because there are circumstances where different PLMN support different OTA service [4, 5].

III. LIMITATION OF PWS SECURITY

The existing NAS based security solution for PWS on discussion in 3GPP is conducted in accordance with the following main procedures: Under such a condition as shown in Fig. 1, the UE sends key identity in a NAS message such as
Attaching a public key to MME, the MME sends SMC, Attach Accept, or Tracking Area Update Accept message to UE including the public key and key index.

The aforementioned mechanism for the delivery of security keys using NAS message has limitations in system implementation. First of all, the security key delivery using NAS message causes additional message overhead. The maximum message length with variable length fields runs as follows: the Security Mode Command (SMC) message of 21 octets and Tracking Area Update (TAU) Accept of 246 octets. If security mechanism using NAS message is adopted, the public key for decoding of digital signature, key index, and CBE identifier are transferred. Even if we consider the method only for sending public key, the method requires at least 160–3072 bits with original message. Moreover, depending on selection of security level (High/Middle/Low) or digital signature algorithm, such as Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), the length of public key changes and the whole security system performance is different.

If TAU Accept message is employed, the overhead for security key delivery is higher than using SMC message. The reason is that TAU Accept message is longer than SMC message and the period is shorter than SMC. However, TAU Accept message has advantage in PWS security key update due to short update period. Next, the mapping information for message delivery area and key delivery site is necessary for security key mapping. The Cell Broadcast messages are transferred by unit of cell or a group of cells. In contrast, the security key is delivered by NAS message delivering unit such as Tracking Area. Finally, the possibility of information inconsistency can emerge due to the fact that the key information is updated in NAS message unit and the Cell Broadcast messages are delivered by Cell, Tracking Area, or Public Land Mobile Network (PLMN) unit. Therefore, message decoding or key update can have a possibility of performing incorrectly.

Next, in addition to key update with time, the updated key is delivered to other mobile phones in the same area when the key is updated for a specific mobile phone. Even if we consider the method only for sending public key, the method requires at least 160–3072 bits with original message. Moreover, depending on selection of security level (High/Middle/Low) or digital signature algorithm, such as Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), the length of public key changes and the whole security system performance is different.

If TAU Accept message is employed, the overhead for security key delivery is higher than using SMC message. The reason is that TAU Accept message is longer than SMC message and the period is shorter than SMC. However, TAU Accept message has advantage in PWS security key update due to short update period. Next, the mapping information for message delivery area and key delivery site is necessary for security key mapping. The Cell Broadcast messages are transferred by unit of cell or a group of cells. In contrast, the security key is delivered by NAS message delivering unit such as Tracking Area. Finally, the possibility of information inconsistency can emerge due to the fact that the key information is updated in NAS message unit and the Cell Broadcast messages are delivered by Cell, Tracking Area, or Public Land Mobile Network (PLMN) unit. Therefore, message decoding or key update can have a possibility of performing incorrectly.

IV. PERFORMANCE IMPROVEMENTS FOR PWS SECURITY

The proposed solution for performance improvements of public warning security enhancement system has the following characteristic features. First, the transferring unit of Cell Broadcast Message is aligned with security key delivery unit. The solution eliminates the problem caused by inconsistency in security key information. Therefore, the additional mapping is not required for information consistency. The security key can be properly applied for the verification of digital signature. Next, in addition to key update with time, the updated key is delivered to other mobile phones in the same area when the key is updated for a specific mobile phone. By updating security keys in the same area, the key inconsistency problem after key update is solved.

The proposed solution in this paper is designed as shown in Fig. 2: we consider a situation when the UE moves within an area or from the area to others. The area consists of cells, tracking areas, or a PLMN. The CBEs exist in multiple locations to take emergency actions for different purposes.

A CBE and a CBC are connected securely, and the CBE is positioned in the area where public warning message is delivered. The configured area in which message is delivered, namely, the security key area level is cell, PLMN, or Tracking Area unit. The CBE stores public key, private key, key index, CBE identifier, digital signature algorithm, and security level. Among all the relevant information, the key and key index are stored in the MME. An MME checks match of the area information designated by CBC with the area information of mobile phones. An MME transfers the key and key index pair to eNB, and eNB forwards information to mobile phone. The mobile phone stores the received public key and key index pair. The public key is used for the verification of message sender by decoding digital signature when mobile phone receives the warning messages.

The main algorithm of the proposed solution works as follows. A key is configured depending on security key area level, such as cell, Tracking Area, and PLMN, and it is delivered with a key index. If a key is updated at the expiration time, the updated key is applied for other mobile phones in the same area. In addition, if a new mobile phone joins the same site, the key update can happen for this site. If several security keys exist in the same area, a number of candidate solutions are possible. One is using the last update key. The other is configuring the message with several keys and the key, which is success for the verification, is used for PWS security. The former is more efficient than the latter. Algorithm 1 presents the above explained procedure.

V. PERFORMANCE EVALUATION

The performance comparison between the proposed solution and the existing solution is made from two perspectives: one is the number of required bits and the other is the required time for key distribution and update. The comparison is based on the 3GPP specification which describes both the individual message format and required time [3, 6]. For TAU accept and SMC message, the maximum is assumed for the fields with variable length. For the message sender verification, the digital signature algorithm such as DSA and ECDSA is employed.
Algorithm 1 Proposed Solution for PWS Security

1: if AreaLevel == Cell then
2:   set Key1
3:   send PublicKey, KeyIndex
4:   if Timer expires then
5:     update Key1
6:     apply key update to UEs in the same area
7:   end if
8:   if new UE join to cell then
9:     update Key1
10:  end if
11: else if AreaLevel == TA then
12:   set Key2
13: else
14:   set Key3
15: end if
16: if several Keys exist in the same area then
17:   use last updated Key
18: end if
19: if several Keys exist in the same area then
20:   configure messages with Keys
21: if UE success verification of messages with Keys then
22:   use successful Key
23: end if
24: end if

Fig. 3. Security information transmission efficiency.

Security strength is associated with the amount of operations that are required to break a cryptographic algorithm. Security strength, namely, security level (Low/Middle/High), can be specified in terms of the number of bits. Among possible values {80, 112, 128, 192, 256}, three values in the set {80, 112, 128} are considered in this paper. In the required time comparison, the proposed solution considers the fixed schedule for system information distribution.

As shown in Fig. 3, the performance gain comes from the fact that the security key information is delivered using Access Stratum (AS) message instead of NAS message. Because the proposed solution does not use NAS message for security key delivery, the minimum bits are necessary for security information delivery through AS message.

Fig. 4 presents the required time comparison between the proposed solution and the existing solution using NAS message for PWS security key distribution and update. Using NAS message, initial security key distribution requires extra procedures. The state transition from idle state to connected state or tracking area update might cause additional procedure for key distribution. In contrast, using AS message does not require such an additional process for key distribution due to state transition. The performance gain for update time depends on scheduling. Therefore, the overall performance of the proposed scheme is better than that of mechanism using NAS message thanks to the simplified procedures.

VI. Conclusion

In this paper, we identify the problems in security key distribution based on Non Access Stratum (NAS) message in existing PWS security enhancement mechanism. To improve the message overhead of existing NAS based solutions, we propose a mechanism with which the security key is distributed with a cell or a group of cells as a unit. In addition to this distribution, the renewal method of security key is proposed. According to the performance comparison between the existing solution and the proposed solution, the proposed solution reduces the overhead required for the Public Warning message protection, and it simplifies the key mapping procedures.

REFERENCES