ISSN 2395-1621

Subscription Period Aware Key Management for Secure Vehicular Communication

[#1]Prof. A.S.Deshpande, [#2]Shamal S. Chaudhari, [#3]Shivangi L. Buragoni, [#4]Damini K. Lagad

[2]shamal220@gmail.com
[4]sailagasd6@gmail.com

[#1]Prof. Department of Electronics and Telecommunication
[#234]Department of Electronics and Telecommunication

JSPM's Imperial College of Engineering & Research, Wagholi.

ABSTRACT

As many applications based on wireless communications are depend on a vehicular platform, multicast communications have begun to be essential for efficient information delivery. Vehicle-to-Vehicle Communication gives drivers a sixth sense to know what's going on around them to help avoid accidents and improve traffic flow. For prevention of road accident cases we must have to use modern technologies and safety features used in modern vehicles. Now the auto industries even want to launch such vehicles that provide safety to riding vehicle. One of the latest technology launches in vehicles market known as Vehicle to vehicle communication (V2V). In V2V communication group key management (GKM) is expected to play an essential role as access control. Group key management is one of the essential roles to access between vehicular communication controls but it causes high frequency of group rekeying and highly cost effective. To avoid this problem of the high frequency of group rekeying, we propose a new GKM scheme, which is called subscription-period-aware key management (SPKM), for cost-effective and secure vehicular multicast group rekeying. Here we analyse its key management cost and find an optimal condition to minimize the key management cost. We show that the proposed SPKM scheme can greatly reduce the communication, computation, and storage complexity in multicast group rekeying .And also, we show that the key management cost of the proposed SPKM scheme is lower than those of the well-known. GKM schemes for secure vehicular multicast communications. From this technology we minimize the road accident and save many lives.

Keywords: **Group Key Management, Group Key, SPKM, KDC.**

ARTICLE INFO

Article History

Received :13th March 2016

Received in revised form :

15th March 2016

Accepted : 18th March 2016

Published online :

21st March 2016

I. INTRODUCTION

This project is focused on communication in the network. Group key management is one of the essential roles to access between vehicular communication control but it causes high frequency of group rekeying and highly cost effective. To overcome these problems we introduced a new scheme for communication is SPKM .Here we analyze some parameter to design SPKM and how it will be beneficial, as key management cost, with the communication, computation, and storage costs, for multicast group rekeying, and find an optimal condition to minimize the key management cost. Vehicular Communications, including vehicle-to-vehicle and vehicle-to-infrastructure communications, plays an important role in keeping safer and more efficient driving conditions. By enabling various services, including road safety, driver assistance and driver's convenience, VC creates safer and more efficient driving conditions. To enable these services, VC deploys vehicular multicast communication protocol enables a single host, including a vehicle or a road-side unit , to communicate with a specific set hosts.Vehicular multicast communication protocols must address several requirements, including the setup of a multicast group communications; transport reliability; and timely transmission of data. To set up a multicast group for secure group communication among these requirements, the identification of a specific set of hosts is required, each of which is an authorized service member. As such membership requires that all multicast traffic be delivered only to the authorized group of host , VC can maintain data confidentiality in vehicular multicast communication services , where data confidentiality secure group key management schemes , including logical key hierarchy and topological matching key management ,are generally used. The GKM scheme allows an authorized host with the GK can successfully encrypt the data and decrypt the encrypted data for secure group communications.

However, to preserve data confidentiality through the GKM scheme, we need to determine how to share a GK among the authorized group members for every membership change , which is called group rekeying. This is because a group rekeying operation usually suffers by a scalability problem from a one-affect-all problem, where a single group member in the same group to have key updates. Thus, solutions for the scalability problem aim at minimizing the number of GKs that should be distributed.

The scalability problem is a more serious bottleneck for efficient group rekeying in vehicular multicast communications .This is because, in vehicular networks, the large number of vehicles in narrow-area communication services and their dynamic mobility of the large number of vehicles in narrow-area communication services and their dynamic mobility make the scalability problem more complex. That is, due to the dynamic mobility of the large number of vehicles, group rekeying frequently happens. High communication complexity and computation complexity from the frequent group rekeying cause the delayed key update , which may expose secure data to a previous member , whose membership is already expired.

To reduce the increase in the communication and computation complexity due to the dynamic mobility of vehicle. the TMKM scheme combines a logical tree of keys, which is called a key tree, with topology information, and thus reduces the communication overhead in delivering key update reduces the communication overhead in delivering key update messages through multicast communications.

II. LITERATURE SURVEY

Literature Most GKM schemes are designed using a key tree since a key tree shows good performance in reducing the communication and computation complexity through different key paths. Studies on GKM schemes show that the low communication and computation complexity are based on two categories: LKH and batch rekeying (BR). By using a layered key tree, the LKH scheme reduces the communication complexity from in a single group rekeying. However, as the LKH scheme delivers key update information to the group members through multicast communications, the LKH scheme may require a high bandwidth over the transmission network .To avoid the high bandwidth requirement, BR schemes have been proposed.

In the BR schemes, after a batch of join and leave requests has been collected in a certain period, the KDC rekeys. The BR schemes show good performance in reducing communication overhead through the low frequency of rekeying compared with that of individual rekeying, i.e., rekeying after each join or leave request. However, the BR schemes may sacrifice forward and backward confidentiality. In vehicular networks, an RSU establishes the physical communication link with vehicles through multicast communications.

When a KDC transmits data to a vehicle and vice versa, the mobility of the vehicle is managed by the RSU. For the stable management of each vehicular movement, the KDC and the RSU should continually keep track of the location of every vehicle under the high-speed vehicular mobility. Because of the high-speed mobility of vehicles in vehicular networks, the legacy GKM schemes, including the LKH and BR schemes, suffer from a critical design problem: the increase in the key management cost, including the communication, computation and storage costs, from the frequent rekeying due to the high speed mobility of vehicles. This is because the KDC and the RSU suffer from very frequent update of GKs caused by the large number of vehicles in the wide service area and their high speed mobility.

To reduce the increase in communication overhead in the cellular network, TMKM schemes, each of which is a type of LKH whose key tree is constructed by considering the network topology, have been proposed. However, TMKM schemes also have a limitation in reducing high communication overhead. The TMKM schemes should send additional rekeying messages for managing key tree structure, whenever the vehicles' network topology is changed due to a handoff between RSUs. In addition, while processing the network topology information, the computation overhead at the KDC increases. As an alternative to reduce the increase in the mobility management complexity at the KDC, Park et al. proposed the RDKM scheme, which assigns some functional blocks of the KDC to RSUs .

To manage the key tree through the vehicular movement information exchange across RSUs, the RDKM scheme requires more leaf nodes in the key tree compared with the TMKM scheme. Thus, the key management complexity of the RDKM scheme increases because the weighted sum of the communication overhead and the storage overhead is logarithmically proportional to the number of leaf nodes. Compared with other GKM schemes for secure vehicular multicast communications, the proposed SPKM scheme can greatly reduce the complexity from communication, computation, and storage in a single group rekeying. In the following, we show the details of the proposed SPKM scheme.

III.SYSTEM ARCHITECTURE

Proposed SPKM scheme according to three membership events:

- service subscription
- service extension

- service expiration

SPKM according to Service Subscription membership:

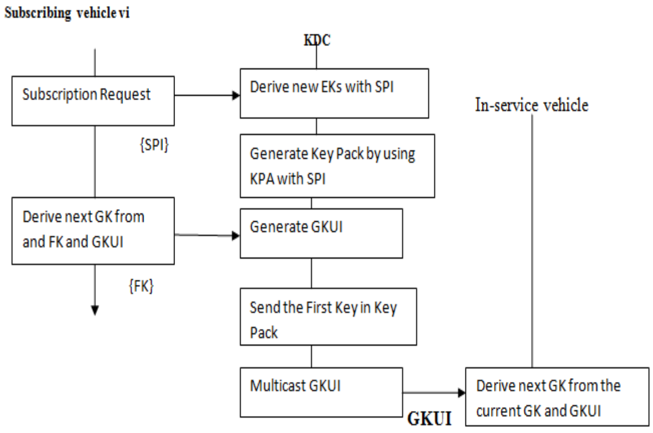
Subscribing vehicle vi
KDC
Subscription Request
Derive new EKs with SPI
In-service vehicle
{SPI}
Generate Key Pack by using KPA with SPI
Derive next GK from and FK and GKUI
Generate GKUI
{FK}
Send the First Key in Key Pack
Multicast GKUI
Derive next GK from the current GK and GKUI
GKUI

Fig 1. SPKM according to Service Subscription membership

In the case of a service subscription, the KDC manages the keys as shown in Fig. 3.1 When vehicle vi subscribes to a service, the vehicle sends a subscription request message, including its SPI. The KDC derives new EKs with the SPI and then, generates a KP, including the minimized number of keys. By using the keys in the KP, a vehicle derives all EKs between the joining time and leaving time. To generate the KP, we propose a new KP generation algorithm, which is called the KPA.

In order of validity time, the keys in KP are delivered to the joining vehicle, which subscribes to a group service. Among the keys in the KP, an FK is delivered to the joining vehicle. By using the FK and Fd(·), the vehicle can derive a GK. To provide confidentiality of the message consisting of the FK, the KDC sends the FK that is encrypted by the vehicle's IK. After sending the FK, the FK is deleted from the KP. In Algorithm 1, we show the operation of the proposed KPA in detail. By using the KPA shown in Algorithm 1, the KDC can generate a specific KP consisting of the keys that are used in deriving all the GKs at a specific subscription period.

SPKM according to Service Extension membership:

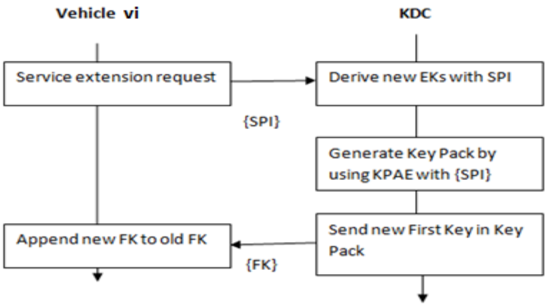
Vehicle vi
KDC
Service extension request
Derive new EKs with SPI
{SPI}
Generate Key Pack by using KPAE with {SPI}
Append new FK to old FK
Send new First Key in Key Pack
{FK}

Fig 2. SPKM according to Service Extension membership

In case of a service extension, the KDC manages the keys as shown in Fig.3.2 When vehicle vi ∈ Nt tries to extend a service subscription period, the vehicle sends a service extension request message with the SPI consisting of a new leaving time to the KDC. After receiving the SPI, the KDC derives new EKs from the received SPI and generates a KP covering the extended time period through a KPAE, whose detailed operation is shown in Algorithm 2. The KPAE generates the KP in the same way as the KPA does. Compared with the KPA, the KPAE can further reduce the size of the KP because the keys in the KP before an extension request time can be used to generate a new KP. Among the keys in the KP, an FK is delivered to the vehicle as well. By using the FK, the vehicle can derive the next GK with a one-way function. To provide confidentiality of the message, including the FK, the KDC should send the FK encrypted through the vehicle's IK. After sending the FK, the FK is deleted in the KP. InAlgorithm2, we show the detailed operation of the KPAE. For example, if a subscribed vehicle (t0 to t6) tries to extend service t6 to t27, as shown in Fig. 3.2, the KDC generates a KP through the KPAE.

SPKM according to Service Expiration membership:

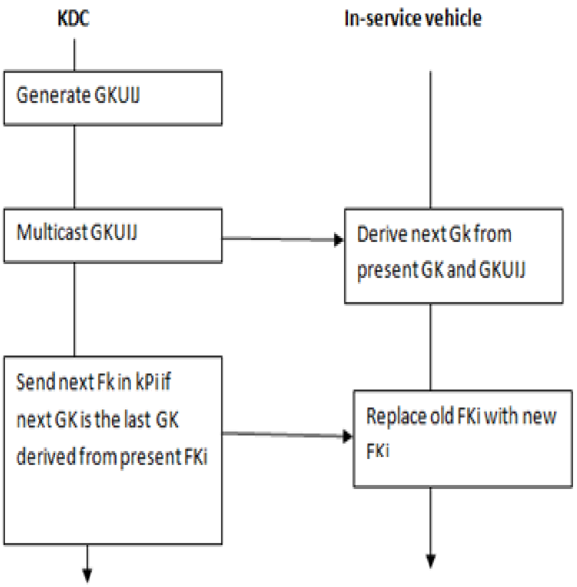
KDC
In-service vehicle
Generate GKUIJ
Multicast GKUIJ
Derive next Gk from present GK and GKUIJ
Send next Fk in kPi if next GK is the last GK derived from present FKi
Replace old FKi with new FKi

Fig 3. SPKM according to Service Expiration membership

In the case of a service expiration of a vehicle, the KDC manages the keys as shown in Fig.3.2. Based on vehicles' SPIs, the KDC is already aware of membership dynamics in a service group and all the key path information for generating GKs. Before a static period is over, the KDC generates GKUI for existing subscribed vehicles to derive the next EK through the proposed GKUA, whose operation is shown in Fig. 4.3. When the service expiration event occurs, the KDC multicasts GKUI. After receiving GKUI, vehicles can successfully derive the next GKs from their own FKs. Detailed operations of the GKUA are shown in Algorithm 3. For some vehicles, their FKs can be expired.

IV. APPLICATION AND ADVANTAGES

Advantages:

- Good performance in terms of computation, storage, and communication costs.
- Provide secure vehicular multicast communications.
- Efficiently combining the unicast and multicast communications.
- SPKM minimizes key management complexity in group rekeying.

Application:

- Many applications based on wireless communications are being embedded on a vehicular platform; multicast communications have begun to be essential for efficient information delivery.
- It plays an essential role as access control.

V. CONCLUSION

To overcome the high frequency of group rekeying in vehicular multicast communications, we proposed a new GKM scheme, which is called SPKM. From the evaluation results under various conditions, we will show the proposed SPKM scheme can greatly reduce the computation, storage, and communication complexity in every group rekeying.
The proposed SPKM scheme can show good performance in terms of computation, storage, and communication costs.

REFERENCE

[1]. D. M. Wallner, E. J. Harder, and R. C. Agee, “Key management for multicast: Issues and architectures,” Internet Eng. Task Force, Fremont, CA, USA, RFC 2627, 1999.

[2]. J. Pegueroles and F. Rico-Novella, “Balanced batch LKH: New proposal, implementation and performance evaluation,” in Proc. IEEE ISCC, 2003, pp. 815–820.

[3] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems, IEEE Std. 802.16-2009.

[4] D. L. Mills, J. Martin, J. Burbank, and W. Kasch, “Network time protocol version Protocol and algorithms specification,” Internet Eng. Task Force, Fremont, CA, USA, RFC 5905, 2010.

[5] T. Billhartz, J. Cain, E. Farrey-Goudreau, D. Fieg, and S. Batsell, “Performace and resource cost comparisons for the CBT and PIM multicast routing protocols,” IEEE J. Sel. Areas Commun., vol. 15, no. 3, pp. 304–315, Apr. 1997.

[6] H. Salama, D. Reeves, and Y. Viniotis, “Evaluation of multicast routing algorithms for real-time communication on high-speed networks,” IEEE J. Sel. Areas Commun., vol. 15, no. 3, pp. 332–345, Apr. 1997.