Subscription Period Aware Key Management for Vehicular Communication

Shamal S Chaudhari[1], Shivangi L Buragoni[2], Damini K Lagad[3], Prof. A.S.Deshpande[4]
[1, 2, 3, 4] Department of Electronics and Telecommunication
[1, 2, 3, 4] JSPM's Imperial College of Engineering & Research, Wagholi.

Abstract- *As many applications based on wireless communications are being embedded on avehicular platform, multicast communications have begun to be essential for efficient information delivery. Since multicast communications are vulnerable to unauthorized access, group key management (GKM) is expected to play an essential role as access control. However, we note that the legacy GKM schemes are not cost effective and adequate for use in vehicular environments. This is because the dynamic mobility of a large number of vehicles causes a high frequency of group rekeying, which is used to share a new group key (GK) among the authorized group members for every membership change. To overcome 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. As a design problem, we analyze its key management cost, including the communication, computation, and storage costs, for multicast group rekeying, and find an optimal condition to minimize the key management cost. Through simulations under different conditions, we show that the proposed SPKM scheme can greatly reduce the communication, computation, and storage complexity in multicast group rekeying from O(logN) to O(1), where N is the number of vehicles in a single group rekeying process. In addition, 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.*

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.

Problem Statement

To design a system for vehicle to monitor vehicle parameters in an following network or area and indicate its joining and leaving time to another vehicle using this software and shows how it will be beneficial, as key management cost, with the communication, computation, and storage costs, for multicast group rekeying, and also find an optimal condition to minimize the key management cost.

Solution

With considering such problems in vehicles we are going to use SPKM system in our system which-

1) Minimize Key Management Complexity in group rekeying
2) Provides secure vehicular multicast communication

II. LITERATURE SURVEY

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.

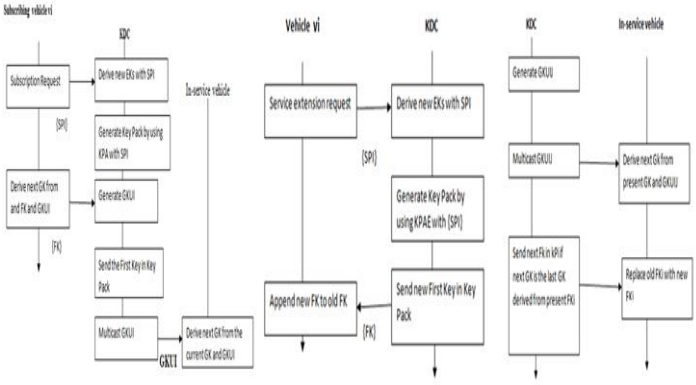
To reduce the increase in communication overhead in the cellular network, TMKM schemes, each of which is a type of LKH whose key tree is constructed by considering the network topology, have been proposed. However, TMKM schemes also have a limitation in reducing high communication overhead. The TMKM 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. BLOCK DIAGRAM



Description:-

Proposed SPKM scheme according to three membership events:

- service subscription
- service extension
- service expiration

In the case of a service subscription, the KDC manages the keys as shown in fig . 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.. The communication is takes place through KDC. 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.

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.

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, the KDC generates a KP through the KPAE.

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. When vehicles receive GKUI from the KDC, the vehicles begin to derive the next GK through the GK derivation algorithm (GKDA). Algorithm 4 shows the detailed operations of the GKDA for deriving a new GK from the current GK by using its own FK. Let us assume that the current GK is k3 and that a vehicle receives GKUI of 00001010. In addition, the vehicle is aware of k1,k 3,k 4.

IV. RESULT

In this project we consider an area. When vehicle will enter in that area then it will pass key through SPI to KDC. Then KDC will pass this key to other vehicle that is it will pass information of entered vehicle to other vehicle. In our simulation scenario, we assume vehicular multicast services.

According to that the result has following steps:

- Simulation of SPKM
- Tree Plotting of all Vehicles in Network
- Vehicle Arrived in Network and Tree plot according to their 'JT','LT'
- Tree Plotting Of Vehicle According To Service Subscription
- Tree plotting of vehicles according to their Service extension
- Simulation Of Keys According To Service Expiration

I. Simulation of SPKM

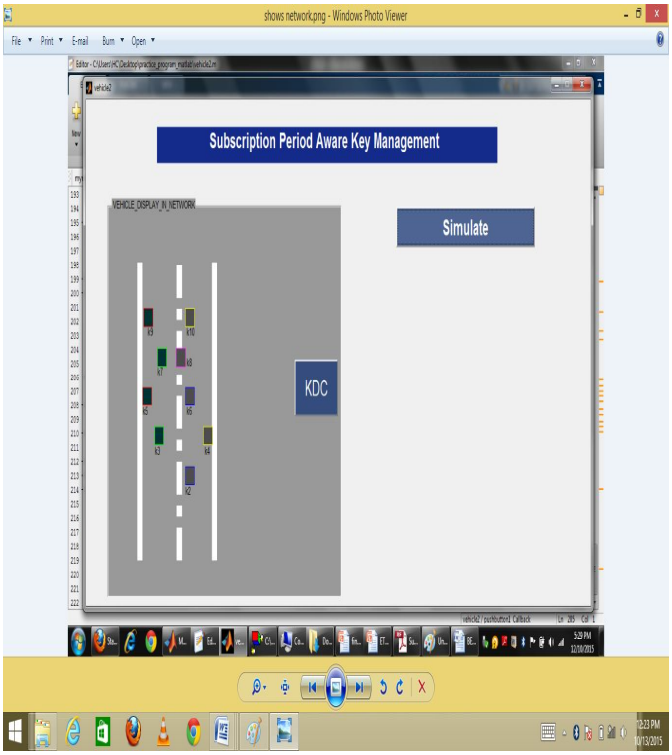


Fig . Simulation of SPKM

In this project we consider an area. When vehicle will enter in that area then it will pass key through SPI to KDC. Then KDC will pass this key to other vehicle that is it will pass information of entered vehicle to other vehicle. In our simulation scenario, we assume vehicular multicast services.

We assume that vehicular service subscription rate follows Poisson distribution, and the service subscription period of each vehicle follows Gaussian distribution.

II. Tree Plotting of all Vehicles in Network:

This is because a vehicle's service subscription event is independent from that of the other vehicles in the vehicular service group. As a ciphering and derivation algorithm, we adopted Advanced Encryption Standard (AES) and SHA-1, and we set the size of keys into 128 bits. Details of parameter values are separately shown according to simulation scenarios.

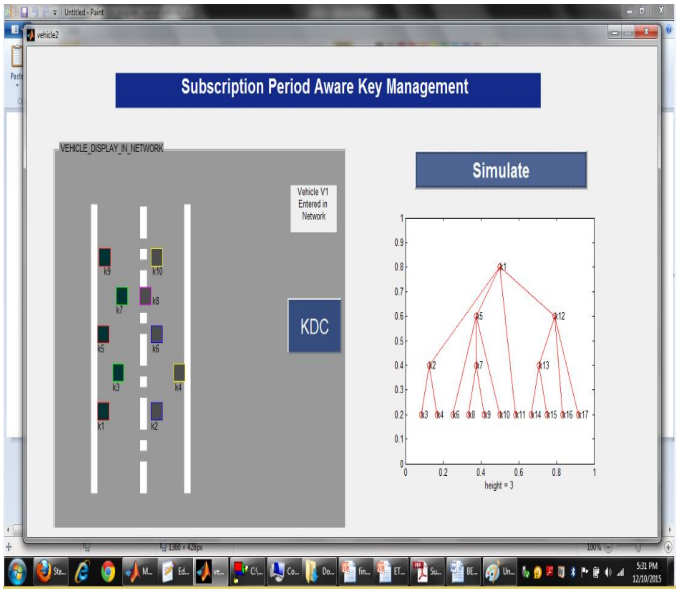


Fig.Tree Plotting of all Vehicles in Network:

III Vehicle Arrived in Network and Tree plot according to their 'JT','LT' :

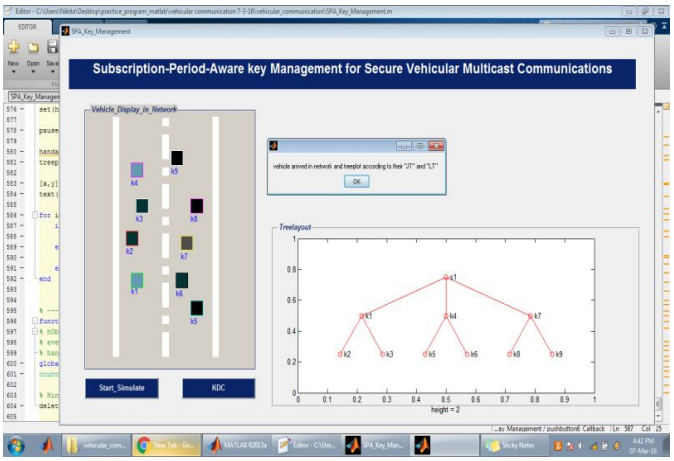


Fig.Vehicle Arrived in Network and Tree plot according to their 'JT','LT'

According to our programe here we entered nine vechicles at a time in particular area.When we start our simmulation these nine vehicles are enter into the area. The communiction takes place through Key Distribution Center that is nothing but the KDC. Hence now enter the KDC button .here we alredy designed the programe for each key.If we want to enter a new vehicle into the area we have to enter joinig time(JT), and leaving time(LT) of that vehicle. According to its 'JT', 'LT' the tree will be plot as shown. Here K1,K4,and K7 are parents key and other K2,K3,K5,K6,K8,K9 are child key. S1 is simmulation key.

IV. Tree Plotting Of Vehicle According To Service Subscription

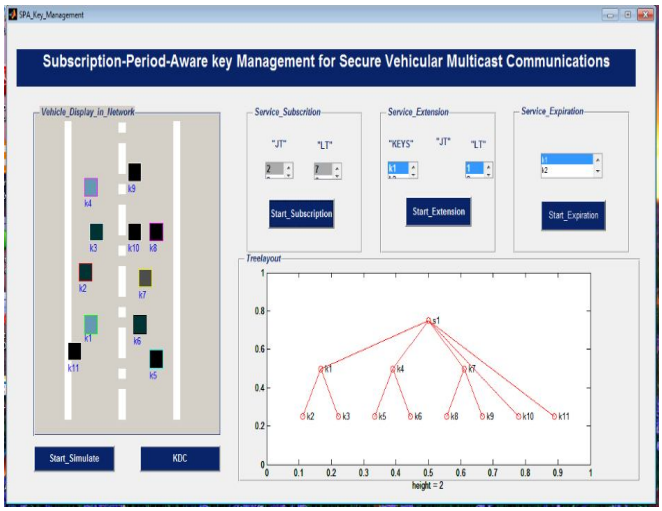


Fig. Tree Plotting Of Vehicle According To Service Subscription

When we enter the new vehicle into the area the key distributionwill generate its new key according to its joining time and leavingtime. Here we metioned fix time for allready entered vehicles in the programme. According to that new vehicle will join the key And after that the tree will be plot according totheir joing time and leaving time.

V. Tree plotting of vehicles according to their Service extension:

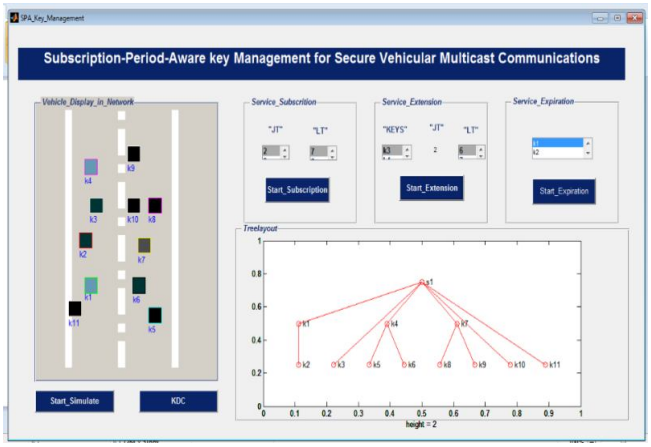


Fig.Tree plotting of vehicles according to their Service extension

In case of a service extension, the KDC manages the keys as shown in Fig.8.5. 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.

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, the KDC generates a KP through the KPAE.

VI. Simulation Of Keys According To Service Expiration:

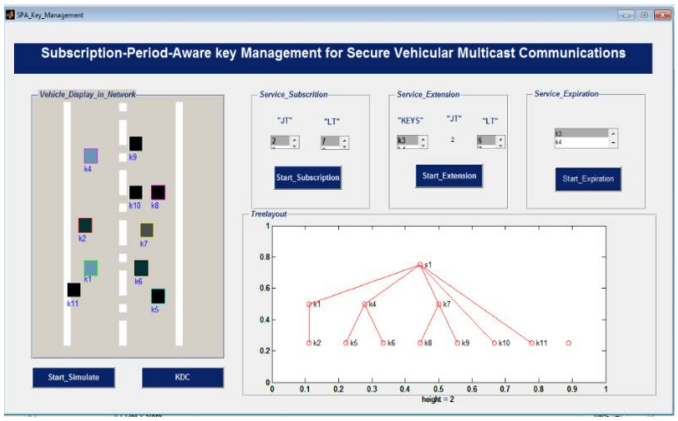


Fig.Simulation Of Keys According To Service Expiration

In the case of a service expiration of a vehicle, the KDC manages the keys. 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 algorithm. When the service expiration event occurs the KDC multicasts GKUI. After receiving GKUI, vehicles can successfully derive the next GKs from their own FKs. For some vehicles, their FKs can be expired.

The KDC should deliver the next FKs in their KP to the specific vehicles, and by using the next FKs, the vehicles derive the new GKs. For data 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. The GKUI is the path information used to derive the next EK from a present EK.

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.

ACKNOWLEDGMENT

We are pleased to acknowledge many individuals for their invaluable guidance during the course of this project work. It is our great pleasure to express our heart full gratitude towards all of them.

We would like to acknowledge the foremost gratitude and deep appreciation to our internal Project Guide Prof. A. S. Deshpande for her valuable advice, guidance, encouragement and support for project, who continuously helped us throughout the project and without her guidance, this project would have been an uphill task.

We extend our sincere thanks to our H.O.D Prof P.R. BADADAPURE for giving us motivation and consistent support.

We are also great full to all the teaching and non-teaching staff of our department who co-operated with us regarding some issues.

Lastly we would like to thank our Principal Dr. S.V. ADMANE & all the people who had directly or indirectly helped and co-operated with us nicely for the smooth development of this project.

REFERENCES

[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 communicatio