IJBMTP

MAMAN & SHAHZAIN

International Journal of Business Management and Technological Perspectives

Distributed Group Key Management Scheme for Vehicular Ad Hoc Network

Tahir Ahmed[a] and Asmara Maryam[b]

[a]Lecturer, Higher Education Department Punjab, Pakistan.
[b]Department of Computer Science, COMSATS University Islamabad Lahore Campus, Lahore.

ARTICLE INFO

Keywords:
Vehicular ad hoc network,
Group key management,
multicast,
Vehicle-to-infrastructure communication

ABSTRACT

Purpose - Vehicular ad hoc networks (VANET) are gaining popularity now days. With the use of VANET, multiple security issues have been arisen. Key Management is the most critical security concern that has grabs the attention of the researchers, academia and industries. In VANET, group key management schemes, previous studies only show key management system within a single region. In this paper, a hybrid approach has been proposed for group key management in VANET.

Design/Methodology/Approach - In this scheme we used media mixing approach for group creation and CSET Management protocol for key management to reduce computation and storage cost of key update.

Findings - Results obtained through model simulation to show the computation and cost effectiveness of proposed scheme.

Practical Implications – This scheme reduces the risk of single point failure and enhance the network's resilience to attacks and reduce the communication and storage cost.

INTRODUCTION

Vehicular ad hoc networks (VANETs) have significantly expanded to enhance the wireless communication. As mobile wireless devices and networks gain importance, the demand for Vehicle=to-infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication is rapidly increasing. VANETs are used for both safety and non-safety applications, offering value-added services such as automated toll payments, traffic management, and location-based services like finding nearby fuel stations, as well as providing internet access. On a broader scale, VANETs have gained global attention form governments, academic institutions, and industries due to their potential to improve vehicle safety and reduce traffic ongestion.

In Vehicular Communication, each vehicle performs the role of sender and receiver. It can also act as a router to broadcast information to the vehicular network. Every vehicle is equipped with Onboard Unit (OBU) for communication between vehicles and Roadside Units (RSUs), that sets short-range wireless ad hoc networks for communication. Vehicles also supports the position-based information system such as Global Positioning System (GPS). RSUs, plays a vital role for communication. In roadside units' installation, some protocols demand that RSUs have to be distributed evenly in the road network, some demands on at intersections, while others requirements are only at region borders. Vehicle-to-roadside and Vehicle-to-vehicle communications depends upon precise and update information of the surrounding network, which required accurate positioning systems and smart communication protocols for information sharing.

*Corresponding author. Higher Education Department, Punjab, Pakistan.

E-mail addresses: tahirahmed1044@gmail.com (T. Ahmed), asmaramaryam22@gmail.com (A. Maryam).

Available online 20 November 2024
Ahmed, T. (2024). Distributed group key management scheme for vehicular Ad Hoc network. *International Journal of Business Management and Technological Perspectives*, *1*(1), 44-48.
Received 20 April 2024; Received in revised form 20 August 2024; Accepted 20 September 2024

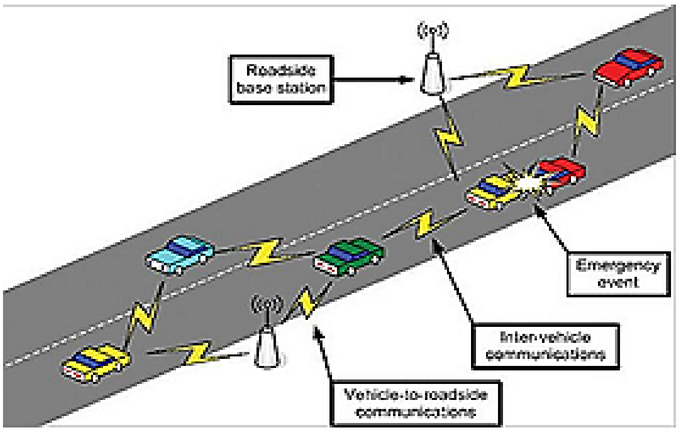
Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Figure 1: *VANET Architecture*

In vehicle-to-roadside communication, RSU broadcast to all equipped vehicles in the network. For fast communication the roadside units may be located at every kilometer or less. Roadside unit periodically broadcast the message regarding on the speed limit and also issues the warning message in case of violation request that the driver should reduce his speed. In Vehicle-to-vehicle communication, each vehicle communicates with other vehicles to share its current position, direction, velocity and road information. Among the VANET characteristics, any member can join or leave the group freely.

As any member can join or leave the group so it's possible that an adversary can attack on the network. To secure the VANET, key management has gained popularity, but the key management and updation of group keying in the dynamic and high-speed mobility is a major issue. We proposed a scheme that uses media mixing technique for group creation and group leader selection and CSET-Computation and storage effective tree.

The paper outline is as follows: the related work is discussed in section 2, problem statement has been discussed in section 3, proposed model architecture is introduced in section 4, Experimental evaluation in section 5 and conclusion of the paper is explained in section 6.

Related Work

In past few years, lot of research has been carried out in wireless networks particularly Vehicular ad hoc network. Chain-Based structure is used for key management [2]. Nodes are organized in a chain and chain is formed by the order of least important bits of public key. Each member maintains a single public/secret key pair. One sender and multiple receiver concepts are used in the chain. A remote sender, knowing the public keys of group members, can securely broadcast a secret session key to a specific subgroup. This allows any message to be encrypted with the session key for the intended recipients. A group member can be excluded by removing their public key from the public key chain, or new members can be enrolled by adding their public keys to the appropriate position on recipients' public key chain. The Certificate Authority (CA) in only involved during the initial key creation process and does not participate in ongoing communication. Group formation is based on proximity [3]. To protect against attacks by compromised Roadside Units (RSUs) or malicious vehicles, a security protocol is designed, using a cooperative message authentication protocol to reduce computational and communication overhead within the group. The round-trip time for communication is 3 seconds. All vehicles involved in collision will experience a delay of 03 Seconds.

Tree-based Structure is used for key management [4]. Most left node will be selected as super node for coordination. A pair wise keys are defined, when two nodes decided to establish a pair wise key, they only need three rounds of communication and one round encryption and one round decryption. Low computation and communication overhead is the main theme of this technique. Tree-Based structure is used by RSU for Key Management and Multicast service [5]. RSU based distribution reduces the rekeying overhead by delegating a part of key management function to RSU. Identification Management, Key Management, Privacy achieved [6]. IEEE 1609.2 protocol should be supported by every vehicle.

Distributed group key management and Anonymous authentication is formed by dividing domain into several sub-regions [7]. Decrease the revocation checking cost, Distributed groups will increase the localized management and anonymous authentication. Novel Group Key Management (GKM) scheme based on leaving probability (LP) of vehicles and block chain concept to simplify the distributed key management [8]. The time cost for transporting keys is much less than that of standard network structure. Group key distribution mechanism is used in this paper [9]. This method provides better security and management than other non-group key management systems. PKR is used with a centralized TA [10]. This method is more efficient and scalable than the certificate-based PKC scheme. Trust Metric [0-1] is used to recognize the vehicles good behavior and mobility metric with respect to relative velocity of a vehicle [11]. Distribute the role of the CA among a set of vehicles traveling on the road.

Table 1
Summary of Group Based Key Authentication Schemes

Paper	Techniques	Strength
[2]	Chain-Based Structure	During Communication CA is not involved, CA is involved only key creation process
[3]	Groups are formed on the bases of Distance (300 m)	Security Protocol design for compromised RSU and malicious vehicles from attacking
[4]	Tree-based Structure	Low Computation and communication Overhead
[6]	CA used for Keys	Identification Management, Key Management, Privacy Achieved

Paper	Techniques	Strength
[13]	HMAC (Hash Message Authentication Code)	Replace the Conventional Certificate Revocation List (CRL) checking method to reduce time
[15]	HMAC (Hash Message Authentication Code) with distributed group private key and cooperative authentication	Distributed groups increase the localized management and cooperative authentication, reduce the number of invalid messages in batch to improve the efficiency, 600 message can be verified per second.
[7]	distributed group key management and Anonymous authentication by diving domain into several sub-regions	Decrease the revocation checking cost, Distributed groups increase the localized management and anonymous authentication
[12]	Cooperative Message Authentication Protocol (CMAP) to alleviate vehicles computation burden.	3 Verifier Selection Algorithms: N-nearest Method, Most-Even Distributed Method, Compound Method
[8]	novel Group Key Management (GKM) scheme based on leaving probability (LP) of vehicles and block chain concept to simplify the distributed key management	the time cost for transporting keys is much less than that of standard network structure.
[9]	Group key distribution mechanism is used in this paper	This method provides better security and management than other non-group key management systems.
[10]	PKR is used with a centralized TA	This method is more efficient and scalable than the certificate-based PKC scheme
[11]	Trust Metric: Tm [0-1] with respect to vehicles good behavior and mobility metric with respect to relative velocity of a vehicle	Distribute the role of the CA among a set of vehicles traveling on the road.
[5]	Tree-Based structure is used by RSU for Key Management and Multicast service	RSU based distribution reduces the rekeying overhead by delegating a part of key management function to RSU.

3. PROBLEM STATEMENT

Need an efficient way of group creation and group leader selection and to reduce the computation overhead and storage in key management.

4. PROPOSED DISTRIBUTED GROUP KEY MANAGEMENT SCHEME

Network Initiation

Every node that wants to be the part of network will send his PKI and preference to RSU that whom he wants to send messages only or receive or both. RSU will examine the request and check the available networks. According to the preference of node RSU will pass node request to existing group or will create a new group on the basis of new number of requests. Table II (a) shows list of nodes preferences. We are assuming here that each node knows about other nodes that how many nodes have requested to form a group. Node preference request gives information to RSU that how node want to treat other nodes in the group. In send to Column nodes are mentioned that the node wants to send messages and in receive from list contains list of nodes from that node will allow to get messages. Third column shows new node preference that any new node can send or receive a message from the node. First value "Y" for yes of Send to and second value "Y" means yes to receive messages and "N" for No to send or receive messages from new node. RSU will apply media mixing algorithm [14] on the requests of nodes to formulate a list. Table II (b) shows the list after applying media mixing algorithm on user preferences list. Now from the list RSU will select a group leader on the basis of maximum nodes in send to and receive from preference and new node yes preference for send to and receive from. And send the list of all nodes with their preferences and PKI's to the group leader. Group leader will create a group key and will manage the group for further communication. On the basis of example in Table II (b) V3 will be elected as group leader.

Table 2(a)
Node Preferences List

Node	Send To	Receive From	New Node
V1	V2,V4,V5,V7	V2,V3,V5,V7	Y,N
V2	V1,V3,V4,V5,V6	V1,V3,V5,V7	Y,Y
V3	V1,V2,V4,V7	V1,V2,V4,V5,V6	Y,Y
V4	V1,V3,V5,V6	V1,V3,V5,V6	N,N
V5	V2,V3,V4,V6	V3,V4,V6	Y,Y
V6	V2,V3,V4	V1,V3,V4,V5	N,Y
V7	V1,V2,V4,V5,V6	V1,V3,V4,V5,V6	Y,Y

Table 2(b)
Media Mixing Algorithm results

Node	Send To	Receive From
V1	V2,V4,V7	V2,V3,V7
V2	V1,V3	V1,V3,V5,V7
V3	V1,V2,V4,V7	V2,V4,V5,V6
V4	V3,V5,V6	V1,V3,V5,V6
V5	V2,V3,V4,V6	V4
V6	V3,V4	V4,V5
V7	V1,V2	V1,V3

Key Generation and Distribution Process

Group leader will construct a level homogenous tree using CSET management protocol for Key generation [16]. Group key and sub keys that nodes will use for inter communication will be generated by this protocol. Fig II Shows Computation-Storage-effective Key Tree to illustrate to above example.

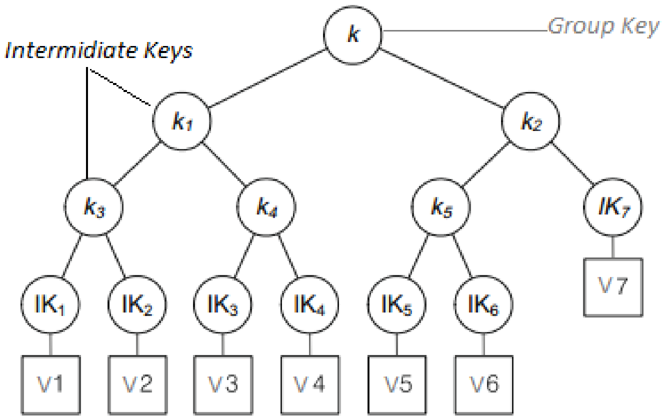

Figure 2: *CSET of above Example*

Each node has its unique key IK and intermediate keys are generated from corresponding IKs and K group key will be generated from intermediate keys. All keys will be given to all nodes for further group communication.

Key Updation Scnarios

Joining a New Node

Group Key will be updated in case of joining a new node in the tree. Fig III illustrates the joining Operation of nodes and changes in tree structure after joining new nodes. In the below example we have selected K=2 for level homogenous tree in CSET management protocol [16]. (b) Shows the tree structure after joining node V8 and (d) shows the changes in tree after joining node V9. Group leader will perform these operations every time will when a new node will come to join the group. New key will be generated and will be broadcasted using old keys to all other nodes.

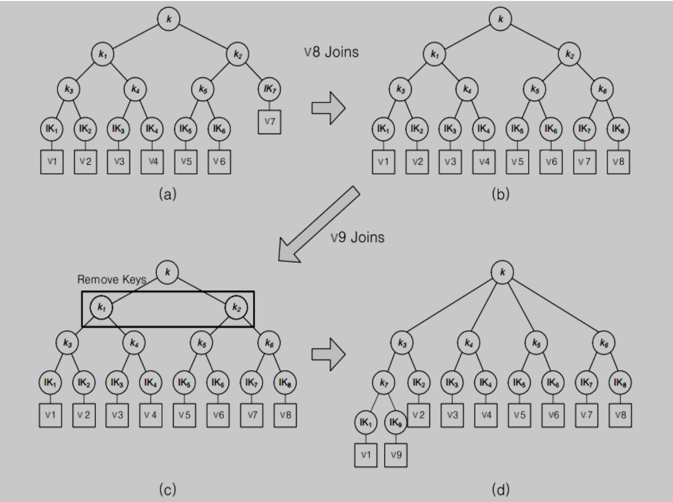

Figure 3: *Illustration of new Node Joining Operation with k=2*

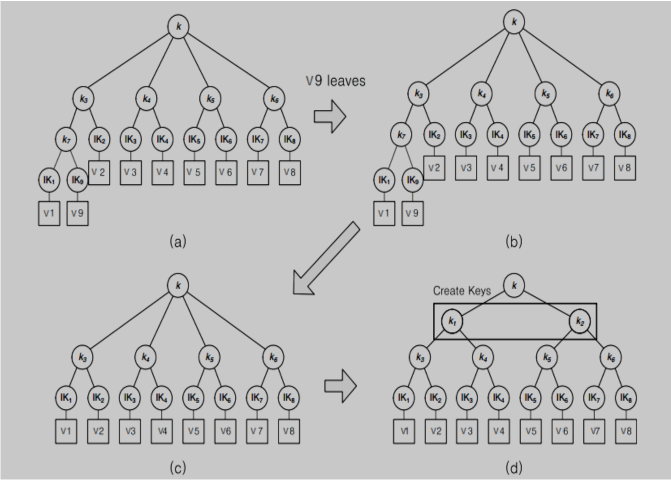

Figure 4: *Illustration of Node Leaving Operation*

In the above example node V9 wants to leave the group. V9 will send the leave request to group leader and group leader will re compute the key after removing node V9. as we are using k=2 in level homogenous tree so k1 and k2 will be created to complete the tree levels.

5. EXPERIMENTS

In Experiments to evaluate the performance of our hybrid scheme using CSET we used two kind of cost matrices to evaluate communication overhead and reduction of storage and computation cost.

Simulation Setup

In this simulation, we consider a centralized group communication in which a group leader that will be selected by predefined criteria, will manage the group key for communication. Let's assume that there are N number of nodes that sent request to the RSU to formulate a group. RSU evaluated their requests and selected a Node as group leader to manage the group key. RSU sent all nodes information to group leader. Now group leader will manage the key using CSET. Considering N(=2^H) CSET will be (T(2,2,2,.....2,2^{H-K}). In a general scenario we supposed group members leaving randomly the communication group regardless of their position in key tree. Number of messages will be counting unit of communication cost.

Performance Evaluation of CSET

Communication Overhead

Figure 5 shows the communication cost of CSET, as the ratio of leaving nodes increases, when H=10. The communication cost of CSET is identical in most of the part.

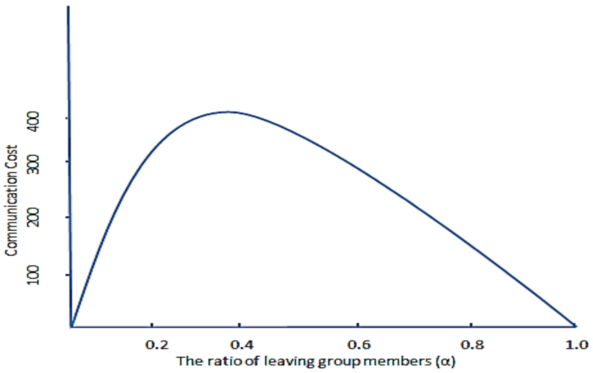

Figure 5: *Communication cost of CSET*

In the portion where α is small the increment of communication cost can be observed by the following equation [14].

$$\triangle m(K,e) = \triangle m(K,\langle \alpha N\rangle) \cong \sum_{i=K+1}^{H} \{2^{H-i}(1-\alpha)^{2^{i}}\}.$$

Reduction of Storage and Computation Cost

According to Table III when α=0.01 (1% ratio of leaving group members) normalized increment is 1% when H=15. Even for small H the protocol makes the normalized increment less than 1% by slightly increasing α. The normalized increment is 4.22% (0.0422) when α=0.01, H=14 and K=6.

Table 3
Normalized Increment of Cost for Computation and Storage Reduction (α=0.01)

(H-K-1)/H (50%)	**5/10**	**6/12**	**7/14**	**8/16**	**9/18**
Increment	**0.5196**	**0.1825**	**0.0422**	**0.0053**	**0.0002**

CONCLUSION

In this paper we presented a hybrid group key management scheme which provides an efficient way to select a group leader and communication and storage cost effective method to manage group key using CSET protocol. We showed to communication overhead and reduction of communication and storage cost by evolution matrices to prove the effectiveness of over scheme using CSET protocol for key management in VANET.

REFERENCES

[1] Ahmed H. Salem, Ayman Abdel-Hamid, and Mohamad Abou El-Nasr, "The Case for Dynamic Key Distribution for Pki-Based VANETS". *International Journal of Computer Networks & Communications (IJCNC),* January 2014.

[2] Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow, IEEE, and Jesús A. Manjón, "Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm". IEEE/ACM Transactions on Networking, 2013.

[3] Yong Hao, Student Member, IEEE, Yu Cheng, Senior Member, IEEE,Chi Zhou, Senior Member, IEEE, and Wei Song "A distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE Journal on selected areas in communications,2011.

[4] Eric Ke Wang, Yuming Ye, and Xiaofei Xu, "Location-Based Distributed Group Key Agreement Scheme for Vehicular Ad Hoc Network", Hindawi-International Journal of Distributed Sensor Networks, 2014.

[5] Min-Ho Park, Gi-Poong Gwon, Seung-Woo Seo, and Han-You Jeong, Member, IEEE, "RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications" IEEE Journal on selected areas in communications, 2011.

[6] Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri, "Short-Lived Key Management for Secure Communications in VANETs", IEEE Telecommunications, 2011.

[7] Yipin Sun, Zhenqian Feng, Qiaolin Hu and Jinshu Su, "An Efficient Distributed key Management scheme for group-signature based anonymous authentication in VANET", Security and Communication Networks, 2011.

[8] LEI Ao, Chibueze Ogah, Philip Asuquo, Haitham Cruickshank, and SUN Zhili, "A Secure Key Management Scheme for Heterogeneous Secure Vehicular Communication Systems", ZTE Communications, 2016.

[9] Ming-Huang Guo, Horng-Twu Liaw, Der-Jiunn Deng and Han-Chieh Chao, "Centralized Group Key Management Mechanism for VANET", Security and Communication Network, 2013.

[10] Pei-Yuan Shen, Vicky Liu, Maolin Tang, William Caelli, "An Efficient Public Key Management System: An Application in Vehicular Ad Hoc Network", Pacific Asia Conference on Information Systems, 2011.

[11] Tahani Gazdar, Abderrahim Benslimane, Abdelfettah Belghith, "Secure Clustering Scheme Based Keys Management in Vanets", IEEE VTC, 2011.

[12] Yong Hao, Tingting Han and Yu Cheng, "A Cooperative Message Authentication Protocol", Globecom, 2012.

[13] Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow, "EMAP: Expedite Message Authentication", IEEE Transactions on Mobile Computing, January 2013.

[14] Je, Dong-Hyun, et al. "Computation-and-storage-efficient key tree management protocol for secure multicast communications." Computer Communications 33.2 (2010): 136-148.

[15] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, February 2014.

[16] Zeeshan Shafi Khan, Mohammed Morsi Moharram, Abdullah Alaraj, and Farzana Azam, “A Group Based Key Sharing and Management Algorithm for Vehicular Ad Hoc Networks,” The Scientific World Journal, vol. 2014, Article ID 740216, 8 pages, 2014. doi:10.1155/2014/740216

Impact of Statement

The results of the study show by evolution matrices that communication overhead and reduction of communication and storage cost, which prove the effectiveness of proposed scheme using CSET protocol for key management in VANET.

Tahir Ahmed, currently serving as

Lecturer, Higher Education Department Punjab Pakistan. I bring with me 10 years teaching and research experience of Computer Science subjects at graduate and undergraduate level in renowned Institutions. I have done MS in Information Security; have published research papers in national and international impact factor journals.

Asmara Maryam, I am a postgraduate computer science researcher at COMSATS University Islamabad Lahore Campus Lahore. My current research focusing on networking and telecommunications. My work explores advanced methodologies for secure, efficient data processing in network security, cloud computing, and data transmission protocols. I have participated in various projects and internships, gaining hands-on experience in network design and administration. My research interests include optimizing network performance and exploring innovative solutions for emerging networking challenges.