I J C T A, 9(34) 2016, pp. 433-445
© International Science Press

A New Master Key Agreement Scheme for Secure Group Communication in Vehicular ad hoc Network

Raju Barskar[1*] and Meenu Chawla[2]

ABSTRACT

Vehicular ad-hoc networks are obtained by applying important features of mobile ad hoc networks, in this application, it is not easy to preserve security and make this network private. Various attackers try to exploit VANETs and send forgery messages to deceive other vehicles which may lead harmful for driver/ passenger. To improve traffic safety and comfort of driving and travelling, it is required to obtain integrity of the messages, identifying and defending against the misbehaving vehicles that should be signed and verified before they are trusted while the real identity of vehicles should not be revealed. In this paper, we propose a master key agreement schemes for VANETs, vehicles are divided into separate different groups. In each group, group leader manages its members and distributes public / private key pairs to members for communication. Here group leader contains master key, which may require for encrypting session key and other communication information in the same groups or different groups securely. To provide secure communication we use, master key and asymmetric cryptography, and appropriate rekeying structure this raises the concern of security, privacy preservation and defends against the misbehaving vehicles. Performance evaluation and analysis of our scheme provides better rekeying structure comparison to existing mechanisms and also preserves security requirements including authentication, confidentiality, data integrity, non-repudiation, and unforgeability.

Keywords: Vehicular ad hoc networks, Key Agreement, master key, group leader, ECC, security.

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANET) has turned up as a new dominant technology because it uses the applications in a large number of intelligent transportation systems (ITS), vigilance systems, and safety signals on the road, using or without using existing infrastructure support, vehicles can communicate with each other on the road. On Board Unit (OBU) and Application Units (AU) are those functional units which exist only in the modern vehicles. The major use of these units is to communicate with the nearest Road Side Units (RSUs) which provide infrastructure support to the moving vehicles. The communication between OBUs and AUs is achieved by handling OBUs communication potential, whereas the connection between AUs and OBUs can be done by wired/wireless technology and the connection between OBUs and RSUs are of only wireless standards. Because of the interesting and talented functionalities which include vehicular safety, traffic congestion control, and location-based services, VANET has grabbed a massive attention [1-2].

Privacy is the acid issue which comes under VANET. The important information can leak easily while exchanging the messages without any particular protection due to the nature of wireless communication which is sharing the medium. In recent times, VANET has been given a lot of attention by academia and the automobile industry along with the government. There is an On Board Unit (OBU) communication device which is present in each vehicle which grants the vehicles to communicate with each other [3].

[1] Research Scholar, Department of Computer Science and Engineering;

[2] Professor, Department of Computer Science and Engineering, Maulana Azad National Institute of Technology, Bhopal (M.P.) India; *E-mails: rajubaraskar@rgtu.net, chawlam@manit.ac.in*

In the actual world, there are tons of vehicles which leave/joins a VANET in metropolitan areas or the highways, and it is absurd or impossible that all the vehicles certified to a single group. Therefore, several constraints must be met in security algorithms. This happens because when a particular vehicle joins/ leaves the network; all the other vehicles should adjust their public parameters. The structure of adjusting public parameters has been studied in some initial algorithms that have used group keys. To improve the scalability, reliability, and security of a network, a particular method is used which is known as group key management process. Since group key management needs to direct the security issue related to membership adjustments, the membership modification requires the group key refreshment. This can be executed either by periodic rekeying or updating right after member adjustment. Rekeying is required in a secure multicast communication to prevent a new member (before its joining) from decrypting multicast data, and it also prevents a leaving member from listening in future multicast data. A crucial problem with any rekeying technique in multicast key distribution is unauthenticated with high packet loss rate due to periodic node mobility [4]. A vehicular ad hoc network can be taken into consideration as groups of logic and in this network, the group members are the nodes which are introduced initially. Considering such a network that can be formed in an ad hoc way or process, we need a perfectly initialized way to form a group key that particularly makes a way for the group members to communicate in a manner. For example, in a particular region, if a small group of vehicles agrees to share the chat, they can establish a small group of network and can form a group key for group communication securely. If they can grab each and every single message of the particular discussion, then also the contents of that discussion cannot be accessed or understand by other groups outside. Under VANET, the members can join or leave the group freely at any moment, that’s why the group management can be considered as the crucial issue and the primary block in this scheme. Moreover, the Bandwidth in the particular network is restricted to a level and the devices are perfect energy constrained, so a beneficial scheme for VANETs must be of fewer communication rounds and of low computation level [5]. Group communication generally provides a process or manner for a user or a subgroup of users to receive (or send) data streams from (or to) other users. Many emerging Internet applications, e-newspaper, and play-on-paid multicast services are particularly formed and used in the group communication. Using these applications, the issue of access control must be checked and saved. When the particular legitimate users have the access to the data streams which is authorized, then the control of access for communication of the group is ensured and no legitimate users will authorize the data stream. Hence, the data streams are encrypted using an encryption key and the access of the data streams is been done by the users [6].

2. RELATED WORKS

LDGKA scheme is proposed in [7]. It is based on location based group key agreement, where vehicles in the same region form groups. The virtual key tree model is used in each group so that the process of leaving and joining of nodes become efficient with minimum of O(Log (n)) keys required for rekeying. In [8] a data forwarding strategy in VANETs is proposed. It uses link lifetime predictions and link utility metric for efficient data transmission. Furthermore, this strategy reduces the number of hops in a high traffic situation. In [9] the management protocols in VANETs based on mobility of vehicles are proposed. The mobility is divided into two parts, intra-highway mobility, and global mobility. In intra-highway, handoffs are managed locally whereas Mobile IPv6 is used for managing global mobility. In [10] a security scheme is proposed named as Aggregate signatures and certificates verification scheme. ASIC scheme allows verifying the digital signatures and certificates of the sender. This allows achieving high safety levels in VANETs. In [11], a key management framework with distributed framework is proposed. The framework takes into vision the problem for detecting the compromised roadside units and conspiring vehicles. Moreover, a message authentication protocol is also proposed which is quite cooperative in nature.

In [12] a key establishment scheme is proposed for providing authentication among vehicles and road side units (RSUs). This scheme is called SECPP. Moreover, the scheme also proposes the logic of blind signatures which can be exchanged between vehicles and RSUs. In [13] a secure communication model using dynamic establishment is proposed. It provides a key management technique in the situations when there is no central unit or RSU. DESCV provide secure communication among vehicles which travel with a relative velocity of 240 kmph or higher. [14] Proposes a key management framework where vehicles are grouped and a group leader is selected. The group leader is answerable for managing group members and for certificate authentication. It provides the security mechanism to protect data privacy. But this method also suffers from loopholes. In [15] techniques for remote software distribution in a base station for secure multicasting are given. In VSDN large region is split into several small regions which are managed by RGM. Moreover, VSDN system is divided into two parts. First, are fully trusted systems where base stations are used for accessing the multicast data and take part in GKM. Second, is semi-trusted system where base station does not access the multicast data rather they act as proxies for the vehicles. In [16] distributed group key distribution (DGKD) protocol is stated, this protocol wins over the shortcomings of different group key management (GKM) protocols like centralized group key distribution (CGKD), decentralized group key management (DGKM), and contributory group key agreement (CGKA). Introduces [18] a public key infrastructure in VANET based on physical layer assisted message authentication (PAA). In this advantage of the channel response of physical layer is taken. Moreover, PAA is very efficient and meets the security requirements as well. Pairing-based cryptography is considered in [19]. Bilinear pairings have been used to design ingenious protocols for such tasks as one-round three-party key agreement, identity-based encryption, and aggregate signatures. In [21] there are a number of routing schemes which are viewed especially in the field of safe communication among vehicles. These provide a significant application for inter-vehicular communications in transferring vehicle safety information. In [22] a protocol is stated which guarantees to preserve security and privacy in VANET. It also provides for disclosure of the identity of the malicious sender by the central authority. Many simulations are conducted in order to prove the efficiency of this protocol. Introduces [23] a message authentication model which is helped by roadside units(RSUs). This model is called as RAISE. In this, the RSUs hold the responsibility for checking the message’s truthfulness and then providing a positive feedback. This scheme deals with the scalability issue. In [24] a security protocol is proposed based on distributed key management. The protocol identifies the compromised RSUs and their interaction with the malicious vehicles. Mostly distributed key management suffers from an issue that the semi-trust RSUs may be compromised and these protocols aid as some solution to this protocol. An early warning intelligence broadcasting algorithm is proposed in [26]. The proposed algorithm distributes early warning messages based on TTC concept i.e. time to collision concept. EW-CAST also provides a use of efficient broadcasting algorithm using fuzzy logics. Simulations show that EW-ICAST is better than its counter algorithms. A key distribution protocol is proposed in [27]. Euler’s Totient function ö(n) is used to achieve the good amount of security. It breaks the re-keying information so it increases the key space.

Packet frame-based architecture along with procedures on packet communication procedures for link setup with 5.8 GHz DSRC is proposed in [28]. In this, the basic requirements related to DSRC system are also discussed. In [29] it is proposed about a protocol named EDR (efficient decentralized revocation). It is based on probabilistic key distribution and pairing based schemes. It provides a scheme for the elimination of misbehaving vehicles which can affect the safety of other vehicles. A highway broadcast model is proposed in [30]. It solves the flooding problem caused due to broadcasting. This is done by calculating the relative gain of each neighbour and selects the neighbour with maximum gain for the upcoming hop. A security based infrastructure is proposed in [32]. It uses two types of cryptographic techniques that are asymmetric and symmetric cryptography, both ensures privacy and security of data that is shared between vehicles. This infrastructure also proposes the use of hardware which is tamper resistant. Proposed [33] a scheme for tracing the message originator in the both posterior and prior form. It helps in finding out the malicious or malfunctioning vehicle. This ensures message trustworthiness in VANET.

3. THE PROPOSED MASTER KEY AGREEMENT SCHEME

In MKAS scheme vehicles are divided into a number of the different groups which is called as groups. Vehicles of the same group or two different groups communicate to each other to exchange safety and non-safety-related information which is encrypted using session key. Each vehicle has also the pair of the public and private key. Each group has a group head to manage these keys as the production of keys, distribution of keys to group members, updating and revocation of keys. Vehicles moving at very high speed before exchanging information encrypt the message using the pair of public/private key and session keys while group head encrypts and decrypt the information using the master key.

In the following section, management of keys is discussed in many phases:-

3.1. Key Production

Each vehicle V_k in network is certified as a legal member by a certificate authority and head of the group is selected using leadership selection algorithm [19] to manage all keys used in communication.

Following steps are taken in production of keys:

Step 1: V_m Calculates session key by taking two random numbers Z_i and Z_j to encrypt communication between vehicles of the group.

Step 2: V_m Calculates master key K_m using master key generation algorithm [26] which is only known to the leader of the group.

Step 3: V_m Provides $List_k^{ID}$ of members of the group which is in nearest transmission range of group leader. Each vehicle takes a random number Z_k. If V_m leaves the group V_c selects new group leader V'_m based on the random number Z_k. New group leader V'_m updates the old session key K_{GS} by calculating new session key $K_{GS'}$ and new master key K'_m. This $K_{GS'}$ new session key is encrypted using updated master key and sends to its group member V_c. Now new session key $K_{GS'}$ will be used for communication among group member.

Step 4: Each vehicle V_k takes its private key V_k^{pri} and calculates public key V_k^{pub} using elliptic curve cryptography $V_k^{pub} = BP \otimes V_k^{pri}$.

NOTATION TABLE

Natations	*Description of Notations*
V_k	Vehicle k
V_m	Leader of group
V_c	Member of group
V_k^{pub}	Public key of vehicle
V_k^{pri}	Private key of vehicle
K_{GS}	Group session key
K_m	Master key of group leader
$List_k^{pub}$	List of public keys
$List_k^{rev}$	Key revocation list
Z_i, Z_j	Random number selected by group leader
Z_k	Random number taken by vehicle to select group leader
T_s	timestamp
$List_k^{ID}$	List of vehicles' ID
U_M	Message to update key

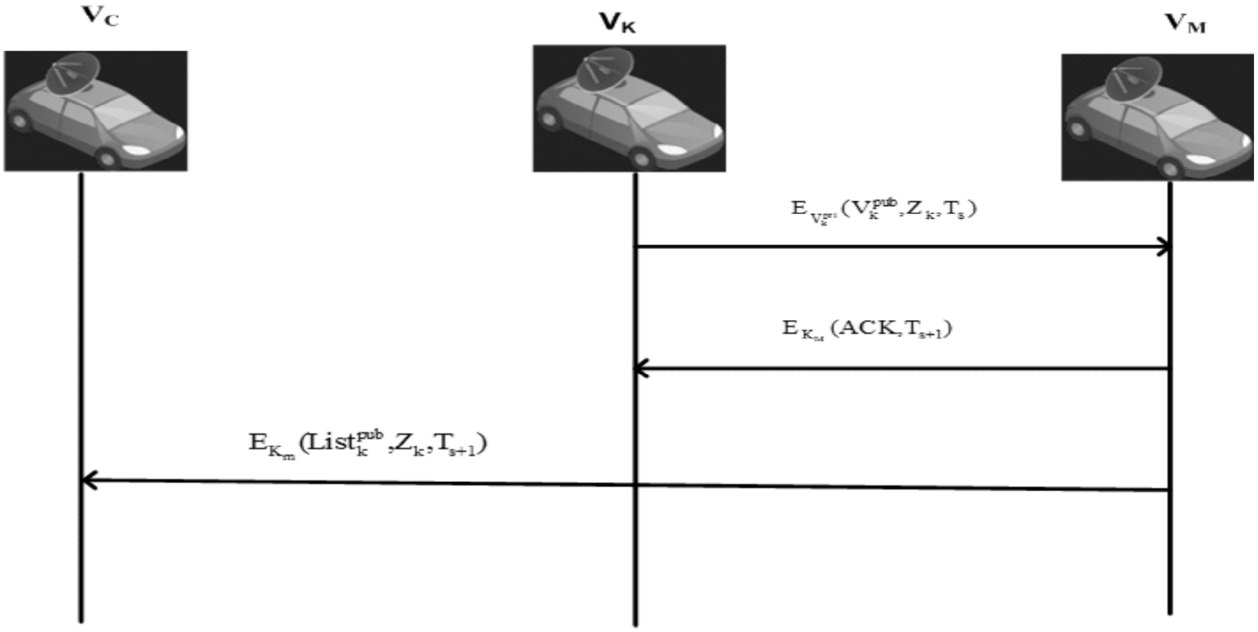
3.2. Key Distribution

The public key of all vehicles is transmitted to the group leader to be validated and then distributed to all group members. Following steps are taken to distribute keys. Apart from that, group leader broadcasts session key encrypted using master key to all vehicles.

Step 1: Vehicle V_k sends public key V_k^{pub} with timestamp T_s and to V_m.

Step 2: V_m receives the public key V_k^{pub} of all group members and check timestamp. V_m creates an acknowledgment with a timestamp $T_s + 1$ and encrypt using master key and sends to each group member V_c.

Step 3: In next step V_m creates a list of all public key $List_k^{pub}$ and random number Z_k encrypted using the master key K_m then broadcast to all member of the group with a timestamp.



$\mathbf{V_C}$
$\mathbf{V_K}$
$\mathbf{V_M}$
$E_{V_k^{pub}}(V_k^{pub}, Z_k, T_s)$
$E_{K_M}(ACK, T_{s+1})$
$E_{K_m}(List_k^{pub}, Z_k, T_{s+1})$

Figure 1: Key Distribution Process

Figure 1 shows that each vehicle sends its public key to the group leader who creates a public key list of group members and then encrypts this message using its master key. After that group leader broadcasts this list to all members of the group with a timestamp.

3.3. Key-Updating

In VANET vehicles are highly mobile in nature. Therefore if any vehicle or group leader leaves or joins a group forward and backward secrecy is necessary to maintain. When vehicle joins or leaves any group, session key of the group is updated and when the leader of the group departs from the group then master key and session key both are updated immediately to preserve the secrecy of group. Following are an illustration of above two conditions to update the content of key.

3.3.1. Group Member Leave: A group member knows its entire group key to communicating among themselves in a group. When a group member leaves the group it is the responsibility of group leader to immediate update entire group key to preserving secrecy.

Following steps are taken to update keys in above case:

Step 1: If the location of the vehicle V_k cannot be find by V_m in group then V_m assumes that V_k has left the group.

Step 2: Therefore V_m broadcast the information to update the key, $K_{GS} V_k^{pub} List_k^{pub}$ of leaving member to another group member V_c.

Step 3: V_c create an acknowledgement and encrypt using V_k^{pri} with a timestamp and sends to V_m.

Step 4: V_m decrypts the acknowledgement message K_m using and validates timestamp Then. V_m Updates session key from K_{GS} to $K_{GS'}$ and V_m revoke K_{GS}, it inserts into $List_k^{rev}$.

Step 5: V_m encrypts new session key $K_{GS'}$ using K_m and distributes encrypted $K_{GS'}$ to each group member V'_c

Step 6: V'_c decrypts using their private key, verifies timestamp and get updated session key K_{GS}'. V'_c Encrypts acknowledgement with a timestamp and sends to V_m.

Step 7: V_m decrypts acknowledgement using its master key and validates timestamp and hence key updating procedure is completed.

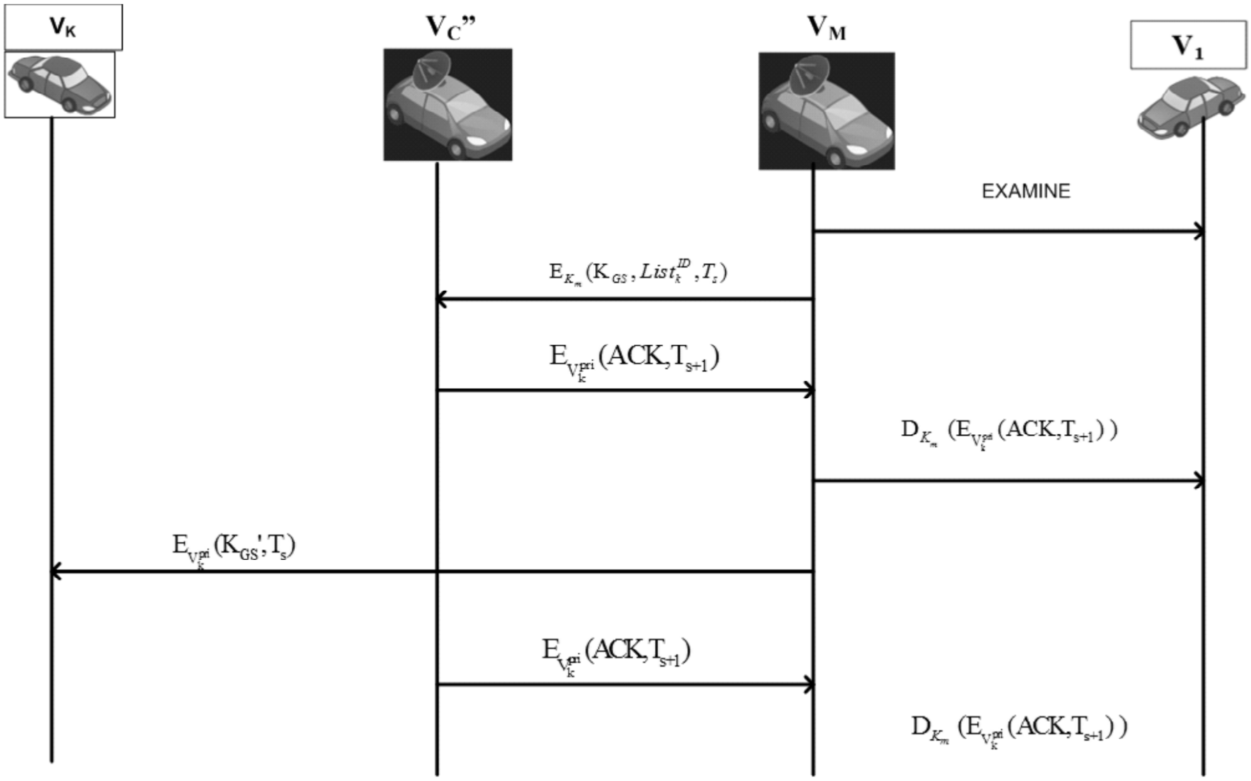

V_K
V_C"
V_M
V_1
EXAMINE
$E_{K_m}(K_{GS}, List_k^{ID}, T_s)$
$E_{V_k^{pri}}(ACK, T_{s+1})$
$D_{K_m}(E_{V_k^{pri}}(ACK, T_{s+1}))$
$E_{V_k^{pri}}(K_{GS}', T_s)$
$E_{V_k^{pri}}(ACK, T_{s+1})$
$D_{K_m}(E_{V_k^{pri}}(ACK, T_{s+1}))$

Figure 2: Departure of Group Member

Figure: 2 shows that group leader examines departure of group member after which it broadcasts session key updating message to its old group members encrypted using master key. Group leader generates new session key and transmits to each vehicle of group and inserts old session key into key revocation list.

3.3.2. Departure of Group Leader : When group leader departs from any group its members update old keys (public, private, session and master key) and reselect a new group leader V'_m. All group members initially take a random number to select group leader and after the departure of old group leader they selects a new group leader gain because group leader manages the entire group.

Step 1: When a group leader V_m departs from the group it informs all member of the group.

Step 2: Other group members compare Z_k of selected group leaders and select a new group leader. Departing group leader transmits old $List_k^{rev}$ to V'_m.

Step 3: V_m ' calculates new session key K_{GS} 'and check its presence in old $List_k^{rev}$. If this is the new one then V_m ', sends a message to update the key $List_k^{ID}$ and to group members' encrypted using master key.

Step 4: Group members receive this message of new group leader and send acknowledgement to V_m '.

Step 5: V_m ' revoke the old master key and insert into $List_k^{rev}$, then calculates a new master key K_m 'to maintaining secrecy and check whether it is present in, if yes then it recalculates new master key.

Step 6: V_m ' receives an acknowledgement message from all group members and verifies timestamp. If timestamp is verified as correct, new group leader will deliver K_{GS} ' to all group members.

Step 7: After receiving updated session key group members reselect new Z_k, private key V_k^{pri} and public key V_k^{pub} .

Step 8: Group members encrypt a message of updated keys using new V_k^{pri} and transmit to V_m '.

Step 9: New V_m 'decrypts the message using the new master key and enters updated key in new $List_k^{rev}$.

Step 10: New group leader creates $List_k^{pub}$ of all group members and encrypts this list using the new master key and sends to all group members.

Step 11: All group embers decrypt this message using their V_k^{pri} and gets V_k^{pub} of each member of the group. Here key updating procedure is completed.

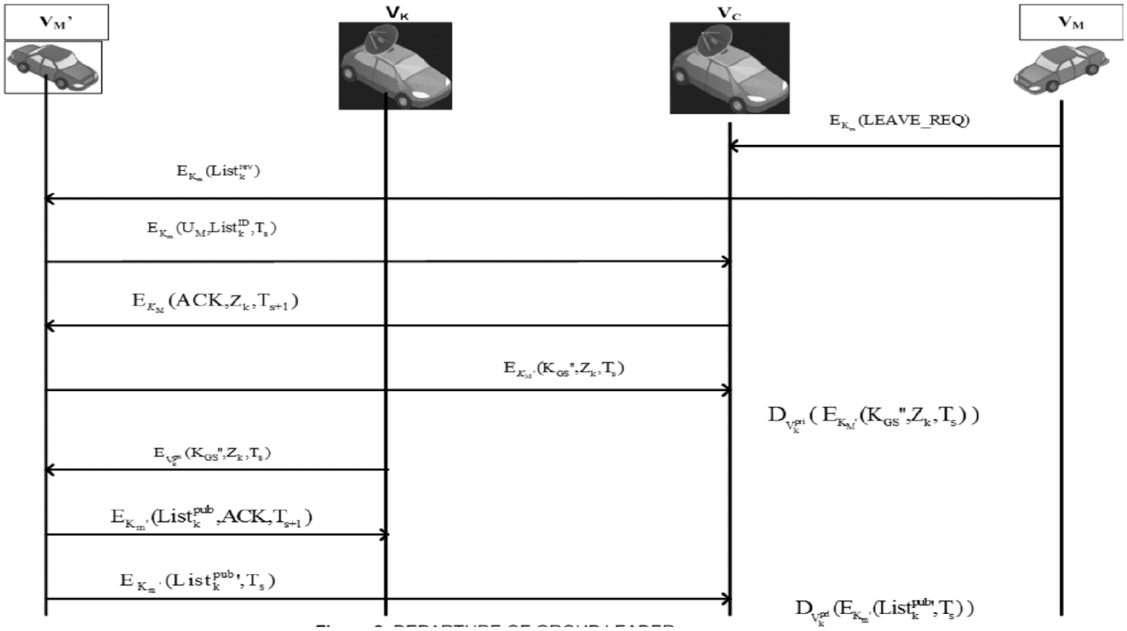

V_M'
V_K
V_C
V_M
$E_{K_m}(LEAVE\_REQ)$
$E_{K_m}(List_k^{rev})$
$E_{K_m}(U_M, List_k^{ID}, T_s)$
$E_{K_M}(ACK, Z_k, T_{s+1})$
$E_{K_M'}(K_{GS}'', Z_k, T_s)$
$D_{V_k^{pri}}(E_{K_M'}(K_{GS}'', Z_k, T_s))$
$E_{V_k^{pri}}(K_{GS}'', Z_k, T_s)$
$E_{K_m'}(List_k^{pub}, ACK, T_{s+1})$
$E_{K_m'}(List_k^{pub}', T_s)$
$D_{V_k^{pri}}(E_{K_m'}(List_k^{pub}', T_s))$

Figure 3: Departure of Group Leader

In figure: 3, when a group leader leaves the group, remaining group members select new group leader based on previously taken random numbers. New group leader calculates new master key and session key. Public key list and new session key of the group are transmitted to all group members by the new group leader.

3.3.3. Joining of New Group Member: When any vehicle cannot receive information from any group member or group leader, group leader considers this vehicle as it left the group. If this vehicle wants to join the group again key of the group will be updated again to maintain the secrecy of group. Public/private key pair of a group member and group session key is updated in this case.

Step 1: Vehicle V_k who wants to join the group again calculates its new public key and sends a request to V_m.

Step 2: V_m verifies the certificate of V_k. If V_k is a legal vehicle V_m, will generate a new session key and broadcasts a message to update the public/private key pair to all group member.

Step 3: After receiving updated session key, group members send acknowledgement message with a timestamp to V_m.

Step 4: V_k takes to Z_k select new group leader V_m ' and sends an acknowledgement to V_m encrypted using new private key.

Step 5: After selecting V_k as group member V_m inserts old session key into and updates timestamp of Z_k, $List_k^{pub}$ transmission time and encrypt the message using master key and distributes to all group members.

Step 6: V_c decrypt this message using their V_k^{pri}. It completes group key management process.

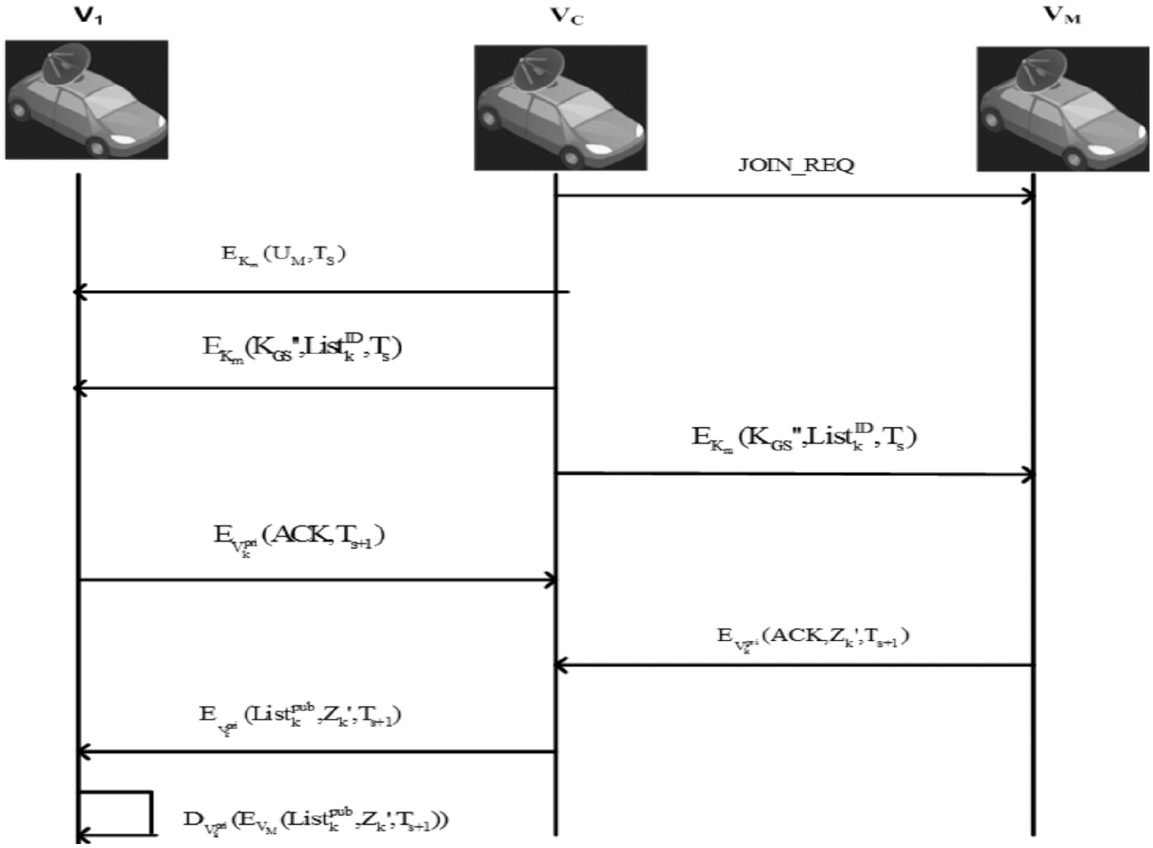

V_1
V_C
V_M
JOIN_REQ
$E_{K_m}(U_M,T_S)$
$E_{K_m}(K_{GS}",List_k^{ID},T_s)$
$E_{K_m}(K_{GS}",List_k^{ID},T_s)$
$E_{V_k^{pri}}(ACK,T_{s+1})$
$E_{V_k^{pri}}(ACK,Z_k',T_{s+1})$
$E_{V_k^{pri}}(List_k^{pub},Z_k',T_{s+1})$
$D_{V_k^{pri}}(E_{V_M}(List_k^{pub},Z_k',T_{s+1}))$

Figure 4: Joining of Group Member

Figure: 4 shows that a new vehicle who wants to join a group sends a request to the group leader who verifies the certificate of a new vehicle after which it joins the group and then session key of the group is updated.

3.4. Group Key Revocation Process: In above cases of key updating, all old keys are revoked and new keys are calculated to preserve the privacy of group. All these old keys are entered into key revocation list $List_k^{rev}$ which is maintained by the group leader V_m and it is checked that whether newly calculated key is in key revocation list or not. If it presents then a new key is recalculated to stop the repetitive use of old keys. Procedure of group key revocation in this scheme is illustrated as follows:

Step 1: V_m updates K_{GS} and calculates a new session key $K_{GS}{}'$ when any member joins or leave the group and checks whether newly calculated session key is in the revocation list, if yes V_m, will again calculate group session key.

Step 2: V_m encrypts new session key $K_{GS}{}'$ using the public key of each member V_k^{pub} and distributes to each group member.

Step 3: Each group member decrypts the message and gets the new session key $K_{GS}{}'$. V_k creates acknowledgement message with a timestamp and encrypts using the new private key and sends to V_m.

Step 4: V_m decrypts acknowledgement using its master key K_m.

Step 5: To maintain forward and backward secrecy group member replaces old session key by new session key.

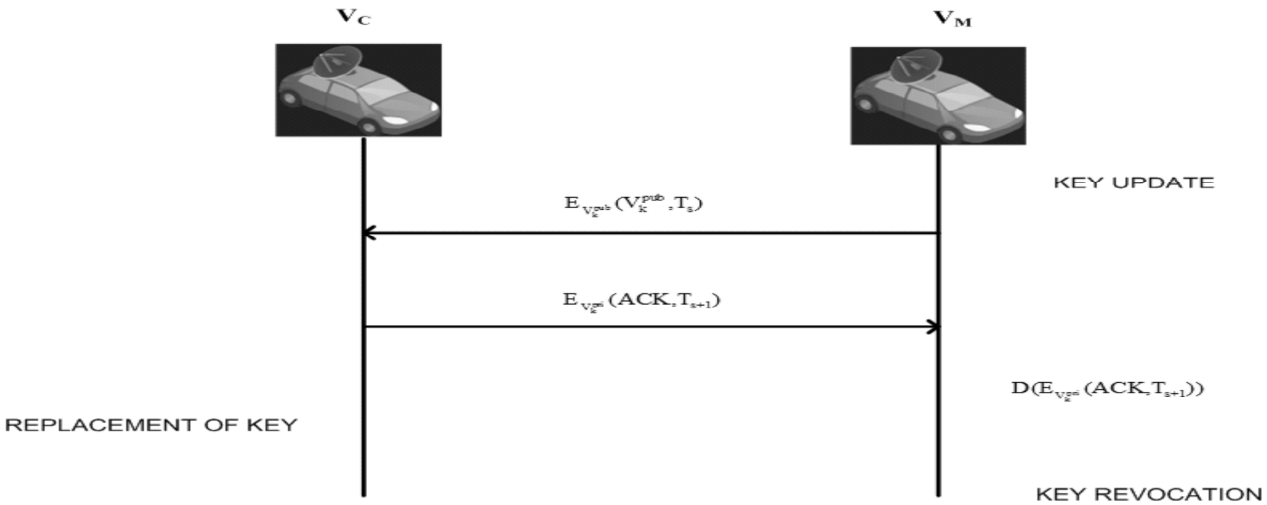

V_C
V_M
KEY UPDATE
$E_{V_k^{pub}}(V_k^{pub}, T_s)$
$E_{V_k^{pri}}(ACK, T_{s+1})$
$D(E_{V_k^{pri}}(ACK, T_{s+1}))$
REPLACEMENT OF KEY
KEY REVOCATION

Figure 5: Group Key Revocation Process

Figure: 5 shows that when any group member leaves or joins the group, leader of the group sends updated session key to its group members encrypted using their public key and session key is revoked and get entered in the key revocation list.

4. EVOLUTION OF SECURITY ANALYSIS AND COMPARISON

(i) Updating of keys: Privacy of vehicle user is maintained in this scheme by updating the key whenever a vehicle leaves the group or joins a group. Therefore this scheme achieves the goal of forward and backward secrecy.

(ii) Data integrity and privacy: If vehicles are attacker they cannot generate a new key with the help of old key because each time key is updated and a random number is used to calculate a new key.

(iii) Using master key: In this scheme, group leader itself calculates a new key which is master of all other keys to encrypt/decrypt the message received from its all group member and this key is kept secret as not distributed to any member vehicle. Attackers should have a master key to access the communication. It preserves the secrecy of all other keys.

(iv) Using timestamp: Timestamp is used with each message and an acknowledgement message is received on each node communicating with other nodes which identify the attack on message by malicious vehicle if there is a delay in the message.

(v) Unforgeability: No vehicle can claim that it is a member of a particular cluster to obtain any information because each vehicle is certified in its group with its identity and claimed vehicle should have a pair of public-private key and session key of that group.

(vi) Security of key during transmission: Session key is encrypted every time using master key during transmission which is known to group leader only so its content cannot be modified in case of stolen of the key furthermore secret key is calculated using random numbers in this scheme.

(vii) Revocation of key: When the key is revoked by group leader it enters revoked key into key revocation table which stops the repetitive use of old key and generates fresh key every time.

(viii) Authentication: Here each vehicle is certified as the legal vehicle by a certification authority which tells that identity of a particular vehicle is valid and it can communicate to another vehicle.

(ix) Collusion freedom: There is a distinct group which has different public/private key pairs, session key and master key. So the key of each group is independent of other group and the rekeying process is done every time when a node leaves or joins the group. Compromised vehicle cannot collude with it's accomplish vehicle.

Table 1
Comparison of Security Parameters among related works

Security Parameters	*[15]*	*[17]*	*Decentralized [20]*	*Centralized [25]*	*SCKD [31]*	*Proposed-MKAS*
Anti-Eavesdrop	Yes	Yes	Yes	Yes	Yes	Yes
Encryption of Key During Transmission	No	Yes	No	Yes	Yes	Yes
Forward Secrecy	No	-	Yes	Yes	Yes	Yes
Backward Secrecy	No	-	Yes	Yes	Not Discussed	Yes
Vulnerable to Message Alteration	Yes	No	No	No	No	No
Secrecy of Master Key	Not Discussed	Not Discussed	Not Discussed	Not Discussed	Not Discussed	Yes

In Table 1, we have presents the comparison of security parameters among related works for different mechanisms, which can prevent malicious users from wiretapping, replay, speculation, falsification, and attack; moreover, key transmission is completely encrypted in the whole process. Other mechanisms overlooking the significance of key encryption in transmission raise the possibility of the key being stolen by malicious users in the process. In this study, this mechanism delineates that the key produced after updating is incapable of calculating the new or old key content and achieves the goal of forward and backward secrecy; whereas the session key and master key used for secure communication.

5. PERFORMANCE ANALYSIS OF TIME COMPUTATION AND COMPLEXITY

Computation cost of MKAS scheme is listed Table 2. Parameters of computation are also defined. According to Table 2 in MKAS in initial status phase, session key and master key is calculated, similarly in key updating phase when group leader departs from group both session key and the master key is recalculated which costs computationally while when any group member joins or leaves group only session key is recalculated. Security is a most important requirement in VANET therefore in proposed approach in key distribution phase, the session key is encrypted through master key which is secret and works as one private key of the group leader. All Key is updated during transmission in this scheme. Here, symmetric and asymmetric encryption/decryption technique both are applied symmetric encryption is faster than asymmetric encryption. For better security, this scheme is good in spite of the high computational cost.

Table 2
Comparison of Computation Cost among related works

Schemes		*GKMPSM [15]*	*SeGCOM [17]*	*DGKM [20]*	*CGKM [25]*	*SCKD [31]*	*Proposed-MKAS*
Initial status		$2T_{sym}$	$6T_r+3T_{hash}$	$2T_{asym}+T_{hash}$	$T_{sym}+2T_r+T_{EC}$	$2T_{asym}+2T_{hash}+T_r$	$T_{sym}+T_{ECC}+3T_r+T_m$
Key update	Join Member	$(2+n)T_{sym}$	$6T_r+3T_{hash}$	$2T_{asym}+T_{hash}+T_r$	$T_{sym}+2T_r$	$2T_{asym}+2T_{hash}+T_r$	$T_{sym}+2T_r$
	Leave Member	$2T_{sym}$	Not Discussed	T_i+T_{asym}	$T_{sym}+2T_r$	Not Discussed	$T_{sym}+2T_r$
	Leave of Group Leader	Not Discussed	Not Discussed	$T_{xor}+3T_{asym}$	$T_{sym}+2T_r+T_{EC}$	Not Discussed	$T_{sym}+T_{ECC}+3T_r+T_m$

T_{sym} = Time to calculate symmetric key, T_{asym} = Time to calculate asymmetric key, T_r = Time to calculate random number, T_{ECC} = Time to calculate session key using elliptic curve cryptography, T_{hash}= Time to calculate hash, T_{XOR} = Time to compute exclusive OR operation, T_i = Time to compute invert.

6. CONCLUSIONS

This paper proposes a master key agreement scheme for communication of vehicles' information in VANETs. In this scheme, group leader calculates two keys which are session key and master key. The session key is used to encrypt safety and non-safety-related information of vehicle's transmitting among vehicles of the same group and vehicles of different groups while the master key is used to encrypt keys i.e. session key, public key and other information which group leader sends to vehicles of the group. As the master key is known to group leader only, therefore, no other vehicle can forge key information, this provides authentication. If attacker reveals encrypted message transmitting between the group leader and member vehicles he cannot decrypt the message because he should know the private key of the vehicle. In proposed key management scheme group leader fairly distributes the key to vehicles of the group and taking random numbers to calculate session key results in the more secure key. The environment of VANET is dynamic mobile; therefore, to preserve the secrecy of data when a member joins a group or departs from the group, the group key is updated instantly in this scheme.

REFERENCE

[1] Zhu, J., & Roy, S., "*MAC for dedicated short range communications in intelligent transport system*", IEEE Communications Magazine, vol.*41* (12), pp.60-67, 2003.

[2] Bera, R., Bera, J., Sil, S., Dogra, S., Sinha, N. B., & Mondal, D., "*Dedicated short range communications (DSRC) for intelligent transport system*", In 2006 IFIP International Conference on Wireless and Optical Communications Networks (pp. 5-pp), 2006.

[3] Mejri, M. N., Ben-Othman, J., & Hamdi, M., "*Survey on VANET security challenges and possible cryptographic solutions*", Vehicular Communications, vol*1* (2), pp.53-66, 2014.

[4] Rafaeli, S., & Hutchison, D., "*A survey of key management for secure group communication*.", ACM Computing Surveys (CSUR*)*, vol*35*(3), pp.309-329, 2003.

[5] Challal, Y., & Seba, H., "*Group Key Management Protocols: A Novel Taxonomy*", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. *2*(10), pp.3620-3633, 2008.

[6] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H., " *A comprehensive survey on vehicular Ad Hoc network*", Journal of network and computer applications, vol.*37*, pp.380-392, 2014.

[7] Wang, E. K., Ye, Y., & Xu, X., "*Location-based distributed group key agreement scheme for vehicular ad hoc network*", International Journal of Distributed Sensor Networks, 2014.

[8] Zhu, W., Gao, D., & Foh, C. H., " *An efficient prediction-based data forwarding strategy in vehicular ad hoc network*", International Journal of Distributed Sensor Networks, 2015, 1, 2015.

[9] Lee, D., Kim, Y. H., & Lee, H., "*Route prediction based vehicular mobility management scheme for VANET*", International Journal of Distributed Sensor Networks, 2014.

[10] Plößl, K., & Federrath, H., "*A privacy aware and efficient security infrastructure for vehicular ad hoc networks*", Computer Standards & Interfaces, vol.*30*(6), 390-397, 2008.

[11] Wasef, A., & Shen, X., "*ASIC: Aggregate signatures and certificates verification scheme for vehicular networks*", In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE ,pp. 1-6 ,2009.

[12] Hao, Y., Cheng, Y., Zhou, C., & Song, W., "*A distributed key management framework with cooperative message authentication in VANETs*", IEEE Journal on selected areas in communications, vol.29 (3), pp.616-629, 2011.

[13] Li, C. T., Hwang, M. S., & Chu, Y. P., "*A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks*" , Computer Communications, vol. 31(12), pp.2803-2814, 2008.

[14] Yeh, C. H., Huang, Y. M., Wang, T. I., & Chen, H. H. , " *DESCV—A Secure Wireless Communication Scheme for Vehicle ad hoc Networking*", Mobile Networks and Applications, vol.*14*(5), pp. 611-624, 2009.

[15] Yeh, C. H., Hsieh, M. Y., & Li, K. C., "*A certificate enhanced group key framework for vehicular Ad Hoc networks*" , In Ubiquitous Information Technologies and Applications, pp. 215-222, 2013.

[16] Hossain, I., & Mahmud, S. M., "*Analysis of group key management protocols for secure multicasting in vehicular software distribution network*" , In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), pp. 25-25, 2008.

[17] Adusumilli, P., Zou, X., & Ramamurthy, B., "*DGKD: Distributed group key distribution with authentication capability*" In Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, pp. 286-293, 2005.

[18] Verma, M., & Huang, D., "*SeGCom: secure group communication in VANETs*", In *2009 6th IEEE* Consumer Communications and Networking Conference, pp. 1-5, 2009.

[19] Wen, H., Ho, P. H., & Gong, G. "*A novel framework for message authentication in vehicular communication networks*", In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pp. 1-6, 2009.

[20] Wang, N. W., Huang, Y. M., & Chen, W. M., "*A novel secure communication scheme in vehicular ad hoc networks*", Computer communications, vol. 31(12), pp.2827-2837, 2008.

[21] Guo, M. H., Liaw, H. T., Chiu, M. Y., & Deng, D. J. , "*On decentralized group key management mechanism for vehicular ad hoc networks*", Security and Communication Networks, 2012.

[22] Chennikara-Varghese, J., Chen, W., Altintas, O., & Cai, S., "*Survey of routing protocols for inter-vehicle communications*", In 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1-5, 2006.

[23] Lin, X., Sun, X., Ho, P. H., & Shen, X. , "*GSIS: a secure and privacy-preserving protocol for vehicular communications*", IEEE Transactions on vehicular technology, vol.56(6), pp.3442-3456, 2007.

[24] Zhang, C., Lin, X., Lu, R., & Ho, P. H., "*RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks*", In 2008 IEEE International Conference on Communications, pp. 1451-1457, 2008.

[25] Hao, Y., Cheng, Y., & Ren, K., "*Distributed key management with protection against RSU compromise in group signature based VANETs*", In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference , pp. 1-5,2008.

[26] Wu, Q., Domingo-Ferrer, J., & González-Nicolás, U., "*Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications",* IEEE Transactions on Vehicular Technology, vol.59 (2), pp.559-573, 2010.

[27] Plößl, K., & Federrath, H., “*A privacy aware and efficient security infrastructure for vehicular ad hoc networks”,* Computer Standards & Interfaces, vol. 30 (6), pp. 390-397, 2008.

[28] Daeinabi, A., & Rahbar, A. G., “*An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks*”, Computers & Electrical Engineering, vol.40 (2), pp.517-529, 2014.

[29] Chuan, D., & Jian, W., “*A Reliable and Efficient Highway Multihop Vehicular Broadcast Model*”, ISRN Communications and Networking, 2012.

[30] Wasef, A., & Shen, X., “*EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks*”, IEEE Transactions on Vehicular Technology, vol.58 (9), pp.5214-5224, 2009.

[31] Oh, H., Yae, C., Ahn, D., & Cho, H., “*5.8 GHz DSRC packet communication system for ITS services*”, In Vehicular Technology Conference, 1999. VTC 1999-Fall. IEEE VTS Vol. 4, pp. 2223-2227, 1999.

[32] Kim, B., Cho, H., & Lee, J., “*Efficient key distribution protocol for secure multicast communication*”, In International Conference on Computational Science and Its Applications, pp. 1007-1016, 2004.

[33] Bae, I. H., “*An intelligent broadcasting algorithm for early warning message dissemination in VANETs*”, In International Conference on Computational Science and Its Applications, pp. 668-681, 2014.

[34] Guo, M. H., Liaw, H. T., Deng, D. J., & Chao, H. C., “*Centralized group key management mechanism for VANET*”, Security and Communication Networks, vol. 6(8), pp.1035-1043, 2013.