Key Management Techniques for VANETs

G.Sasikala
PG Student
Department of ECE,
Kalasalingam University,
Krishnankovil

K.S. Dhanalakshmi
Assistant Professor-I
Department of ECE
Kalasalingam University
Krishnankovil.

ABSTRACT

Vehicular adhoc network is commonly used network among the vehicles in a centralized way. This network is built in order to send and receive messages from the vehicles which are present in the network. Since it is a centralized network, hence many problems have be occurs in the network. The main issues of vanet are maintaintenance of the system and revocation of malicious vehicles. The new efficient management frameworks that have been framed to overcome the above said problems. It is known as the shared key management technique. The road side unit (RSU) which is present distributes the keys to the various key. The framework is assisting the above said three major problems. This framework can be simulated using NS2.The major architecture of this framework is built in order to get the desired output like avoiding road traffic blockage, safe and secure travel and a volume of high security is imposed in sending and receiving the messages. The message is send and receives without any blockages by the means of cooperative message authentication.

General Terms: VANET, Security, Shared Key Management

Keywords: Vehicular adhoc networks, security, shared key management, RSU, co-operative message authentication

1. INTRODUCTION

The vehicular adhoc networks [VANET] is very popular among the networks due to their interesting and promising functionalities like vehicular safety, traffic congestion avoidance, and location based services [1].In this paper we mainly focus on overcoming the various problem defined in distributed key management framework and how to overcome the problems by adopting a separate management framework known as shared key management frame [1].

In Fig. 1 the Road side unit measure road conditions at several position on the surface. The main object of the architecture for VANET is Safety driving, Traffic congestion avoidance and Location based services, the vehicle generates a warning message and distributed in to all vehicles in a certain geographical region, potentially using wireless multihop communication. A VANET communication architecture assume that vehicles equipped with an On Board Unit (OBU) and two wireless network interface IEEE802.11 and IEEE802.15.4 .In addition, the impact of packet loss at the medium access control (MAC) layer on security performance is not investigated .

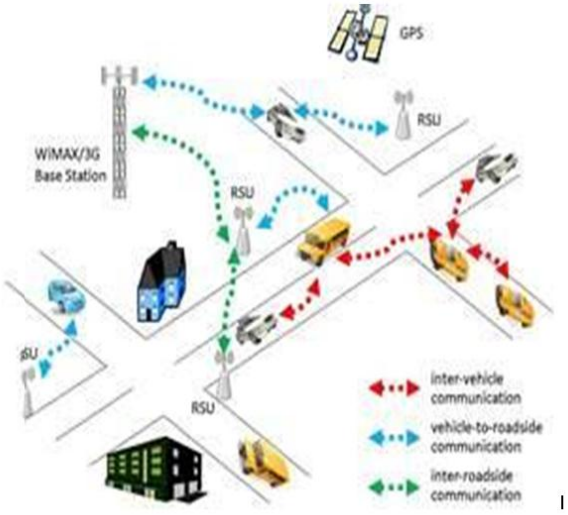

Fig 1.Vehicular adhoc network (VANET) image

The delay control for vanet and data aggregate is an efficient technique for minimizing the redundant data and improve communication efficiency by using adaptive forwarding delay control scheme known as the catch-up scheme [2].In this paper R&D ecosystem are adopted to improve the security system in VANETS. The R&D ecosystem are created by academic research, car manufactures, government authorities and end user [3].

The safe driving and infotainment services on the move can be develop by the usage of hash chaining concept of cryptography [4]. Security and Reliability like road travel collision, traffic congestion, fuel consumption are overcome by destination making system which are created by physics, vehicle dynamic and historical data collected from GPS system [5].

Cooperative approach to get self management to enhanced the privacy and integrity, detecting the nodes and distributing the network operation [6].For the development of security and privacy the public key infrastructure protocol are used which defines the security requirements and detailed definitions the security requirements and detailed definition of the scheme for the security and privacy by using shared asymmetric keys [7].

In order to decrease the delay in geodynamic group based authentication the symmetric key based cryptography is introduced as group communication by creating groups and maintaining then geodynamic ally by group leader [8]. Effective vehicular communication can be done by message authentication scheme which enhance cooperation,privacy,and vehicular communication, a separate edited message authentication scheme name RAISE is introduce[10].

Computation overhead is another critical issues in VANETs.In the safety driving application, vehicles broadcast safety messages every 300ms [14].The authors propose a promising protocol which let vehicles have to verify message cooperatively by employing probabilistic verification . However ,in order to guarantee efficient cooperation, vehicles have to verify at least twenty –five message within 300ms which is still a heavy computation burden for the on-board unit (OBU)installed on a vehicle.

In this paper we proposed and develop Shared key management framework. In the framework the RSU may not be responsible because the key is shared among them self, when a vehicle approach another vehicle. It gets connected to the vehicle automatically without the help of RSU.But the message is send and receive from one vehicle to another vehicle needs the help of the RSU.The centralized server is not required, since the keys are shared group authentication is not necessary for transferring the information because the key them self will shared the information separate protocols is not needed to send and receive message out of the range because each vehicle can spread the message.

2. EXISTING SYSTEM

In the Distributed key management framework, since keys are distributed and the distributed keys are connected to the centralized server. Sending and Receiving messages ends up in delay in delivering the messages security related issues in hacking the packet data and the message authentication is distance biased.

This technology uses the below said techniques for this frame work

1. Centralized server (or) Centralized authenticator
2. Extra protocols for beyond the range
3. Group authentication

Centralized server:

Centralized server are centralized authenticator will be the roadside connected with the key distributor.

Extra protocols for beyond the range:

Extra protocols may be added for sending and receiving messages beyond the range

Group authentication:

Group authenticator is done for the connected keys with group leader.

3. PROPOSED METHOD

In our proposed method (Shared key management framework) key components can connect the RSU by group key distribution and cooperative message authentication for the safe communication.

Our framework mainly uses data encryption and also client authentication for which the centralized server may not be required. Since the keys are distributed each key can communicated among them by cooperative message authentication and does not required the group authentication.

By our proposed method there is no necessity for extra protocol for the authentication beyond the range why because every participating key is given priority message authentication.

4. PROPOSED ALGORITHM

The proposed frame work uses the algorithm for secure communication of messages, the algorithm are hash and RSA. The hash key technique is used because the framework does not need a specific range. Why because the key length is fixed and larger which is defined in the RSU. The nodes are ordinary vehicles on the road that can communicate with each other and RSU's though radio. In a highway scenario RSU are normally away from each other.

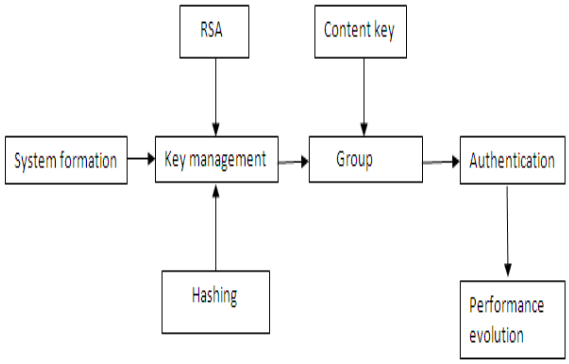

Fig 2.Block diagram of RSA and Hash algorithm

In Fig.2 clearly illustrates the flow of message authentication in our Shared key management framework. The management framework is the intermediate between the system information and the groups, system information gives the necessary information above the three aspects which are covered our management framework. The group is set of 7 RSU and 150 nodes. This technology of connection is done by RSA and hashing technology. Thus the authentication process is done by the flow as shown. In Fig.2 further the group is connected for the performance evolution.

5. SIMULATION

In this section, we use NS2 simulations to examine the performance of the proposed shared key frame work and cooperative authentication protocol. In our simulation the typical city road scenario with seven RSU to cover a cross lane is used. The physical and MAC layer parameters of the 802.11 broadcast protocol used in our are listed as shown in TABLE 1.

TABLE 1. List of parameters

Parameter	Value
Preamble length	16μs
PLCP header length	50 μs
Slot time σ	0.000009
SIFS	0.000016
MAC header size	28 bytes
Wireless channel rate	6Mbps

SIMULATION RESULT

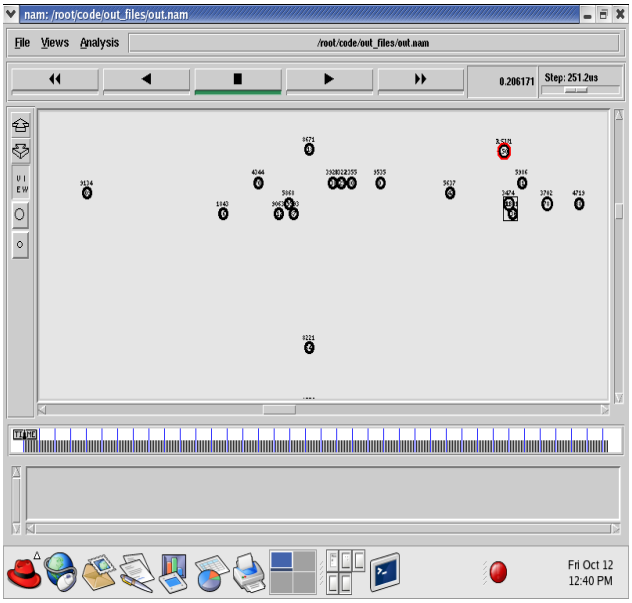

Fig.3 Independent vehicle creation

The Fig.3clearly explains about the creation of independent vehicle which are participating in the network. Nodes are ordinary vehicles on the road with communicate which each other with help of RSU. The Fig.4 explains that every RSU issues keys to the set of vehicles. If the vehicle is beyond the particular limit of the RSU, then vehicle can be connected to the nearby RSU. The authentication limit of the RSU IS 300m.if the node cross beyond the said limit then the nodes will be automatically connect to the faceable RSU.

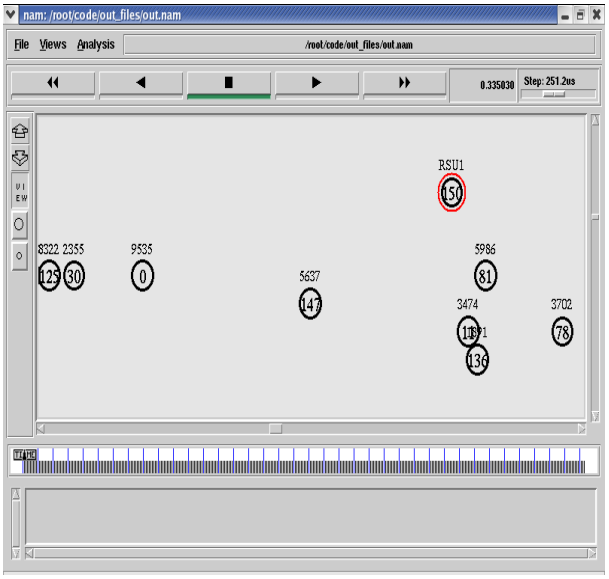

Fig 4.RSU creation with independent vehicles

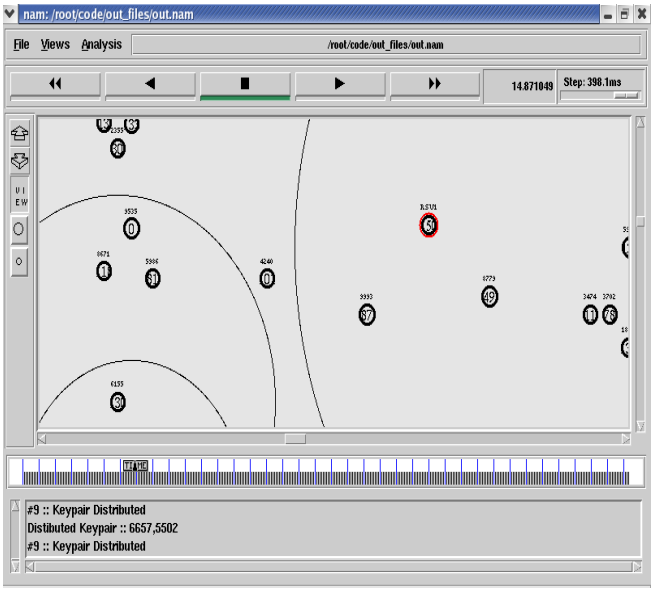

Fig 5.Key allocation

The Fig.5 shows how the keys are connected with the RSU, It is assume that the participating vehicle is equipped with GPS receiver. It is assume that the participating vehicle is equipped with GPS receiver

6. CONCLUSION

This paper has addressed, the Shared key management framework is based upon the cooperative message authentication, where the participating keys are given priority in this method which is not done in Distributed key management framework. Hence the keys are allowed to authenticate among themselves by using this Shared key management system, Thus the Shared key management frame work over comes the RSA and Hash key algorithm. When compared to the Distributed key management framework our proposed Shared key management framework techniques is effective by providing safety and security in VANET.

7. FUTURE ENHANCEMENT

The performance evolution of Shared key management framework in VANET with our proposed architecture by comparing it's like packet delivery rate, message overhead, computation overhead with no of vehicles on a day.

Further, we can compare our proposed method with the exiting method of Distributed key management framework. This will be considered as future work

8. REFERENCES

[1] Youg Hao ,Yu Cheng ,Chi Zhou and Wei Song, "A Distributed key management framework with cooperative message authentication in VANETs" *IEEE Journal on selected areas in communications*, vol.29, no.3, march 2011

[2] Bo Yu, Cheng-Zhong Xu,and Minyi Guo, "Adaptive forwarding delay control for VANET data aggregation"*IEEE Transaction* vol .23,no.1,january2012

[3] Irshad Ahmed Sumra, halabi hasbullah, Jamalul-Iail Ab Manan "VANET Security Research and Development Ecosystem "*International conference 2011*

[4] Vighnesh N V,N Kavita, Dr.Shalini R.Urs "A Novel Sender authentication Scheme Based On Hash chain For Vehicular Ad-hoc Networks " *IEEE Transaction 2011*

[5] Vineetha Paruchuri , "Inter-vehicular communications: Security and reliability issues" *International conference2011*

[6] J.Molina-Gil, C.Caballero-Gil, and p.Caballero-Gil "Cooperative Approach to Self-managed VANETS" *International conference2010*

[7] Ali Osman Bayrak, Tankut Acarman "S3P: A Secure and Privacy Protecting Protocol for VANET" *International conference2010*

[8] Marshall Riley, Kemal Akkaya and kenny Fong "Delay-efficient geodynamic group-based authentication in VANETs"*International conference2010*

[9] Cristina Gil,Leticia Gonzalez,Neftis Atallah,Juan Antonio Abanades,Nicolas Jean Leconte, " Self-Recusation Protocol for Blockage of Misbehaving Applications in Vehicular Networks" *International* conference2010

[10] Chenxi Zhange ,Xiaodong Lin,Rongxing Lu, "An efficient message Authentication scheme for vehicular communications" *IEEE Transaction on vehicular technology"*, vol.57, no.6, nov2008

[11] Y. Hao, Y. Cheng and K. Ren, "Distributed key management with protection against RSU compromise in group signature base VANETs," I*n Proc.IEEE Globecom*, New Orleans, Nov., 2008.

[12] S. Park and C.C.Zou, "Reliable traffic information propagation in vehicular ad-hoc networks," *IEEE Sarnoff Symposium*, Apr. 2008

[13] Sampigethava, L.Huang, M.Li, R.Poovendran, K.Matsuura and K.Sezaki,"AMOEBA: Robust location privacy scheme for VANET,"*in IEEE J. Sel. Areas Commun*., vol. 25,no. 8, pp.1569-1589, 2007.

[14] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007

[15] B. Xiao, B. Yu and C. Gao, "Detection and localization of sybil nodes in VANETs," in Proc. ACM/SIGMOBILE Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, 2006.