ISSN:0975-9646

Hybrid Message Authentication Protocol in VANET

R.Rajan[1], S.Narendran[2], M.Prasanth[3], R.Raj kumar [4]

[1]*Assistant Professor, Department of Information Technology,*
Sri Ramakrishna Engineering College, Coimbatore

[2,3,4]*UG Scholar, Department of Information Technology,*
Sri Ramakrishna Engineering College, Coimbatore

***Abstract* —–The group signature based security scheme is a promising approach to provision privacy in vehicular ad hoc networks (VANETs). In this paper, we propose an distributed key management scheme instead of centralized key management for group signature based VANETs, which is expected to considerably facilitate the revocation of malicious vehicles, location privacy protection, heterogenous security policies, and maintenance of the system, compared with the centralized key management assumed by the existing group signature schemes. In the proposed scheme the road side units (RSUs) will be responsible for distributing group private keys in a localized manner.**

Key words— road side units (RSUs), vehicular ad hoc network (VANET), Safety messages

I .INTRODUCTION

Wireless network consist of nodes which communicate with the help of radio waves. Each node has a communication range and the nodes can communicate with nodes that are within its communication range. Range in such networks is often limited restricting the use of networks to small offices and homes; however, it is possible to use nodes to forward packets for others thereby extending the communication range of individual nodes. Networks that employ packet forwarding are called Multi-Hop Ad-hoc Network.

Advantages of wireless networks over wired networks are as follows:

- Mobility
- Installation Speed
- Simplicity
- Reduced cost
- Scalability

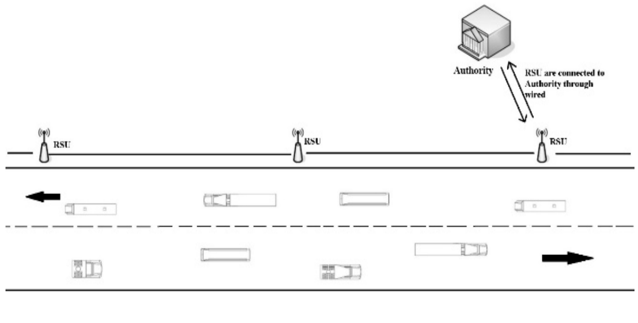

Fig 1.HMAP Architecture

Vehicular Ad hoc Network (VANET), intelligent vehicles can communicate among themselves (Vehicle-to Vehicle (V2V) communications) and with road-side infrastructure (Vehicle-to-Infrastructure (V2I) communications). The VANET enables useful functions, such as cooperative driving and probe vehicle data, that increase vehicular safety and reduce traffic congestion, and offer access to Location Based Service (LBS) applications. A VANET typically involves two modes of communications, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Privacy is a very important issue in the VANET. As the wireless communication channel is a shared medium, just exchanging messages without any security protection over the air can easily leak the information that the users may want to keep private. In this paper we use group signature for the privacy protection.

II .RELATED WORK

Each vehicle sends periodically broadcasted messages (PBM) which include its current geographic information every 300ms. When its neighboring vehicles receive the PBM, they will decide whether they are verifiers of this message distributed according to the verifiers selection protocol. If a vehicle is the verifier of the message, it will start to verify the message by itself. Non-verifiers will wait for cooperative warning messages (CWM) from verifiers. Once an invalid message is identified, verifiers will broadcast a one hop warning message to others. Otherwise, verifiers will keep silent. When a non-verifier receives the CWM from other vehicles, it will verify the message by itself to double check whether the message is really invalid. Non-verifiers will consume the message if it does not receive any CWM from others within 100ms. With a public key (PKA) or asymmetric key algorithm, a pair of keys is used. One of the keys, the private key, is kept secret and not shared with anyone. The other key, the public key, is not secret and can be shared with anyone. When data is encrypted by one of the keys, it can only be decrypted and recovered by using the other key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key. The RSA algorithm is an example of a public key algorithm.

A.Group Signature based VANET

Entities in VANET are classified into 3 categories. Network nodes are ordinary vehicles on the road that have ability to communicate with each other through radio. Network nodes have the lowest security level. Roadside infrastructure is the set of RSUs .RSUs are agents of the authority which are deployed at the roadsides, traffic lights or road signs can be used as RSUs after renovation. An RSU can be a powerful device or a comparatively simple one. Authorities are responsible for management in VANET. They hold all the secrets and have responsibilities to solve disputes. The authority has the highest security level. We assume it cannot be compromised. In the group signature scheme, member group sign messages under the name of the group. In a group, there are one group public key and many group private keys corresponding to the group public key. The message that is signed by any group private key can be verified by the unique group public key, and the signer's identifier will not be revealed. However, there is an authority who holds a tracing key which can be used to retrieve the group private key from the signature. If one group private key is assigned to only one user, we can identify the user after we get his group private key.

B. Distributed Key Management

In our scheme, the authority generates and holds tracing keys which can be used to recover the identity from the signature .It also chooses group private key generators and transmits them to corresponding RSUs which are in charge of the group private key distribution, vehicle starts a registration when it is approaching a RSU. The RSU sends a group private key to the vehicle after it gets vehicle's identity information and then stores vehicles' information locally, this can be used later for tracing the vehicles. The authority uses tracing keys to retrieve.A higher probability to find that two messages are transmitted by the same sender. Security policies can be implemented in our scheme. While, in the centralized scheme, the policy is difficult to be changed after it is deployed.

C. Security Model

In this paper, we assume that attackers are inside, rational, active and global. In side attackers are legitimate members of the VANET. In this paper, attacker scan be network nodes or roadside infrastructure .Rational attackers only attack for their own benefits. They know the security mechanism and they want to attack without being detected. If there is a mechanism that can detect them, they tend not to attack if the punishment is severe enough. Active attackers have the ability to send packets into wireless channels. Global attackers have an unlimited scope in the network which means they can hear any information in the network. We assume that the majority of vehicles and RSUs are honest and vehicles will report to the authority when they find that a vehicle is sending false messages. We also assume that wired network transmits data in secure without packets loss. Our protocol is used to judge whether a vehicle is a legitimate user. If accusers and accused are all legitimate users, we assume the authority has an evaluation system to judge the malicious. The evaluation system design is out of the scope of this paper.

CONCLUSION

In this paper, we propose a key management scheme based on the short group signature to provision privacy in the VANETs. The key management is further enhanced with a cooperative message authentication protocol to alleviate the heavy computation overhead. Moreover, by a cooperative message authentication protocol, a vehicle only needs to verify a small amount of messages, and the computation burden of vehicles is reduced greatly. We give detailed analysis of possible security attacks and the corresponding defense, as well as develop a MAC layer analytical model.

REFERENCES

[1] D. Chaum and E. van Heyst, "Group signatures ," in Proc. Advances in Cryptology-Eurocrypt, vol.547,pp.257-265,1991.

[2] J.Guo,J.-P. Baugh and S. Wang ,"A group signature based secure and privacy-preserving vehicular communication framework," in Proc.IEEEINFOCOM, Anchorage, Alaska, May,2007.

[3] K. Sampigethava, M. Li, L. Huang, R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET,"IEEEJ.Select.Areas Commun.,vol.25,no.8,pp.1569-1589,2007.

[4] X. Sun, "Anonymous, secure and efficient vehicular communications," Master Thesis, University of Waterloo, 2007.

[5] Y. Hao, Y. Cheng and K. Ren,"Distributed key management with protection against RSU compromise in group signature based VANETs," in Proc. IEEE Globe com, New Orleans, Nov.,2008.

.