ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Privacy in VANET using Shared Key Management

Jessy Paul[1], Elizabeth Saju[2], Mercy Joseph Poweth[3]

Professor, Dept. of Civil Engineering, MACE, Kothamangalam, Kerala, India

P.G Student, Dept. of Computer Science & Engineering, VJCET, Kerala, India

Professor, Dept. of Civil Engineering, MACE, Kothamangalam, Kerala, India

***Abstract*: Vehicular Ad-Hoc Networks (VANET) are very likely to be emerged in the coming years. The main objective of this paper is to provide privacy in VANET using shared distributed key management. In shared key management, a short group signature scheme is used to facilitate the revocation of malicious vehicles and heterogeneous security policies. In this framework, road side unit (RSU) acts as the key distributor. A new problem encountered is that a RSU may misbehave. A secure key distribution protocol is used to detect such misbehaved RSUs. The protocol guarantees the traceability of compromised RSUs and malicious vehicles. Moreover, the issue of large computation overhead is also addressed in this paper. A group authentication protocol is proposed to mitigate the communication and computation overhead that occur while using the group signature scheme. Here only a small number of vehicles participate in verification process.**

Keywords*:* VANET, privacy, shared key management, Road side units, ad-hoc networks

I INTRODUCTION

VANET is a form of ad-hoc network that enables communications between nearby vehicles (V2V communications) and the road-side infrastructure (V2I communications).In other words , VANET is a special kind of mobile ad-hoc networks where wireless equipped vehicles form a network. VANET research came into existence with the Fleet-Net project in mid 2001. The main aim of that was to develop a communication platform for inter-vehicle communication.

Privacy is an important issue in VANETS [2]. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. In this paper a shared distributed key management based on group signature scheme is proposed for ensuring privacy by revoking malicious vehicles. Computation overhead [13] is another issue in VANET. In this paper, a more efficient and practical message authentication protocol with an assumption that each safety message carries the location information of the sender vehicle which can be generated by a global positioning system (GPS) device). Verifiers of each message are defined according to their locations in relation to the sender. Only the selected verifiers check the validity of the message while other vehicles rely on verification results from these verifiers.

II BACKGROUND KNOWLEDGE

A VANET is a form of MANET which provides communication between vehicles and between vehicles and road-side base stations. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network. VANET is mainly designed to provide safety related information, traffic management, and infotainment services.

Privacy and security are the two important issues in VANET. Without security, a Vehicular Ad Hoc Network (VANET) system is wide open to a number of attacks such as propagation of false warning messages as well as suppression of actual warning messages, thereby causing accidents. Another form of attack in VANET is tracking. This makes security and privacy a factor of major concern in building such networks.

There have been several proposals for privacy preservation of VANETs. Some of them are using pseudonyms, silent period [4], mix-zones [3] etc. Each vehicle in a mix zone will keep silent in transmission, and randomly update its pseudonyms when it travels out of the mix zone and becomes reactivated. Given a reasonable large mix zone, the location privacy can be well protected due to the untraceability of location and pseudonym updating in the silent period. In the AMOEBA [5], vehicles form groups. The messages of all group members are forwarded by the group leader, which implies that the privacy of group members is protected by sacrificing the privacy of group leader. Moreover, if a malicious vehicle is selected as a group leader, all group members' privacy may be leaked by the malicious leader. While the pure pseudonym schemes do not support the secure functionality of authentication, integrity, and nonrepudiation, an anonymous signing protocol [1] is proposed to provide such functions as well as privacy. In the protocol, each vehicle preloads a large number of certificated anonymous public/private key pairs. A key pair will be used for a short period of time and then be discarded. Each key pair is assigned to only one user, and authorities maintain the key distribution records which can be used to trace possible malicious vehicles. The shortcoming of this protocol is that it requires vehicles to store a large number of pseudonyms and certifications, where a revocation scheme for abrogating malicious vehicles is difficult to implement.

The group signature [6] is a promising security scheme to provide privacy in VANETs. In the group signature, one group public key is associated with multiple group private keys. Under the group signature scheme, although an eavesdropper can know that a message is sent by the group, it cannot identify the sender of the message. A general vehicular communication framework based on group signature is given in [6]. Lin *et. al.* systematically discuss how to implement group signature protocol in VANETs [7]. The work in [9] combines pseudonym schemes with the group signature to avoid storing pseudonyms and certifications in vehicles. While all these studies assume a centralized key management scheme, a distributed key management framework is developed in this paper to achieve privacy based on group signature.

III THE PROPOSED APPROACH

A. System model

The system model as in Fig. 1 contains entities which are divided into three categories: authorities, RSU and nodes.

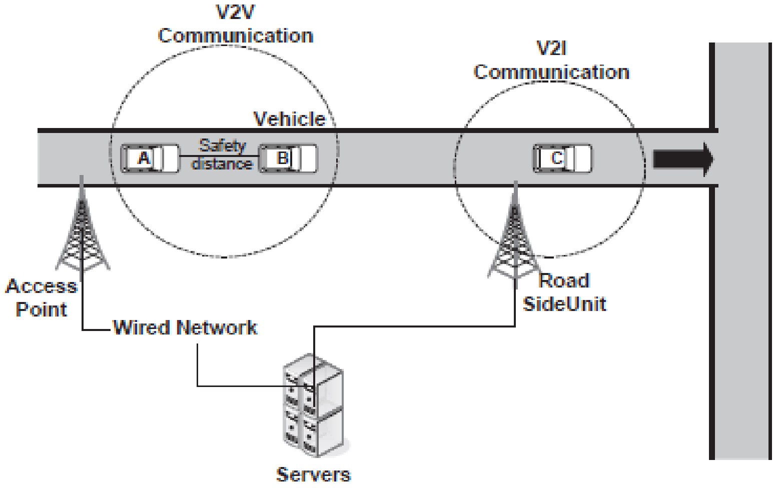

Fig. 1: System model

Authorities are responsible for key generation and malicious vehicle judgment. Authorities have powerful firewalls and other security protections. Therefore, they have the highest security level. We assume that they cannot be compromised.

Road side infrastructure consists of RSUs deployed at the road sides which are in charge of key management in our framework. Traffic lights or road signs can be used as RSUs after renovation. RSUs communicate with authorities through wired network. We assume a trusted platform module is equipped in each RSU. It can resist software attacks but not sophisticated hardware tampering. The cost of a trusted platform module is only a few tens of dollars which is affordable [1]. RSUs are semi-trust with the medium security level [5].

Node**s** are ordinary vehicles on the road that can communicate with each other and RSUs through radio. We assume that each vehicle is equipped with a GPS receiver using DGPS [9] with accuracy on the order of centimeters and an on board unit (OBU) which is in charge of all communication and computation tasks. Nodes have the lowest security level.

B. Shared distributed key management

The shared distributed key management uses group signature scheme and also a shared key approach is used. The steps involved in this are:

1) Registration: The procedure of registration is shown in Fig. 2. In Table I, we list physical meanings of symbols. Firstly**,** RSUs broadcast I-public keys, remaining portion of the G-public keys of themselves and their neighbor RSUs with certificates and identities of revoked RSUs in their neighborhoods regularly to the registered vehicles. One portion of current G-public key will be issued by the Previous RSU the vehicle had visited.

When a vehicle detects the hello message, it starts registration by sending its I-public key and the certificate to the RSU if the RSU is not revoked. Normally, a public key should not be encrypted. However, in this system model, each vehicle's I-public key is unique, so it is also an identifier of the vehicle. We encrypt it to protect vehicle's privacy. The RSU sends the hash value of the G-private key which plans to be assigned to the vehicle and the signature of the hash value, vehicle's I-public key and RSU's I-public key to the vehicle. RSU's I-public key is also unique. The vehicle can identify the RSU's legitimacy after it verifies this message because the RSU uses its I-private key in the message.

The vehicle encrypts its *Npri* and the timestamp by using authorities' public key. Then, it sends the encryption data with the timestamp and the signature of corresponding information, shown in Fig. 2 message 4, to the RSU.The RSU sends the G-private key and portion of G- public keys of the next RSU to the vehicle. The vehicle finishes registration procedure after it gets a valid G-private key. If authorities need the information of a vehicle when there is a dispute, the RSU has to send the vehicle's corresponding information to authorities. The group keys produced at RSU are shared among the vehicles in the group. Few keys are generated and they are given to vehicles as unique pairs of keys. This reduces the overhead in generating key. A portion of current group public key will be obtained from the neighbor or previous RSU the vehicle has visited. This avoids RSU compromise to an extent.

Table I: Physical Meanings of Symbols

Notations	**Descriptions**
R_{pub}/ R_{pri}	RSU's public/private key pair(I-key of RSU)
N_{pub}/N_{pri}	Vehicles public/private key pair
$Sig_A(M)$	Signature of message M signed by A's private key
$(M)_k$	Message M is encrypted by k's public key
G_{pubk}/G_{prik}	Group public/private key pair for user k
T	Timestamp
h(.)	A one-way hash function

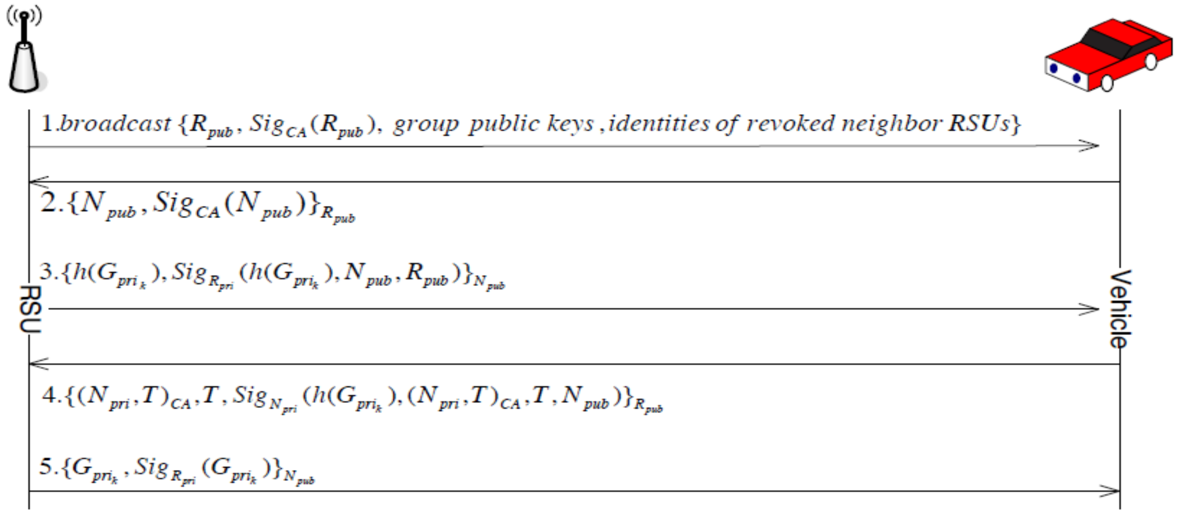
$1.broadcast\ \{R_{pub}, Sig_{CA}(R_{pub}),\ group\ public\ keys\ ,identities\ of\ revoked\ neighbor\ RSUs\}$
$2.\{N_{pub}, Sig_{CA}(N_{pub})\}_{R_{pub}}$
$3.\{h(G_{pri_k}), Sig_{R_{pri}}(h(G_{pri_k}), N_{pub}, R_{pub})\}_{N_{pub}}$
RSU
Vehicle
$4.\{(N_{pri}, T)_{CA}, T, Sig_{N_{pri}}(h(G_{pri_k}), (N_{pri}, T)_{CA}, T, N_{pub})\}_{R_{pub}}$
$5.\{G_{pri_k}, Sig_{R_{pri}}(G_{pri_k})\}_{N_{pub}}$

Fig. 2: Registration message flow

2) Message Broadcasting: Vehicles can broadcast messages under the name of the group after they get G-private keys from the RSU.

3) Accusation: When a vehicle finds that other vehicles send false messages, it will report to authorities. For example, a vehicle may maliciously detour traffic by claiming a traffic jam at a certain place but there is not in fact. Other vehicles at that place will report such claim as a false message. After receiving an accusation, authorities verify the signature in the accusation message by using *Gpub*. Then, authorities perform key retrieve operations to get the accuser's and the accused's G-private keys. Whereafter, authorities contact RSUs which assign G-private keys to the accuser and the accused according to group IDs. RSUs will send corresponding information back to authorities after they receive the requests from authorities. After that, authorities will calculate accuser's and accused's h (*Npri*, T) by using vehicles' I-private keys and timestamps which are obtained from the accusation message and the broadcast message respectively.

If the value that authorities calculate is the same with the value they get from the report, the user will be considered as legitimate. If both of them are authorized users, authorities will start the evaluation mechanism to decide which user tells the truth.

C. Message authentication

A message authentication protocol is used, which augments the basic short group signature protocol by mitigating the computation overhead in the regular broadcast phase. In a typical public safety application, each vehicle broadcasts safety messages every 300 ms, which implies that each vehicle can at most process messages from 27 (300/11) other vehicles in a stable system. However, according to the measurement there may exist as many as 87 vehicles broadcasting messages within the 300m communication range of a receiving vehicle, far exceeding its processing capability. Therefore, it uses a message authentication protocol to fill the gap between the workload and the processing capability.

1) Workflow: The workflow for message authentication is given in Fig. 3. Each vehicle maintains two processes which are verifier's selection process and an authentication process, a neighborhood list, a process queue and a buffer. The verifiers selection process is in charge of selecting verifiers, neighborhood list and process queue maintenance. The gap authentication process controls message authentication and warning message sending. In other words, verifier's selection process fills the process queue while authentication process clears it up after verifications. The neighborhood list contains neighbor vehicles' geographic information. Messages which will not be processed are stored in the buffer. When a vehicle receives a regular broadcast message (RBM), it extracts information of the location, speed, direction and acceleration of the sending vehicle and decides whether to verify the message or not according to geographic information. If a verifier finds an invalid RBM, it will broadcast one-hop warning information, which is termed as group authentication messages (GAM), to inform others. A non-verifier resorts to the GAM broadcasted by other vehicles to authenticate RBM.

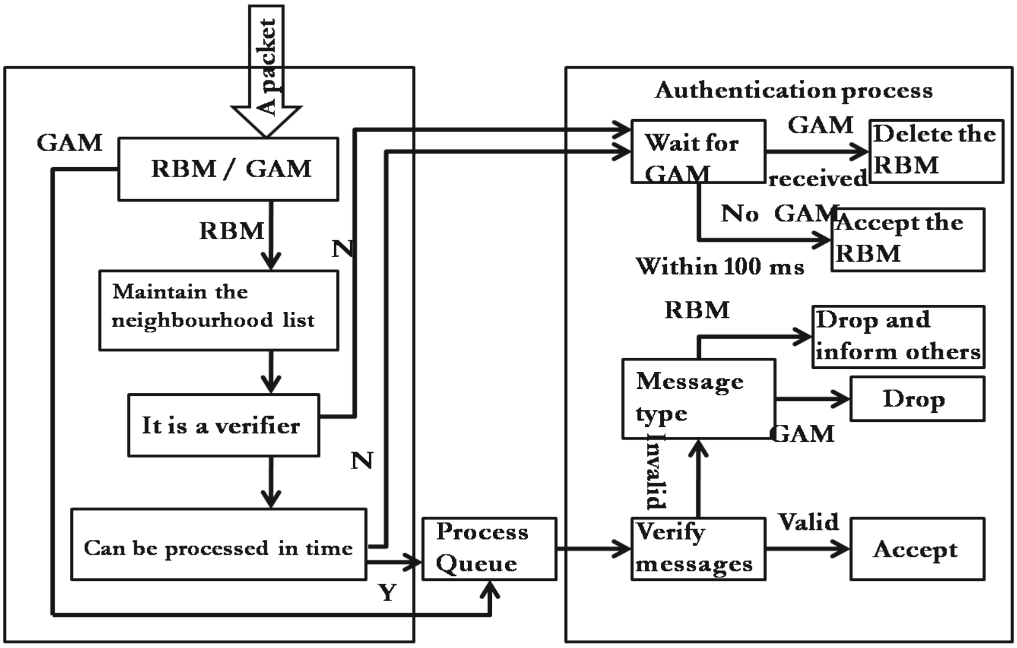

Fig.3: Workflow of message authentication protocol

2) Verifiers Selection Process: The verifier's selection process starts when the tagged vehicle receives a message. If an RBM is received, the tagged vehicle updates the neighborhood list and calculates the receiver sender distance (RSD) between itself and the sender at the sending time. After that, it tries to decide whether it is the verifier of the message by comparing its RSD with RSD of its neighbors. Verifiers are decided in a distributed manner by vehicles themselves according to their locations regarding to the sender. If the tagged vehicle is the verifier, it will insert the RBM to the process queue on the condition that it can be processed within the verification period, such as 100ms1. If the tagged vehicle is not the verifier or the verifier cannot process the message in time, the received message will be put into the buffer. When a GAM is received and the corresponding RBM is found in the buffer, then delete it from the buffer. Then the tagged vehicle will insert the GAM to the process queue. A GAM without the corresponding RBM in the buffer will be dropped.

2) Authentication Process: The cooperative authentication process verifies messages in the processing queue one by one. As shown in Fig. 3, if the message is valid, it will be accepted. If a GAM is invalid, it will be dropped. An invalid RBM will be informed to others by the tagged vehicle. Missed detection means invalid RBM are considered as valid by receivers which are caused by packet loss due to limited computation capacity of verifiers or the collisions in wireless channel. Our protocol improves the performance by reducing the computation overhead of OBUs and the number of GAM that a vehicle needs to send.

IV SIMULATION RESULTS

In this section, NS2 simulations are used to examine the performance of the proposed shared key distribution framework and group authentication protocol. The packet delivery ratio is defined as the proportion of transmissions that can be successfully received. The PDR is a critical performance measure affecting both the network utilization and security performance. A low PDR (or a high packet loss ratio due to collision) means a low bandwidth utilization, and the loss of GAM tends to result in missed detection. A probabilistic verification protocol is used, in which a vehicle receiving an RBM decides to be a verifier with a probability. However, in order to guarantee that there are verifiers selected at both sides of the sender, on average 25 verifiers should be randomly incurred for each RBM according to the protocol.

Fig. 4 compares the CMAP with the probabilistic verification protocol in terms of missed detection ratio. We can see that with the same number verifiers $V = 8$, the performance of probabilistic verification protocol deteriorates significantly, because $V = 8$ cannot ensure with high probability that verifiers exist on both sides of a sender. The good performance of CMAP is because the pattern of selecting verifiers is fixed according to position information.

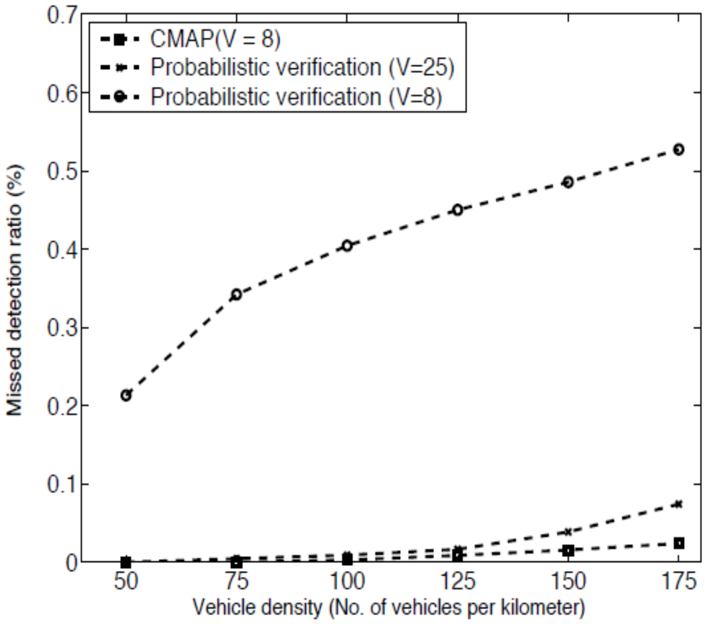

Fig. 4: Missed Detection Ratio vs Density of Vehicles

V CONCLUSION

In this paper, a novel distributed key management scheme is proposed to provision privacy in the VANETs. The distributed key management is further enhanced with a message authentication protocol to alleviate the heavy computation overhead. A security protocol to prevent compromised RSUs and malicious vehicles from attacking. This design guarantees that RSUs distribute keys fairly and provide some mechanisms to detect compromised RSUs and malicious vehicles. Moreover, by a message authentication protocol, a vehicle only needs to verify a small amount of messages, and the computation burden of vehicles is reduced greatly.

REFERENCES

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

[2] R. Lu, X. Lin and X. Shen, "SPRING: A social-based privacy- preserving packet forwarding protocol for vehicular delay tolerant networks", in Proc. IEEE INFOCOM, San Diego, California, 2010.

[3] J. Freudiger, M. Raya, M. Feleghhazi,P. Papadimitratos and J.- P.Hubaux., "Mix zones for location privacy in vehicular networks," in Proc. International Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia, Aug., 2007.

[4] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in Proc. IEEE WCNC, pp. 1187-1192, 2005.

[5] K.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.

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

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

[8] G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in Proc. ACM Mobicom, pp. 19-28, QC, Canada, Sept. 2007.

[9] P. Enge, "Retooling the global positioning system," Scientific American, May 2004.

[10] N. Banerjee, M.D. Corner, D. Towsley and B.N. Levine, "Relays, base station and meshes: enhancing mobile networks with infrastructure," in Proc. ACM Mobicom, San francisco, California, Sep. 2008.

[11] Sun, "Anonymous, secure and efficient vehicular communications," Master Thesis, Univeristy of Waterloo, 2007.

[12] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357-3368, 2008.

[13] C. Zhang, X. Lin, R. Lu and P.-H. Ho., "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE ICC, Beijing, China, May 19-23, 2008.

BIOGRAPHY

Elizabeth Saju received the B.Tech degree in Computer Science and Engineering from Adi Shankara Institute of Engineering and Technology,Kalady, Mahatma Gandhi University, in 2009. She is currently doing his MTech program at Viswajyothi College of Engineering and Technology, Vazhakulam.