Privacy Preserving Authentication Scheme for VANET's Using HMAC Algorithm

K.Manimekalai[1] Dr.B.Gopalakrishnan[2]
[1,2]Department of Information Technology
[1,2]Bannari Amman Institute of Technology, Sathyamangalam

Abstract— An efficient privacy-preserving authentication theme supported cluster signature for conveyance surprising networks (VANETs). although cluster signature is wide used in VANETs to understand cluster signatures suffer from long computation delay at intervals the certificate revocation list (CRL) checking and at intervals the signature verification technique is leading to high message. throughout that edge units (RSUs) square measure chargeable for distributing cluster personal keys and managing vehicles throughout a localized manner. A hash message authentication code (HMAC) to avoid time overwhelming CRL checking and to substantiate the integrity of messages before batch cluster authentication. it'll cooperative message authentication among entities and each vehicle entirely should verify a little low form of messages greatly assuaging the authentication burden. The projected work is high security, needed vehicles communication and performance analysis is further economical in terms of authentication speed, keeping conditional privacy in VANETs.

Key words: RSUs, HMAC, VANETs

I. Introduction

Vehicular ad hoc networks (VANETs) is massive development of wireless communications and it have attracted extensive attention and research efforts from academia, industry, and governments in recent years. In a general setting, Vehicular ad hoc networks are also known under a number of different terms such as inter vehicle communication (IVC), Dedicated Short Range Communication (DSRC). Create new network algorithms or modify the existing for use in a vehicular environment. In the future vehicular ad hoc network will assists the drivers of vehicles and help to create safer roads by reducing the number of automobile accidents. A VANET is composed of three components, onboard units (OBUs) equipped in mobile vehicles, fixed roadside units (RSUs), and a central trust authority (TA). Being aware of the traffic condition, VANETs are expected to improve the driving experience, traffic safety, and multimedia infotainment dissemination for drivers and passengers. In VANETs vehicles communicate with each other as well as with RSUs through an open wireless channel in which attackers can easily get users private information, such as identity, tracing, preference, etc., if they are not properly protected.

Another characteristic of VANETs is high-speed mobility, leading to limited communication time among RSUs and vehicles. As a result an efficient authentication scheme with privacy preservation for VANETs. In VANETs, group signature is widely used for vehicles to achieve anonymous authentication since it allows any group member to sign a message on behalf of the group without revealing its real identity. When receiving a message from an unknown entity, a vehicle has to check the certificate revocation list (CRL) to avoid communicating with revoked vehicles and then verify the sender's group signature to check the validity of the received message. The security and performance analysis show that the proposed scheme can achieve more efficient group signature based authentication while keeping conditional privacy for VANETs.

II. Algorithm

A. Hash Message Authentication Code (HMAC)

HMAC instead of pairing operation to verify a message. Because the operation time of HMAC is much shorter than that of pairing, it is very efficient. We assume that two parties A and B have a shared secret key t, and ENCt(M) and HMACt(M) are the symmetric encryption and HMAC values of the message M using the key t respectively. If A wants to send a message M to B, it first computes ENCt(M) and HMACt(M), and sends them to B, B decrypts ENCt(M) to get the message M, and then computes the HMAC value of the message M. If the computed HMAC value is the same as the received one, B accepts the message. In the above method we mainly use a symmetric en-cryption and a HMAC computation under a shared secret key to protect the message. The operation of the symmetric encryption can protect the privacy of the message, which makes the message not leaked, and only the person that knows the shared secret key can get the message.

B. Bilinear Group

The bilinear map can be constructed on elliptic curves. Each operation for computing a pairing operation. Pairing operation is the most expensive operation in this kind of cryptographic schemes. The fewer the number of pairing operations, the more efficient the scheme, So we replace it by HMAC technique. The groups G and GT are called bilinear groups. The security of it relies on the fact that the discrete logarithm problem (DLP) on bilinear groups is computationally hard, The implication is that we can transfer Q in an open wireless channel without worrying that a (usually some secret) can be known by the attackers.

C. Binary Search Algorithm

The binary search algorithm works only on sorted lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted (with respect to the certificate's identity) database of the revoked certificates included in previous CRLs and the recently received CRL. The main idea of the binary search algorithm is to cancel out half of the entries under consideration after each comparison in the search process. In the binary search, the revocation status of a certificate is checked by comparing the identity of the certificate with middle value (which in this case will be the median value) of the sorted database. If the identity of the certificate is greater than the median value, the right half of the database will be considered in the next comparison process and vice versa. This process continues until a match is found, i.e., the certificate is revoked, or the process is finished without finding a match which means that the certificate is unrevoked.

III. Performance Analysis

VALUE	PARAMETER
Simulation area	1000m*1000m
Simulation time	30s
Speed of vehicle	10-30m/s
Wireless protocol	802.11p
Agent	PCB
Network generation tool	ns2
Channel bandwidth	6Mbs
Radio propagation model	TwoRayGround

Table.1: Simulation Parameters

A. *Average communication delay*

The total transmission delay slowly increases with the number of vehicles in the communication range. When using HMAC scheme, the average transmission delay is reduced. It is the group key materials to vehicles, which makes the message size is larger than that in the other scheme. However, the size of additional messages is very small therefore, the communication delays of both schemes are very close. The detail analysis of computation overhead since both schemes have almost the same computation overhead.

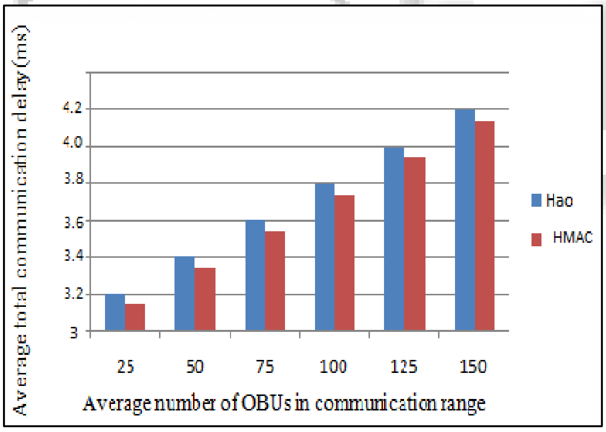

Fig. 1: Average communication delay

B. *End-to-End Delay*

The different number of vehicles in the communication range, where the speed of vehicles is from 10 to 30 m/s. The average of other scheme is about 17.6 ms, which increases very slowly with the number of OBUs in the communication range. It is the largest among that of other scheme. Since, the other schemes employ the batch group signature algorithm, the average verification delay for each message decreases. Moreover, in the last three schemes, keep a small fluctuation. It is because the average number of OBUs in the communication range increases, and the transmission delay is increasing, whereas the average verification delay is decreasing. The HMAC scheme is larger than other's scheme since cooperative authentication makes the number of messages in the batch verification to be reduced. With the increase in OBUs' number, the performance of HMAC scheme is better. However, in the aforementioned comparison, It do not consider the time constraint. To further show HMAC scheme's performance, the average message loss ratio as another measurement in HMAC evaluation. The average message loss ratio is defined as the ratio of the number of messages dropped to the total number of messages received.

C. *Verification Delay*

The verification delay and the signature size of the proposed scheme, the short group signature(SGS) scheme, and the batch group signatures verification(GSV) scheme proposed in [6].The cryptograph delay due to only the pairing and multiplication operations on elliptic curves, and the exponentiation operations are the most time consuming operations. It should be noted that if the message signatures are verified individually as indicated in HMAC Algorithm, the verification delay will be identical to that of the SGS scheme .presents the verification delay in msecvs. the number of the received messages. It can be seen that the BGS scheme provides the lowest verification delay among the protocols under comparison.

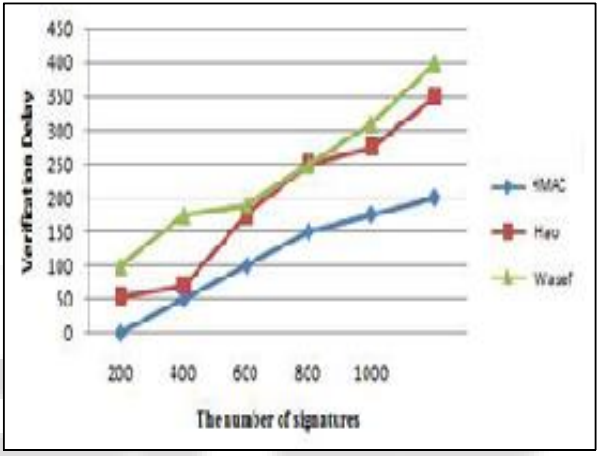

Fig. 2: Verification delay

D. *Message Loss Ratio*

The average message loss ratio, which is defined as ratio between the number of messages dropped due to signature verification delay and the total number of messages received .According to DSRC, each OBU has to disseminate information about the road condition. In order to react properly and instantly to the varying road conditions, each OBU should verify the messages received before disseminating a new message about the road condition. It can be seen that the simulated average message loss ratio closely follows the analytical message loss ratio. Also, the proposed HMAC scheme provides the lowest message loss ratio, and the message loss ratio increases as the number of OBUs within communication range increases. The reason of the superiority of the HMAC scheme is that it can aggregately verify a large number of signatures than that of its counterparts.

IV. System Architecture

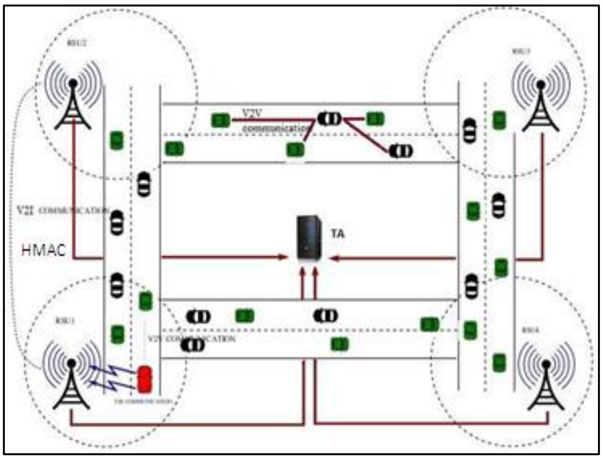

Fig. 3: System Architecture

The interested in the computation complexity of the revocation status checking process which is defined as the number of comparison operations required to check the revocation status of an OBU. Let Nrev denote the total number of revoked certificates in a CRL. To check the revocation status of an OBU using the linear search algorithm, an entity has to compare the certificate identity of OBU with every certificate of the Nrev certificates in the CRL the entity performs one-to-one checking process. The computation complexities of employing the linear search algorithm to perform a revocation status checking in the middle half of the CRL with identities lower than that of OBU are discarded from the upcoming comparisons. If the certificate identity of OBU is lower than that of the entry in the middle, then half of the CRL with identities higher than that of OBU are discarded. The checking process is repeated until a match is found or the CRL is finished. It can be seen that at each step in the binary search method half of the entries considered in the search is discarded. The computation complexity of the binary search algorithm to perform a revocation status checking.

V. Security Requirement

A. Trusted Authority

Hash message authentication code to avoid time consuming CRL checking and to ensure the integrity of messages before batch group authentication. The adopt cooperative message authentication among entities vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. The security and performance analysis show that efficient in terms of authentication speed conditional privacy in VANETs.

B. Forward Secrecy

Since the values of the hash chain included in the revocation messages are released to non-revoked OBUs starting from the last value of the hash chain. A hash function is irreversible; a revoked OBU cannot use a hash chain value received in a previous revocation process to get the current hash chain value.

C. Message Authentication

A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA. OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2V communications

D. Resistance to Colluding Attacks

A legitimate OBU colludes with a revoked OBU by releasing the current secret key such that the revoked vehicle can use this key to pass the revocation check process by calculating the correct HMAC values for the transmitted messages. All the security materials of an OBU are stored in its tamper-resistant

VI. Conclusion

An economical privacy-preserving cluster signature based authentication theme for VANETs .In this techniques of distributed management, HMAC, batch cluster signature verification and cooperative authentication to appreciate the design goal. First, divide the complete network into several domains, that allows localized management. HMAC is utilized to exchange the long CRL checking and to substantiate the integrity of messages before batch verification, reducing the quantity of invalid messages among the batch.The time required to perform a degree multiplication on associate degree elliptic curve. The verification of a certificate and message. It use cooperative authentication to a lot of improve the efficiency by exploitation the given ways that. it'll meet the necessity of substantiating messages per second. the security and performance analysis show that economical group signature based authentication whereas keeping conditional privacy for VANETs.

References

[1] XiaoyenZhu, ShunrongJiang, LiangminWang and Hui Li "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks" IEEE Transaction On Vehicular Technology,VOL. 63, NO. 2, FEBRUARY 2014.

[2] A.Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 78–89. Jan. 2013.

[3] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[4] Y. Hao, Y. Chen, C. Zhou, and S. Wei, "A distributed key management framework with cooperative message .vol. 29, no. 3, pp. 6, 16–629, Mar. 2011.

[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,"IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589–3603,Sep. 2010.

[6] A.Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in Proc. IEEE ICC, Cap Town, South Africa, May 2010, pp. 1–5.