IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Secured Expedite Message Authentication Protocol for Vehicular Adhoc Network

Mrs.M.Rajalakshmi[1], R.Kasthuri[2], J. Nivesha[3], J.Varalakshmi[4]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Adhiparasakthi Engineering College, Melmaruvathur, Tamil Nadu, India

[2, 3, 4]Department of Electronics and Communication Engineering, Adhiparasakthi Engineering College, Melmaruvathur, Tamil Nadu, India

Abstract

Vehicular networks have been envisioned to play an important role in the future wireless communication service market for safety communications. Vehicular ad hoc network (VANET) enable vehicles to communicate among themselves (V2V communications)and with road- side infrastructure for vehicle safety, congestion reduction in traffic and location based service (LBS).The requirements of maintaining proper communication of vehicles involved in accidents and ensuring the safety provided by the communication between vehicles, challenge the network performance, privacy and certain security methods in VANET.
We propose a protocol called EMAP for VANET that uses a fast HMAC function which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process that use Secure Hash Algorithm-256(SHA-256) and novel key sharing scheme employing probabilistic random key distribution which allows an OBU to update its compromised keys even if it is previously missed some revocation messages.

Keywords: *revocation of certificate, vehicular network, public key infrastructure.*

1.Introduction

With sharp increase of vehicles on roads, driving has not stopped from being more challenging and dangerous. There is a large body of research work related to the security and privacy in VANETs the most related are on the design of privacy-preserving schemes. The privacy

issue by proposing a pseudonym based approach using anonymous public keys and Public Keys Infrastructure(PKI),where the public key certificate is needed giving rise to extra communication and storage overhead. The vehicles communicate through wireless channels: variety of attacks such as wrong information, modifying and replaying the messages can be easily launched. Safety information exchanged enables life critical applications such as altering functionality during intersection traversing and lane merging and thus plays a key role in VANET applications.

A security attack on VANETs can have severe or fatal consequences to large number of users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. VANET turns every participating car into a wireless router or node, allowing cars approximately 100-300 meters of each other to connect and in turn, create a network with wide range as cars call out of the signal range and drop out of the network, such that cars can join with vehicles to connect one another so that a mobile internet is created. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI) and to use Certificate Revocation Lists (CRLs) for managing the revoked certificate. In PKI, each entity in the network holds an authentic certificate and every message should be digitally signed before its transmission. A CRL is issued by a Trusted Authority (TA) which contains all the revoked certificates. The TA distributes the CRL to the infrastructure points which then takeover the TA's responsibilities to execute the revocation process. The advantage of this approach is that vehicles never need to download the entire CRL. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL. the first part of authentication ,which checks the revocation status of the sender in a CRL may incur long delay depending on CRL size and the employed mechanism for searching the CRL. Unfortunately, the CRL size in VANETs is expected to be large for the following

reason:1)to preserve the privacy of drivers i.e., to decline leakage of real identities and location information of drivers from any attackers, each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to frequently change its anonymous certificate to mislead attackers.2) the scale of VANETS is very large. According to the Dedicated Short Range Communication (DSRC) where, each OBU has to broadcast a message about its location, velocity and other information. In such scenario, each OBU may receive a large number of messages, and it has to check the current CRL for all the received certificates, which may take long authentication delay depending on the CRL size and the number of certificates received. The ability to check CRL for many number of certificates quickly leads an inevitable challenge to VANETs.

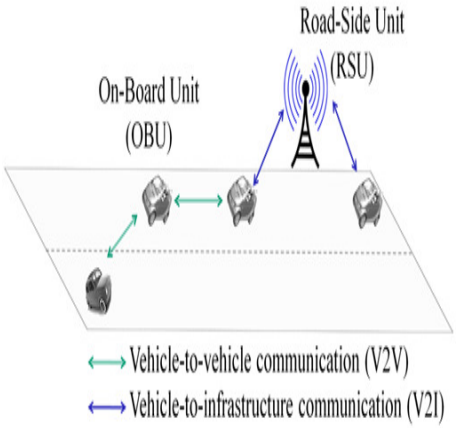


Fig. a SYSTEM MODEL

2. Emap

The proposed EMAP uses a fast HMAC function for authentication and novel key sharing scheme employing probabilistic random key distribution.

2.1 System model

The system model has the following:

- A Trusted Authority, is an entity the issues digital certificates and distributes secret keys to all OBUs in the network.
- Road Side Units(RSUs),are fixed units distributed over the networks that provides secure storage, processing and time information.
- On Board Units (OBUs), are lodged in vehicles. They can communicate either through V2V communications or V2I communications.

As per the WAVE standard, every OBU is inbuilt with a Hardware Security Module (HSM), which is a physical computing device that posses controls providing tamper evidence such as logging, alerting and tamper resistance like deleting keys upon tamper detection. It is used to store the security materials, e.g., certificates, secret keys, etc., of the OBU. HSM safeguards and manages digital keys for strong authentication and provides crypto processing. We consider that legitimate OBUs cannot collude with the revoked OBUs as it becomes difficult for authorized OBUs to extract their security materials from their HSMs. finally, we consider that a compromised OBU is instantly detected by the TA.

2.2 Initialization of System

The TA initialize the system by executing algorithm1. In step (20), it should be noted that: PK^i_u denotes i^{th} public key for OBU_u, where the corresponding secret key is SK^i_u:PIDi denotes the i^{th} pseudo identity(PID) for OBU_u, where the TA is the only entity that can relate PIDiu to the real identity of OBU_u:$sigTA(PID^i_u||PK^i_u)$denotes the TA signature on the concatenation(||) of PID^i_u and PK^i_u;and C is the number of certificates loaded in each OBU.

1: Select two generators P;Q €G1 of order q,
2: for i 1; l do
3: Select a random number ki € Z*q
4: Set the secret key K-i =kiQ € G1
5: Set the corresponding public key K=1/kiP €G1
6: end for
7: Select an initial secret key Kg €G2 ->to be shared between all the non-revoked OBUs
8: Select a master secret key s €Z_q
9: Set the corresponding public key P0=sP
10: Choose hash functions H :{0,1}* → G1 and h{ 0,1}*→Z*q
11: Select a secret value v € Z*q and set v0 =v
12: for i← 1; j do ->to obtain a set V of hash chain values
13: Set $v_i = h(v_i\text{-}1)$
14: end for
15: for all OBUu in the network, TA do
16: for i ←1;m do
17: Select a random number a €[1; l]
18:Upload the secret key K^-_a=kaQ and the corresponding public key K^+_a =1/kaP in HSM_u which is the HSM embedded in OBU_u
19: end for

20: Generate a set of anonymous certificates $CERT_u$={certiu(PID^i_u PK^i_u; $sigTA(PID^i_u||PK^i_u)$)|1≤ i≤Cg ->for privacy authentication

21: Upload $CERT_u$ in HSM_u of OBU_u

22: end for

23: Announce H, h, P, Q, and P_0 to all the OBUs

After the system is initialized, the TA has the following:

•A secret key pool U_s = {K^-_i= k_iQ|1 ≤ i ≤ l}.

•The corresponding public key set Up ={k^+_i=1/kiP|1≤ i ≤ l}.

•A master secret keys and corresponding public key P_0.

•The secret key K_g.

•A set of hash chain values V = {v_i|0 ≤ i ≤ j}, where j is large enough to accommodate with the number of revocation processes occur during the life-time of the network.

- The public parameters H, h, P, and Q. Also, each OBU will have the following:
- A set of anonymous certificates ($CERT_u$) used to achieve privacy-preserving authentication.

A set of secret keys RS_u consisting of m keys randomly selected from Us, i.e., RS_u . The set of the public keys RP_u corresponding to the keys in RS_u, i.e., RP_u. The secret key K_g, which is shared between all the legitimate OBUs.

3. PRELIMINARIES

The bilinear pairing, search algorithms and hash chains have been employed for checking a CRL.

3.1 Bilinear Pairing

The bilinear pairing [22] is one of the foundations of the proposed protocol. Let G1 denote an additive group of prime order q, and G2 is a multiplicative group of the same order q. Let P be a generator of G1, and :G1×G1→G2 be a bilinear mapping with the following properties:

1.Bilinear: (aP,bQ)= 〖e (P,Q)〗 ^ab, for allP;Q∈ G1 and a,b ∈R Zq.

2. Nondegeneracy: (P,Q)≠1G2.

3. Symmetric: (P,Q)=e (Q,P) for all P,Q∈G1.

4. Admissible: the map is efficiently computable

The bilinear map can be implemented using the Weil [23] and Tate [24] pairings on elliptic curves. The security of the protocol proposed depends on solving the following problem:

Elliptic curve discrete logarithm problem (ECDLP) Consider point P of order q on an elliptic curve, and a point Q on the same curve. The above problem [25] is to determine the integer l,0≤l≤q- 1, such that Q= lP.

3.2 Hash Chains

A hash chain [26] is the successive application of a hash function h:{0,1}*→Zq with a secret value as its input. A hash function is efficient to compute, but it is computationally impossible to invert. Fig. 1 shows the application of a hash chain to a secret value.

MESSAGE AUTHENTICATION

We adopt a generic PKI system and we concentrate on how to accelerate the revocation check process, which is conventionally performed by checking the CRL for every received certificate.

4.3.1 Message Signing

Before any OBU_u broadcasts a message M, it calculates its revocation check REV_{check} as REV_{check} =HMAC(K_g; $PID_u||Tstamp$)2, where Tstamp is the current time stamp, and HMAC (K_g; $PID_u||T_{stamp}$) is the hash message authentication code on the concatenation of PID_u and T_{stamp} using the secret key K_g. Then, OBU_u broadcasts(M||T_{stamp}||$cert_u$)PID_u;PK_u;$sig_{TA}(PID_u||PK_u)$)||sig_u(M||T_{stamp})||REV_{check});where $sig_u(M||T_{stamp})$ is the signature of OBU_u on the concatenation of the message M and T_{stamp}.

4.3.2 Message Verification

Any OBU_y receiving the message (M||T_{stamp} ||certu)PID_u,PK_u;$sig_{TA}(PID_u||PK_u)$)||sig_u(M||T_{stamp})|| REV_{check}) can verify it by executing Algorithm 2.

Algorithm 2. Message verification

Require:(M||T_{stamp} || certu(PID_u;PK_u;$sig_{TA}(PID_u||PK_u)$) ||sig_u(M||T_{stamp})||REV_{check} and K_{g1}

1: Check the validity of T_{stamp}
2: if invalid then
3: Drop the message
4: else
5: Check REV_{check} = HMAC(K_g; $PID_u||T_{stamp}$)
6: if invalid then
7: Drop the message
8: else
9: Verify the TA signature on certOBU$_u$

10: if invalid then
11: Drop the message
12: else
13: Verify the signature $sig_u(M||T_{stamp})$ using OBU_u public key (PK_u)
14: if invalid then
15: Drop the message
16: else
17: Process the message
18: end if
19: end if20: end if
21: end if

In step(5), OBU_y calculates HMAC(K_g; $PID_u||T_{stamp}$) using its K_g on the concatenation $PID_u||T_{stamp}$, and compares the calculated HMAC (K_g; $PID_u||T_{stamp}$) with the received REV_{check}.

4.4 Revocation

The revocation is done by the TA when there is an OBU to be revoked. In addition, the secret key of OBU_u and the current secret key K_g are considered to be revoked. Hence, a new secret key K_g should be securely distributed to all the non-revoked OBUs. Also, each nonrevoked OBU should securely update the compromised keys in its key sets RS and RP [19].

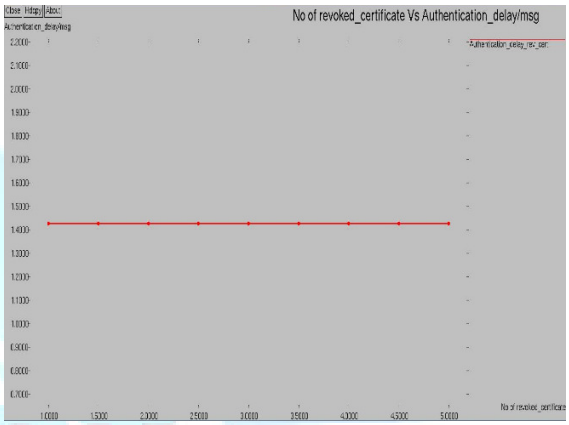
The revocation process is as follows:

1. The TA searches its database to determine the identity (M) of the non compromised secret key $K^-_M=k_MQ$ that is shared by the majority of the non-revoked OBUs, and finds the corresponding public key $K^+_M=1/k_MP$. The TA then selects a random number t €Z^*_q, and calculates the intermediate key $K_{im} = tK^+_M = t/k_M$ P €G1, and the new secret key K_g as follows:

$K_g = \hat{e}(K_M ; K_{im})$
$= \hat{e}(k_MQ, t/k$
$= \hat{e}(Q,P)kMt/kM$
$= \hat{e}Q,P)t$

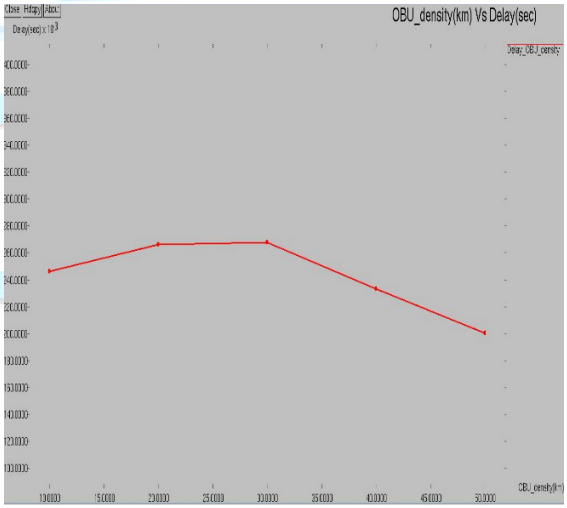
PERFORMANCE EVALUATION AUTHENTICATION DELAY

We compare the message authentication delay employing the CRL with that employing EMAP .As stated before, the authentication of any message is performed by three consecutive phases:1. check the sender's revocation status.2. verify the sender's certificate.3.verifying the sender's signature. For the first phase we check the revocation status of the sender, and employ CRL. For EMAP, for encryption we adopt the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC AES) [28] and Secure Hash Algorithm 1 SHA-1 [29] as the HMAC functions. We consider the PID of OBU and the time stamp ðTÞ having equal lengths of 8 bytes. We adopt the Crypto++ library [30] for calculating the delay of the HMAC functions. The delay incurred by using CBC-HMAC AES and SHA-1 to calculate the revocation check REV.



a) no. of revoked certificate vs authentication delay

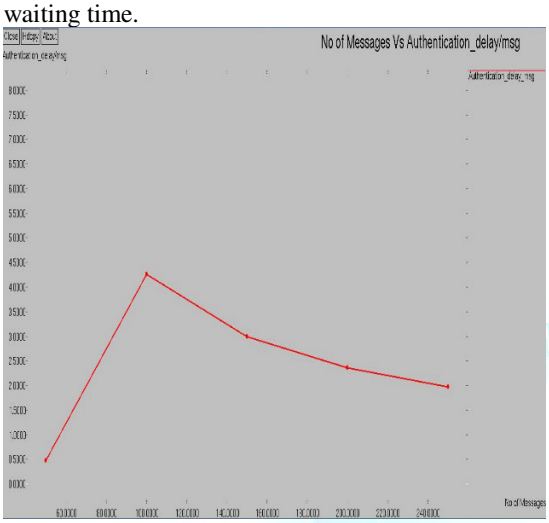
We have computed the graph for number of revoked certificate v_s authentication delay transmitted by the each OBUs.The revoked certifictes indicates the CRL size. The authentication delay is constant with respect to number of revoked certificates.



a) OBU density vs DELAY(ms)

We have computed the graph for OBU density v_s delay in msec.The OBU density predicts the communication

overhead. The delay gets increased when number of OBU is increased,as number of OBU increases results in long waiting time.



b) no. of messages vs authentication delay (ms)

We have computed the graph for number v_s delay in msec using EMAP.it is seen that the number of message verified within a region gets decreased with the CRL size.

CONCLUSIONS

We have developed a security architecture for VANETs systems, aiming at a solution that is both comprehensive and practical. We have studied the problem systematically, identifying threats and models of adversarial behavior as well as security and privacy requirements that are relevant to the VANETs. We introduced range of mechanism, to handle certificates and large number of users, and to secure communication while enhancing privacy. In the second paper of this contribution, we discuss implementation and performance aspects, present a gamut of research investigations and results towards further strengthening secure VC systems and addressing remaining research challenges towards further development and deployment of our architecture.

REFERENCES

[1] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.

[2] A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

[3] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Net- works," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[4] 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. Vehi- cular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010

[5] "5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/ index.html, 2012.

[6] A. Wasef and X. Shen, "MAAC: Message Authentication Accel- eration Protocol for Vehicular Ad Hoc Networks," Proc. IEEE GlobeCom, 2009.

[6] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), pp. 1-9, 2009.

[7] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Net- works," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557- 1568, Oct. 2007.

[8] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Sys- tems," Proc. Fifth ACM Int'l Workshop VehiculAr Inter-NETworking, pp. 86-87, 2008.

[9] K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'l Workshop VehiculAr Inter-NETworking, pp. 88-89, 2008

[10] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Net- works," J. Computer Security, vol. 14, pp. 301-325, 2006

.[11] S. Frankel, R. Glenn, and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec," IETF RFC 3602, Sept. 2003.

[12] D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," IETF RFC 3174, Sept. 2001. [30] "Crypto++ Library 5.5.2," http://www.cryptopp.com, 2012.

[13] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Int'l J. Information Security, vol. 1, no. 1, pp. 36-63, 2001.

[14] "The Network Simulator - ns-2," http://nsnam.isi.edu/nsnam/ index.php/User Information, 2012.