International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

AMAP: Advance Message Authentication Protocol for Vehicular Ad Hoc Networks

Akanksha Botke
Information Security and Computer Forensic
SRM University
Kattankulathur, Chennai, Tamil Nadu, India

A. Arokiaraj Jovith
Assistant Professor(Sr.G)
Information Security and Computer Forensic
SRMUniversity
Kattankulathur, Chennai, Tamil Nadu, India

Abstract* - Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) are adopting by Vehicular Ad hoc network (VANET) for their security and privacy. In PKI system we are checking the sender's certificate for authentication of a received message and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose an Advance Message Authentication Protocol (AMAP) for VANETs, which replaces the time-consuming CRL checking process. The revocation check process in AMAP uses a keyed Cipher Block Chaining Message Authentication Code CMAC, where the key used in calculating the CMAC is shared only between nonrevoked On-Board Units (OBUs). In AMAP we are using a novel probabilistic key distribution, which helps nonrevoked OBUs to securely share and update a secret key. AMAP helps to decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting AMAP we can secure VANET efficiently.

***Index Terms*—Vehicular Ad hoc networks, location privacy, communication security, message authentication, safety**

I. INTRODUCTION

Vehicular networking applications necessitate continuous information of the location of vehicles and tracking of the paths they follow, including, e.g., real-time traffic monitoring, e-tolling, and liability attribution in case of accidents. Locating and tracking vehicles has still strong implications in terms of security and user privacy. On the one hand, there should be a mean for an authority to verify the accuracy of positioning information announced by a vehicle, so as to identify potentially misbehaving cars. On the other, public expose of identity and position of drivers should be evaded, so as not to endanger user privacy. Vehicular ad hoc networks (VANETs) have fascinated wide attentions recently as a promising technology for reforming the transportation systems and given that broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to Vehicle (V2V) and Vehicle-to-Infrastructure (V2I)
Communications are the two modes of communication which respectively permit OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate with each other through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the dispersed messages can be easily propelled. A security attack on VANETs can have severe harmful or fatal penalties to legitimate users. Consequently, ensuring secure vehicular communications is a requirement before any VANET application can used into practice. We introduced a solution to secure VANETs by implementing Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network grasps an authentic certificate, and every message should be digitally signed before its transmission. A CRL issued by a Trusted Authority (TA) is a list enclosing all the revoked certificates. In a PKI system, the authentication of any message is performed in 3 steps 1) checking if the sender's certificate is comprised in the current CRL, i.e., checking its revocation status. 2) Verifying the sender's certificate. 3) Verifying the sender's signature on the received message. The first part of the authentication is checking the revocation status of the sender in current CRL, may suffer long delay depending on the CRL size and the engaged mechanism for searching the CRL. The size of CRL in VANETs is estimated to be large for the following reasons:

1) To preserve the privacy of the drivers, i.e., to desist the leakage of the real identities and location information of the drivers from any exterior eavesdropper [1], [2], [3], each OBU should be preloaded with a set of unidentified digital certificates, where the OBU has to sporadically change its unidentified certificate to deceive attackers[4],[5],[6]. Consequently, revocation of a certificate results in revoking all the certificates of that OBU, which leads to a large increase in the CRL size.

2) The area of VANET is very large. According to the United States Bureau of Transit Statistics, there are almost 251 million OBUs in the Unites States in 2006. Since the number of the OBUs is gigantic and each OBU has a set of certificates, the CRL size will increase melodramatically if only a small portion of the OBUs is revoked. To have an idea of how large the CRL size can

be, consider the case where only 100 OBUs are revoked, and each OBU has 15,000 certificates that means the CRL contains 2.5 million revoked certificates. According to the working mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard does not affirm that either a nonoptimized search algorithm, e.g., linear search, or some kind of optimized search algorithm such as binary search, will be used for searching a CRL. Here we consider both nonoptimized and optimized search algorithms. According to the Dedicated Short Range Communication (DSRC), each OBU has to broadcast a message every 300 msec about its site, velocity, and other telematics information. In that condition, each OBU may receive a huge number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may deserve long authentication delay depending on the CRL size and the number of received certificates. The capacity to check a CRL for a large number of certificates in a suitableapproach leads an inevitable challenge to VANETs. To ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. In this paper, we introduce advance message authentication protocol (AMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure CMAC function. AMAP is suitable not only for VANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

II. RELATEDWORK

In VANETs, the most important security necessities are identified as entity authentication, message integrity, nonrepudiation, and privacy protection. The PKI is the most feasible technique to achieve these security necessities. PKI employs CRLs to powerfully manage the revoked certificates. Since the CRL size is estimated to be very large, the stoppage of checking the revocation status of a certificate included in a received message is expected to be time-consuming. Discover the specific issues of security and privacy in VANETs, and specify that a PKI should be well deployed to defend the transmitted messages and to commonly authenticate network entities.

In [4], Raya and Hubaux use a traditional PKI to provide secure communications to VANETs. In VANET each vehicle needs to preload a vast pool of anonymous certificates. The number of the weighed down certificates in each vehicle should be large enough to provide security and privacy protection for a long time, e.g., one year. Each vehicle has to update its certificates from a central authority during the annual assessmentof the vehicle. In VANET revoking one vehicle implies revoking the vast number of certificates loaded in OBUs. In [13], Studer et al. recommendancapable authentication and revocation scheme called TACK. TACK adopts a ladder system architecture consisting of a central trusted authority and regional authorities (RAs) spread all over the network. In TACK system, the trusted authority acts as the group manager and the vehicles act as the group members. When a vehicle entering a new region, it must update its certificate from the RA devoted for that region. First the vehicle sends a request signed by its group key to the RA to update its certificate, and then RA verifies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (RL). After the RA authenticates the vehicle, it issues short lifetime region-based certificate. This certificate is legal only within the coverage range of the RA. THE disadvantage of TACK that it requires the RAs to wait for some time e.g., 2 seconds, before sending the new certificate to the requesting vehicle. During that time period the vehicle is not able to send message to neighboring vehicles, which makes TACK not suitable for the safety applications in VANETs as the WAVE standard requires each vehicle to transmit messages about its location, speed, and direction every 100-300 msec. Also, TACK requires the RAs to absolutely cover the network; otherwise, the TACK technique may not function accurately. This requirement may not be practicableespecially in the early deployment stages of VANETs.

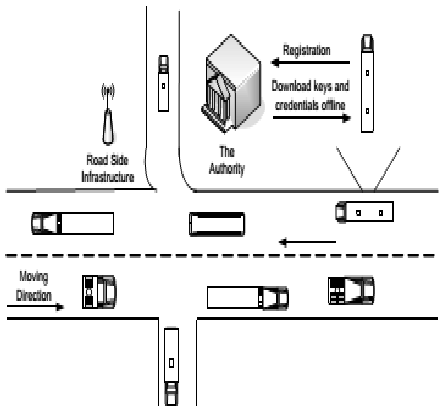

FIGURE 1. Vehicular ad hoc networks.

Even though TACK eliminates the CRL at the vehicles level, but it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates for short period of time. To check the revocation status of a vehicle, the RA has to confirm that this vehicle is not in the current RL, for that RA'sperforming a check against all the entries in the RL. Each checking requires three pairing operations. Checking the revocation status of a vehicle may be a time consuming process in VANET. The authors recommendedusing an optimized search technique to cure the computationally exclusive RL check. The proposed technique can decrease the RL checking to two pairing operations. However, this resolution is based on setting up some parameters in the group signature attach to every certificate request, which reduces the privacy protection of TACK. In this paper, we propose an Advance Message Authentication Protocol (AMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. AMAP employs keyed Cipher Block Chaining Message Authentication Code CMAC in the revocation checking process, where the key used in calculating the CMAC for each message is shared only between unrevoked OBUs. In addition, AMAP is free from the false positive property.

III. PRELIMINARIES

In this segment, we introduce the search algorithms that can be employed for checking a CRL.

3.1 Search Algorithms

The WAVE standard does not believe a specific method for searching CRLs to check the revocation status of certificates. The most common search algorithms [14] include a nonoptimized search algorithm that is linear search algorithm, and optimized search algorithms such as binary search algorithm and CMAC. The conceptof each algorithm is as follows:

3.1.1 Linear Search Algorithm

In this algorithm, the revocation status of a certificate is checked by comparing the certificate with each entry in the CRL. If a match occurs in the CRL, the certificate is revoked and vice versa.

3.1.2 Binary Search Algorithm

The binary search algorithm is applicable only on sorted lists. In VANET when a vehicle receiving a new CRL, each OBU has to preserve a sorted database of the revoked certificates built-in in earlier CRLs and the recently received CRL. The main scheme of the binary search algorithm is to cancel out half of the entries beneath consideration after each comparison in the search process. In this algorithm, the revocation status of a certificate is checked by comparing the identity of the certificate with median value of the sorted database. If the uniqueness of the certificate is larger than the median value, the right half of the database will be considered in the next comparison process and vice versa. This procedure continues until a match is found or the procedure is finished without finding a match which means that the certificate is unrevoked.

3.1.3 CMAC – CBCMAC

The cipher block chaining message authentication code is applied in VANET for security against attackers. Only messages of one fixed length of mn bits are processed, where n is the cipher block size and m is a fixed positive integer.

The CBCMAC of a one block message X, say T = MAC(K,Y) , the adversary immediately knows the CBCMAC for the 2- block message X ‖ (X⊕T) since this one again T. This limitation could be overcome using 3 keys

1. One key of length ‘k’ to be used at each step of the cipher block chaining.
2. Second key of length ‘n’, where ‘k’ is the key length and ‘n’ is the cipher block length

This proposed construction was refined by Iwata and Kurosawa so that the 2 n-bit keys could be derived from the encryption key, rather than being provided separately. This refinement has been adopted by NIST cipher based message authentication code (CMAC) mode of operation, for use with AES and TDES.

Let us consider the operation of CMAC when the message is an integer multiple n of the cipher block length b. for AES, b = 128 and for TDES, b = 64. The message is divided into n blocks, M_1 ,M_2,M_3_ _ _ _ M_n. The algorithm makes use of k-bit encryption key k and n-bit constant K_1.

For AES, the key size k is 128,192 or 256 bits for TDES, the key size is 112 or 168 bits. CMAC is calculated as follows

C_1 = E (k,M_1)

C_2 = E (k, [$M_2 \oplus C_1$])

C_3 = E (k, [$M_3 \oplus C_2$])

:

:

C_n = E (k, [$M_n \oplus C_{n-1} \oplus K_1$])

T = MSB T_{len} (C_n)

Where,

T = message authentication code, also referred to as the tag.

T_{len} = bit length of T.

MSB(X) = the S leftmost bits of the bit string X.

If the message is not an integer multiple of the cipher block length, then the final block padded to the right LSB with a 1 and as many 0s as necessary so that the final block is also of length b. the CMAC operation then proceeds as before except that a difference n-bit key K_2 is used instead of K_1. The 2 n-bit keys are derived from the k-bit encryption key as follows

L = E (k,0^n)

k1 = L· x

k2 = L· = (L· x) · x

Where multiplication (·) is done in the finite field GF (2^n) and x and x^2 are first and second order polynomials that are elements of GF (2^n). Thus the binary representation of x consists of n-2 zeros followed by 10, the binary

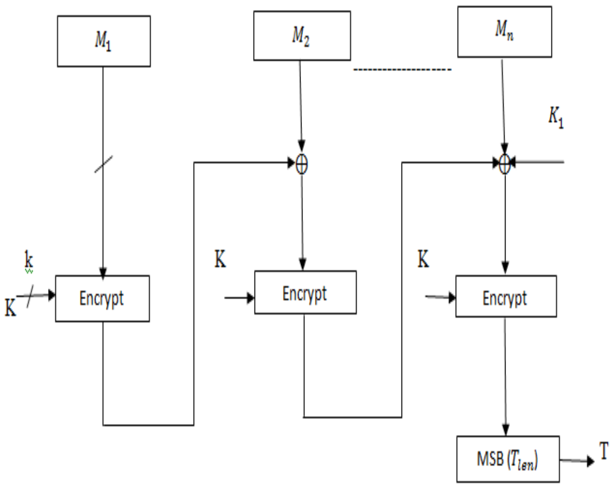

Fig – (a) Message length is integer multiple of block size

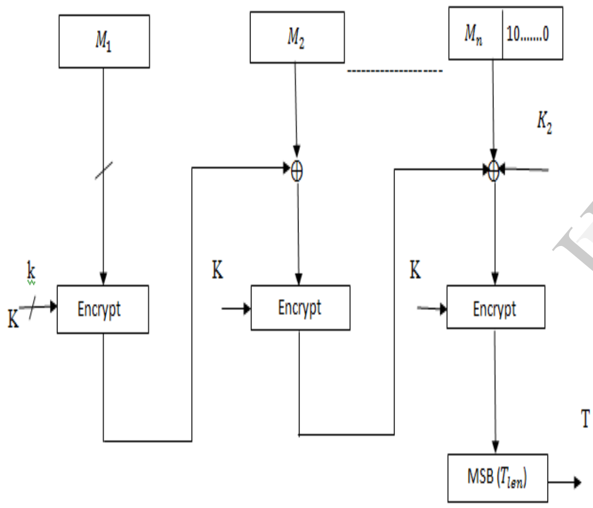

Fig – (b) message length is not an integer multiple of block size.

IV.MESSAGE AUTHENTICATION

Since we adopt a generic PKI system, the details of the TA signature on a certificate and an OBU signature on a message are not discussed in this paper for the sake of generality. We only focus in how to accelerate the revocation checking process, which is conventionally performed by checking the CRL for every received certificate. The message signing and verification between different entities in the network are performed as follows:

4.3.1 Message Signing

Before any OBU_u broadcasts a message M, it calculates its revocation check REV_{check} as REV_{check} = CMAC

representation of x^2 consists of n-3 zeros followed by 100. The finite field is defined with respect to an irreducible polynomial that is lexicographically first.

$(K_g, PID_u||T_{stamp})$, where T_{stamp} is the current time stamp, and CMAC $(K_g, PID_u||T_{stamp})$ is the Cipher message authentication code on the concatenation of PID_u and T_{stamp} using the secret key K_g. Then, OBU_u broadcasts.

$(M||T_{stamp}||cert_u(PID_u, PK_u sig_{TA}(PID_u||PK_u))$

$||sig_u(M||T_{satmp})||REV_{check})$,

Where

T_{stamp} – The current time stamp

PID_u – The pseudo identity for each node

K_g – Shared secret key

$sig_u(M||T_{stamp})$ is the signature of OBU_u on the concatenation of the message M and T_{stamp}.

4.3.2 Message Verification

Any OBU_u receiving the message

$(M||T_{stamp}||cert_u(PID_u, PK_u sig_{TA}(PID_u||PK_u))$

$||sig_u(M||T_{satmp})||REV_{check})$

Can verify it by executing Algorithm

Algorithm -Message verification

Require:
$(M||T_{stamp}||cert_u(PID_u, PK_u sig_{TA}(PID_u||PK_u))$

$||sig_u(M||T_{satmp})||REV_{check})$

1: Check the validity of T_{stamp}

2: if invalid then

3: Drop the message

4: else

5: Check REV_{check} = CMAC $(K_g, PID_u||T_{stamp})$

6: if invalid then

7: Drop the message

8: else

9: Verify the TA signature on $cert_{OBUu}$

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 if

20: end if

21: end if

In step (5), OBU_y calculates CMAC ($K_g, PID_u||T_{stamp}$) using its Kg on the concatenation$PID_u||T_{stamp}$, andcompares the calculated CMAC ($K_g, PID_u||T_{stamp}$) withthe received REV_{check} .

V. SECURITYANALYSIS

In this segment, we analyze the security of the proposed protocol against some frequent attacks.

5.1 Resistance to Forging Attacks

To falsify the revocation checkREV_{check} = CMAC ($K_g, PID_u||T_{stamp}$) of anyOBU_u, an attacker has to find the currentKg, which is equivalent to finding T_{stamp} .Similar analogy applies to finding the TA secret key from the TA message signature.It is concluded that EMAP is resistant to forging attacks.

5.2 Resistance to Replay Attacks

Since in every message an OBU includes the current time stamp in the revocation check valueREV_{check} = CMAC ($K_g, PID_u||T_{stamp}$), an invader cannot recordREV_{check} at time T_i and replay it at a later timeT_{i+1} to pass the revocation checkingprocedure as the receiving OBU compares the current time T_{i+1} with that built-in in the revocation check. Consequently, AMAP is secure against replay attacks.

5.3 Resistance to Colluding Attacks

For this type of attack, alegal OBU colludes with a revoked OBU by releasing the existing secret key K_g such that the revoked vehicle can use this key to pass the revocation check procedureby calculating the correct CMAC values for the transmitted messages. All the security resources of an OBU are stored in its tamper-resistant Hardware Security Module(HSM). In addition, all the keys renew processes are executed in the HSM, which means that the new secret key K_g stored in the HSM, and it cannot be transmitted in clear under any circumstances. The HSM only sends $K_g$encrypted with the public key included in the certificate of the OBU requesting K_g after checking that the certificate of that OBU is not in the CRL. Accordingly, only that OBU is the entity that can decrypt and obtain K_g using its secret key which is entirely known to itself. Since it is infeasible to dig up the security materials from the tamper-resistant HSM, an unrevoked OBU cannot collude with a revoked OBU by passing the new secret key $K_g$to the revoked OBU. Hence, AMAP is secure against colluding attacks.

5.4 Authentication Delay

Here weevaluate the message authentication delay employing the CRL with that employing AMAP to check the revocation status of an OBU. The authentication of any message is performed by three successive steps: checking the sender's revocation status, verifying the sender's certificate, and verifying the sender's signature. For the first authentication step which checks the revocation status of the sender, we utilize either the CRL or AMAP. For AMAP, we implement the Cipher Block Chaining CMAC (CBC-CMAC). We consider the PIDof OBU and the time stamp T_{stamp} having equal lengths of 8 bytes. The linear CRL checking program performs progressive search on a text file containing the unsorted identities of the revoked certificates, while the binary CRL checking plan performs a binary search on a text file containing the sorted identities of the revoked certificates. It can be seen that as the CRL size increases the number of messages that can be verified within a specific time is drastically decreased using the linear CRL checking procedure.

5.5 Message Loss Ratio

The standard message loss ratio is defined as the average ratio between the numbers of messages dropped every 300 msec, due to the message authentication delay, and the total number of messages received every 300 msec by an OBU of a vehicle. We are only concerned in the message loss incurred by OBUs due to V2V communications. According to DSRC, each vehicle has to broadcast a message containing information about the road condition every 300 msec. In order to respondappropriately and instantly to the varying road conditions, each OBU should verify the messages received during the last 300 msec before broadcasting a new message about the road condition. Employing AMAP appreciably decreases the messageloss ratiocompared to that linear orbinary CRL revocation status checking.

VI. CONCLUSIONS

We proposed AMAP for VANETs, which decreases themessage authentication delayby replacing the time-consuming CRL checking process with a quick revocation checking procedure employing CMAC Algorithm. The proposed AMAP uses a PKImechanism which allows an OBU to update its compromised keys in VANET. In addition, AMAP has an advantage rendering it integrable with any PKI system. AMAP opposing the common attacks while performing the authentication techniques. Therefore, AMAP can appreciablyreduce the message loss ratio due to message verification delay compared to the conservative authentication techniques employing CRL checking.

REFERENCES

1. P. Papadimitratos, A. Kung, J.P.Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,”Proc. Workshop Standards for Privacy in User Centric Identity Management, July 2006.
2. 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.
3. 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.
4. M. Raya and J.-P.Hubaux, “Securing Vehicular Ad Hoc Networks,”J. Computer Security,vol. 15, no. 1, pp. 39-68, 2007.
5. Y.Sun, R.Lu, X.Lin, X.Shen, andJ.Su,“an EfficientPseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,”IEEE Trans. Vehicular Technology,vol. 59, no. 7, pp. 3589-3603, Sept. 2010.
6. R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,”IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.
7. US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/Passenger_vehicles_in_the_United_States, 2012.
8. J.J. Haas, Y. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,” Proc. Sixth ACM Int’l Workshop Vehicular Internetworking,pp. 89-98, 2009.
9. IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,IEEE, 2006.
10. “5.9 GHz DSRC,” http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2012.
11. A. Wasef and X. Shen, “MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks,” Proc. IEEE GlobeCom,2009.
12. J.P. Hubaux, “The Security and Privacy of Smart Vehicles,”IEEE Security and Privacy,vol. 2, no. 3, pp. 49-55, May/June 2004.
13. 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.
14. T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, Introduction to Algorithms. MIT, 2001.
15. M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of Misbehaving and Faulty Nodes in Vehicular Networks,”IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.
16. P.P. Papadimitratos, G. Mezzour, and J. Hubaux, “Certificate Revocation List Distribution in Vehicular Communication Systems,”Proc. Fifth ACM Int’l Workshop Vehicular Inter-Networking, pp. 86-87, 2008.