RESEARCH ARTICLE OPEN ACCESS

Secure Authentication Using Certificate Revocation List (Crl) and Message Signature in Vanet

R. Saranya[1], J. Hariharan[2]
[1]M.E. Student, [2]M.E. Student, Department of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Trichy and [2]Regional Centre of Anna University, Madurai.

ABSTRACT
A vehicular ad hoc network (VANETs) provides the security through the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs). In any PKI system, the signature of sender and certificate should be verified in CRL list. Also verifying the certificate of the sender then authentication is provided to received message. In this paper, secure hash authentication protocol (SHAP) verifies digital signature and encryption functions. It not only provides message confidentiality, authentication, integrity, and nonrepudiation, but also forward secrecy for message confidentiality and public verification. In addition, SHAP uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key. SHAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, SHAP is demonstrated to be secure and efficient.

Index terms- certificate revocation, communication security, Message authentication, vehicular networks

I. INTRODUCTION

A **Vehicular Ad-Hoc Network**, or **VANET**, is a form of Mobile ad-hoc network. It is used in communicating among people moving in vehicles. Vehicles can communicate with roadside traffic equipment's.

Transportation system uses VANET to provide a broadband communication. The entities of VANET are On-Board Units (OBU), Infrastructure Road Side Units (RSU). The two basic communication modes in VANET are Vehicle to Vehicle and Vehicle to Infrastructure. OBU sometimes called as In Vehicle equipment (IVE), which contains single hop and multi hop. There are some possibilities for the attack of information in wireless network. PKI and CRL are now the solution for these arising threats in wireless network. PKI ensures that the certificate should be signed before transmission. For the current CRL, it is important that it should contain sender's certificate. At the receiver end, the sender's certificate is checked. PKI list provide the certificate to the user to communicate through vehicles. CRL lists are mainly provided by a Trusted Authority (TA). All the revoked certificates are listed in CRL. In PKI system, the authentication of message are determined by checking the list provide by the sender certificate. CRL checks whether the sender certificates are included in list.

The revocation status of all the received certificates should be checked at regular time interval. OBU helps for this activity. VANET communicate and checks the revocation status of the sender certificate in CRL. This leads to long delay in checking depending upon the CRL size.

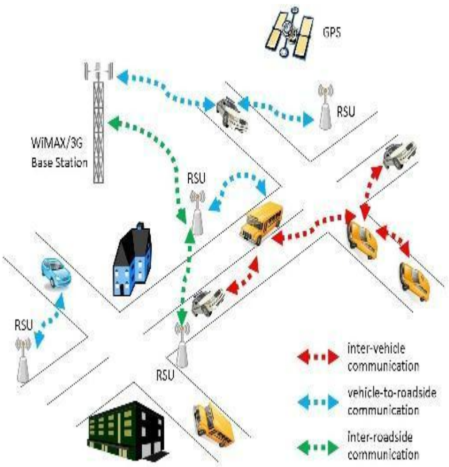

GPS
WiMAX/3G Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig. 1.1 Vehicle Communication

To improve the VANET performance with the security standards, optimized search algorithm are used. Wireless Access in Vehicular Environments (WAVE) states either optimized or non-optimized search algorithm.

A protocol is used in this paper, which is the combination of digital signature and encryption function. It is Signcryption Message Authentication protocol (SMAP). Its functions are to provide message confidentiality, authentication, integrity, non-repudiations, forwarding secrecy for message confidentiality and public certification. SMAP replaces CRL by efficient revocation checking process using HMAC function. SMAP is suitable for

both PKI and CRL system, by reducing time. This believed to be the first solution to reduce authentication delay from checking CRL in VANET.
It is evident that any malicious behavior of a user, such as injecting false information and modifying and replaying the disseminated messages, could be fatal to other legal users. Furthermore, the privacy of users must be guaranteed in the sense that the privacy-related information of a vehicle should be protected to prevent an observer from revealing the real identities of the users, tracking their locations, and inferring sensitive data.

The centralized certificate update process in the classical PKI may be impractical in large-scale VANETs due to the following reasons: 1) Each CA encounters a large number of certificate update requests, which can render the CA with a bottleneck, and 2) the certificate-update delay is long relative to the short V2I communication duration between the immobile RSUs and the highly mobile OBUs, during which the new certificate should be delivered to the requesting OBU. The long certificate-update delay is due to the fact that a request submitted by an OBU to an RSU must be forwarded to the CA, and the CA has to send the new certificate to that RSU, which, in turn, forwards the new certificate to the requesting OBU.

II. RELATED WORKS

In VANETs, the primary authentication are identified, message authentication, integrity and privacy preservation. The PKI is the important list to provide the authenticated user. The CRL size is expected to be very large, the revocation checking processes are employed with receive message.

In [7], Yixin Jiang, and Xuemin Shenthe specific security include DCS provide an efficient way for OBU mainly used to update its certificate from any available infrastructure RSU. These schemes also include aggregate batch verification technology used for authenticating certificate based signature. MA generates a public verification key for verifying the certificate that is provided by RSU\OBU units.CA is used to verify the certificate signing key, issued by MA. To sign a certificate set for every RSU and OBU. DCS allow OBU to update its certificate from an RSU. Certificate Revocation list are employed in WAVE standard. CA responsible for all certificate of comprised entity to current CRL.

In [6], Yanjun Sun, David B. Johnson proposes an efficient authentication enhanced MAC protocol in multi-hop wireless network. EMAC improve the efficiency of wireless medium access with asynchronous multi-hop wireless network limit the routing information in MAC layer, thus allows asynchronous station along a delivery path to access random medium.

EMAC is different from RMAC with number of aspects. EMAC is designed for multi-hop wireless network and does not allow clock synchronization. When the network layer introduces a new technique to improve the authentication, EMAC transaction which build a PION frame and send it to next node. Synchronized intra flow coordination across multiple asynchronous hops by using CSMA/CA access randomly and alleviate hidden terminal problem.

In [9], Jinshu Su, Xiaodong Lin proposes an efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communication. PASS not only satisfy the security and privacy requirements of VANET but also significantly reduce the revocation cost and certificate updating overhead. PASS provide strong privacy preservation to vehicle that adversaries cannot trace the legitimate vehicle even though they have compromised all RSU.PASS store a large set of pseudonym certificate that are provided by TA.RSU range also act as certificate user in PASS, the certificate are treated as unrelated to number of update certificate.

In [3], Christoph Sommer, Reinhard German proposes Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IVC protocol which provide demand routing plan to observe traffic congestion mainly for safety application. Bidirectionally coupling used to evaluate network simulation for evaluating IVC protocol. When some road traffic simulators are in VANET are employed in offline to speedup network simulation performance. An alternative and different approach used for monitoring the traffic and distribute the received traffic message to another vehicles is to decentralized self-organizing. The decentralized SOTIS approach in vehicle share the information about local traffic situation by mean of IVC.

In [10], Jason J. Haas, Yih-Chun Hu proposes a light weight mechanism for revoking security certificate for limit the bandwidth and hardware cost constrains of a VANET. The vehicle use mechanism for passing CRL, update rather the entire CRL, which mainly reduce the network overhead and similar to delta CRL.

In [1], Rongxing Lu, Xiaodong Lin proposes effective pseudonym changing at social spots (pcs) strategy for location privacy in VANET. It also determines a key insulated pseudonym self-delegation (kpsd) model to mitigate the hazards caused by vehicle theft.

III. PRELIMINARIES

In this section, we introduce the encryption, decryption and SHA1 algorithm that can be employed for checking a CRL and PKI list.

3.1. Search Algorithm

The WAVE standard does not allow some specific mechanism for searching the CRL list to check the authenticated user. The revocation status is updated at each entry of the vehicle.

3.1.1. Binary search algorithm

The binary search algorithm is mainly used for sorting lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted database of the revoked certificates included in previous CRLs and the recently received CRL [5]. 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 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.

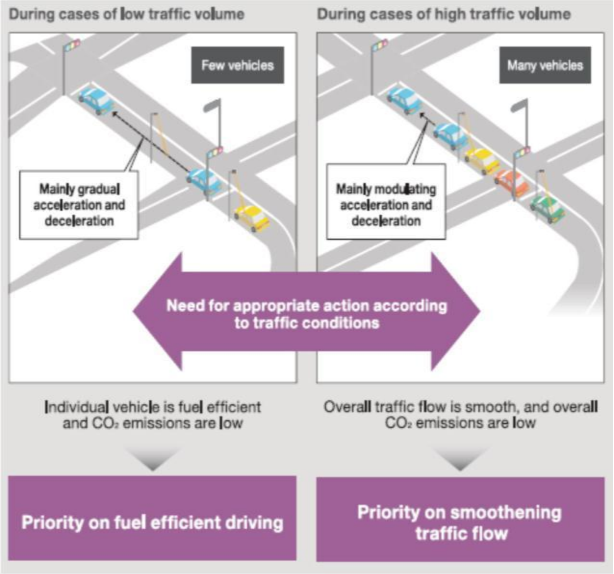
This process continues until a match is found, i.e., the certificate is revoked, or the process is finished without finding a match which means that the certificate is unrevoked.

Algorithm 1:

```
bool jw_search ( int *list, int size, int key, int*& rec )

{ // Binary search

bool found = false; int low = 0, high = size - 1;

while (high >= low) {
 int mid = (low + high) / 2;

if (key < list [mid]) high = mid - 1;

else if (key > list [mid])
low = mid + 1;

else {

found = true;

rec = &list [mid]; break;

}}return found;

}
```

3.1.2 Hash Tables

In this approach, the set of all certificates list is mapped using hash values. To determine the revocation status of the certified list, the hash of the certificate is identified by the entry of the index. Since the VANETs are the very large scale and each time OBUs are verified with the set of certificate.


During cases of low traffic volume
During cases of high traffic volume
Few vehicles
Many vehicles
Mainly gradual acceleration and deceleration
Mainly modulating acceleration and deceleration
Need for appropriate action according to traffic conditions
Individual vehicle is fuel efficient and CO₂ emissions are low
Overall traffic flow is smooth, and overall CO₂ emissions are low
Priority on fuel efficient driving
Priority on smoothening traffic flow

1.2 Vehicle to Vehicle and Vehicle to Infrastructure

IV. SECURE HASH MESSAGE AUTHENTICATION PROTOCOL

The proposed SHA uses a fast revocation and novel key sharing employed in random key distribution. Security analysis and performance evaluation, SMAP is demonstrated to be secure and efficient.

4.1. System Model

. 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 V2I communications.

4.2. System Initialization

The TA initializes the system by providing some algorithm. The authenticated users are identified and the number of certificate loaded in each OBU.

Step1: Initialize hash values:
(first 32 bits of the fractional parts of the square roots of the first 8 primes 2..19):
h0 := 0x6a09e667
h1 := 0xbb67ae85
h2 := 0x3c6ef372
h3 := 0xa54ff53a
h4 := 0x510e527f

h5 := 0x9b05688c
h6 := 0x1f83d9ab

step2: Pre-processing:
append the bit '1' to the message append k bits '0', where k is the minimum number >= 0 such that the resulting message length (modulo 512 in bits) is 448. append length of message in bits, as 64-bit big-endian integer

step3: Process the message in successive 512-bit chunks:

Break message into 512-bit chunks **for** each chunk copy chunk into first 16 words of the message schedule array w[0..15]

Extend the first 16 words into the remaining 48 words of message schedule array:

for i from 16 to 63
s0 := (w[i-15] rightrotate 7) xor (w[i-15] rightrotate 18) xor (w[i-15] rightshift 3)

s1 := (w[i-2] rightrotate 17) xor (w[i-2] rightrotate 19) xor (w[i-2] rightshift 10)

w[i] := w[i-16] + s0 + w[i-7] + s1 Produce the final hash value (big-endian): digest := hash := h0 append h1 append h2 append h3 append h4 append h5 append h6 append h7

4.3. Message Authentication

The TA signature on the certificate and an OBU signature are not detailed this paper. Message verification and digital signature are performed as follows.

```
Check the validity of $T_{stamp}$
if invalid then
    Drop the message
else
    Check $REV_{check}$ = HMAC ($K_g$, $PID_u$ || Tstamp)
    if invalid then
        Drop the message
    else
        Verify the TA signature on $cert_{OBUu}$
        if invalid then
            Drop the message
        else
            Verify the signature $sig_u$ ($M||T_{stamp}$) using $OBU_u$ Public key ($PK_u$)
            if invalid then
                Drop the message
            else
                Process the message
            end if
        end if
    end if
end if
```

V. Security Analysis

To forge the revocation check of any on board unit an attacker has to find the current problem. And find the TA secret key and signature. To the revocation check and TA message and signature are unforgivable. 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, and given the fact that 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, a revoked OBU cannot update its secret key set.

5.1 Adversary Model

The following possible attack models can be used during the V2V authentication procedure.

- Modification attack: The adversary modifies the packet resulting in the message against the integrity of the information.
- Message replay attack: The adversary resends valid messages sent previously in order to disturb the traffic flow.
- Movement tracking: Since wireless communication is based on a shared medium, an adversary can easily eavesdrop on any traffic.
- Impersonation attack: The adversary pretends to be a valid LE/TV to cheat the unauthenticated OBUs.

5.1 Security Requirements

Since the authentication scheme is susceptible to malicious attacks, our objective is to design a scheme that is robust to such attacks.

- Efficiency: In VANETs, the computational cost of vehicles must be as low as possible in order to have a real-time response.
- Anonymity: The anonymous authentication procedure verifies that an OBU does not use its real identity to execute the authentication procedure.
- Location privacy: An adversary collects the serial authentication messages of the OBU but it still failed to track the location of the vehicle.
- Mutual authentication: A mutual authentication procedure is implemented whereby the LE must verify that the OBU is a legal user and the OBU must ensure that the LE is genuine.
- Integrity: The message integrity means that data cannot be modified undetectably.

5.2. Hash Chain Value

The value of the hash chains are continuously used in the revocation processes and hence the TA can consume all the hash chain values. The hash keys are trust-linked via public keys and certificates to a certifying authority. hash chain h1, h2, .. . , hn generated by a cryptographic hash function H. Two types of packets are broadcast by a vehicle O:

- data packets P_j
- key release packets k_r _ P_j

5.3. Resistance of forging Attack

To forge the revocation check of any on board unit an attacker has to find the current problem. And find the TA secret key and signature. To the revocation check and TA message and signature are unforgivable.

5.5. Resistance to Replay Attack

Since in each message an OBU includes the current time stamp in the revocation check value REV_{check} = HMAC (Kg; PID_{uk} || Tstamp), an attacker cannot record REV_{check} at time Ti and replay it at a later time T+1 to pass the revocation checking process as the receiving OBU compares the current time T+1 with that included in the revocation check. Consequently, EMAP is secure against replay attacks.

5.6. 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

5.7. Demand Distributed Authenticated Algorithm

The binary search algorithm works only on sorted lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted database of the revoked certificate included in previous CRLs and the recently received CRL. The 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 of the sorted database. A root certificate is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

VI. PERFORMANCE EVALUTION

6.1 Authentication delay

The message authentication delays are employed in checking the revocation status of the OBU units. The authentication messages are performed by three processes: checks the sender revocation status, verify the sender certificate and also check the sender signature. For VANET the CRL adopt secure hash algorithm by encrypting the message. For the second and third authentication phases, we employ Elliptic Curve Digital Signature Algorithm (ECDSA) to check the authenticity of the certificate and the signature of the sender. ECDSA is the digital signature method chosen by the WAVE standard.

6.2 Cryptanalysis and validation

For a hash function for which L is the number of bits in the message digest, finding a message that corresponds to a given message digest can always be done using a brute force search in approximately 2^L evaluations. This is called a preimage attack and may or may not be practical depending on L and the particular computing environment. The second criterion, finding two different messages that produce the same message digest, namely a collision, requires on average only about 1.2 * $2^{L/2}$ evaluations using a birthday attack. For the latter reason the strength of a hash function is usually compared to a symmetric cipher of half the message digest length. Thus SHA-1 was originally thought to have 80-bit strength.

In the case of document signing, an attacker could not simply fake a signature from an existing document—the attacker would have to produce a pair of documents, one innocuous and one damaging, and get the private key holder to sign the innocuous document. There are practical circumstances in which this is possible; until the end it was possible to create forged SSL certificates using an MD5 collision.

Due to the block and iterative structure of the algorithms and the absence of additional final steps, all SHA functions are vulnerable to length-extension and partial-message collision attacks. These attacks allow an attacker to forge a message signed only by a keyed hash –SHA (message || key) or SHA (key || message) by extending the message and recalculating the hash without knowing the key. The simplest improvement to prevent these attacks is to hash twice: SHA_d (message) = SHA (SHA (0^b|| message)) (the length of 0^b, zero block, is equal to the block size of hash function)

6.3 Ends-to-End Delay

The end-to-end delay, which is defined as the time to transmit a message from the sender to the receiver.

It can be seen that the end-to-end delay increases with the OBUs density because the number of the received packets increases with the OBUs density resulting in longer waiting time for the packets to be processed by the application layer in each OBU.

VII. CONCLUSION

In proposed SHA2 for VANET, which allows digital signature verification and encrypt the message by lacing time consuming with CRL checking process with a fast revocation checking process. In existing system EMAP uses a novel keysharing mechanismwhich allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, EMAP has a Modular feature rendering it integral with any PKI system. Furthermore, it is resistant to common Attacks while outperforming the authentication techniques employing the conventional CRL. Therefore, SHA2 can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking. My future work will focus on the certificate and message signature authentication acceleration using SMAP.

REFERENCES

[1] 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, 2012.

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

[3] Christoph Sommer, Reinhard German, and Falko Dressler, ―Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis‖, IEEE Transactions on Mobile Computing, Vol. 10, No. 1, January 2011.

[4] Gramaglia.M, ‖Optimized IPV6 internet access from vehicles in multi-hop and heterogeneous environment‖, pp.1-3, IEEE international symposium on a world of wierless, mobile and mulgimedia network, 2011.

[5] Sheng-Tzong Cheng, Gwo-Jiun Horng and Chih-Lun Chou,―Using cellular automata to form car society in vehicular Adhoc networks‖, intelligent transportation system,IEEE transactions on,vol:12,issue:4,2011.

[6] Shu Du, Yanjun Sun and David B.Johnson,‖ EMAC: An Asynchronous Routing-Enhanced MAC Protocol in Multi-hop Wireless Networks‖, IEEE Globecom by the U.S. National Science Foundation 2010.

[7] Albert Wasef, Yixin Jiang, and Xuemin Shen,‖ DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks‖, IEEE Transactions On Vehicular Technology, Vol. 59, No. 2, February 2010.

[8] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures,‖ Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)‖ Universiti Sains Malaysia. Downloaded on June 28, 2010 UTC from IEEE Xplore.

[9] Yipin Sun, Rongxing Lu, Xiaodong Lin, ―An efficient pseudonymous authentication scheme with strong privacy preservation‖, IEEE transactions on vol: 12, issue: 4, 2010.

[10] 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. [11] 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.

[12] Kejie Lu and Moayeri.N, ?A Secure VANET MAC Protocol for DSRC Application‖ ,Global Tele communications Conference, 2008. IEEE GLOBECOM 2008