International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Replacing the Time-Consuming CRL Checking Process with a Fast Revocation Checking PROCESS (EMAP) on VANET

Vimala Kulkarni
M.Tech (CSE)
GNDEC Bidar-585401
Email-Vimala26july@gmail.com

Durgesh Shastri
Asst. professor (CSE)
GNDEC Bidar-585401
Email-Durgeshshastri@gmail.com

ABSTRACT: **Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for security. In PKI system, the authentication of a received message is performed by checking the certificate of the sender included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code (HMAC), where the key used in calculating the HMAC is shared only between non revoked On-Board Units (OBUs).**

1. INTRODUCTION:

Vehicular ad hoc networks (VANETs) have promising technology for revolutionizing the transportation systems and providing 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 basic communication modes that allow OBUs to communicate with each other and with the infrastructure RSUs. Vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched A security attack on VANETs can have severe harmful or fatal consequences to legitimate users.

VANET is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates. 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, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender's signature on the received message.

According to the Dedicated Short Range Communication (DSRC) [10], which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telematic information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner 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 authentication delay resulting from checking the CRL for each received certificate.

An expedite message authentication protocol (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function. EMAP 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.

2. RELATED WORK:

In VANETs, the primary security requirements are identified as entity authentication, message integrity, non repudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements [2],[3]. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long.

In [2], use a classical PKI to provide secure and privacy preserving communications to VANETs. In this approach, each vehicle needs to preload a huge pool of anonymous certificates. The number of the loaded certificates in each

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

vehicle should be large enough to provide security and privacy preservation for a long time.

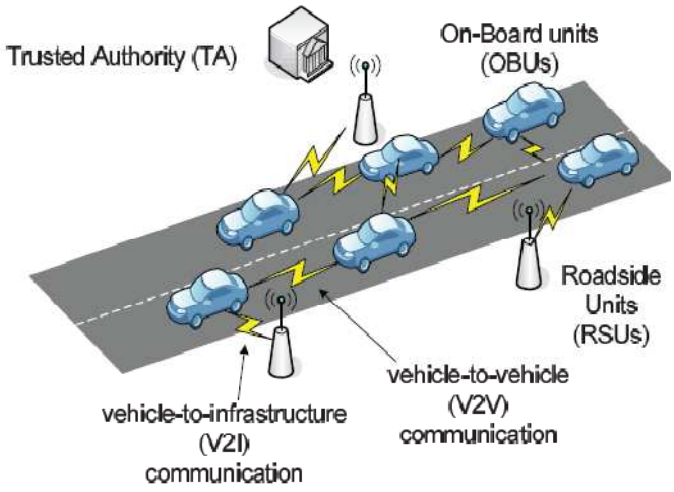
In [4], propose an efficient authentication and revocation scheme called TACK. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. The authors adopted group signature where the trusted authority acts as the group manager and the vehicles act as the group members. Upon entering a new region, each vehicle must update its certificate from the RA dedicated for that region. The vehicle sends a request signed by its group key to the RA to update its certificate, the RA verifies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (CRL).

Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. EMAP employs keyed Hash Message Authentication Code (HMAC) in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs.

3. PROPOSED SYSTEM:

- Expedite message authentication protocol (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function.
- EMAP enables OBUs to securely share and update a secret key. EMAP decrease the message loss ratio due to the message verification delay compared with the CRL.
- The messages that can be verified using EMAP within 300 msec.
- EMAP is secure and efficient.

4. SYSTEM ARCHITECTURE:



System consists:

1. A Trusted Authority-which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.
2. Roadside units (RSUs)-which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.
3. OBUs-which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

4. SEARCH ALGORITHMS:

CRL check the revocation certificates by using two algorithms they are,

Linear search algorithm, Binary search algorithm.

1. Linear Search Algorithm

   Linear search algorithm, the revocation status of a certificate is checked by comparing the certificate with each entry in the CRL. If a match occurs, the certificate is revoke otherwise it is unrevoked.

2. Binary Search Algorithm

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 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 of the sorted database. 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.

5. SECURITY ANALYSIS

a. Hash Chain Values

The values of the hash chains are continuously used in the revocation processes, and hence, the TA can consume all the hash chain values. As a result, there should be a mechanism to replace the current hash chain with a new one.

b. Resistance of forging attacks

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.

c. Forward secrecy

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

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.

d. Resistance to replay attacks

Each message of an OBU includes the current time stamp in the revocation check value check an attacker cannot record REV check at time T and replay it at a later time process as the receiving OBU compares the current time.

e. 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.

6. PERFORMANCE EVALUATION:

7.

1. Computation Complexity of Revocation Status Checking

The computation complexity of the revocation status checking process is defined as the number of operations required to check the revocation status of an OBU. Nrev used to denote number of revoked certificates in a CRL. To check the revocation status of an OBU using the linear search algorithm, an entity 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 linear search algorithm performs revocation checking for OBU. In the binary search algorithm, the certificate identity of OBU is compared to the certificate identity in the middle of the sorted CRL. The certificate identity of OBU is greater than that of the entry in the middle, and then half of the CRL with identities lower than that of OBU are discarded from the comparisons. 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.

2. Authentication Delay

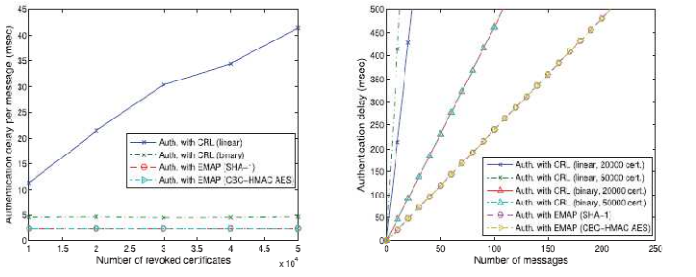
The message authentication delay with the CRL with the EMAP to check the revocation status of an OBU. The authentication of any message is performed by three consecutive phases: checking the sender's revocation status, verifying the sender's certificate, and verifying the sender's signature. For the first authentication phase which checks the revocation status of the sender, with the CRL or EMAP. EMAP uses the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC AES) and Secure Hash Algorithm1 SHA-1 as the HMAC functions.

Comparing between the authentication delay per message using EMAP, linear CRL checking process, and binary CRL checking process versus the number of the revoked certificates, where the number of the revoked certificates is indication of the CRL size. The authentication delay using the linear CRL checking process with the number of revoked certificates with the size of the CRL. Authentication delay using the binary CRL checking process is constant.

The number of revoked certificates in the conducted simulation ranges from 10,000 to 50,000 revoked certificates is corresponding to 14 to 16 comparisons.
The range of the number of the comparison operations is very small; the authentication delay is almost constant. The authentication delay using EMAP is constant and independent of the number of revoked certificates. The authentication delay using the EMAP outperforms that using the linear and binary CRL checking processes.

The linear CRL checking performs progressive search on a text containing the unsorted identities of the revoked certificates, while the binary CRL checking program performs a binary search on a text file containing the sorted identities of the revoked certificates. For the second and third authentication phases, uses Digital Signature Algorithm (DSA) to check the authenticity of the certificate and the signature of the sender.DSA is the digital signature.

The total authentication delay in msec versus the number of messages to be authenticated using EMAP and the linear and binary CRL checking processes. The CRL size increases the number of messages that can be verified within a specific period is significantly decreased using the linear CRL checking process.



(a) Authentication delay per message (b) Total authentication delay vs. the number of the received messages

7. CONCLUSIONS:

EMAP for VANETs, which expedites CRL checking process with a fast revocation checking process employing HMAC function. EMAP uses key sharing mechanism which allows an OBU to update its keys even if it previously missed some

revocation messages. EMAP can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking.

REFERENCES:

[1]. Albert Wasef and Xuemin (Sherman) Shen," IEEE, transactions on mobile computing", vol. 12, no.1, January 2013.
[2]. M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks,"J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
[3]. J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.
[4]. 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.