



## **SECURE MESSAGE AUTHENTICATION AND ACCELERATION PROTOCOL FOR MANETS**

**Nagalatha.K<sup>#1</sup>, Tharmine.N<sup>\*2</sup>**

Department of CSE, Magna College of Engineering,  
Chennai, India

<sup>1</sup>[kbavi238@outlook.com](mailto:kbavi238@outlook.com), <sup>2</sup>[ntharminie@gmail.com](mailto:ntharminie@gmail.com)

---

### **ABSTRACT**

Vehicular Ad hoc Networks (VANETs) are used in transportation systems and it is used for providing broadband communication services similar to Mobile Ad hoc Network (MANETs). Attacks are common in wireless communication. To control these attacks and provide authentication to sender and receiver Certificate Revocation List is used. Trusted authority will issue the certificate to the requested sender and receiver. This list will deny permission for unauthenticated sender and receiver. EMAP for MANET which speed message security by on demand hop by hop source authentication protocol. Secure Content Automation Protocol is used to overcome the injection attack. It is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Distributed Certificate Service sharing algorithm is used. Security Content Automation Protocol is used to overcome the injection attack. SHMAC algorithm is used to create hash code. It will improve the secure communication.

---

### **I. INTRODUCTION**

Mobile computing is human-computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deal with the characteristics and requirements of mobile applications. Mobile computing is taking a computer and all necessary files and software out into the field. "Mobile computing: being able to use a computing device even when being mobile and therefore changing location.

Mobile computing device is any device that has been created using mobile components such as mobile hardware and mobile software. Mobile computing devices are portable device capable of operating, executing and providing services and applications like a typical computing device. Mobile computing devices are also called as portable computing devices or handheld devices. Portability is one aspect of mobile computing. Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information. The main aim of the project is to secure data transmission by using certificate and

to overcome the attacks. In this Distributed Certificate Service algorithm is used to distribute certificate.

### **II. RELATED WORK**

Hubaux identify the specific issues of security and privacy challenges in VANETs, and indicate that a PKI should be well deployed to protect the transited messages and to mutually authenticate network entities. In [4], Raya and Hubaux 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 vehicle should be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle can update its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking one vehicle implies revoking the huge number of certificates loaded in it.

Studer et al. 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.[2] 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 (RL). After the RA authenticates the vehicle, it issues short life time region-based certificate. This certificate is valid only within the coverage range of the RA. It should be noted that TACK requires the RAs to wait for some time, e.g., 2 seconds, before sending the new certificate to the requesting vehicle. This renders the vehicle not able to send messages to neighboring vehicles within this period.

### III. MESSAGE AUTHENTICATION

#### A. Algorithm:

##### 1) DCS –Distributed Certificate Sharing algorithm

The initialization stage in the DCS scheme consists of two phases:

- 1) phase I, to generate the security keys necessary for the operation of the DCS scheme.
- 2) phase II, which is performed by each CA to upload the required security materials, e.g., keys, certificates.

#### Algorithm 1

- I. Select a random number  $s$  as the master key
- II. Set  $P=S$
- III. Select random numbers
- IV. Set a hash function  $H1:\{0,1\}\rightarrow G$
- V. Set a hash function  $H2:\{0,1\}\rightarrow Z$
- VI. For all CA with identity do
- VII. Upload  $Ski$ , Certificate-signing key
- VIII. End

#### Algorithm 2

- I. For all MU in the domain ,do
- II. Select random number and pseudo identity PID for MU
- III. Set Secret Key
- IV. Set Public Key
- V. Set Validity  $V_j$  period
- VI. Select minimum and maximum of  $V$ period
- VII. End

##### 2) Foreigner Certificate Delivery Algorithm

As a node enters a foreign region it initiates a foreigner certificate delivery protocol in order to obtain the foreign certificate.

##### 3) Key Generation Algorithm

It uses encryption technique and decryption technique. To generate necessary secret keys and public keys this algorithm is used.

Architecture diagram shows the relationship between different components of the system. This diagram is very important to understand the overall concept of the system.

Architecture diagram is a diagram of a system, in which the principle parts or functions are represented by blocks connected by lines that show the relationships of the blocks.

The proposed system architecture is shown in Fig.1. explains the message forwarding process and receiving process. Node 1 wants to send message to node 3. Both node approaches trusted authority for certificate. Trusted Authority will issue certificate to both the sender and receiver nodes by using DCS. Sender sends the message with certificate. Updating is done by TA every time.[5]Receiver can read the message only when it had the certificate. No other attackers can read the message.[4]In Proposed System each node in a network has different certificate. The proposed method can reduce the RL[2]. On demand hop-by-hop source authentication protocol is used. Validation time for certificate is given. 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. In addition, EMAP is free from the false positive property.

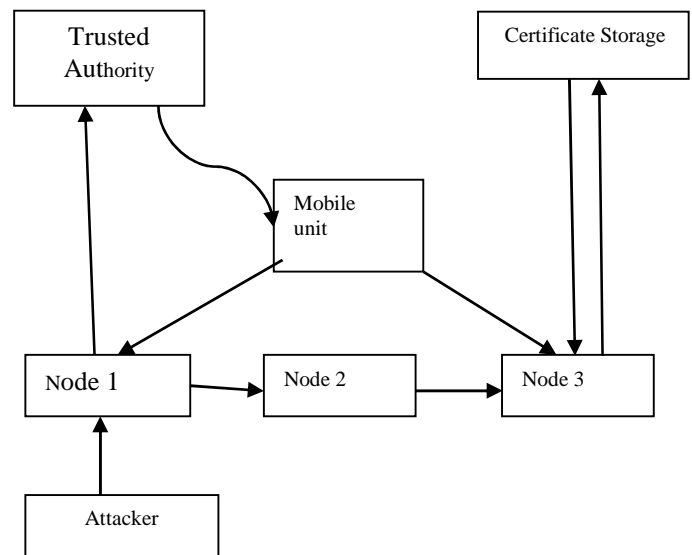


Fig. 1. System Architecture

#### Renewing the 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 as follows: After using the last value  $v$  in the current hash chain, the TA generates a new hash chain.

In the upcoming revocation messages where the new hash chain values will be used, the TA will always broadcast the last value of the old hash chain  $v$  and the current value  $v_j$  of the new hash chain. Having the last value of the old hash chain  $v$  and the current value  $v_j$  of the new hash chain, any OBU missed revocation

messages corresponding to some values of the old hash chain[1] and some values in the new hash chain can regenerate all the values.

The communication model we consider is group-oriented communication; that is, messages are addressed to all the members. For the ease of presentation, in this section, we assume that all nodes in an ad hoc network are members of a group. How this scheme can be extended for networks where not all nodes are members of a group. In Fig.2.Trusted Authority work is explained. For secure group communication, a group-wide symmetric key is used to encrypt group broadcast messages.

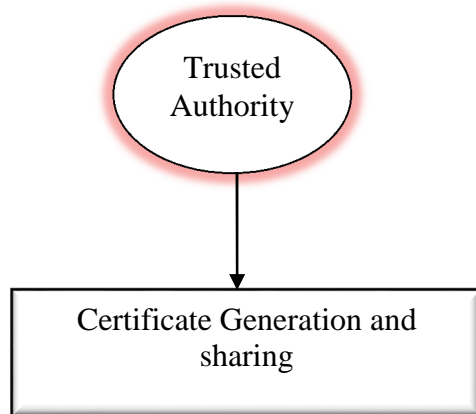


Fig. 2. Responsibility of TA

Note that using pairwise shared keys for securing group communication does not improve security in comparison to a scheme based on group keys. This is because under both schemes an adversary only needs to compromise one node to obtain the group data; moreover, if pairwise keys are used for securing group data, a node will have to perform decryptions and re-encryptions for the data packets it is forwarding. Nevertheless, if the network needs to provide pairwise keys for private communication between pairs of nodes, we can directly employ the probabilistic pairwise key establishment scheme in without making any additional security and network assumptions. Certificate is generated by TA and it is shared by using DCS algorithm [5]. The certificate consists of id, date and time of the sender, name of the sender, signature of the sender. Updating is done automatically. When the validity of the certificate expires the trusted authority will update the certificate.

We assume that the resources of a node, such as power, computational and communication capacity, and storage are relatively constrained;[10] thus a node neither can afford public-key operations nor has space for storing pre-deployed pairwise shared keys for all the nodes in the network. Assume that every node has space for storing hundreds of bytes or a few kilobytes of keying materials, depending on the security requirements. One type of such nodes is the current generation of sensor nodes

*Authentication Delay*

Compare the message authentication delay employing the CRL with that employing EMAP to check the revocation status of an OBU. As stated earlier, the authentication of any message is performed by three consecutive phases: checking the sender’s revocation status, verifying the sender’s certificate, [2] and verifying the sender’s signature. For the first authentication phase which checks the revocation status of the sender,[1] we employ either the CRL or EMAP. For EMAP, we adopt the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC AES) [8] and Secure Hash algorithm 1 SHA-1 [9] as the HMAC functions. We consider the PID of MBU and the time stamp  $\delta T_{stamp}$  having equal lengths of 8 bytes. We adopt the Crypto++ library for calculating the delay of the HMAC functions, where it is compiled on Intel Core2Duo 2 GHz machine. The delay incurred by using CBC-HMAC AES and SHA-1 to calculate the revocation check  $REV_{check} \frac{1}{4} HMACK_g;PID_u kT_{stamp}^b$  is 0.23 and 0.42 sec, respectively. Also, we have simulated the linear and binary CRL checking process. The linear CRL checking program performs progressive search on a text file containing the unsorted[3] 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, we employ Secure Content Automation Protocol(SCAP)) to check the authenticity of the certificate and the signature of the sender. SCAP is the digital signature method chosen by the WAVE standard. In SCAP, a signature verification takes  $2T_{mul}$ , where  $T_{mul}$  denotes the time required to perform a point multiplication of sending and receiving. Consequently, the verification of a certificate [6] and message signature takes  $4T_{mul}$ .

A comparison between the authentication delay per message using EMAP, linear CRL checking process, and binary CRL checking process versus the number of the revoked certificates,[7] where the number of the revoked certificates is an indication of the CRL size. It can be seen that the authentication delay using the linear CRL checking process increases with the number of revoked certificates, i.e., with the size of the CRL. Also, the authentication delay using the binary CRL checking process is almost constant.

This can be explained as follows: the number of revoked certificates in the conducted simulation ranges from 10,000 to 50,000 revoked certificates; this is, respectively, corresponding to 14 to 16 comparison operations. Since 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. Moreover, the authentication delay using the EMAP outperforms that using the linear and binary CRL checking processes. For example, the authentication delay per message using the linear CRL checking process, the binary CRL checking process, and EMAP (SHMAC-1) for a CRL.

#### **IV. CONCLUSION**

In VANET and MANET data transmission will be the same. Secure message sending is a tedious process. For achieving secure message sending EMAP protocol is used. Distributed Certificate Sharing algorithm and Secure Content Automation Protocol is also for secure message transmission. Data transmission is secure. So message loss ratio gets reduced. Distributed Certificate Service Algorithm is used to share the certificate. Certificate Revocation List checking process thereby reduced. Both sender and receiver authentication is checked to achieve secure communication. Message can be send to the receiver in a secure way. There are some problems that need to be investigated in the future. Attackers can attack the node. Upcoming research is about the certificate distribution to nodes will be done. Distributed Certificate Sharing Algorithm is used to share the certificate. Data transmission causes attacks in message. It also causes attackers to involve in the message transfer. So, in future how to overcome the attackers will be discuss. And also propose to share the certificate without Distributed Certificate Service algorithm.

#### **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, and J. Su, "An Efficient Pseudonymous 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, 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 Internet working, 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] J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004