International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 43-47
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

SECURE MESSAGE AUTHENTICATION AND ACCELERATION PROTOCOL FOR MANETS

Nagalatha.K [#1], Tharmine.N[*2]
[#] *pg Scholar, Department of CSE, Magna College of Engineering, Chennai, India*
[1] kbavi238@outlook.com [2] ntharminie@gmail.com
[*] *Head of the Department, Magna College of Engineering, Chennai, India*

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.

1. 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.

2. 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 messagesand 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 thisapproach, revoking one vehicle implies revoking the hugenumber of certificates loaded in it.

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 43-47
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

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 wherethe trusted authority acts as the group manager and the vehicles act as the group members.[2] Upon entering a newregion, each vehicle must update its certificate from the RAdedicated for that region. The vehicle sends a requestsigned by its group key to the RA to update its certificate. The RA verifies the group signature of the vehicle andensures 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 validonly within the coverage range of the RA. It should benoted that TACK requires the RAs to wait for some time,e.g., 2 seconds, before sending the new certificate to therequesting vehicle. This renders the vehicle not able to sendmessages to neighboring vehicles within this period.

3. 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}->G
V. Set a hash function H2:{0,1}->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 Vj period
VI. Select minimum and maximum of Vperiod
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 partsor 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.

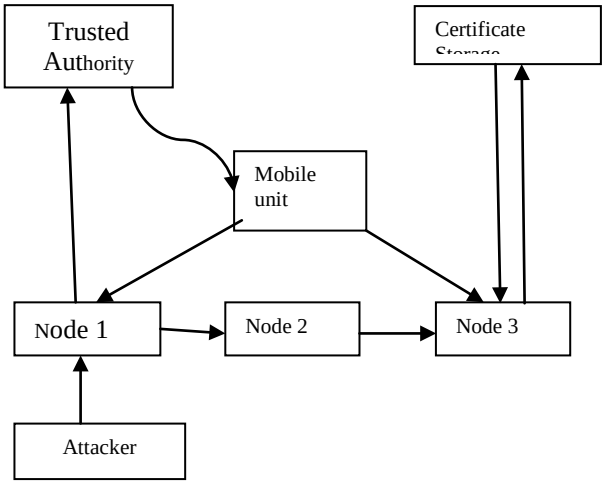

Figure. 1. System Architecture

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 43-47
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

RenewingtheHash Chain Values

Thevalues ofthehash chains arecontinuously used inthe revocationprocesses,andhence,theTAcanconsumeallthe hashchainvalues.

Asaresult, thereshouldbeamechanism toreplace thecurrenthashchainwithanewoneasfollows: After using the lastvalue vinthe currenthash chain, theTAgeneratesanew hash chain.

In theupcomingrevocationmessageswherethe new hash chain values will beused, the TAwill alwaysbroadcastthe last value oftheoldhashchainvand thecurrentvalue $v_j$of the new hash chain. Havingthe last value ofthe old hash chain vand thecurrentvalue $v_j$ofthenew hash chain, any OBU missed revocation messages corresponding to some values ofthe old hash chain[1]and some values inthe newhashchaincanregenerateallthevalues.

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.

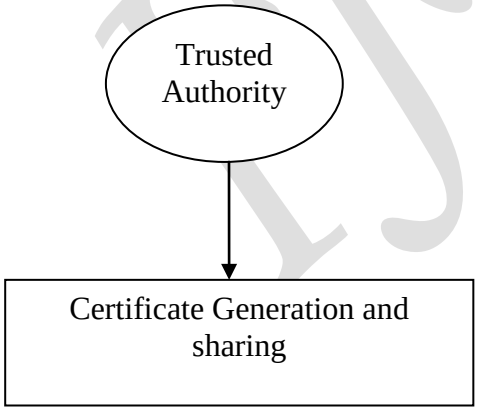

Figure. 2. Responsibility of TA

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

Comparethe message authentication delay employing theCRLwiththatemployingEMAPtocheckthe revocation status ofanOBU.Asstatedearlier,theauthenticationofany messageisperformedbythreeconsecutivephases: checking thesender's revocation status, verifyingthesender's certificate, [2] and verifyingthesender'ssignature.Forthefirst authenticationphase which checks therevocationstatus of thesender,[1]weemployeither theCRLorEMAP.ForEMAP, weadopt theCipherBlockChainingAdvancedEncryption Standard(CBC-HMAC AES)[8]and Secure Hash algorithm1SHA-1[9]astheHMACfunctions.Weconsiderthe PID of MBU and the time stamp$\eth T_{stamp}\flat$ havingequal lengthsof8bytes.

Weadoptthe Crypto++library for calculatingthe delay ofthe HMAC functions,whereitis compiledon Intel Core2Duo2GHz machine.The delay incurredbyusing CBC-HMAC AESandSHA-1tocalculate therevocationcheckREV_{check}¼$HMAC_{K_g}$; $\flat ID_u kT_{stamp}\flat\flat$ is0.23and 0:42sec,respectively.Also,wehave simulated the linear and binaryCRL checking process.Thelinear CRLchecking programperformsprogressivesearch onatextfile containingtheunsorted[3] identitiesoftherevokedcertificates, while thebinary

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 43-47
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

CRLchecking programperforms abinary search onatext filecontainingthe sortedidentitiesofthe revokedcertificates.

Forthesecond andthirdauthentication phases,we employSecure Content Automation Protocol(SCAP)) to check the authenticity of the certificate and the signatureofthe sender.SCAP isthe digital signature methodchosen bytheWAVEstandard.In SCAP, a signature verificationtakes $2T_{mul}$,whereT_{mul}denotesthetimerequiredtoperformapoint multiplication of sending and receiving. Consequently,the verificationof a certificate [6]and messagesignaturetakes$4T_{mul}$.

Acomparisonbetweenthe authentication delay per message using EMAP, linear CRL checking process, and binary CRL checkingprocess versus the numberofthe revokedcertificates,[7]wherethe number of the revokedcertificatesisanindicationofthe CRLsize.It can beseen that the authenticationdelay using the linear CRL checking process increases with the number of revoked certificates,i.e., with the size of the CRL. Also, the authenticationdelay using the binaryCRL checkingprocess isalmost constant.

Thiscanbeexplainedasfollows: thenumber ofrevokedcertificates intheconducted simulationrangesfrom10,000to50,000revokedcertificates;thisis, respectively, correspondingto14to16comparison operations.Sincethe range ofthe numberofthe comparison operationsis very small, the authenticationdelay is almost constant.The authenticationdelay using EMAPis constantand independentofthenumber ofrevoked certificates.Moreover,the authenticationdelay using the EMAP outperformsthat using the linear and binary CRL checking processes.Forexample,the authenticationdelay per messageusing the linear CRL checking process, the binaryCRL checking process, and EMAP (SHMAC-1) for a CRL.

4. 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 senderand 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 thecertificate distribution to nodes will be done. Distributed Certificate Sharing Algorithm is used to share the certificate. Data transmission causes attacksin message. It also causes attackers to involve in the message transfer. So, in future how to overcome theattackers 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.

International Journal of Power Control and Computation(IJPCSC)
Vol 6. No.1 – Jan-March 2014 Pp. 43-47
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-268X

[9] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for "Wireless Access in Vehicular Environments" - Security Services for Applications andManagement 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