International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Secure Data Transmission in VANETs

Mrs. Bhuvaneswari. M. S.
Assistant Professor, Computer Science and Engineering,
Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India

ABSTRACT

A number of technical problems are arising with the widespread distribution of vehicular ad-hoc networks. Privacy and authentication mechanisms are of major concern. If security is not integrated with the system, it leads to anti-social and criminal behavior and endanger the benefits of the deployment of VANETs. A suitable authentication procedure is to implement the Public-Key Infrastructure (PKI) , where each node in the VANET has a set of authentic certificates. Traditional PKI systems makes use of Certificate Revocation Lists to check the validity of the certificate and thereby the signature. In this paper, a new method that replaces CRL with revocation checking process is proposed. When a node is found to be illegitimate or compromised, it is revoked by generating a revocation message and broadcasting to all other nodes in the network. The time consuming CRL checking need not be done for each message received. The method proves to be faster in authenticating messages securely. This is suitable not only for VANETs, but for any other network that deploys PKI.

Keywords: *Cryptography, certificate revocation, security, VANET*

I. INTRODUCTION

The vehicular adhoc network is a special kind of mobile adhoc networks. But unlike many adhoc networks, VANETs also includes Road Side Units (RSU) which are stationary along the roads and on-board units (OBU) which are the vehicles on the roads. Taking advantage of this hybrid architecture, the VANET opens way for road safety and traffic management applications. Prior to the implementation of these applications privacy and security measures have to be put into practice. Without this, an adversary in the network can bogus messages, mislead the drivers, over utilize the pathways on road and even cause accidents which can be sometimes fatal. Thus, some means of authentication mechanism is necessary for VANETs.

A well known authentication is to deploy a Public Key Infrastructure (PKI) and to use Certificate Revocation Lists (CRL) to check for revoked certificates. In PKI, each node of the network has an authentic certificate and it has to digitally sign each message before it is broadcasted or sent to a specific node. A CRL issued by a Trusted Authority (TA) consists of all the revoked certificates. In PKI, when a message is received, first the CRL is checked to verify whether the sender's certificate is included in it, and then the sender's certificate and signature is verified. Checking the CRL for the revocation status of the sender may take a long time depending on the CRL size and the search algorithm used to traverse the list. The CRL size is usually large due to the size of VANETs. Also to mislead attackers, a single OBU has a number of anonymous certificates and periodically change them. Hence, revoking an OBU results in revoking a large number of certificates and it adds up to the size.

According to the Dedicated Short Range Communication (DSRC), each OBU has to broadcast a message every 300 ms regarding its location, velocity and other related information. Thus, each OBU may receive a large number of messages every 300 ms, and there is a need of checking the certificate

of each such OBU. Checking a large CRL everytime when a message is received may lead to delay in processing the messages. The delay may result in missing of some life safety messages on roads. Hence, the ability to check the CRL in short time duration remains a challenge in VANETs.

To ensure reliable operation of VANETs and to increase the receipt of useful messages on time, the OBUs should check the revocation status of each certificate in a timely manner. Most of the existing works implements the authentication with CRLs. The proposed work replaces the CRL checking process with an efficient revocation checking process. The method can be integrated into any network that implements PKI.

2. RELATED WORK

The PKI is the most efficient techniques to achieve authentication and security. The method employs CRL to manage the revoked certificates. Since the CRL certificates are usually large, the time for checking the revocation status and then the processing of messages takes a longer time.

The distributed certificate service (DCS) [3] is a widely followed method to decrease revocation cost. Here vehicles can update their pseudonymous certificate sets from the certificate issuer by vehicle-to-RSU (V2R) communication on the road. The CRL that is broadcasted in a region can decrease owing to the smaller geographic region that it covers. However, the CRL size still depends on the number of pseudonymous certificates held by the revoked vehicles. Also, the certificate updating overhead becomes a heavy burden for the RSUs.

The authors of [4] proposed an efficient pseudonymous authentication scheme with strong privacy preservation (PASS) that allows a vehicle to store a large set of pseudonymous certificates which it has to obtain in prior from the trusted authority (TA). Based on the proxy re-signature cryptography technology, the vehicle requires only the re-signature keys from an RSU and re-sign numbers of the certificates issued by the TA to be the same as those issued by the RSU itself. This way, the service overhead is independent of the number of updated certificates. But the overhead may be high during the initial stages and some messages may be dropped due that.

In [5], Studer et al. implements a revocation scheme called TACK. The method uses a hierarchy system architecture which has a central trusted authority and regional authorities (RAs) which are distributed throughout the network. Group signature is used where the trusted authority acts as the group manager and the vehicles in that region act as the group members. When a vehicle enters a new region, each vehicle has to update its certificate from the RA of that region. Once the RA ensures that the vehicle is authenticated, it issues short lifetime certificate. This certificate is valid only within the coverage range of the RA. TACK takes some time, eg. 2 seconds to issue a new certificate to the requesting vehicle. This makes the vehicles unable to send messages to the neighboring vehicles within this period, which means the approach is not suitable for safety applications.

An optimized method for organizing, storing and exchanging CRL information is proposed in [6]. The CA can revoke a vehicle's certificates with a single addition to the CRL, thus the size of the CRL or CRL updates is minimized. Certificate identifiers are stored in Bloom filters, which have a constant cost in terms of searching and storage.

In [7] a variant of key pre-distribution scheme is proposed for Distributed Sensor Network (DSN). Here it is considered that the probability of node which compromises in different deployment regions is known apriori. The cluster based hierarchical topology aids to simplify the design of key management scheme in sensor networks. With apriori knowledge, an effective and scalable security mechanism is implemented which is also resilient to various network attacks.

3. SYSTEM MODEL

The system model which is considered in our project consists of the following components :

- A *Trusted Authority(TA)* generates anonymous certificates and key sets to all vehicles in the network.
- *Road Side Units(RSU)* which are distributed in the network, communicates securely with the TA.

On Board Units(OBUs) are embedded in vehicles. They communicate with the other vehicles or with the infrastructure nodes such as RSUs.

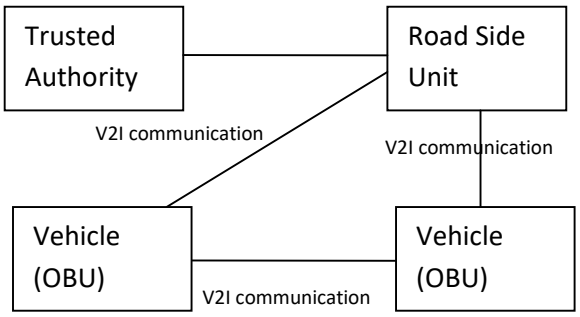

Figure 1 : System model

Figure 1 gives a view of our system model. Every OBU in the vehicles has a Hardware Security Module (HSM). The HSM is a tamper-resistant module. It stores the security keys, certificates and all the security related information and performs the cryptographic operations such as signing messages and verifying the received certificates of the messages. It is assumed that the revoked OBUs do not collide with the unrevoked counterparts and that the TA instantly detects compromised OBU to revoke it.

The aim of the project is to achieve the following security measures.

1) *Authentication*: This ensures that the messages received by an OBU are from legal members and that the contents of the message remains unaltered. Entity authentication prevents illegitimate users from injecting bogus messages into the network. Data authentication ensures that the messages are original and are not replayed or altered.

2) *Nonrepudiation*: This ensures that no entity denies the messages sent by it to others. This gives a high level of liability in the network and is useful for accident investigations. A vehicle involved in a crash should pay for the cause.

3) *Privacy:* This is concerned with the prevention of disclosing the original identity of vehicles and the location information. Pseudonymous identities should not be related with the real identities of vehicles.

4) Conditional anonymity: This ensures that only the TA can relate the pseudonymous identities to the corresponding real vehicles. Other entities could neither know the real identities nor correlate the messages sent to the sending vehicles.

5) Identity Revocation: This is done for removing an unexpired membership of a vehicle from the network. This defense mechanism is essential against faulty and compromised vehicles and improves the trust of the network.

When a vehicle is revoked, messages from that corresponding vehicle will be ignored by the other vehicles. Implementing revocation with Certificate Revocation List(CRL) poses many problems. Distribution of CRL across the wide spread network is the fundamental issue. Also, it has to be delivered in a timely manner and the problem magnifies as the number of vehicle increases. Another issue is that the CRL distribution should incur low overhead within the available bandwidth constraints.

The incorporation of security measures in VANETs mandates that each vehicle has an identity and a set of cryptographic information and tools. Pseudonymity is achieved when each vehicle has a set of pseudonymous certificates and keys and the vehicle uses these pseudonyms alternately in different periods of time. Thus the real identity of vehicles is concealed and that the messages signed by the same vehicle cannot be linked by means of signatures.

4. Implementation

Initialization of the system loads the following cryptographic material in TA and each OBU.

The TA has

- A secret key set U_s containing the secret keys of all OBUs
- The corresponding public key set U_p
- A master key s and corresponding public key P
- The secret key K shared over the network
- Hash functions and parameters

Also, each OBU has

- A set of anonymous certificates
- Its own secret key and public key
- The secret key K
- Hash functions and parameters

The cryptographic model that implemented is a Public Key Infrastructure(PKI). Each OBU has a set of anonymous certificates to have a secure communication with the legitimate nodes of the network. The secret key of a OBU_u and the corresponding public key which is included in the $cert_u$ are used to sign and verify the messages that are in transit. The set of secret and public keys are used for the generation of shared secret key K that is to be shared securely between unrevoked OBUs of the network.

4.1 Message authentication

4.1.1 Message signing

When any OBU wants to send a message, it encrypts the message with its secret key.Let the encrypted message be denoted as M. Then the revocation check REV_{check} is calculated using a hash function. The final message that is sent by the OBU_u is
$(M||T_{stamp}||cert_u||signature_u||REV_{check})$
where || denotes the concatenation operation.

4.1.2 Message verification

An OBU receiving the message in the above said format verifies it in the following sequence of steps as given in the flow below in Figure 2. Verification includes checking the validity of T_{stamp} to ensure that the message is not old. The REV_{check} is verified to check for the correctness of shared secret key K.

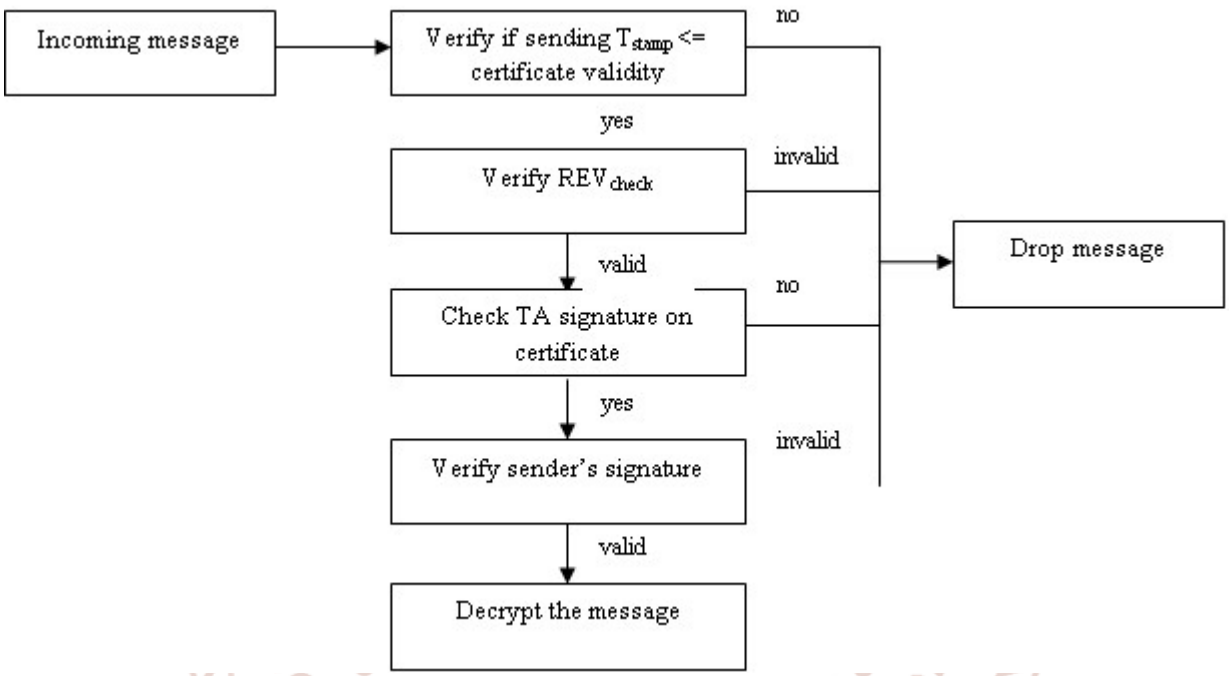

Figure 2 : Message Verification

The TA and OBU's signature are verified in the received certificate to check for the authenticity of the message. If all the above credentials are valid then the received message is decrypted to obtain the original information.

4.2 Revocation

The revocation is triggered by the TA when an OBU_u has to be revoked from the network. The certificates of that particular OBU must be revoked. The secret and public key sets are revoked. The current shared secret key K is considered revoked and a new secret key is generated and securely distributed to all the non revoked OBUs in the network. Also each non revoked OBU has to securely update the compromised key sets.

The proposed work and security features are added to the source code of ns2 and the following observations are made.

- The work uses a rekeying mechanism that updates keys that were compromised so far.
- The PKI module implemented can be integrated into any network that needs security other than VANET.

5. Conclusion

The proposed work will expedite message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process using hash function. The work uses a novel key sharing mechanism which allows an OBU to update its compromised keys. The keys are up-to-date at any time of conversation. Furthermore, it is

resistant to common attacks and out-performs several other authentication techniques employing the conventional CRL. The proposed work thus adds up to the security of the messages that are transmitted, also it takes lesser time to verify the authenticity and confidentiality. Our future work will aim to accelerate message signature and certificate generation process.

6. References

1) Albert Wasef and Xuemin Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Trans. Mobile Computing, vol. 12, no. 1, pp. 78-89, Jan. 2013.

2) 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.

3) 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) 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.

5) 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.

6) M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

7) L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

8) 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.

9) J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

10) H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 197-213, 2003.

11) L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

12) N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography," Designs, Codes and Cryptography, vol. 19, no. 2, pp. 173-193, Mar. 2000.

13) L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772, 1981.

14) T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, Introduction to Algorithms. MIT, 2001.

15) S. Frankel, R. Glenn, and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec," IETF RFC 3602, Sept. 2003.

16) D. Eastlake and P. Jones, "US Secure Hash Algorithm 1 (SHA1)," IETF RFC 3174, Sept. 2001.

17) "Crypto++ Library 5.5.2," http://www.cryptopp.com, 2012.

18) D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Int'l J. Information Security, vol. 1, no. 1, pp. 36-63, 2001.

19) C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM, pp. 246-250, 2008