EMAP: Expedite Message Authentication Protocol For Vehicular Ad Hoc Networks

Shwetha M
M.tech 1st year,CSE
S J B Institute of Technology
Banglore,India
Shwetha29muniraju@gmail.com

Mrs. Archana R. A
Asst Prof,CSE Dept
S J B Institute of Technology
Banglore,India

Abstract: Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose an 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, where the key used in calculating the HMAC is shared only between non revoked On-Board Units (OBUs).In addition, EMAP uses a novel probabilistic key distribution, which enables non revoked OBUs to securely share and update a secret key. EMAP 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, EMAP is demonstrated to be secure and efficient.

1. INTRODUCTION

VEHICULAR ad hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VA-NETs 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, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs. Since 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. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs 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. The first part of the authentication, which checks the revocation status of the sender in a CRL, may incur long delay depending on the CRL size and the employed mechanism for searching the CRL. The CRL size in VANETs is expected to be large for the following reasons: 1) To preserve the privacy of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external eavesdropper each OBU should be preloaded with a set of anonymous digital certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size. 2) The scale of VANET is very large. According to the United States Bureau of Transit Statistics, there are approximately 251 million OBUs in the Unites States in 2006. Since the number of the OBUs is huge and each OBU has a set of certificates, the CRL size will increase dramatically if only a small portion of the OBUs is revoked. To have an idea of how large the CRL size can be, consider the case where only 100 OBUs are revoked, and each OBU has 25,000 certificates. In this case, the CRL contains 2.5 million revoked certificates. According to the employed mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard does not state that either a non optimized search algorithm, e.g., linear search, or some sort of optimized search algorithm such as binary search, will be used for searching a CRL.

We consider both non optimized and optimized search algorithms. According to the Dedicated Short Rang Communication (DSRC) which is part of the WAVE standard, each OBU has to broadcast a message every 300 m sec about its location, velocity, and other information. In such scenario, each OBU may receive a large number of messages every 300 m sec, and it has to check the current

IJERT

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 and 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 existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. In this paper, we introduce 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.

A few basic ideas transcend all these VC security architectures: they all build on top of a currently accepted networking protocol stack, with primary security requirements being message authentication, integrity, and, as well as protection of private user information. They all rely on a Certification Authority (CA), and public key cryptography to protect V2V and V2I messages, with each node(VC-equipped vehicle or RSU) are registered one CA and can participate in the network operation. Of course, it is also clear that a node equipped with a certificate is not necessarily y complying with the implemented protocols, neither is it operating correctly (e.g., it may simply inject faulty data). A line of defence against faulty or compromised nodes is crucial for the trustworthiness of the VC system.

A well-understood method is to defend the system is to evict the misbehaving nodes. In the context of current secure VC architectures, revocation of the certificate of such nodes is an appropriate approach that has been utilized in other types of systems. Moreover, revocation can be useful for other reasons; for example, credentials of stolen vehicles can also be revoked. Once revoked, messages from that node will be ignored by system nodes.

We propose a collaboration scheme between regional CAs that allows CRLs to contain only regional revocation information; a low-rate, randomized method for RSUs to broadcast the CRL; the use of erasure codes to enhance the robustness and flexibility of the CRL distribution. Our scheme does not require any communication and cooperation between RSU on the CRL distribution task, and minimizes the CA-RSU and vehicle-CA-RSU interactions. Our results show that allocating a bandwidth of few K Bytes/s to the CRL distribution broadcast is sufficient for a very high percentage of (practically, all) vehicles to receive securely the complete CRL within minutes. In the rest of the paper, we provide the system model in followed by a more precise problem statement and solution overview. The detailed description of our scheme component is provided and an analytical and simulations-based evaluation of our scheme.

Information received from corrupted nodes should be disregarded or not trusted by legitimate vehicles, otherwise, a malicious vehicle could, for example, obtain a less congested route for itself by over stating the number of vehicles on its desired roadway. As a second example, a corrupted node could trigger erroneous driver warnings to be displayed in other vehicles by falsifying its position information.

2. SYSTEM DESIGN AND ANALYSIS

System Architecture

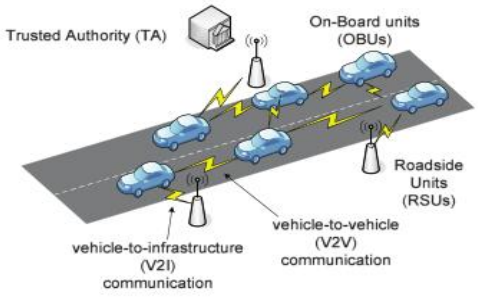


Figure1: The system architecture

Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure

Vehicle-to-vehicle communication and Vehicle to Infrastructure are two communication modes. In this Module, the two basic communication modes, which respectively allow OBUs to communicate with each other and with the infrastructure RSUs. Since 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. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice. A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificate. 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 certificate. In a PKI system, the authentication of any message is performed by checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender' certificate, and finally verifying the sender's signature on the received message.

IJERT

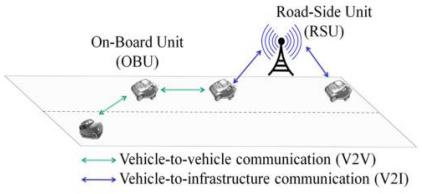


Figure 2: Elements of VANETs

System architecture consists of components are

1. On-Board Unit(OBU):

On-Board Units which are embedded in vehicles. Each OBU has a long-term unique identity. OBUs mainly communicate with each other for sharing local traffic information, and with the RSUs for updating the short time certificates. Digital maps are available for the OBUs. It provides the street-level map, the communication coverage of RSUs and the traffic statistics such as vehicle speed on roads, and traffic signal schedule at intersections.

According to the WAVE standard , each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the security materials, e.g., secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. We consider that legitimate OBUs cannot collude with the revoked OBUs as it is difficult for legitimate OBUs to extract their security materials from their HSMs. Finally, we consider that a compromised OBU is instantly detected by TA.

2. Roadside units(RUS):

RSUs issue short-time certificates for the OBUs. RSUs are erected at intersections for the considerations of power and management. RSUs use the same communication technology and the deployment cost is constant at any intersections. RSUs connect with TA by wired links, and act as certificate proxies of TA. An RSU can issue short-time certificates for the OBUs with valid membership.

3. Trusted Authority:

Trusted Authority which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. TA is in charge of the registration of the RSUs and OBUs. TA can reveal the real OBU identity of a safety message and publishes the CRL periodically to the RSUs. Moreover, TA can be a road authority, such as the government. It has the basic information about streets and traffic statistics, and proposes the RSUs deployment plan according to the trade off between the requirements of most OBUs and the investment budget.

3. PUBLIC KEY INFRASTRUCTURE

The main components of a public key infrastructure are the users, the certificates, and the certificate authority (CA). Private keys are used to cryptographically sign messages that can be authenticated using the matching public key. Public key certificates are used for authentication to prevent attackers from causing harm. Cryptographically signed messages also provide message integrity; any changes to the message will cause signature verification to fail. Certificates normally have a time period for which they are valid, defined by a start time and an end time, or simply a life time.The main components of a public key infrastructure are the users, the certificates, and the certificate authority (CA). Private keys are used to cryptographically sign messages that can be authenticated using the matching public key. Public key certificates are used for authentication to prevent attackers from causing harm. Cryptographically signed messages also provide message integrity; any changes to the message will cause signature verification to fail. Certificates normally have a time period for which they are valid, defined by a start time and an end time, or simply a life time.

3.1 Certificates

Certificates are ―data structures that bind public key values to subjects . In other words, a certificate is proof that a public key belongs to a certain user. The certificate authority (CA) generates certificates upon a request from an individual user. The CA is a trusted source that cryptographically signs a user's public key, thus creating a certificate for the user. The user must trust at least one CA in order to validate certificates; thus, a user that places trust in the CA can also trust that objects signed by the CA are trustworthy. Researchers have discussed several issues pertaining to the trade-offs between privacy (confidentiality) and authenticity. Pseudonyms have been proposed as a method to handle the opposing requirements of non-anonymous authentication and end-user anonymity. A pseudonym is a short-lifetime certificate that does not contain identity-linking information. Users request pseudonyms from a CA using a longer-lifetime certificate, such as the electronic chassis number or electronic license plate. CA that generated the pseudonym holds the linking information in escrow in case of a legal necessity for proving the identity of the pseudonym owner. Changing pseudonyms periodically greatly increases end-user anonymity while still maintaining a reliable means of authentication includes the specification for the use of non-anonymous authentication using certificates and elliptic curve digital signature algorithms (ECDSA), certificate revocation lists, and end-user anonymity.Every certificate issued by a CA must have a certificate identification number to identify the certificate. The CA generates the certificate identification number by calculating the SHA-256 hash of the certificate. The resulting size of the certificate identification number can be either 64 or 80 bits .

Using 224-bit ECDSA for OBUs, the current size of an OBU signing certificate is 125 bytes, 29 bytes of which are the OBU public key. The size of the private key associated with an end-user certificate is 28 bytes. For every pseudonym stored, the certificate and private key must be stored; therefore, 153 bytes of memory are required in the OBU to store the certificate and the private key associated with that certificate. Table 2 summarizes these numbers. The size of the pseudonyms is important because an OBU

IJERT

will change pseudonyms frequently to prevent others from tracking the vehicle's location.

3.2 Threat Model to Privacy in VANET

One threat to privacy in VANETs is tracking a vehicle based on its radio transmissions. Vehicles will broadcast beacons, safety messages, and other application messages regularly. Any other vehicle in range is capable of storing these messages due to the broadcast nature of WAVE. The beacons and safety messages will require cryptographic signing of the message to prove authenticity and membership in the VANET. The identification sent with signed messages, known as the certificate, is enough to link messages sent by the same vehicle thus, while certificates provide a means for authentication, they do not provide privacy when the same certificate is used for a prolonged period, this the need for pseudonyms in VANETs.

4 . CERTIFICATE REVOCATION LIST

Introduction to CRL

When a node's certificate is identified for revocation, the currently used certificate must be revoked along with every pseudonym stored in that OBU. This assumes that whatever caused the current certificate to be revoked will cause future uses of certificates by the same node to also trigger a revocation. Examples that would cause this event include a malfunction in the vehicle's sensors causing erroneous warning messages to other vehicles, or malicious activity by a given vehicle. By revoking all of the pseudonyms, further damage is avoided. The information regarding which certificates are no longer valid, i.e., revoked, is sent out in a certificate revocation list (CRL). The size of the CRL is directly proportional to the revocation rate, the number of nodes in the system, and, for VANETs, the number of pseudonyms used by each vehicle. In 1609.2, the CRL is referred to as the WAVECRL. Actual WAVECRL sizes have been discussed briefly in the literature. Several authors have discussed issues with managing pseudonyms, certificate life-time, and certificate revocation methods, such as Escher, in [35], examines revocation in an ad hoc network, but only looks at 100,000 nodes with an assumed 10% annual revocation rate. Also, his work does not take into account VANET conditions.

The literature makes the assertion that the security of the VANET is improved if participants receive timely revocation information, most notably by distributing the CRL as quickly as possible. The common theme among discussed methods to reduce distribution time is to reduce the size of the CRL, since smaller files can be distributed more quickly. Methods for reducing the CRL file size include limiting the cases where revocation is needed and using fewer pseudonyms per vehicle.

A certificate revocation list (CRL) is a list of certificate identification numbers that are no longer valid prior to the expiration date of the certificate. The lists are generated and issued by either the actual CA or an entity authorized by the CA. The CRL is cryptographically signed by the CA or authorized entity, so the communication channel and storage medium do not need to be secure since any modification to the CRL during transmission or by other nodes will result in signature validation failure. The CRL is published publicly at a time interval specified by the particular revocation policy. This time interval may be regular, such as hourly, weekly, or monthly, or it may be based on measures other than time, such as a certain number of revocations. The information contained in a CRL includes the expiration date of the CRL, the next time the CRL will be published, and the list of revoked certificates. Each user maintains the CRL and checks the list as part of the message verification process.

CRL Size

Let Neq be the total number of equipped vehicles in the region that the CRL needs to cover, pr the average proportion of certificates revoked per time period e.g. day,and Lf the life time of a certificate in times periods. Let N CRL be the number of certificates in the CRL. NCRL is the number of non expired certificates that were revoked. The average number of revoked certificate each time period is N eq∗ pr. We assume that a revoked certificate has equal probability to become revoked at any time period of its life time i ∈ {1,...,Lf}. When a certificate is revoked at time period of its life time, it will stay in the CRL for Lf− i time periods. Thus, the expected time a revoked certificate stays in the CRL is E(Lf− i) =

Lf/2.From the above two equations, the expectation of NCRLIs E(NCRL) = (Nek∗ pr) ∗Lf/2. We consider the CRL to consist of the identifiers of all the revoked certificates plus a security overhead of 500 Bytes. We expect that 4 Byte identifiers should be sufficient for vehicles, as this the current size of the IP space nowadays. Therefore, the expected CRL size is E(SCRL) = E(NCRL) ∗ 4Bytes + 1KBytes.The table in Fig. 1 from the National Insurance Crime Bureau gives numbers about the motor vehicle theft .U.S. metropolitan areas in 2005, ranked by the rate of vehicle theft reported per 100,000 people based on the 2000Census, and the size of the CRL that would result from including the identifiers of all these vehicles in the CRL. In the early deployment phase, only a ratio r < 100% of vehicles will be equipped, and thus the size of the CRL. E(SCRL). According to FBI's Uniform Crime Reports, motor vehicles were reported stolen. Inserting all the identifiers of these vehicles would result of a CRL of5MBytes. The coordination between regional CAs makes it possible to distribute regional CRLs.

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

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. Algorithm:

1. *Linear Search Algorithm:*

In the 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 revoked and vice versa.

2. Binary Search Algorithm:

The binary search algorithm works only on sorted lists. Consequently, upon receiving a new CRL, each OBU has to maintain a sorted (with respect to the certificate identity) database of the revoked certificate 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 (which in this case will be the median 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 finish without a match which means that the certificate is unrevoked.

3.Lookup Hash Tables

In this approach, the set of all possible certificates is mapped using a hash function into a table of n entries. To check the revocation status of a certificate, the hash of the certificate's identity is the index of the entry in the look up table which should be checked to determine the revocation status of the certificate. If nil is found in that entry, the certificate under consideration is unrevoked and vice versa. Since VANETs scale is very large and each OBU has a set of certificates, the size of U will be huge compared to the size of the lookup table. Consequently, the probability of hash collisions will be high, which directly translates to a high probability of false positives. Here, a false positive means that the certificate of an innocent OBU is falsely considered revoked which results in rejecting all the messages containing the certificate of that OBU. The rejected messages may include a warning from dangerous situations. Hence, rejecting these messages may deprive the recipient OBU from taking the appropriate counter measures ensure its safety. Accordingly, lookup hash tables may not be practical for VANETs. Hence, lookup hash tables will not be considered in this paper. It should be noted that hash functions which map an input to one entry of possible entries used in the lookup tables, are different from cryptographic hash functions which map an input to a unique output. Throughout the rest of the paper, the considered hash functions are cryptographic hash functions.

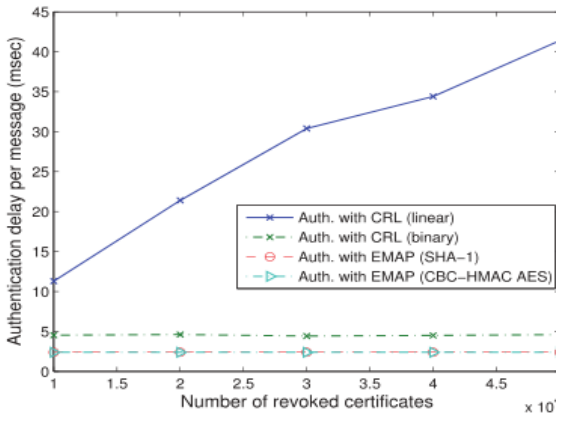
7.Performance Evaluation

1. Complexity of Revocation Status Checking

We are interested in the computation complexity of the revocation status checking process which is defined as the number of comparison operations required to check the revocation status of an OBU. Let N denote the total number of revoked certificates in a CRL. To check the revocation status of an OBU using the linear search algorithm, an entity has to compare the certificate identity of OBU with every certificate of the certificates in the CRL, i.e., the entity performs one-to-one checking process. Consequently, the computation complexity of employing the linear search algorithm to perform a revocation status checking for an OBU. In the binary search algorithm, the certificate identity of OBU is compared to the certificate identity in the middle of the sorted CRL. If the certificate identity of OBU is greater than that of the entry in the middle, then half of the CRL with identities lower than that of OBU are discarded from the upcoming comparisons. If the 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.

2. Authentication Delay

We 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, and verifying the sender's signature. For the first authentication phase which checks the revocation status of the sender.



(a) Authentication delay per message

IJERT

needed to check CRLs with 20,000 and 30,000 certificates .

3. Message Loss Ratio

The average message loss ratio is defined as the average Ratio between the number of messages dropped every 300 m sec, due to the message authentication delay, and the Total number of messages received every 300 m sec by an OBU. It should be noted that we are only interested in the message loss incurred by OBUs due to V2V communications. According to DSRC, each OBU has to disseminate a message containing information about the road condition every 300 msec. In order to react properly and instantly to the varying road conditions, each OBU should verify the messages received during the last 300 m sec before disseminating a new message about the road condition. Therefore, we chose to measure the message loss ratio ever 300 msec. Fig. shows the analytical and simulated average message loss ratio versus the average number of OBU the communication range of each OBU for message authentications employing CRL linear checking, CRL binary checking, and EMAP, respectively, for a CRL containing 20,000 certificates. It can be seen that the simulated average message loss ratio closely follows the analytical message loss ratio which is calculated based on the maximum number of messages that can be authenticated within 300 msec. The difference between the analytical an simulations results stems from observing that some zone in the simulated area become more congested than other zones, thus, some OBUs experience higher message loss than other OBUs, which leads to that difference between the analytical and simulations results. It can also be seen that the message loss ratio increases with the number of OBUs within communication range for all the protocols under considerations. In addition, the message authentication employing EMAP significantly decreases the message loss ratio compared to that employing either the linear or binary CRL revocation status checking. The reason of the superiority of EMAP is that it incurs the minimum revocation status checking delay compared to the linear or bilinear.

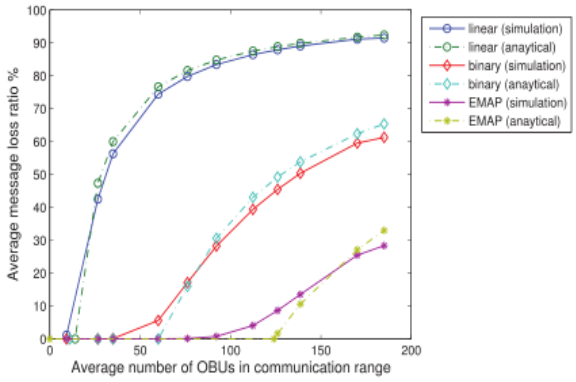


Figure: Comparison between message loss ratio for different schemes

8. CONCLUSION

EMAP for VANETs which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. The proposed EMAP uses a novel key sharing mechanism which 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, EMAP can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking. Our future work will focus on the certificate and message signature authentication acceleration.

REFERENCES

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacand 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 forVANET,” Proc. Embedded Security in Cars (ESCAR) Conf., Nov.2005.

[3] A. Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed 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 Net-works,” 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, “PseudonymChanging at Social Spots: An Effective Strategy for LocationPrivacy in Vanets,” IEEE Trans. Vehicular Technology, vol. 61, no. 1,pp. 86-96, Jan. 2012.

[7] US Bureau Transit Statistics, http://en.wikipedia.org/wiki/ 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 Vehicul ArInterNET 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.

IJERT