Move on Message Backing Protocol for Vehicular Ad Hoc Networks

[1]T. Sai Krishna, [2]S. Nagalakshmi,
[1]M.Tech Research Scholar, Department of CSE,
[2] Assistant Professor, Department of CSE
Priyadarshini Institute of Technology & Science, Chintalapudi, India

Abstract: *A Vehicular Ad hoc Network (VANET) is a type of mobile Peer-To-Peer wireless network that allows providing communication among nearby vehicles and between vehicles and nearby fixed roadside equipment. The lack of centralized infrastructure, high node mobility and increasing number of vehicles in VANETs result in several problems discussed in this paper, such as interrupting connections, difficult routing, security of communications and scalability. Existing system for VANET communication is proved to have several drawbacks. We have proposed a mechanism in order to provide secure and efficient communication in VANET environment. We overcome the drawbacks of the existing system by using Malicious Vehicular Analyzer algorithm and Elliptic Curve Cryptography (ECC). Using these algorithms, malicious messages are identified. It also detects the accident and other problems in the path of the vehicles. Elliptic Curve Cryptography (ECC) algorithm is used for stronger security during communication.*

Keywords: ECC, emergency messages, VANET security, vehicular analyzer, warning messages, etc.

1. INTRODUCTION

An ad hoc wireless network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range (peer-to-peer communication) or one that is outside their radio range (remote-to-remote communication) using intermediate node(s) to relay or forward the packet from the source (sender) toward the destination (receiver). An ad hoc wireless network is self-organizing and adaptive.

Vehicular Ad Hoc Networks (VANET) is used to collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it. VANET comprise of entities such as sensors and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance.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. When the cars go out of its network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. 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.

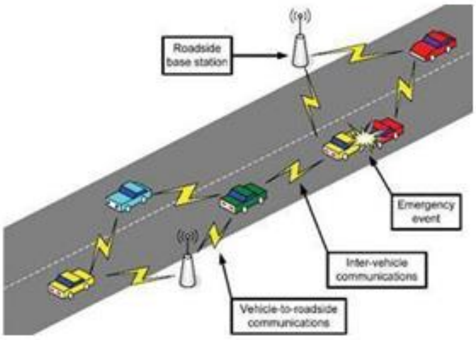

Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Fig.1 General VANET architecture

2. RELATED WORK

A. Initialization Of vehicles

Vehicles are initialized by creation and registration process.The vehicles are first created in the network and get registered to the TA using the information Vehicle id (Vid) and signature id (Sig id). The signature id is created using the algorithm DSA. After registration; TA issues the following parameters to each vehicle.

1. Public Key (PKU) , Private Key (PRu), which is used for both encryption and decryption purposes using RSA algorithm.

2. Secret Key (Kg), which is used for generating MAC code to ensure message integrity and authentication generated using the algorithm MD5.

3. Shared Key, which is used for secure communication between vehicles.

4. Time Stamp denotes the time when the vehicles are registered to the network.

5. Certificate owned for each vehicle that binds the public key.Finally TA stores the information such as Vehicle id, signature id and Time stamp for each vehicle.

B. Message Authentication

Message Authentication involves two processes such as:-

1. Message Broadcasting

2. Message Verification

OBU which is installed in each vehicle performs all the cryptographic operations such storing the keys, certificates and performing message encryption and decryption. Before starting the process of communication, shared key is exchanged between vehicles for the purpose of secure communication. After sharing the key, the vehicles can disseminate the safety-related message to other vehicles such as vehicle’s speed, acceleration, deceleration, velocity and so on.

1. Message Broadcasting:

The source vehicle, OBUU broadcast its safety related message to the other nearby vehicles along the roadside. Before broadcasting, the OBUU calculates a REV Check i.e. HMAC using the secret key and the message to be sent. The MAC which is generated ensures message integrity and the authentication services.

REVcheck=MAC (Kg,M)

After calculating the REV Check, OBUu broadcast the message by encrypting with public key. Finally the message is broadcasted to other nearby vehicles.

2. Message Verification:

The destination vehicle, OBUY before receiving the message checks CRL status that the certificate of the intended OBUU is revoked or not. After verification, if the certificate is no revoked OBUY receives the message and decrypt it using the public key since asymmetric key cryptosystem is used. Else progress the revocation process. After decrypting, the OBUY generates a REV Check by itself using the secret key and the message. It then verifies the generated REV check and the received REV Check matches or not. If match occurs, the message integrity is verified. Else it specifies that false information or replay attacks has been involved and indicates that integrity is lost. Once the integrity is verified, the safety-related message is accepted and displayed. Otherwise the message is ignored.

C. RSU - Aided Verification

The CRL consists of list of revoked certificates. The certificate which belongs to the identity of each vehicle is revoked due to the reasons like certificate expiration or any other validation problems. The certificates can be accepted only when they are in state of non-revoked else it is considered as revoked and the safety-related message that is broadcasted is no more accepted by the destination vehicle OBUY. The CRL verification is performed using the concept of hash chain. RSU, a fixed infrastructure unit on the roadside. Each OBU belongs to their corresponding RSUs depending upon their timestamp value, the time when they get registered to the network. The certificate update is performed through a Trusted Authority (TA), which sends the updated certificate to the requesting OBU through the available RSUs on the Roads. RSU does this verification rather than by TA in a timely manner since RSU can securely communicate with TA. Due to this communication overhead is reduced. Thus, the SM-MAP scheme offers a distributed certification services. Finally, when a certificate is found to be revoked it must progress the non-revocation process. Thereby ensuring fast revocation verifying process without any delay. Considering the requirement for each vehicle to verify a large number of messages in a timely manner, SMMAP introduces an efficient batch verification technique, which enables any vehicle to simultaneously verify a mass of messages. The verification is done by using Secure Hash algorithm (SHA-1). Therefore, the SM-MAP can meet the security and efficiency requirements for certificate service in vehicular communications.

E. Revocation Process

The revocation process is carried out by altering the revoked certificate into a non-revoked. Once the certificate has been non-revoked it can used further by the OBUs for disseminating the Safety-related message without ignorance. The process can be performed by gathering the revoked OBU's secret key which is used for secure communication and the hash value from the hash chain. Update both the secret key and the hash value and finally redistributed. The updated CRL is now distributed by the RSU to the all other OBUs.

F. Security Services:

In order to better understand the data flows of message exchanges employing a certificate-based PKI scheme in VANETs, two services are used to provide a conceptual view of data flows in the certificate-based PKI scheme. The two services occurring in a VANET includes:

1. Communication that require the provision of data integrity.

2. Communications that require the provision of confidentiality.

Case 1: Communications require the provision of data integrity

Vehicle A broadcasts a safety-related message to the relevant vehicles and Roadside Units in the area. The data flows for a message exchange pattern requiring data integrity in VANETs are illustrated.

Sender's End:

Step 1: Creation of safety-related message:

The sender initiates a safety-related message.

Step 2: Creation of a MAC code for the safety-related message:

The safety-related message and secret key is used to create a MAC code.

Step 3: Message delivery:

The message and the MAC code are ready for message dissemination to the intended recipient.

Receiver's End:

Step 4: Message reception:

The intended recipient receives the message (safety-related message and MAC code).

Step 5: Certificate verification:

Notice that there is not a universal sequence in which these processes should be performed.

Step 5.1: To examine the validity time period of the certificate against the current time.

Step 5.2: To check if the certificate is revoked against the CRLs.

Step 6: Client authentication and data integrity verification:

Step 6.1: To authenticate the received message from the sender.

Step 6.2: To verify the MAC code on the received message by using the secret key.

Step 7: Message display:

Upon successful validation, the received message is rendered to the recipient.

Case 2: Communications requiring the provision of confidentiality services

Vehicle A sends a safety-related message to Vehicle B requiring confidentiality. The confidentiality is achieved using the asymmetric key cryptography algorithm RSA. The data flow for a message exchange pattern requiring confidentiality is illustrated.

Key exchange:

The public/private keys are issued by the TA as soon as the vehicles get registered in the network. These keys are used for encryption/decryption.

Vehicle A:

Step 1: Creation of safety-related message:

Vehicle A initiates a safety-related message.

Step 2: Message encryption:

Vehicle A uses the public key to encrypt the message.

Step 3: Message delivery:

The encrypted safety-related message is ready for message dissemination to the intended recipient.

Vehicle B:

Step 4: Message reception:

Vehicle B receives the encrypted safety-related message.

Step 5: Message decryption:

Vehicle B uses the private key to decrypt the message.

Step 6: Message display:

Upon successful validation, the received message is rendered to the recipient.

3. PRELIMINARIES

The bilinear pairing, search algorithms and hash chains have been employed for checking a CRL.

3.1 Bilinear Pairing

The bilinear pairing [22] is one of the foundations of the proposed protocol. Let G1 denote an additive group of prime order q, and G2 is a multiplicative group of the same order q. Let P be a generator of G1, and $\hat{e} : G1 \times G1 \rightarrow G2$ be a bilinear mapping with the following properties:

1. Bilinear: (aP, bQ) = e ^(P,Q)^ab, for all P;Q∈ G1and a,b ∈ R Zq.

2. Nondegeneracy: e ^(P, Q) ≠1G2.

3. Symmetric: e ^((P,Q)= e ^(Q,P) for all P,Q ∈ G1.

4. Admissible: the map is efficiently computable The bilinear map can be implemented using the Weil [23] and Tate [24] pairings on elliptic curves. The

security of the protocol proposed depends on solving the following problem:

Elliptic curve discrete logarithm problem(ECDLP) Consider point P of order q on an elliptic curve, and a point Q on the same curve. The above problem [25] is to determine the integer 1, 0≤1≤q-1, such that Q = lP.

3.2 Hash Chains

A hash chain [26] is the successive application of a hash function h: {0,1}* → Zq with a secret value as its input. A hash function is efficient to compute, but it is computationally impossible to invert. Fig. 1 shows the application of a hash chain to a secret value.

4. EXPEDITE MESSAGE AUTHENTICATION PROTOCOL

Expedite Message Authentication Protocol (EMAP) have some entities

A. Trusted Authority (TA):

This is responsible for providing anonymous certificate and Distributing secret keys to all OBUs in the network. Roadside units (RSUs): which are fixed units distributed all over the network? The RSUs can communicate securely with the TA. On-Board Units (OBUs): which are embedded in vehicles? OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

B. Vehicle -to-Vehicle (V2V) and Vehicle-to-Infrastructure:

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 the entire revoked certificate. 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’ certificate, and finally verifying the sender’s signature on the received message.

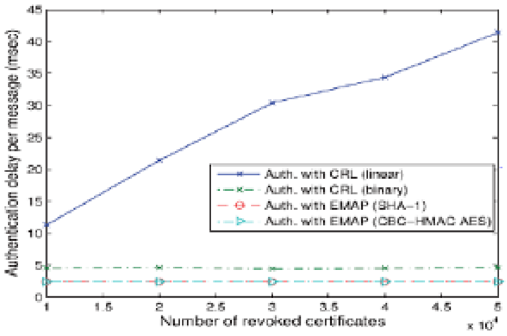
C. Search algorithms

In existing system have two algorithms one is linear search algorithm which is only comparison of each entry in the CRL checking process and the second one is binary search algorithm which is worked only sorted list. 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 finished without finding a match which means that the certificate is unrevoked. We employ Elliptic Curve Digital Signature Algorithm (ECDSA) to check the authenticity of the certificate and the signature of the sender. ECDSA is the digital signature method chosen by the WAVE standard.

5. PERFORMANCE EVALUATION

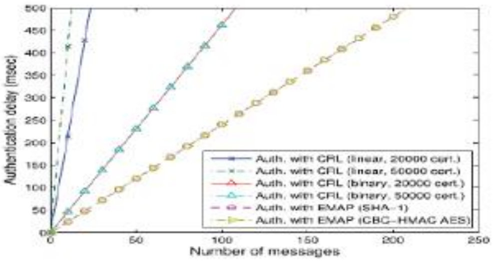
A. Authentication delay

Compare the message authentication delay employing the CRL with that employing MAAC to check the revocation status of an OBU. To employ either the CRL or EMAP. For MAAC, To adopt the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC AES) Also, It have simulated the linear and binary CRL checking process using C++ programs compiled on the same machine. We employ Elliptic Curve Digital Signature Algorithm (ECDSA) to check the authenticity of the certificate and the signature of the sender. ECDSA is the digital signature method chosen by the WAVE standard. In ECDSA, signature verification takes 2Tmult, where Tmult denotes the time required to perform a point multiplication on an elliptic curve. Consequently, the verification of a certificate and message signature takes 4Tmul, Tmul is found for a super singular curve with embedding degree k ¼ 6 to be equal to 0.6 msec.



(a) Authentication delay per message

Fig.2 Authentication delay per message



(b) Total authentication delay vs. the number of the received messages

Fig.3 Authentication delay of received messages

B. Message loss ratio

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 and simulations results stems from observing that some zones 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 MAAC 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 and binary CRL revocation checking processes.

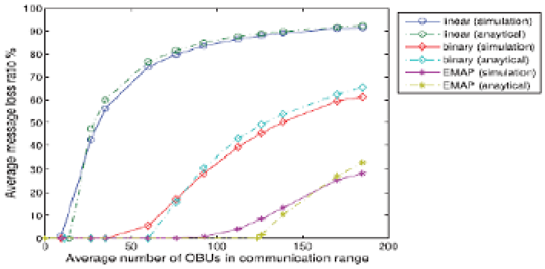


Fig.4 Comparison between message loss ratio for different schemes

C. Communication overhead

A signed message in the WAVE standard should include the certificate of the sender, a time stamp, and the signature of the sender on the transmitted message. Consequently, the additional communication overhead incurred in EMAP and MAAC compared to that in the WAVE standard is mainly due to REVcheck. The length of REVcheck depends on the employed hash function. For example, when SHA-1 is employed in EMAP for calculating REVcheck, this is corresponding to an additional overhead of 20 bytes. The total overhead incurred in a signed message in the WAVE standard is 181 bytes. Consequently, the total overhead in EMAP (SHA-1), assuming the same message format of the WAVE standard, is 201 bytes. In WAVE, the maximum payload data size in a signed message is 65.6 Kbytes. Accordingly, the ratio of the communication overhead in a signed message to the payload data size is 0.28 and 0.31 percent for the WAVE standard and MAAC, respectively. EMAP incurs 0.03 percent increase in the communication overhead compared to the WAVE standard, which is acceptable with respect to the gained benefits from EMAP.

6. CONCLUSION

We have developed security architecture for VANETs systems, aiming at a solution that is both comprehensive and practical. We have studied the problem systematically, identifying threats and models of adversarial behavior as well as security and privacy requirements that are relevant to the VANETs. We have developed security architecture for VANETs systems, aiming at a solution that is both comprehensive and practical. We have studied the problem systematically, identifying threats and models of adversarial behavior as well as security and privacy requirements that are relevant to the VANETs.

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 on Standards for Privacy in User-Centric Identity Management, Zurich, Switzerland, 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), November 2005.

[3] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," IEEE Trans. on Vehicular Technology, vol. 59, pp. 533–549, 2010.

[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[5] "US bureau of transit statistics." [Online]. Available:
http://en.wikipedia.org/wiki/Passenger vehicles in the United States

[6] J. J. Haas, Y. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," Proc. 6th ACM international workshop on VehiculAr InterNETworking, pp. 89–98, 2009.

[7] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages," IEEE Std 1609.2-2006, 2006.

[8] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[9] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks," Proc. IEEE GLOBECOM'09, 2009.

[10] J. P. Hubaux, "The security and privacy of smart vehicles," IEEE Security and Privacy, vol. 2, pp. 49–55, 2004.

[11] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," Proc. SECON '09, pp. 1–9, 2009.

[12] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE Journal on Selected Areas in Communications, vol. 25, pp. 1557–1568, 2007.

[13] P. P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate revocation list distribution in vehicular communication systems," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp. 86–87, 2008.

[14] K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," Proc. 5th ACM international workshop on VehiculAr Inter-NETworking, pp. 88–89, 2008.

[15] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," Proc. 2003 IEEE Symposium on Security and Privacy, pp. 197–213, 2003.

[16] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," Proc. ACM conference on Computer and communications security, pp. 41–47, 2002.

[17] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks," Journal of Computer Security, vol. 14, pp. 301–325, 2006.

[18] A. Wasef and X. Shen, "PPGCV: Privacy preserving group communications protocol

for vehicular ad hoc networks," Proc. ICC'08, pp. 1458–1463, 2008.

[19] A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks," IEEE Trans. On Vehicular Technology, vol. 58, no. 9, pp. 5214 – 5224, 2009.

[20] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," Proc. 21st Annual International Cryptology Conference on Advances in Cryptology, pp. 213–229, 2001.