Broadcasting Message Authentication Protocol for Vehicular Ad Hoc Networks Using Cluster Technique

A.Nandini
Nandini549@gmail.com

P.Venkateswara Rao
Varun.apeksha@yahoo.com

ABSTRACT

It is well recognized that security plays a vital for the trustworthy operation of vehicular ad hoc networks (VANETs). One of the critical sanctuary issues is the revocation of misbehaving vehicles, which is essential for the prevention of malicious vehicles from other vehicles. Vehicular ad hoc networks (VANETs) adopt the Public Key infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In this paper 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 Code shared only between non revoked On-Board Units (OBUs). EMAP can 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 by NS2 simulator tool, EMAP is demonstrated to be secure and proficient. In this paper the reprogramming protocols are discussed and also classify the different reprogramming protocols. SDRP is the distributed protocol which supports many users simultaneously and also it is important in large-scale sensor networks used by different users from both public and private sectors. The defense to this protocol is provided by Elliptic curve encryption Scheme but the Elliptic Curve Integrated Encryption Scheme (ECIES) is the best Encryption scheme. The research focuses on achieving privacy using ECIES algorithm for encryption, and certification using Hashing technique. In future we are going to implement the cluster based method in this process.

Keywords: Message Authentication, Certificate Revocation

I. INTRODUCTION

The VANETs consist of entity including on the ship Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to means of transportation (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. regrettably, the CRL size in VANETs is expected to be large for the following reasons: 1) To conserve the privacy of the drivers, i.e., to give up the leakage of the real identities and locality information of the drivers from any external eavesdropper [5][6][7], each OBU should be preloaded among a set of indefinite digital certificate, where the OBU has to periodically change its unidentified certificate to deceive attackers. The ad hoc network (VANET), it is a special kind of mobile ad hoc network, has been
subject to general research efforts not only from the government but also from academic circles and the automobile industry in up to date years. Different from the traditional ad hoc networks, the VANET contains not only mobile nodes—vehicles—but inactive roadside units (RSUs) as well. Due to this crossbreed architecture, the VANET introduces new methods to facilitate road protection and traffic management and providing compact disk services for vehicles on the road. According to the dedicated restricted communications (DSRC) [2] in road safety-related applications, each vehicle unprepared with onboard units (OBUs) will broadcast routine traffic messages with the information of location, current time, route speed, increase of velocity/deceleration, and traffic actions, etc. With this information, drivers can be better aware of their driving atmosphere and take early action to respond to an atypical situation, such as a traffic accident. However, before putting this attractive application into practice, security and seclusion issues in VANETs must be resolved [1]–[3]. Without security and privacy guarantee, an opponent to a VANET can be a false in sequence to misinform other drivers, and even cause a determined traffic industrial accident, or track the location of the interested vehicles by collect their usual traffic messages. Therefore, how to achieve unknown authentication has become a essential requirement for secure VANETs. To make sure consistent operation of VANETs and enhance the amount of valid information gain from the conventional messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the accessible works overlooked the authentication delay follow-on from scrutiny the CRL for each received certificate. In this paper, we introduce an expedite message authentication protocol (EMAP) which replace the CRL checking method by an efficient revocation checking process using a speedy and secure HMAC task. 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 verification delay ensuing from check the CRL in VANETs.

II.RELATED WORK

In spontaneous vehicular communications, the main security supplies are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. deploy an efficient PKI is a well-recognized
explanation for achieve safety and privacy for sensible vehicular networks [4], [8]. Although VANETs have a moment ago gained wide attention, very few works have addressed the design of a PKI that is appropriate for the security necessities of VANETs. In [4], Hubaux identifies the specific issues of safety measures and privacy challenge in VANETs and claim that a PKI should be well deploy to protect the transited messages and to mutually authenticate among network entities. In [1], Raya and Hubaux use a classical PKI to provide secure and privacy-preserving communications to VANETs. For this approach, each vehicle needs to preload a vast pool of mysterious certificates. The number of the weighed down certificates in each vehicle should be large enough to provide safety and taking apart protection for a long time, e.g., one year. Each vehicle can let somebody know its certificates from a central ability during the annual inspection of the vehicle. The precondition to load a large number of certificates in each vehicle incur inefficiency for certificate management, as revoke one vehicle involve revoke the huge number of certificates weighed down in it.

Lin et al. [8] make use of the collected works signature in [9] to secure the road and rail network between vehicles. For the group signature performance, any group member can sign messages on behalf of the group without enlightening its real identity. Signatures can be demonstrated using the group public key, thus providing tremendous confidentiality for the users, as the identity of the users are open to the fundamentals in neither signing nor verify a message. However, the delay incur in this technique to verify a signature is linearly proportional to the number of withdraw vehicles. In this paper the reprogramming protocols are discussed and also pigeonhole the different reprogramming protocols. SDRP is the disseminated protocol which supports multiple users along with and also it is important in across-the-board sensor networks used by different users from both public and private sector. The precaution to this set of rules is providing by Elliptic curve encryption Scheme but the Elliptic Curve Integrated Encryption Scheme (ECIES) is the best Encryption scheme. The research focuses on pull off space to you using ECIES algorithm for encryption, and authentication using Hashing method.

III MESSAGE AUTHENTICATION PROTOCOL

To make sure the consistent process of VANETs and enlarge the quantity of genuine information gain since the arriving messages, each OBU have to be capable to make sure the revocation status of all the received certificates in a apt manner. on the complete of the active work without being seen the verification delay resultant from scrutiny the CRL for each arriving certificate. In the future system, it uses Hasten Message Authentication Protocol which replace the protracted CRL checking process by an well-organized revocation checking progression by means of a speedy and cosseted HMAC purpose.

It can be used as disaster management such as a lot of messages can be occurred at a time.Here we are going to use cluster based method owing to great vehicle capable of in this pitch.

In future we are going to implement the cluster based method in this process. Due to large vehicles equipped in this field we are going to divide it in cluster format and then include the Expedite Message Authentication protocol. Here Credit algorithm is implemented. The transcation can only occur within the credit nodes. Credit method will focus on the certificate and message signature authentication acceleration.

The future EMAP uses a fast HMAC function and work of fiction key sharing scheme
employing probabilistic arbitrary key distribution.

**Figure 1. System model**

**SYSTEM MODEL**

A Trusted Authority, which is to blame for providing unidentified certificates and distribute secretive keys to all OBUs in the network. Another main function of the TA is to issue Certificate Revocation Lists (CRLs)

**On-Board Units (OBU)**, The OBU is DRSC transceiver commonly installed in or on a vehicle; OBU can exchange a few words either with other OBUs through Vehicle-to-Vehicle (V2V) communications or with the road and rail network RSUs through Vehicle-to-Infrastructure (V2I) communications. Each OBU is ready with a Global Positioning Service (GPS) receiver which contains the objective coordinate of the RSUs.

**Hardware Security Module (HSM)**, According to the Wave standard each network is equipped with modify resistant HSM whose purpose is to store its security materials, eg., secret keys, certificates, etc. and physically protect perceptive information and provide a secure time base.

**Figure 2. Design Implementation**
Road Side Units (RSU), is a DSRC transceiver fixed units disseminated in the network. Moreover, RSUs are answerable for update the certificates of the OBUs.

IV. SYSTEM INITIALIZATION

The TA initializes the system by execute Algorithm 1. PKᵢ denotes the ith public key for OBUᵢ, where the corresponding secret key is SKᵢ. PIDᵢᵤ denotes the ith pseudoidentity (PID) for OBUᵢ, where the TA is the only thing that can relate PIDᵢ to the real identity of OBUᵢ; sigTA and (PID||PKᵢᵢ) and PKᵢ is the signature .|| is the concatenation of PIDᵢ and PKᵢᵢ. C is the number of certificates loaded in each OBU.

Algorithm 1. System initialization
1: Select two generators P;Q ∈ GG₁ of order q, 2: for i ->1,l do 3: Select a random number ki € Zq 4: Set the secret key K=kiQ ∈GG₁ 5: Set the corresponding public key K= P/KI 6: end for 7: Select an initial secret key Kg ∈ GG₂ to be shared between all the non-revoked OBUs 8: Select a master secret key s € ZZ 9: Set the corresponding public key PS=SP 10: Choose hash functions H:{0,1} 11: Select a secret value v € ZZ and V₀₀=V 12: for i 13: Set VI=h(v⁻¹) a set V of hash chain values 14: Set VI=h(v⁻¹) 15: for all OBUᵢ in the network, TA do Announce H, h, P, Q, and P to all the OBUs

V. MESSAGE AUTHENTICATION

Since we accept a general PKI system, the details of the TA signature on a certificate and an OBU signature on a message are not discuss in this paper for the sake of generalization. We only focus in how to accelerate the revocation checking process, which is conservatively performed by checking the CRL for every received certificate. The message signing and verification between different entities in the network are performed as follows:

5.1. Message Signing

Before any OBUᵢ broadcast a message M, it calculates its revocation check REVcheck as REVcheck = HMAC(Kg; PIDᵢ||Tstamp)² where Tstamp is the present time stamp, and HMAC(Kg; PIDᵢ||Tstamp)² is the hash message validation code on the concatenation of PIDᵢ and Tstamp using the secret key Kg. Then, OBUᵢ broadcasts M||Tstamp||certu(PIDᵢ;PKᵢ;sigTA(PIDᵢ||u)Ts tamp REVcheck) where HMAC(Kg; PIDᵢ||Tstamp) is the signature of OBUᵢ on the concatenation of the message M and Tstamp.

5.2. Message Verification

Any OBUᵧ in receipt of the message (M||Tstamp||cert(PIDᵢ;PKᵢ;sigTA(PIDᵢ||u)Tstamp REVcheck can verify it by executing Algorithm 2.

Algorithm 2. Message verification
1: Check the validity of Tstamp 2: if invalid then 3: Drop the message 4: else 5: Check REVcheck = HMAC(Kg : PIDᵢ Tstamp) 6: if invalid then 7: Drop the message 8: else 9: Verify the TA signature on certOBUᵢ 10: if invalid then
11: Drop the message
12: else
13: Verify the signature sig(M||Tstamp) using OBUu public key PKu
if invalid then
15: Drop the message
16: else
17: Process the message
18: end if
19: end if
20: end if
21: end if

VI. PERFORMANCE EVALUATION

Authentication Delay contrast the message confirmation delay employing the CRL with that employing EMAP to check the revocation position of an OBU. As stated earlier, the authentication of any message is performed by three uninterrupted phases: checking the sender’s revocation status, verifying the sender’s certificate, and verifying the sender’s signature. For the first certification phase which checks the revocation status of the sender, we employ either the CRL or EMAP. For EMAP, we adopt the Cipher Block Chaining Advanced Encryption Standard (CBC-HMAC AES and Secure Hash Algorithm 1 SHA-as the HMAC functions.

Fig. 2 shows 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, where the number of the revoked certificates is an indication of the CRL size. It can be seen that the confirmation delay using the linear CRL checking process increase with the number of revoked certificates, i.e., with the size of the CRL. By using the binary CRL the authentication delay checking process is almost stable.

VII. MESSAGE LOSS RATIO

The standard message loss relation is defined as the average ratio between the number of messages dropped every 300 msec, due to the message authentication delay, and the total number of messages received every 300 msec by an OBU. It should be noted that interested in the message loss incur by OBUs due to V2V communications. According to DSRC, each OBU has to distribute a message containing information about the road condition every 300 msec. In order to react properly and right away to the varying road conditions, each OBU should verify the messages established during the last 300 msec before disseminating a new message about the road condition. consequently, we chose to
measure the message loss ratio every 300 msec.

VIII PERFORMANCE EVALUATION
AUTHENTICATION DELAY

We consider the PID of OBU and the time stamp to having equal lengths of 8 bytes. We adopt the Crypto++ library for scheming the delay of the HMAC functions. The delay incur by using CBCHMAC AES and SHA-1 to calculate the revocation check REV

a) no. of revoked certificate vs authentication delay

We have computed the graph for number of revoked certificate vs. authentication delay transmit by the each OBUs. The revoked certificates indicates the CRL size. The authentication delay is stable with respect to number of revoked certificates.

b) OBU density vs DELAY(ms)

We have computed the graph for OBU density vs delay in msec. The OBU density predict the communication overhead. The delay gets increased when number of OBU is increased, as number of OBU increases outcome in long waiting time.

c) no. of messages vs authentication delay (ms)

We have compute the graph for number vs wait in msec using EMAP. It is seen that the number of message verified with in a section gets decreased with the CRL size.
We have urbanized a security measures architecture for VANETs systems, aiming at a solution that is both comprehensive and practical. To handle certificates and large number of users, and to safe communication while enhancing privacy. In this paper the reprogramming protocols are discussed and also classify the different reprogramming protocols. SDRP is the distributed protocol which supports numerous users at the same time and also it is important in large-scale sensor networks used by dissimilar users from both public and private sectors. The security to this protocol is provided by Elliptic curve encryption Scheme but the Elliptic Curve Integrated Encryption Scheme (ECIES) is the best Encryption scheme. The investigate focuses on achieving privacy using ECIES algorithm for encryption, and authentication using Hashing technique.

REFERENCES