A Novel Cryptographic Approach Providing Authentication for Vehicular Ad-hoc Network

Shruti S.Dasmani[1], Shubhangi D.C[2], Jyothi Patil[3]

[1](PG M.Tech IV Sem Student, Department of Computer Science & Engineering, VTU RO PG Centre, Gulbarga, Karnataka, India).
[2](Course Co-ordinator & Professor, Department of Computer Science & Engineering, VTU RO PG Centre, Gulbarga, Karnataka, India).
[3](Associate Professor, Department of Computer Science & Engineering, PDACE, Gulbarga, Karnataka, India).

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) for their security make use of Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs). 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 a cryptographic approach for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process here makes use of a protocol having encryption-decryption making use of a public key and private key, where the key used in the process is shared only between non-revoked On-Board Units (OBUs).In addition, cryptographic approach here uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key.

Key words: Vehicular networks, Communication security, Message authentication, Certificate revocation, Trusted Authority.

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) a part of ad-hoc network is gaining attraction, extensive attentions as a reliable technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. Entities of VANETs include On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Along with the two basic communication modes Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications respectively allow OBUs to communicate with each other and with the infrastructure RSUs as shown as in Fig 1 below.

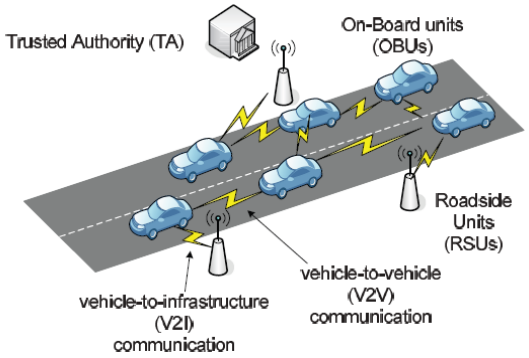

Fig 1: VANET entities along with their communication.

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 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 then 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, obviously not to have the leakage of the real identities and location information of the drivers to any external eavesdropper [1], [4]-[7].
2) The scalability nature of transportation industries, hence vehicles are increasing day by day, so scale of VANET is very large.

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 [2].

According to the employed mechanism for searching a CRL, the Wireless Access in Vehicular Environments (WAVE) standard [3] 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. According to the Dedicated Short Range Communication (DSRC), [13] which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telematic information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current 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 an 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 a cryptographic approach which replaces the CRL checking process by an efficient revocation checking process using a fast and secure cryptographic function.

To the best of our knowledge, this is the solution to reduce the authentication delay resulting from checking the CRL in VANETs. The rest of the paper includes the other sections such as Section II presents the related work, Section III & IV describes existing and proposed system respectively, Section V presents the simulation results. Finally, the concluding remarks are given in Section VI.

II. RELATED WORK

In VANETs, the primary security requirements are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. The Public Key Infrastructure (PKI) is the most viable technique to achieve these security requirements [4]. PKI employs Certificate Revocation Lists (CRLs) to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long.

In [1], Hubaux et al. identify the specific issues of security and privacy challenges in VANETs, and indicate that a Public Key Infrastructure (PKI) should be well deployed to protect the transited messages and to mutually authenticate network entities.

In [4], Raya et al. use a classical PKI to provide secure and privacy preserving communications to VANETs. In this approach, each vehicle needs to pre-load 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 this approach, revoking one vehicle implies revoking the huge number of certificates loaded in it.

Haas et al. [6] develop a mechanism to reduce the size of the broadcast CRL by only sending a secret key per revoked vehicle. On receiving the new CRL, each OBU uses the secret key of each revoked vehicle to re-produce the identities of the certificates loaded in that revoked vehicle, and construct the complete CRL. It should be noted that although the broadcast CRL size is reduced, the constructed CRL at each OBU, which is used to check the revocation status of other entities, still suffers from the expected large size exactly as that in the traditional CRLs where all the identities of the certificates of every revoked OBU are included in the broadcast CRL .Also, the authors propose using bloom filter, which is some kind of lookup hash tables, to perform CRL checking for the received certificates.

In [7] 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 where the trusted authority acts as the group manager and the vehicles act as the group members. Upon entering a new region, each vehicle must update its certificate from the RA dedicated for that region. The vehicle sends a request signed by its group key to the RA

to update its certificate, the RA varies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (RL).After the RA authenticates the vehicle, it issues short- lifetime region-based certificate. This certificate is valid only within the coverage range of the RA. Although TACK eliminates the CRL at the vehicles level, it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check the revocation status of a vehicle, the RA has to verify that this vehicle is not in the current Revocation List (RL) by performing a check against all the entries in the RL. The authors suggested using an optimized search method to remedy the computationally expensive RL check.

In this paper, we propose a cryptographic approach to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. This approach employs keyed encryption-decryption process in the revocation checking process, where the key used in the process for each message is shared only between unrevoked OBUs

III. EXISTING SYSTEM

Vehicles make use of certificates to communicate with other vehicles, certificates are provided by Trusted authority, Trusted authority makes use of Certificate Revocation List to keep track of revoked vehicles and to provide communication between un-revoked vehicles, it has to check the current Certificate Revocation List for all the received certificates, which may make use of optimized or non optimized search algorithms[11] leading to incurring of long authentication delay depending on the Certificate List size and the number of received certificates.

The ability to check a Certificate List for a large number of certificates in a timely manner leads to an 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 Certificate List for each received certificate. Fig. 3.1-3.4 shows the screenshots for existing system making use of CRL.

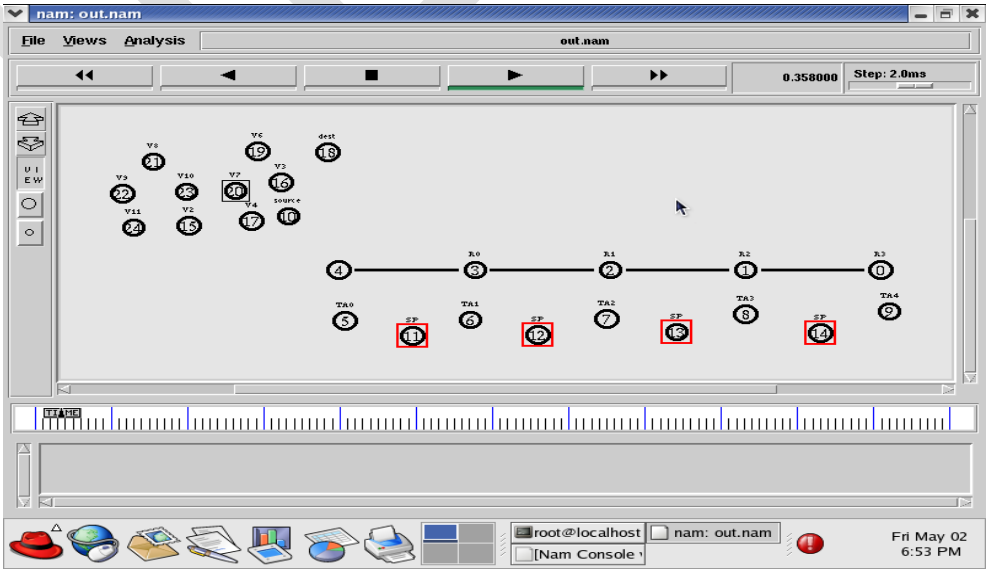

Fig 3.1: A Snapshot displaying VANET deployment

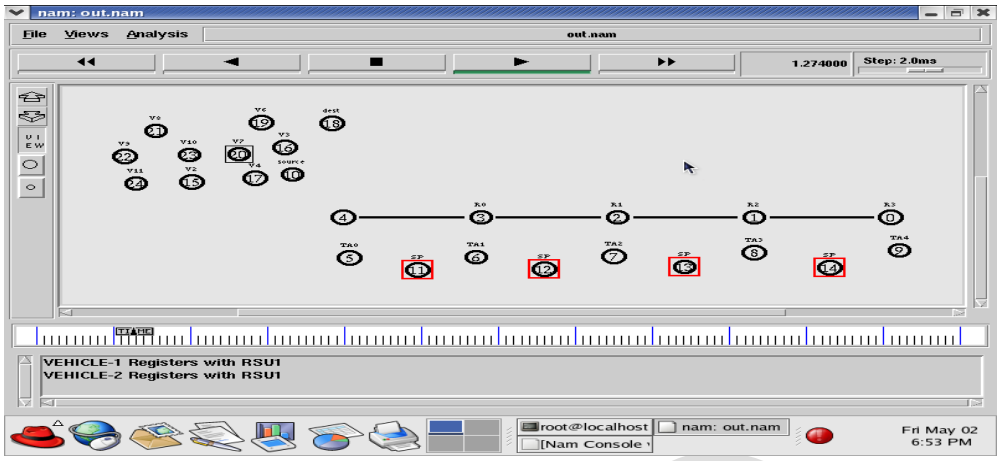

Fig 3.2: A Snapshot for showing the registration of vehicles

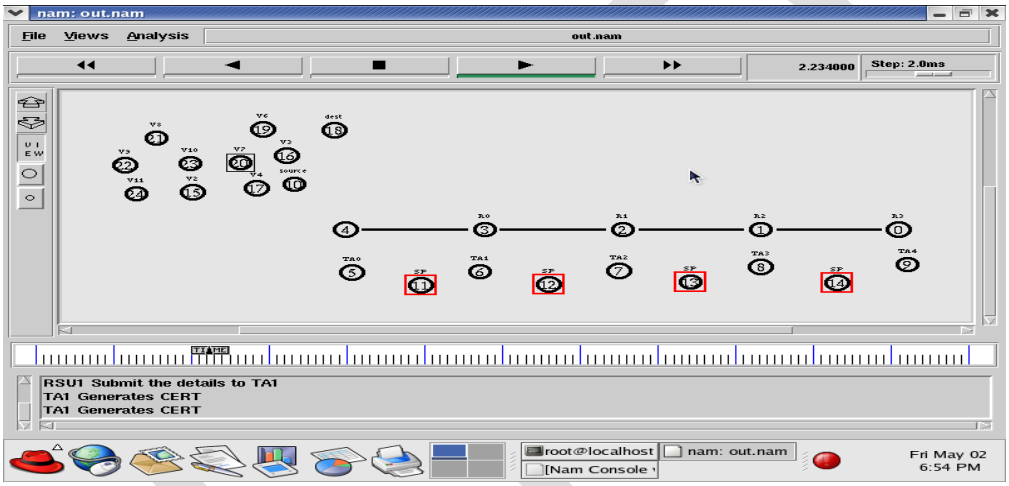

Fig 3.3: A Snapshot displaying the issue of certificate by TA

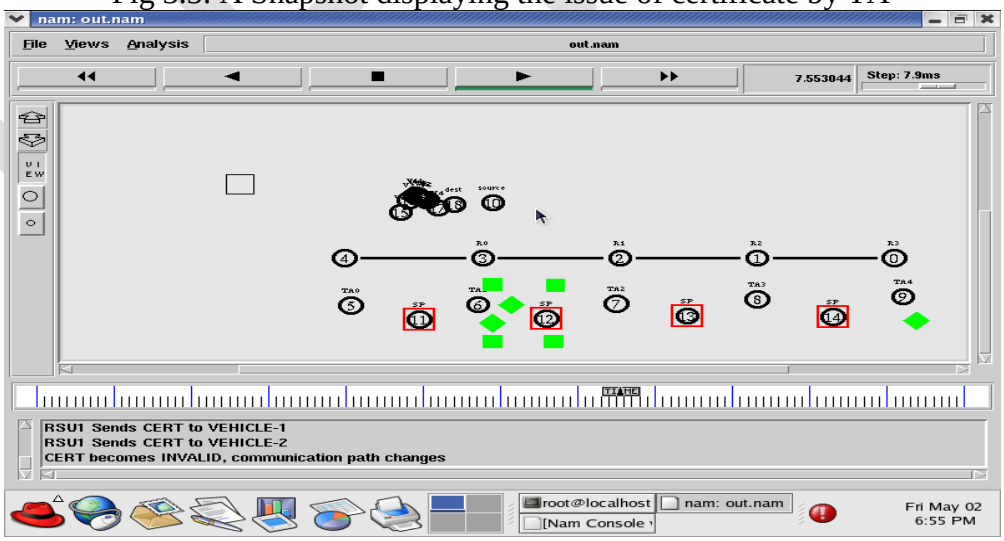

Fig 3.4: Dropping of packets by destination vehicle after knowing about the revocation of certificate

DISADVANTAGES OF EXISTING SYSTEM

- Existing schemes takes much time to provide the authentication because of searching the entire CRL for the revoked certificate, hence delay is more.

- This also leads to end-end delay between the communications among nodes.

IV. PROPOSED SYSTEM

The proposed cryptographic approach uses an encryption-decryption function and novel key sharing scheme employing probabilistic random key distribution.

4.1.System Model

The system model under consideration consists of the followings entities as shown in Fig 1 above.

•A Trusted Authority (TA), which is responsible for providing anonymous certificates 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.

The Proposed System is having 3 modules as explained below,

1) VANET Creation and initialization

In this module, a Vehicular Adhoc Network is created. All the nodes are deployed in the network area. Vehicle nodes are assigned with mobility (movement). Fig 4.1 below shows snapshot for creation of VANET and initialization of nodes.

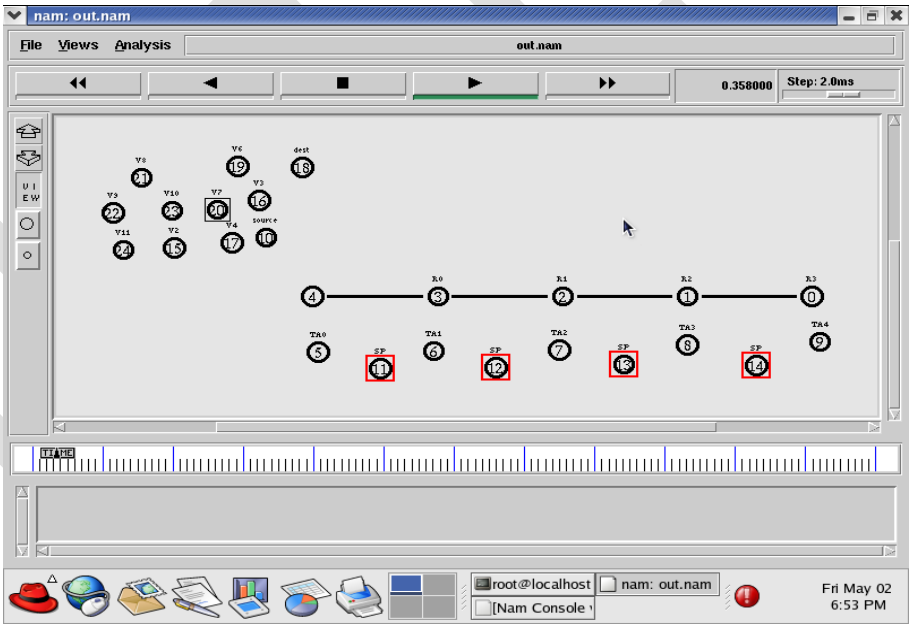

Fig 4.1: A Snapshot for initialization of nodes and Vehicular network creation.

2) Implementation of Cryptographic Approach

We are considering mainly a PKI system, where for example consider OBU_u (u^{th} OBU or vehicle) has a set of anonymous certificates ($CERT_u$) used to secure its communications with other entities in the network. In specific, the public key PK_u, included in the certificate $cert_u$, and the secret key SK_u are used for verifying and signing messages, respectively. Also, each OBU_u is pre-loaded with a set of asymmetric keys (secret keys K^-s in RS_u and the corresponding public keys K^+s in

RP_u).Those keys are necessary for generating and maintaining a shared secret key K_g between unrevoked OBUs. We are making use of encryption-decryption protocol to provide the communication between the vehicles using the keys allotted to them. As we are making use 2 keys one for encryption and other for decryption, it provides the authentication about the message and about the sender.

TA has the following:

- A secret key pool

Us=$\{K_i^- = K_i Q | 1 \leq i \leq l\}$

- The corresponding public key set

$$U_p == \{K_i^+ = (\frac{1}{K_i})P | 1 \leq i \leq l\}$$

- A master secret key s and the corresponding public Key P_0.
- The secret key Kg.

Each OBU will have the following:

- A set of anonymous certificates (CERTu) used to achieve privacy-preserving authentication.
- A set of secret keys RS_u consisting of m keys randomly selected from U_s, i.e., $RS_u \in U_s$.
- The set of the public keys RPu corresponding to the keys in RSu, i.e., $RP_u \in U_p$.
- The secret key K_g, which is shared between all the legitimate OBUs.

If OBU_u wants to send a message to OBU_y then it has to encrypt the message as shown in expression (1) below

$$C = E (k_g , PID_u || T_{stamp} || Msg) \quad (1)$$

Where k_g is the shared secret key provided by T.A, along with identity of its OBU id PID_u with the concatenation of time stamp T_{stamp} and message here represented as Msg, at the receiving end receiver decrypts it using

$M = D (K_g || E (k_g || PID_u || T_{stamp} || Msg)$

or

$M = D (k_g || C)$ (2)

By replacing $E (k_g , PID_u || T_{stamp} || Msg)$ with C from expression (1) we get M

If OBU_u is to be revoked then, the revocation is triggered by the TA. The certificates of OBU_u must be revoked. In addition, the secret key set RS_u of OBU_u and the current secret key are considered revoked. Hence, a new secret key should be securely distributed to all the non-revoked OBUs. Also, each non-revoked OBU should securely update the compromised keys in its key sets RS and RP.

3) Performance analysis and Result Comparison

In this module, the performance of the proposed architecture is analyzed using ns-2 [14]. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters. We compare these values with the values we got using the existing system and plot the graphs.

V. SIMULATION RESULTS

Table I
NS-2 Simulation Parameters

Simulation area	200mx200m
Simulation time	8 sec
MAC protocol	802.11a
Protocol used	AODV
Data Traffic	UDP,CBR

Table-I above shows the NS-2 simulation parameters considered for simulation

Fig.5.1-5.5 shows snapshots with cryptographic approach

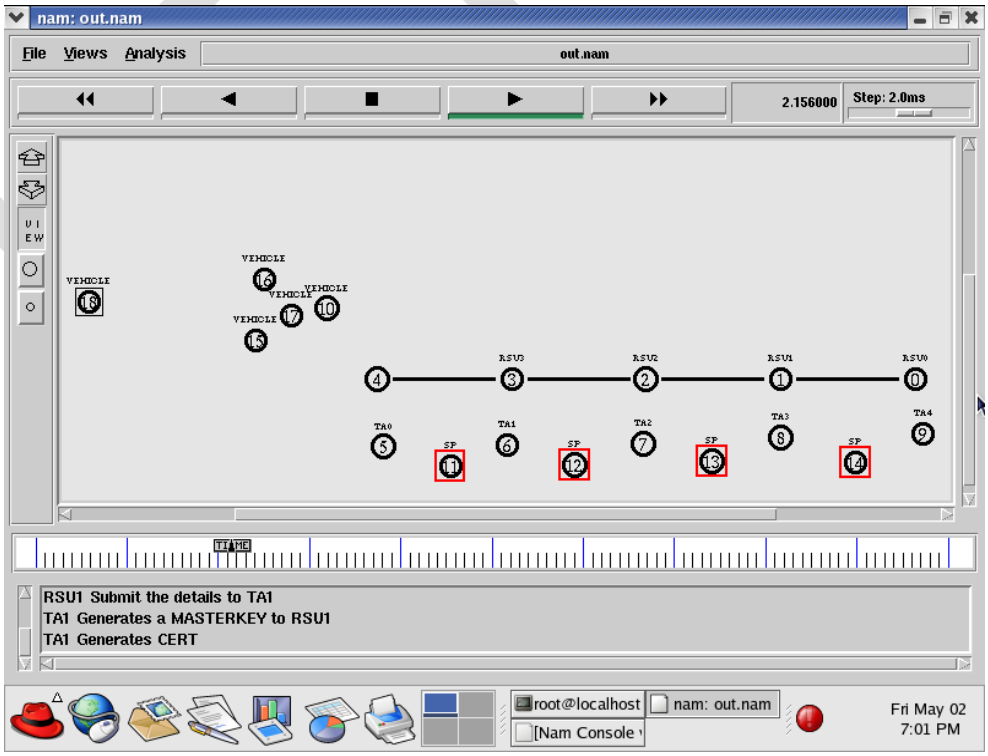

Fig 5.1: A Snapshot for generating of keys and certificate

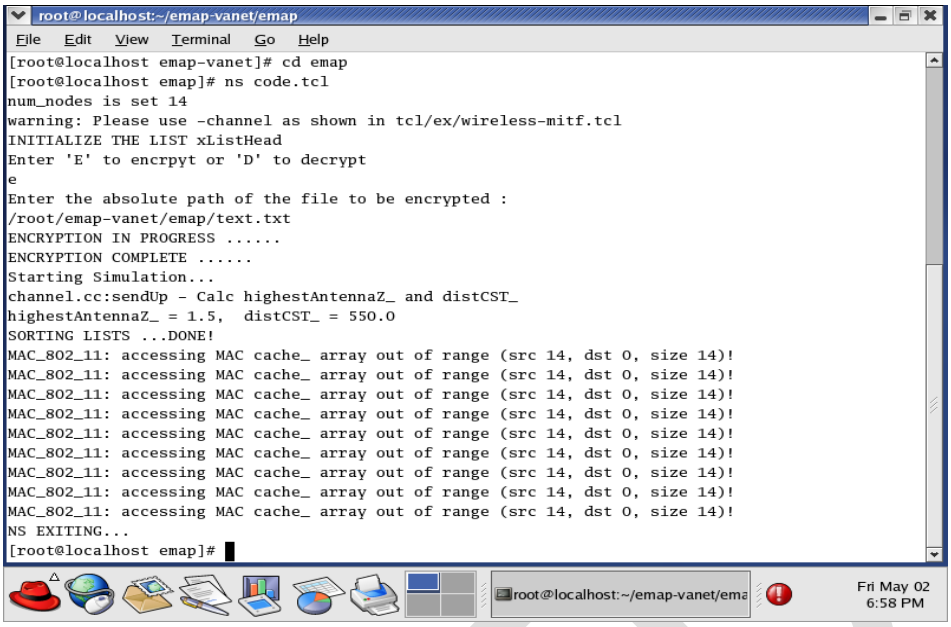

Fig 5.2: A Snapshot displaying the encryption of message using the cryptographic approach

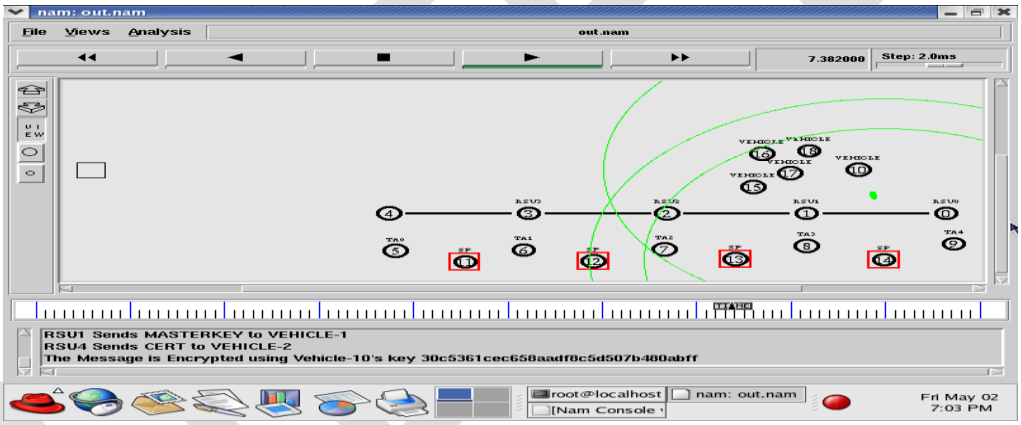

Fig 5.3: A Snapshot displaying the data packet transfer from source node to destination node by encrypting it

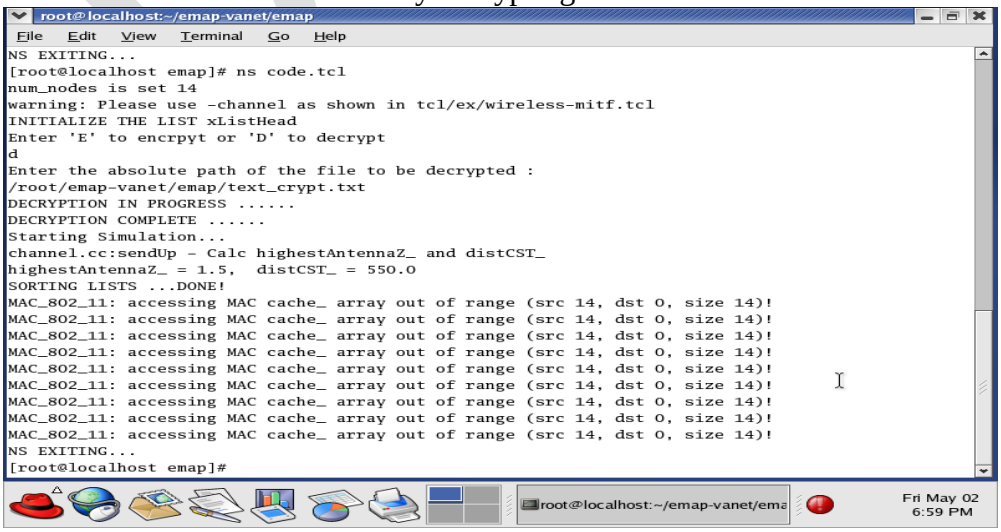

Fig 5.4: A Snapshot displaying the decryption of message using the cryptographic approach

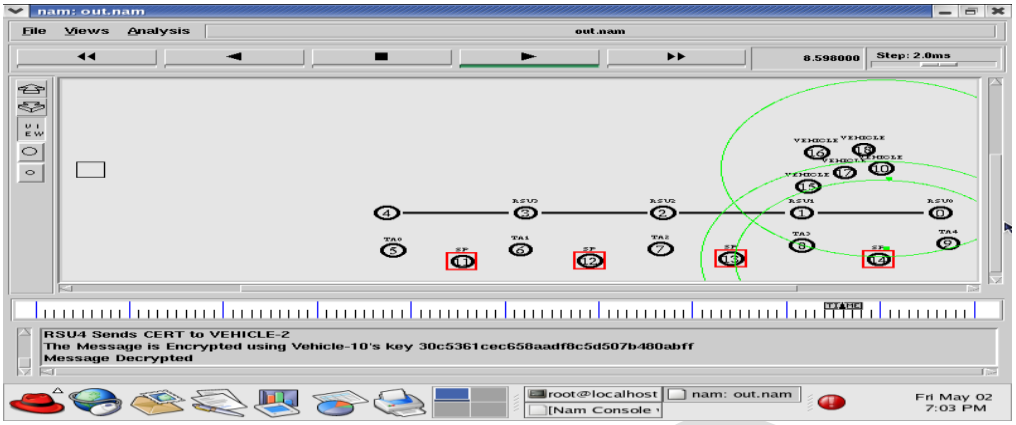

Fig 5.5: A Snapshot of Data packet reception at the destination node by decryption.

GRAPHS

Fig 5.6: Authentication Delay graph.

Fig5.6-5.8 shows the graphs comparing our existing system and proposed system through these graphs we can show that our proposed cryptographic approach is more efficient by consuming less delay for communication as it takes less time to authenticate the message as well as sender, hence throughput will be increased along with less bandwidth consumption.

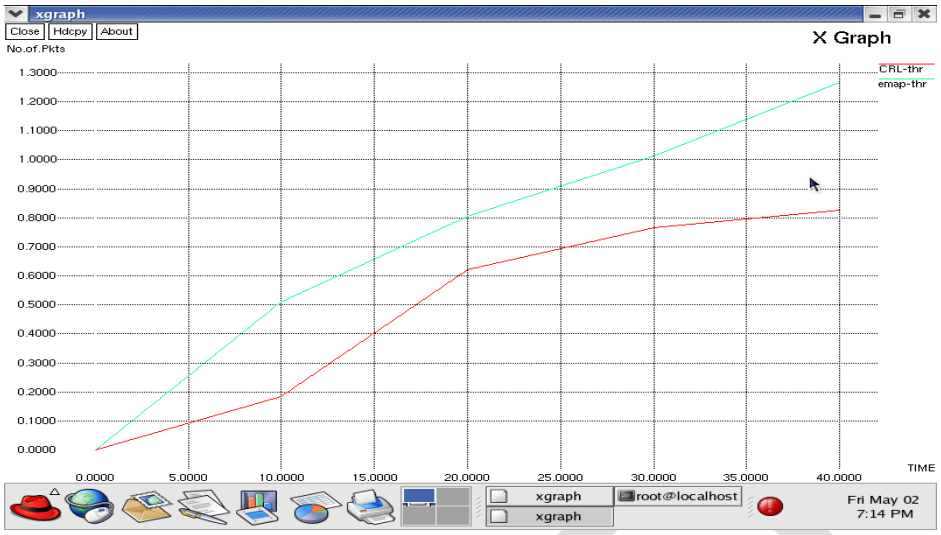

Fig5.7: Throughput graph.

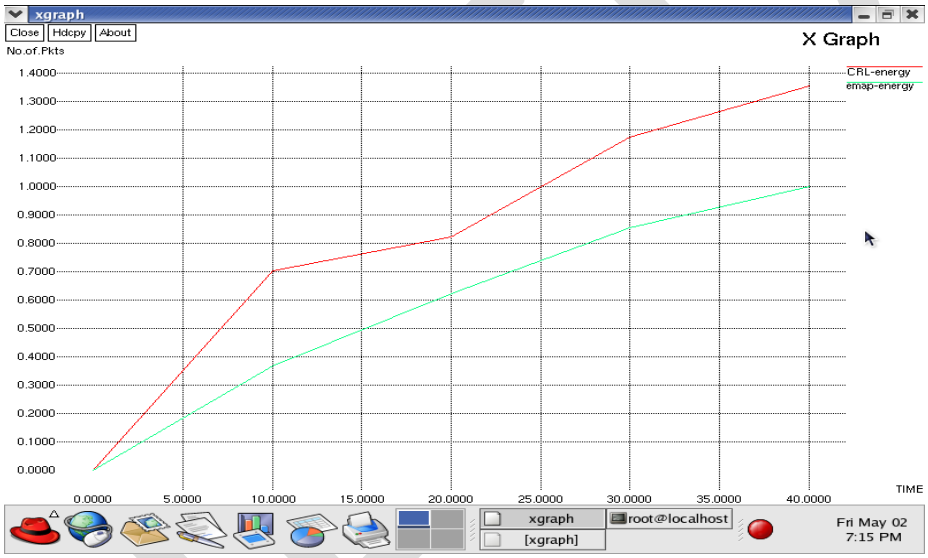

Fig 5.8: Energy Consumption graph.

VI. CONCLUSION

In this paper, we have proposed cryptographic approach for VANETs, which provides message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing encryption-decryption function. The proposed cryptographic approach 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, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Our future work will focus on the certificate and message signature authentication Acceleration.

REFERENCE

[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..29

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

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

[4] 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.

[5] K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'l Workshop Vehicular Inter-Networking, pp. 88-89, 2008.

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

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

[8] 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.

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

[10] A.Wasef and X.Shen, "PPGCV: Privacy preserving group communications protocol for Vehicular ad hoc networks," Proc.ICC '08, pp.1458 –1463, 2008.

[11] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, Introduction to Algorithms. MIT, 2001

[12] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[13] "5.9 GHz DSRC," http://grouper.ieee.org/groups/scc32/dsrc/index.html, 2012.

[14] "The network simulator-ns-2."[Online]. Available: http://nsnam.isi.edu/nsnam/ index.php/ User