EMAP: Expedite Message Authentication Protocol for Transport Unexpected Networks

A.Srinivas[1], Stalin Babu J[2]

[1]Assistant Professor, Computer Science Engineering,
Sri Indu College of Engineering and Technology, Telangana, India

[2]Assistant Professor, Computer Science Engineering,
Nalla Malla Reddy Engineering college, Telangana, India

Abstract— Vehicular ad hoc networks (VANETs) adopt the general public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for his or her security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is enclosed within the current CRL, and substantiating the genuineness of the certificate and signature of the sender. during this paper, we have a tendency to propose associate degree Expedite Message Authentication Protocol (EMAP) for VANETs, that replaces the long CRL checking method by associate degree economical revocation checking method. The revocation check method in EMAP uses a keyed Hash Message Authentication Code HMACP, wherever the key employed in scheming the HMAC is shared solely between non revoked On-Board Units (OBUs). additionally, EMAP uses a completely unique probabilistic key distribution, that permits non revoked OBUs to firmly share and update a secret key. EMAP will considerably decrease the message ratio owing to the message verification delay compared with the standard authentication ways using CRL. By conducting security analysis and performance analysis, EMAP is in contestable to be secure and economical

Index Terms—Vehicular Networks, Communication Security, Message Verification, Certificate Revocation.

1. INTRODUCTION

Vehicular ad-hoc networks (VANETs) have attracted intensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs include entities together with On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications ar the 2 basic communication modes, that severally enable OBUs to speak with one another and with the infrastructure RSUs. Since vehicles communicate through wireless channels, a spread of attacks like injecting false info, modifying and replaying the disseminated messages will be simply launched. A security attack on VANETs will have severe harmful or fatal consequences to legitimate users. Consequently, making certain secure transport communications may be a should before any VANET application will be place into observe. A well-recognized resolution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, every entity within the network holds AN authentic certificate, and each message ought to be digitally signed before its transmission. A CRL, sometimes issued by a trust worthy Authority (TA), may be a list containing all the revoked certificates. in a very PKI system, the authentication of any message is performed by first checking if the sender's certificate is enclosed within the current

CRL, i.e., checking its revocation standing, then, certificatory the sender's certificate, and finally certificatory the sender's signature on the received message. The first a part of the authentication, that checks the revocation standing of the sender in a very CRL, could incur long delay looking on the CRL size and therefore the used mechanism for looking out the CRL. Unfortunately, the CRL size in VANETs is predicted to be massive for the subsequent reasons: To preserve the privacy of the drivers, i.e., to abstain the outflow of the $64000 identities and placement info of the drivers from any external hearer every OBU ought to be preloaded with a collection of anonymous digital certificates, wherever the OBU must sporadically amendment its anonymous certificate to mislead attackers. Consequently, a revocation of AN OBU leads to revoking all the certificates carried by that OBU resulting in a massive an outsized an oversized increase within the CRL size; The scale of VANET is incredibly large. in step with the us Bureau of Transit Statistics, there are just about 251 million OBUs within the Unites States in 2006. Since the quantity of the OBUs is large and every OBU contains a set of certificates, the CRL size can increase dramatically if solely a tiny low portion of the OBUs is revoked. to own a thought of however massive the CRL size will be, contemplate the case wherever solely a hundred OBUs are revoked, and every OBU has twenty-five,25000 certificates. during this case, the CRL contains two.5 million revoked certificates. in step with the used mechanism for looking out a CRL, the Wireless Access in transport Environments (WATE) normal doesn't state that either a non-optimized search algorithmic program.

2. EXISTING SYSTEM:

In this paper, we tend to take into account each non optimized and optimized search algorithms. consistent with the Dedicated Short vary Communication (DSRC), that is an element of the WAVE normal, every OBU has got to broadcast a message each three hundred millisecond concerning its location, velocity, and different telematics data. In such state of affairs, every OBU might receive an outsized variety of messages each three hundred milli second, and it's to see this CRL for all the received certificates, which can incur long authentication delay betting on the CRL size and also the variety of received certificates. the flexibility to see a CRL for an outsized variety of certificates associate exceedingly |in a very timely manner leads an inevitable challenge to VANETs. to confirm reliable operation of VANETs and increase the quantity of authentic data gained from the received messages, every OBU ought to be ready to check the revocation standing of all the received certificates during a timely manner. Most of the present works unnoticed the authentication delay ensuing from checking the CRL for every received certificate.

3. PROPOSED SYSTEM:

In this paper, we have a tendency to introduce an expedite message authentication protocol (EMAP) that replaces the CRL checking method by AN economical revocation checking method employing a quick and secure HMAC perform. EMAP is appropriate not just for VANETs however conjointly for any network using a

PKI system. To the simplest of our information, this can be the primary resolution to cut back the authentication delay ensuing from checking the CRL in VANETs.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ EMAP has the lowest computation complexity compared with the CRL checking processes employing linear and binary search algorithms.
- ✓ The number of messages that can be verified using EMAP within 300 msec is greater than that using linear and binary CRL checking by 88.7 and 48.38 percent, respectively.
- ✓ The proposed EMAP in authentication reduces the end-to-end delay compared with that using either the linear or the binary CRL checking process.

4. SYSTEM ARCHITECTURE

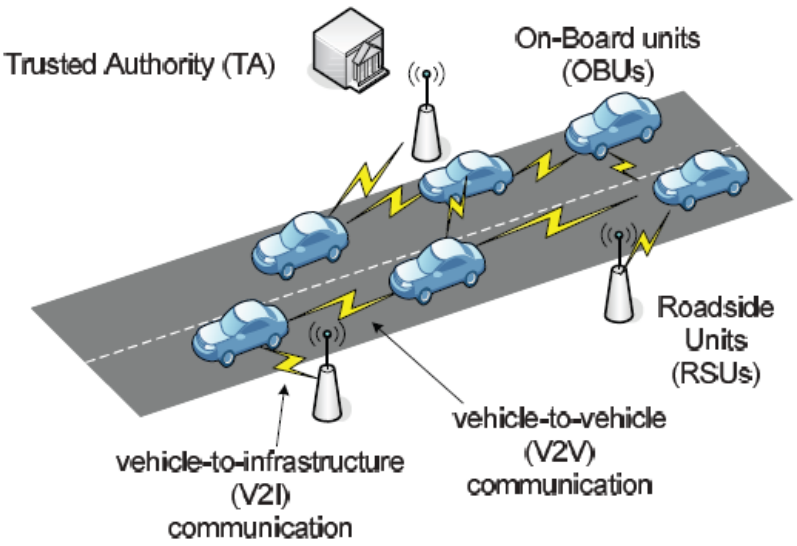


Fig 1. System architecture

5. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

MODULES

1. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure
2. Expedite Message Authentication Protocol
3. Security Analysis
    a. Hash Chain Values
    b. Resistance of forging attacks
    c. Forward secrecy
    d. Resistance to replay attacks
    e. Resistance to colluding attacks

5.1. 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 all the 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.

5.2. Expedite Message Authentication Protocol

In this Module,

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.

5.3. 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. SCREENS:

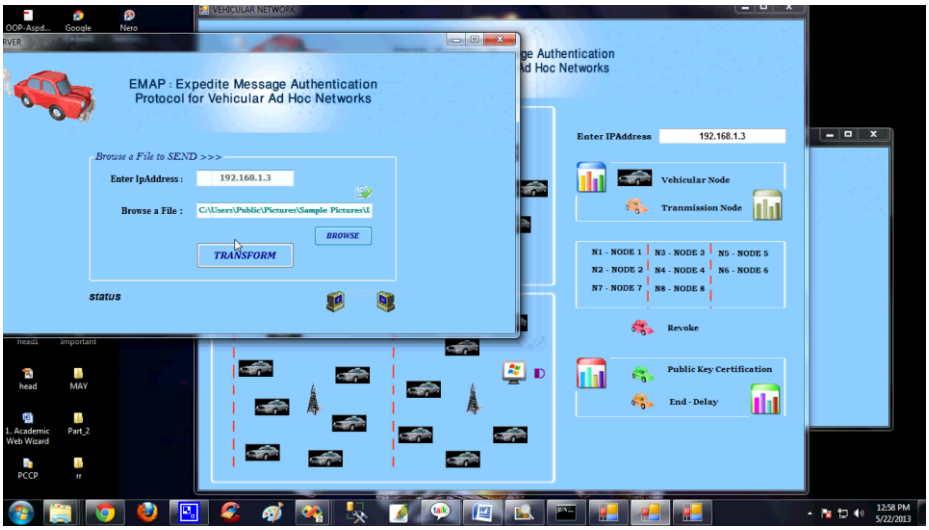


Fig 2. Selecting File in Server

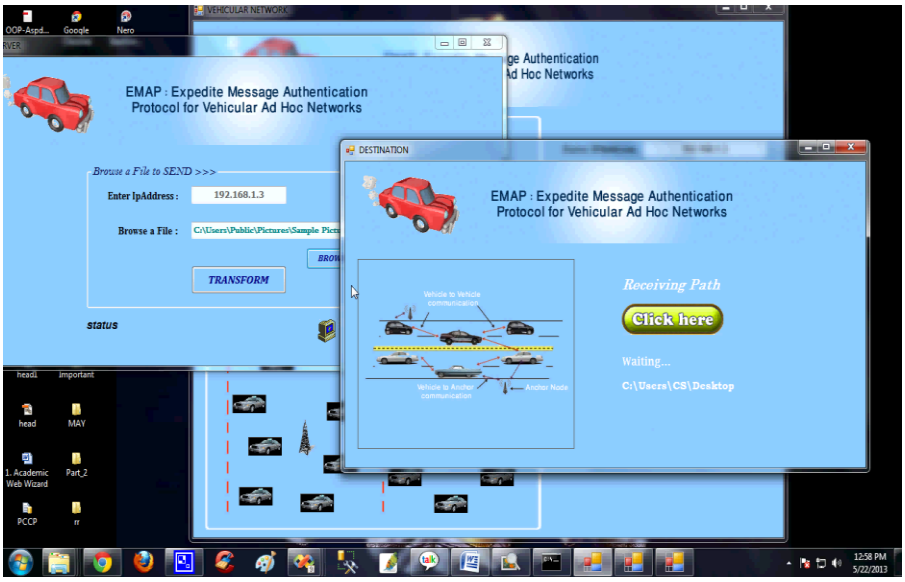


Fig 3. Saving File in Destination

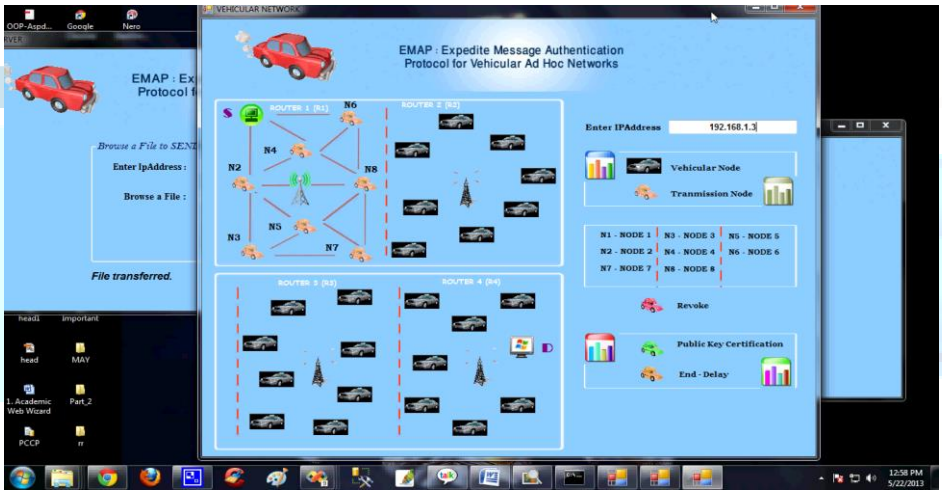
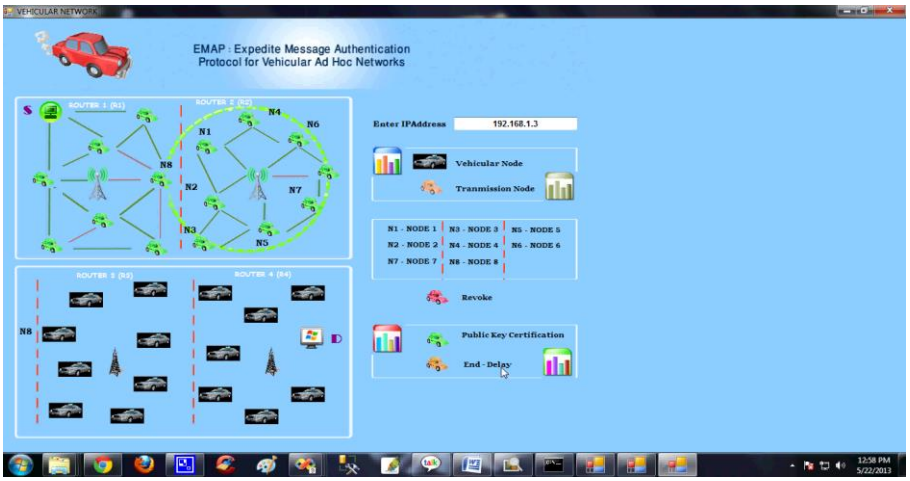


Fig 4. Vehicular Network



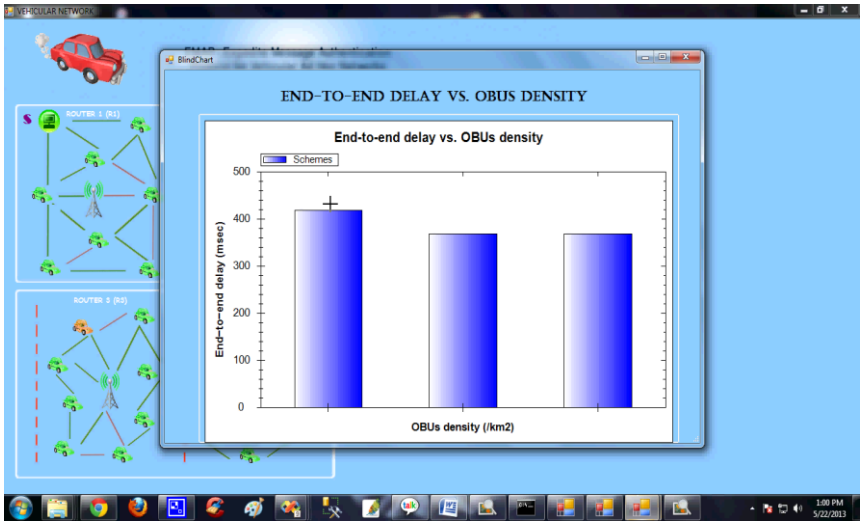


Fig 5. File Transferring through Router

Fig 6. File After Reached to Destination

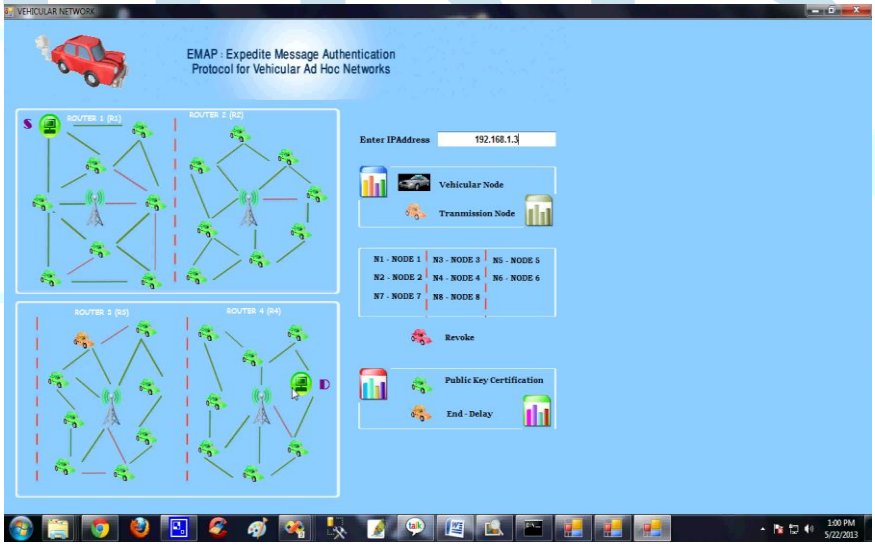
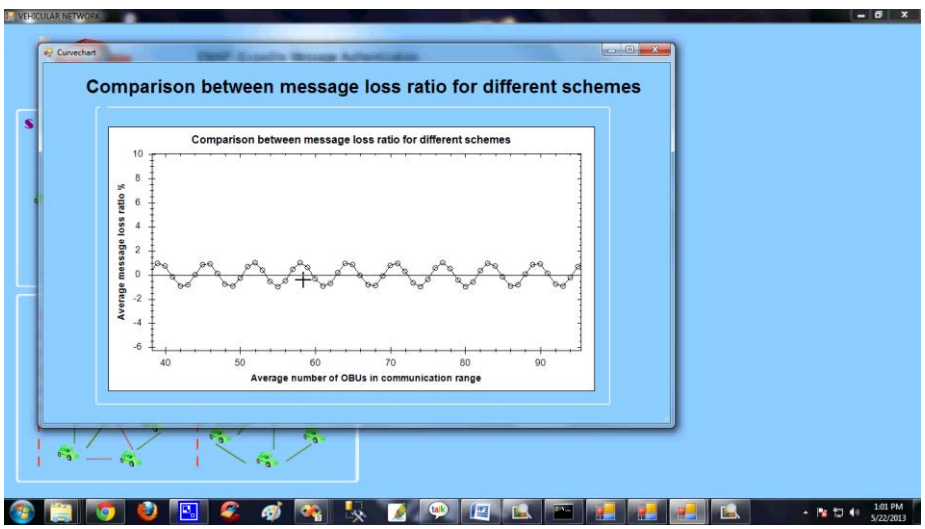


Fig 7. End-to-end delay vs density



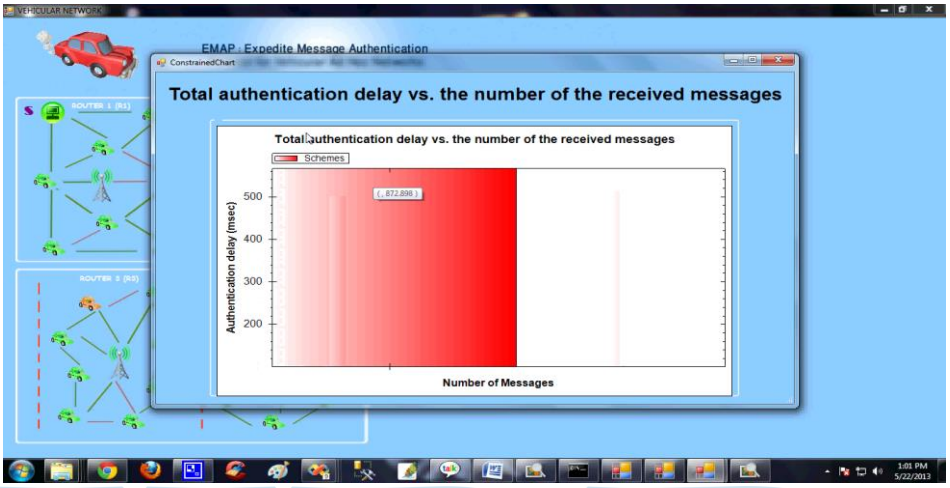


Fig 7. Comparison between massage ratio for different schemes

Fig 8. Total authentication delay vs. the number of the massage

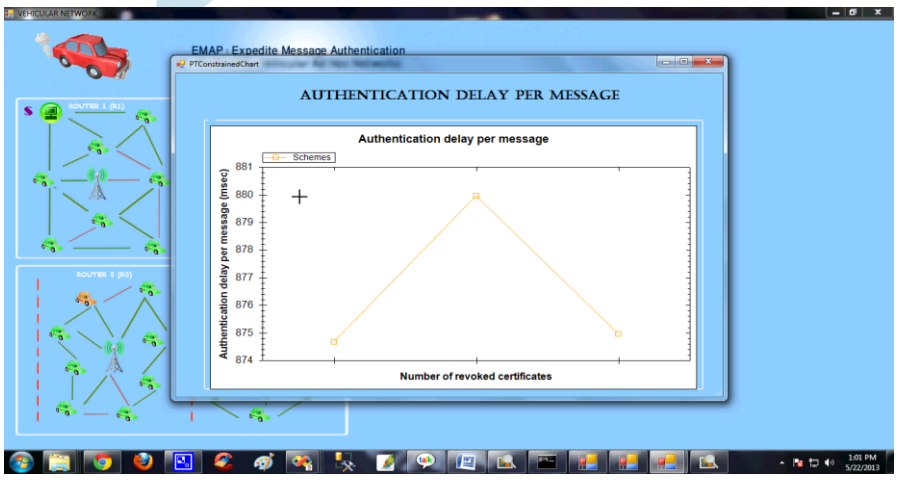


Fig 9. Authentication Delay per message

7.CONCLUSION

We have proposed 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. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/ admnsimp/pl104191.htm, 1996.
2. H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.
3. [7] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. of SP'02, 2002
4. [8] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. of SP'03, 2003.
5. [9] J. Li, N. Li, and W. H. Wins borough, "Automated trust negotiation using cryptographic credentials," in Proc. of CCS'05, 2005.
6. [10] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http: //seclab.cs.ucdavis.edu/projects/history/.
7. [11] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,
8. "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003.
9. [12] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003.
10. [13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005.

AUTHORS:

A.Srinivas, Post Graduated in Computer Science & Engineering (M.Tech) From JNT University, Hyderabad in 2009 and Graduated in Computer Science & Information Technology (B.Tech) from JNTU, Hyderabad in 2004.He is currently working as an Assistant Professor, Department of Computer Science & Engineering in Sri Indu College of Engineering & Technology (SICET), (V) Sheriguda, (M) Ibrahimpatnam, R.R.Dist, and Telangana, India. He has 9+ years of Teaching Experience. His research interests include Cloud Computing, Data Mining, Information Security,Software Testing, Wireless Networks and Software Quality.

Stalin babu J, Post Graduated in Computer Science & Engineering (M.Tech) From JNT University, Kakinada in 2011.He is currently working as an Assistant Professor, Department of Computer Science & Engineering in Nalla Malla Reddy Engineering College (NMREC), (V) Kachvanisingaram, (M) Ghatkesar, R.R.Dist, Telangana, India. He has 8 years of Teaching Experience. His research interests include Cloud Computing, Data Mining, and Information Security.