IJCAT International Journal of Computing and Technology, Volume 1, Issue 5, June 2014
ISSN : 2348 - 6090
www.IJCAT.org

Secure Network Discovery Using Expedite Message Authentication in VANET

[1]Ashwini N H, [2]Anand S Uppar

[1] Computer Science and Engineering Department, VTU University,
SDIT, Mangalore, Karnataka, India

[2] Computer Science and Engineering Department, VTU University,
SDIT, Mangalore, Karnataka, 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 Code(HMAC), 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.

***Keywords* - Vehicular Networks, Communication Security, Message authentication, Certificate revocation.**

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. VANETs 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:

- 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.
- The scale of VANET is very large.

2. Literature Review

Efficient and improved methods of secured data transmission in VANETs are the most recent research issues for full applicability in wide range of applications. Here we look below at the various schemes presented in this regard.

An efficient pseudonymous authentication scheme with strong privacy preservation, named PASS, for vehicular communications is proposed in paper [1]. Unlike traditional pseudonymous authentication schemes, the size of Certificate Revocation List (CRL) in PASS is linear with the number of revoked vehicles and unrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports Roadside Units-aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost irrelated to the number of the updated certificates. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle even all Roadside Units have been compromised. Extensive simulations demonstrate that PASS outperforms previously reported ones in terms of the revocation cost and the certificate updating overhead.

A number of projects have been developing security architectures for Vehicular Communication (VC) systems, with consensus on utilizing public key cryptography to secure communications. In spite of their advanced status on many aspects, none of these projects, has investigated and addressed the problem of Certificate Revocation List (CRL) distribution. As the need to evict compromised, faulty, or illegitimate nodes from the VC system is commonly accepted, a solution tailored to the requirements and constraints of the VC systems is proposed in paper [2]. The design is scalable and efficient, and can deliver seamlessly CRLs to all nodes within a region within tenths of minutes. More general, the analysis and simulation set the basis for the design of such CRL distribution systems, showing how to configure them to achieve more stringent requirements.

An efficient distributed certificate- service (DCS) scheme for vehicular networks is proposed in paper [3]. The proposed scheme offers flexible interoperability for certificate service in heterogeneous administrative authorities and an efficient way for any onboard units (OBUs) to update its certificate from the available infrastructure roadside units (RSUs) in a timely manner. In addition, the DCS scheme introduces an aggregate batch verification technique for authenticating certificate-based signatures, which significantly decreases the verification overhead. Security analysis and performance evaluation demonstrate that the DCS scheme can reduce the complexity of certificate management and achieve excellent security and efficiency for vehicular communications.

The emerging technology of vehicular communications (VC) raises a number of technical problems that need to be addressed. Among those, security and privacy concerns are paramount for the wide adoption of VC. Paper [4] is concerned with privacy and identity management in the context of these systems. The paper identifies VC-specific issues and challenges, considering the salient features of these systems. In particular, it views them in the context of other broader privacy protection efforts, as well as in the light of on-going work for VC standardization, and other mobile wireless communication technologies.

It is well recognized that security is vital for the reliable operation of vehicular ad hoc networks (VANETs). One of the critical security issues is the revocation of misbehaving vehicles, which is essential for the prevention of malicious vehicles from jeopardizing the safety of other vehicles. In paper [5], we propose an efficient decentralized revocation (EDR) protocol based on a novel pairing-based threshold scheme and a probabilistic key distribution technique. Because of the decentralized nature of the EDR protocol, it enables a group of legitimate vehicles to perform fast revocation of a nearby misbehaving vehicle. Consequently, the EDR protocol improves the safety levels in VANETs as it diminishes the revocation vulnerability window existing in conventional certificate revocation lists (CRLs). By conducting detailed performance evaluation, the EDR protocol is demonstrated to be reliable, efficient, and scalable.

3. System Architecture

In VANETs, the primary security requirements are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. A well recognized solution to secure VANETs was 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. 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.

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

In VANETS vehicles are moving in high speed and the duration of connection link between nodes depends on the radio range between them. VANET consists of two types of communications, V2V- Vehicular to Vehicular Communications and V2I- Vehicular to Infrastructure Communications. The main elements of VANETs are

- TA- Trusted Authority
- RSUs-Road State Units
- OBU-On Board Units

TA is the central authority which issues valid certificates for OBUs and contains CRL-Certificate Revocation List. For the secure communication of VANET PKI- Public Key Infrastructure is used. Every node will be having one public key and one private key which are issued by the TA. When one OBU sends message to another OBU, it can be done through either V2V or V2I mode. The receiver accepts the message only if the sender OBU is non-revoked OBU and the message is authenticated. CRL contains information about the certificates of revoked and non-revoked OBUs. TA returns the validity information to receiver OBU through intermediate RSU. If many OBUs want to communicate at the same time, it will result in a queue for message authentication. This will lead to message authentication delay in VANET and increases the workload of TA. To overcome this we can use an EMAP method to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL, and it employs keyed Hash Message Authentication Code (HMAC) in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs and so the queues for the message authentication is reduced. Since the key used in calculating the HMAC for each message is shared only between unrevoked OBUs the workload of TA is also reduced and hence the performance of the entire system is increased by reducing the delay and workload. Fig 1 shows the architecture diagram of VANET and its various elements and their communications for both V2V-Vehicular to Vehicular Communication and V2I- Vehicular to Infrastructure Communication.

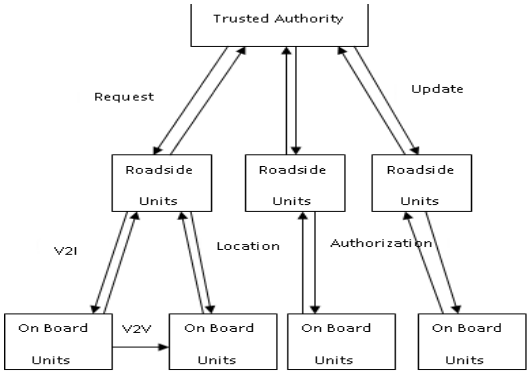

Fig 1: VANET Architecture

TA is in the top most position of the architecture. All the RSUs come under TA. OBUs come under one or more RSUs based on the distance, range, movement of OBUs and also based on the distance and range of each RSU. V2V infrastructure consists of direct contact between OBUs. But in V2I, one OBU contact another OBU through RSU. OBU requests certificate to TA through RSU. TA in return updates the keys and certificate of OBU through RSU. When an OBU receives message from another OBU, it checks the authorization of the message by contacting TA through RSU. When one OBU leaves the coverage of current RSU and it enters the coverage of a new RSU it updates its location information. OBUs accepts message from authorized OBUs only.

3.2 The Trusted Authority

TA contains a public key, a private key, CRL List, RSU List and OBU list. Public and Private keys of TA, RSUs and OBUs are calculated using key RSA algorithm.CRL List contains list of revoked OBUs. When an OBU's time validity becomes zero, TA will revoke it and its name will be entered into the CRL List. If revoked OBU is requesting for key renewal, that OBU will be taken away from CRL List. When any of one OBU becomes invalid, all other OBUs common key will be renewed (same common key for all valid OBUs) by the TA. RSU List contains names of all created RSUs. OBU List includes all OBUs names.

3.3 The Road Side Units

After TA is created RSUs has to be created one by one by entering the distance and range values for each RSU. If the distance value of one RSU is 50m and its range is

40m, its coverage will be between 10m-90m from the initial point for example from zero point. Similarly like TA, RSUs also have public and private keys. Other RSU elements are distance value, range value and OBU List. Whenever an OBU is created under the range of this particular RSU, that OBU name will appear in the OBU list of the corresponding RSU. As the OBU is assumed to be moving continuously, based on its coverage variation, OBU name will be entered and taken away from the OBU list of that RSU.

3.4 The On Board Units

Like TA and RSU, OBU also have public and private keys. In addition to these values OBU have time validity, one common key, supervising RSUs names, coverage value, options to see file to send, options to see file received, neighbor OBUs List, file browse option, send button , save button, clear button, key renewal option, genuine or malicious options .To show that OBU is moving coverage will be increased by 2 and decreased by 2 from the minimum and maximum value of coverage. Minimum value of coverage is OBU's (distance – range) and maximum value of coverage is OBU's (distance + range). Till the value of coverage is equal to covmax (maximum value of coverage), the coverage value will be increased by 2 to show that OBU is a moving node. Similarly till the condition (coverage>covmin) become false, coverage value will be decreased by 2 to show that OBU is moving in opposite direction.

As the OBU move like this, it enters to and leaves from the range of different RSUs. Based on this, the names given under Supervising RSUs will vary. OBU, RSU, port, time validity and system names will be generated randomly with some calculations. After the creations of RSU the OBUs will be created by giving input values for distance and range for each OBU. OBUs will be under the range of one or more RSUs based on its coverage values.

Time Validity will be generated randomly value using some calculations and it represents the validity duration of the OBU. Each second the time validity will be decreased by one and ultimately, it reaches to zero value and at that moment that OBU will be revoked and will be entered into the CRL List of TA. This time all other non revoked OBUs will be given one new same common key value to show that they all are valid OBUs and they can send message and the receivers verify the common key of the sender for accepting the sender's message) Common key (will be generated using key HMAC algorithm (SHA1)). Supervising RSUs include those RSUs unde which this particular OBU is coming. Coverage value varies each second based on the previous discussed calculations. When key renewal option is activated, new time validity will be generated and this particular OBU will become valid (non-revoked) and it can send and receive message. At this time its name will be taken away from CRL list of TA.

Common key of other non revoked OBUs will be given to this new valid OBU. Genuine OBU means that OBU does not hide its identity while sending message. Malicious OBU preserves identity. That means OBU wants to send message, but it do not wants to reveal its identity for safety matters. By using privacy preserving algorithm pseudo identity can be generated.

3.5 Message Sending

Message will be encrypted using RSA encryption algorithm and decrypted using RSA decryption algorithm. Along with the encrypted message, HMAC value which is calculated from the message (using Hmac algorithm) also will be sent to the receiver. Receiver after decrypting the message will calculate the Hmac value from the decrypted message. If both the received and calculated hash values are equal, it means that the message is authenticated.

3.6 Privacy Preserving

If OBU wants to preserve identity, it will select malicious option and correspondingly using privacy preserving algorithm, pseudo identity will be generated and message will be sent using the pseudo identity. RSU verify the validity by verifying pseudo identity using the values given by TA during the execution of privacy preserving algorithm. This perhaps helps in reducing the time delay.

4. Algorithms Used

4.1 HMAC Algorithm

The purpose of a MAC (Message Authentication Code) is to authenticate both the source of a message and its integrity without the use of any additional mechanisms. An HMAC (Keyed-Hash Message Authentication Code) function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input.

The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender, and compares the result computed with the received MAC. If the two values match, the message has

been correctly received, and assured that the sender is in the community of users that share the key.

4.2 RSA Encryption Algorithm

During key generation, whoever wants to receive secret messages creates a public key (which is published) and a private key (kept secret). The keys are generated in a way that conceals their construction and makes it 'difficult' to find the private key by only knowing the public key. While encrypting the secret message to any person can be encrypted by his/her public key (that could be officially listed like phone numbers). After receiving, only the person being addressed can easily decrypt the secret message using the private key.

4.3 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.

4.4 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 finished without finding a match which means that the certificate is unrevoked.

4.5 Privacy Preserving Algorithm

We modify the message signing phase to remedy the weaknesses as described. In addition, to decrease the transmission overhead incurred by delivering the packet from TA to the requesting vehicle in the initial handshaking phase, we propose that OBU does not sign and encrypt the shared secret between itself and the requesting vehicle. Our scheme is presented in the following.

4.5.1 Initial Handshaking Phase

ENC PK TA – Encrypting random id, password and signature using the public key of TA. RID, random id. PWD, password. SIG SK Vi , generating signature with random id and password using the secret key of OBU. Send the encrypted message X to TA through RSU. TA accepts block X and decrypts it to retrieve random id, password and OBU's signature. It then verifies whether the signature and are all valid and is not in the revocation list. The TA then passes to RSU to enable it to verify signatures from even if uses pseudo identity to sign the message.

In addition, the TA randomly selects a number to be the shared secret between TA, RSU and OBU. TA chooses a shared secret ti, a random number mi and then stores RID, ti and mi. By performing XOR operation with RID and ti calculates VPKi. It then computes block Y by encrypting s, VPKi, mi and signature (generated with s, VPKi and mi using secret key of TA.) using the public key of OBU. Similarly computes block Z by encrypting VPKi, mi and signature (generated with VPKi and mi using secret key of TA.) using the public key of RSU. Then it sends Y and Z to RSU. RSU accepts Y, Z from TA and decrypts Z using secret key of RSU. It will store VPKi and mi in its verification table, and forward Y to OBU. OBU accepts Y and then decrypts it using its secret key. Finally it stores the values s, VPKi, ti and mi in its repository. This basically completes the initial handshaking phase.

The following shows the procedure when vehicle leaves the range of an RSU and enters the range of another. It includes a simpler authentication process with the TA so that the TA can pass the information to the new RSU for verifying the signature and the new shared secrets will be generated by the TA. OBU chooses a random nonce and transmits to TA via this new RSU. The random nonce avoids from being tracked even an attacker captures a number of these packets as is moving across RSUs. The TA obtains it by decrypting the block using its private key and then removing the concatenation. This time the TA does not need to verify anymore as it has already done that during the starts up. Instead it directly generates a new key for OBU and transmits it to the new RSU and to the OBU. The TA then adds the new key into its repository. After storing into its verification table, RSU sends the key to OBU which then decrypts it using its conventional private key. From now on, it starts to use the

new shared secret with the new RSU for message signing. Initial handshaking phase algorithm,

OBU:
Step1: X = ENC PK TA (RID, PWD, SIG SK Vi (RID, PWD))
Step 2: Send X to RSU.
Step19: DEC SK Vi (Y).
Step20: Calculate ti = VPKi (+) RID.
Step21: Store (s,, VPKi, ti, mi).
RSU:
Step3: Send X from OBU to TA
Step 15: Accept Y, Z from TA
Step 16: DEC SK R (Z)
Step 17: Store (VPKi, mi).
Step 18: Send Y to OBU
TA:
Step4: Accept X send from OBU through RSU
Step5: Decrypt the block X.
Step6: Retrieve RID and PWD.
Step7: Verify Vi's signature.
Step8: Choose a shared secret ti.
Step9: Compute VPKi = ti (+) RID
Step 10: Select a random number mi.
Step 11: Store (RID, ti, mi)
Step12: Y = ENC PK Vi (s, VPKi, mi, SIG SK TA (s, VPKi, mi)).
Step13: Z = ENC PK R (VPKi, mi, SIG SK TA (VPKi, mi)).
Step 14: Send Y, Z to RSU

4.5.2 Message Signing Phase

To sign a message, a vehicle generates a pseudo identity using Y and the corresponding signing key. A different pseudo identity can be used for a different message. Choose a random number ri. Calculate the pseudo identity IDi using IDi1 and IDi2. H (mi IDi1) represents the hash function. Similarly compute secret key Ski using SKi1and SKi2. It then finds σi using the secret keys and Hmac value of the message and will send IDi, Mi and σi to RSU to communicate with the destination vehicle. Message Signing Phase Algorithm,

OBU:
Step1: Choose a random number ri.
Step2: Compute IDi = (IDi1, IDi2).
Step3: IDi1 = riPpub
Step4: IDi2 = VPKi (+) H(mi IDi1)
Step5: Compute SKi = (SKi1, SKi2)
Step6: SKi1 = mi IDi1
Step7: SKi2 = H(mi IDi1 ‖ IDi2)
Step8: Calculate σi = s (SKi2 + h(Mi) SKi2)
Step9: Send (IDi, Mi, σi) to others.

4.5.2 Message Verification Phase

RSU verify the pseudo identity using Z. σn is the shared secret between nth OBU and RSU. Vn is the nth OBU. Mn is the message of the nth OBU. This procedure allows an RSU to verify signatures using only two pairing operations based on the bilinear property of the bilinear map. After an RSU verifies signatures, it notifies the result to all vehicles within its RVC range. If a vehicle wants to verify a vehicle's signature on the message, checks the notification message as included in the RSU broadcast. When related information does not appear in the notification message, it means that RSU still has not yet verified. So has to wait for the RSU's next broadcasting message. We require an RSU to perform batch verification at a frequency higher than that a vehicle broadcasts safety messages so that a vehicle can verify the safety message of another before it broadcasts a more updated one. In the following, we only show the verification procedure. Notification message generation handle invalid signatures in the batch and extract valid ones from the batch instead of dropping the whole batch are the same in SPECS.

Therefore, our scheme can also reduce the message overhead substantially and enhance the effectiveness of the message verification phase.

Message Verification Algorithm,
RSU:
Step1: (σ1, σ2... σn) from (V1, V2…Vn) on (M1, M2….Mn)
Step2: Find (VPKi (+) H (mi IDi1).

5. Security Analysis

5.1 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.

5.2 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 enforceable.

5.3 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.

5.4 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.

5.5 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. Proposed System Design

In the proposed system HMAC code is used as OBUs can communicate with each without the intervention of the TA. In the EMAP when an OBU receives a message, it sends the senders id to RSU which in turn to TA. TA will check in the CRL for the revoked certificates to check whether the OBU is revoked or not and only after this long checking process the communication takes place. To reduce the time delay caused during this authentication process we use HMAC code. If an OBU wants to communicate with other OBUs, it sends an encrypted message with a HMAC code generated using the HMAC algorithm which will be generated by using the sender id and common secret key which knows all the unrevoked OBUs. The receiver OBU also generates the HMAC code by using common secret key. If the HMAC code is same, it means that the receiver node understands that the sender OBU is an authenticated one. Otherwise it would not process the message. For preserving privacy, OBU does not sign and encrypt the shared secret between itself and the requesting vehicle. To sign a message, a vehicle generates a pseudo identity and the corresponding signing key. In the revocation process, each OBU have the common secret key which is shared between all the legitimate OBUs. Also, each OBU is pre-loaded with a set of asymmetric keys RS and RP .Those keys are necessary for generating and maintaining a common shared secret key between unrevoked OBUs. The revocation is triggered by the TA when there is an OBU to be revoked. The certificates of OBU must be revoked. In addition, the secret key set of OBU and the current secret key Kg are considered revoked. Hence, a new secret key K˜g 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. Pseudo identity provides privacy. It can be traced by RSU using the Y value given by the TA while executing privacy preserving algorithm. Using the Z value of the OBU and using its signature and password etc each time it can create new pseudo identities. So with the previous pseudonym no one can trace it. When an OBU enters under the range of a new RSU, new shared secret key will be generated for Y and Z values, which prevent previous RSUs from revealing the OBUs privacy.

7. Conclusions

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 integrable 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.

Acknowledgments

I would like to acknowledge Prof. Anand S Uppar HOD Dept of CSE Shree Devi Institute of Technology Mangalore, Asst. Prof. Madhuri B Dept of CSE Shree Devi Institute of Technology Mangalore.Insert acknowledgment, if any.

References

[1] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, “Certificate Revocation List Distribution in Vehicular Communication Systems” 2008

[2] A. Wasef and X. Shen, "Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks." 2009

[3] Albert Wasef, Yixin Jiang, and XueminShen, "An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks" 2010

[4] Yipin Sun, Rongxing Lu, Xiaodong Lin, XueminShen, Jinshu Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications" 2010

[5] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: a Position Paper" 2006

[6] Khaleel Mershad, Hassan Artail and Haidar Safa. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "Routing Packets to Distant Locations in VANETs",11th international conference on ITS telecommunication 2011

[7] Y. Ding, C. Wang, L. Xiao, "A static-node assisted adaptive routing protocol in vehicular networks", VANET'07, New York, USA, Sep. 2007.

[8] C. Lochert, H. Hartenstein, J. Tian, H. Füÿler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments", Proc. of the IEEE Intelligent Vehicles Symposium, Piscataway, USA, Jun. 2003, pp. 156-161.

[9] C. Lochert, M. Mauve, H. Füÿler, and H. Hartenstein, "Geographic routing in city scenarios", SIGMOBILE (2005), Vol. 9, No. 1, pp. 69-72.

[10] V. Naumov and T. Gross, "Connectivity-aware routing (CAR) in vehicular ad-hoc networks", INFOCOM 2007, Anchorage, USA.

[11] J. Zhao and G. Cao, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks", IEEE Tran. on Vehicular Technology, Vol. 57, No. 3.

[12] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET Routing on City Roads Using Real-Time Vehicular Traffic information", IEEE Tran. On Vehicular Technology, Vol. 58, No. 7, pp. 3609-26.

[13] Y. Bae and N. H. Vaidya."Location-Aided Routing (LAR) in mobile ad hoc networks", MobiCom'98, Dallas, USA, Oct. 1998, pp. 66-75.

[14] S. Basagni, I. Chlamtac, and V. R. Syrotiuk, "A Distance Routing Effect Algorithm for Mobility (DREAM)", MobiCom'98, Dallas, USA.

[15] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, "MDDV: Mobility-Centric Data Dissemination Algorithm for Vehicular Networks," VANET04,Philadelphia, USA, Oct 2004, pp. 47-56.

[16] A Joint Routing and Location Service for VANETs MarwaneAyaida, MohtadiBarhoumi, HacèneFouchal, YacineGhamri-Doudane and LissanAfilal Global Communications Conference (GLOBECOM), 2012 IEEE.

Author Details

Mrs.Ashwini N H is an M. Tech Student of Computer Science & Engineering Department of SDIT, Mangalore. She graduated with BE (Honours') in Computer Science and Engineering from VTU University, Belgaum. She is currently pursuing her Masters.

Prof. Anand S Uppar. He graduated with BE (Honours') in Computer Science and Engineering from KUD University, Dharwad and Post Graduated With ME(Honours') in Computer Science and Engineering from shivaji University, Kolhapur. He is currently Professor & Head, Department of Computer Science & Engineering, at SDIT(Shree Devi Institute of Technology) affiliated to VTU university. His research areas are: Computer Networks and Cloud computing.