ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Fast and Secure Countermand Verification Process Using MAP in Vehicular Ad Hoc Network

A.Masanam[1], S.Suganya[2], P.RajiPriyadharshini[3]

P.G. Student, Department of Computer Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu- India[1]

P.G. Student, Department of Computer Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu- India[2]

P.G. Student, Department of Computer Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu- India[3]

Abstract: Secure Authentication in VANNET is deploying by 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), contains the list of revoked certificates. In a PKI system, the authentication of any message is performed by first checking in the CRL. The user in the CRL list can be maintained by OBU and the certificate list can be huge. So, checking for the authentication can be performed by using linear search or some other searches in optimized way. In the proposed system, Message Authentication Protocol (MAP) can be used for authentication purposes here to check the revocation list based on Keyed Hash Message Authentication code generated by MAP. The OBU units can maintain the secret keys and it can be communicate with RSU for update the secret keys. The checking authentication shares the secret code only between the non-revoked lists in the On Board Units (OBU) and also updates the secret key. MAP can be reducing the time delay for checking the message verification.MAP method for revocation process uses the keyed Hash Message Authentication Code(HMAC).Such Calculation for HMAC helps in share message between the non-revoked On-Board Units (OBUs).MAP can significantly decrease the message loss ratio. As per the security analysis and performance evaluation, MAP is demonstrated to be secure and efficient. The RSU can convert the revoked vehicle to non revoked vehicle. It is faster than the TA verification. The non revocation process is done by the road side unit and the batch verification is also used for verify the message.

Keyword: Certificate Revocation List, On Board Unit, Trusted Authority, HMAC, RSU.

I. INTRODUCTION

A **Vehicular Ad-Hoc Network** or **VANET** is a technology that uses moving vehicles as nodes in a network to create a mobile network. The primary goal of VANET is to provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created.VANET is a subgroup of MANET where the nodes refer to vehicles.

Since the movement of Vehicles are restricted by roads, traffic regulations we can deploy fixed infrastructure at critical locations. Vehicular network is an emerging network, which vehicles and roadside units are the communicating nodes. They provide each other different information, such as safety warnings and traffic information. As a cooperative approach, vehicular communication can be more effective in avoiding accidents and traffic

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

congestions than if each vehicle tries to solve these problems individually. Vehicles, are equipped with wireless communication capability, are capable of communicating with each other and with roadside and infrastructures. Vehicular network is a special category of Mobile Ad-hoc Networks (MANETs). Even though all the characteristics and concerns apply for vehicular networks, some of the elements are different. Potentially high number of nodes/vehicles, high mobility and frequent topology changes, high application requirement on data delivery, no confidentiality of safety information, privacy issue are the major unique characters. Resource is not limited, especially energy limitation. Vehicles, in communicating with Roadside units different wireless technologies can be used. The wireless technologies used may be short range such as Wi-Fi and a long-range technology of cellular networks. If both technologies exist in together, they will have a collective overall capacity. The preference among the existing wireless channels depends on communication requirement of applications and the different available service i.e. applications use channel that fulfil their communication requirement. The final intention is to provision both safety applications and non-safety applications that enhance the driving experience of drivers with reliable communication. As one of main component of ITS, vehicular network have different entities that makes network communication exists.

VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units(RSUs).

OBU is a component that is putted in vehicles, to make them participate in the network. This generally installed in or on a vehicle; however, in some specific circumstances it may be portable or hand-held. This proposal assumes that each vehicle is equipped with an OBU. The purpose of an OBU is to communicate with other OBUs and RSUs. The OBU contains an in-built smart card reader and its own onboard crypto-processor based on a trusted computing module that is capable of running cryptographic functions in a reliable and safe fashion. This research argues that the OBU should be run on top of trusted hardware, firmware, and an operating system to provide the foundation for secure messaging from both internal and external threats. The on-board unit (OBU) is the device, installed in the motor vehicle of the road user. The battery powered on-board unit can be easily attached to the inside of the windscreen and needs not be connected to a power source in the vehicle. The OBU will be handed over at the Customer Service Points after registration and payment of an established deposit. The on-board unit contains various data specifically assigned to a vehicle for accurate identification. This specific data includes, among others, the license plate number, the number of axles and a unique ID. In case of modification of this data, the old OBU must be reconfigured and newly assigned to the new vehicle at a Customer Service Point before entering the toll road.

RSU is a component that is located on side of road. It provides a lot of safety and convenience related information for vehicles such as information about traffic density, weather information etc. It mostly comprises short-range radio link like Wi-Fi. But it may use long-range radio link. It involves in traffic associated to Vehicle to-Roadside or inter-roadside communication. The Roadside unit (RSU) is a distributed system established and managed by its TA. The RSU contains a read-only copy of the public key directory maintained by its TA to perform key unit can be installed during the manufacturing of the vehicle or can be smart devices that the user uses inside a vehicle.

This is the more interesting part of vehicular network. The Onboard unit (OBU) is a dedicate short range communication verification. Namely, when a key verification request is received at the RSU, the RSU performs the key verification result. The RSU also plays the role of a relay agent to forward relevant information from its TA, participating when require, and vice versa. RSUs are densely distributed in the roadside. In our protocol, RSUs are used to issue secret member keys to vehicles and assist the TM to efficiently track the real identity of a vehicle from any safety message.

II. LITERATURE SURVEY

1. Security requirements and solution concepts in vehicular ad hoc networks

The main benefit of this kind of communication is seen in active safety systems, which aim at increasing passengers' safety by exchanging warning messages between vehicles. Security issues in vehicular ad-hoc networks (VANETs) regarding active safety applications. Provide an overview on solution concepts and evaluate requirements of corresponding mechanisms. One conclusion is that although some concepts can be viewed as strong solutions from a network point of view, they do not fit into the design constraints of VANETs.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

2. Privacy and Identity Management for Vehicular Communication Systems: A Position Paper

Identify VC-specific issues and challenges, considering the salient features of these systems. View 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. Addressing privacy and identity management in VC warrants not only novel approaches but it can also have a strong impact in the overall architecture, beyond security, of those systems.

3. TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs

A Public Key Infrastructure (PKI) can provide this functionality using certificates and fixed public keys. However, fixed keys allow an eavesdropper to associate a key with a vehicle and a location, violating drivers' privacy. Our scheme efficiently prevents eavesdroppers from linking a vehicle's different keys and provides timely revocation of misbehaving participants while maintaining the same or less overhead for vehicle-to-vehicle communication.

4. The Security and Privacy of Smart Vehicles

Consider communications specific to road traffic: safety and traffic optimization (including finding a parking place)

- Messages related to traffic information (and parking availability)
- Anonymous safety-related messages
- Liability-related messages

Do not consider more generic applications, e.g. tolling, access to audio/video files, games.

5. Certificate Revocation List Distribution in Vehicular Communication Systems

In vehicular communication certificate revocation list (CRL) distribution is considered. Compromised, faulty, or illegitimate nodes from the VC system are commonly accepted. The CRL is distributed to all the nodes with in 10 minutes. The CRL is partitioned in to several pieces and send to the nodes.

III. PROPOSED SYSTEM

Fast and secure revocation verifying process can be enhanced by adopting the revocation process by the RSUs rather than by the TA. Thereby, certificate revocation process can be done in a time consumed manner. 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 the 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 OBU. The CRL verification is performed using the concept of hash chain. The RSU can convert the revoked vehicle to non revoked vehicle. It is faster then the TA verification. The non revocation process maintains 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 secure communication and the hash value form the hash chain. Update both the secret key and the hash value and at last redistributed. The updated CRL is now distributed by the RSU to the all other OBUs.

Also, batch verification will be included so that the mass of message verification can be done by the receiver in a fast manner. The destination vehicles verify the received message by using the SHA-1 algorithm. In existing the destination vehicle verify the integrity of the message one by one. But now the destination verifies the integrity of the message by the batch verification. It means the destination get all the data in a batch and verify all that at a same time by the sha-1 algorithm. It consumes less time then the existing method. In existing method the messages are verified one by one. It consumes more time. Performance will be evaluated by comparing the revocation process done by the TA and RSU.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Security of the data is very high because the key size of RSA is very high. So that the security of the data very much improved by using this RSA. Using batch verification the data are verified very fast manner.

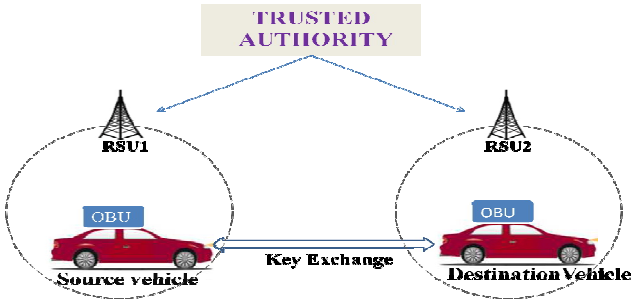


Figure 1 System Architecture

The system architecture consists of roadside units and trusted authorities (CAs) for managing the RSUs. For a single trusted authority there are two roadside units are present in the network. So the roadside unit can perform well then the trusted authority.CRL status verification is done before receiving the message. This could be performed by specifying a timestamp randomly. When submitted the CRL status is displayed whether the vehicle is revoked or non revoked. If the source vehicle is revoked, non revocation process is carried out. This could be performed by getting the id and the hash value from the hash chain of the vehicle. Perform updating process and it is viewed finally. The secret key which is shared must also be updated. The final phase is that authentication by the arrival of message. The roadside unit can manage the data transferred in the network.

IV. MODULES

Several set of modules are developed for find out authorized vehicle or unauthorized vehicle. The modules are i) Vehicle Registration ii)Authentication to Vehicle iii)RSU Verification iv)Non Revocation process v)Batch Verification.

i) Vehicle Registration: 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.

ii) Authentication to Vehicle: 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.

iii) RSU 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 the 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 OBU. The CRL verification is performed using the concept of hash chain. The RSU can convert the revoked vehicle to non revoked vehicle. It is faster than the TA verification.

iv) Non 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

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

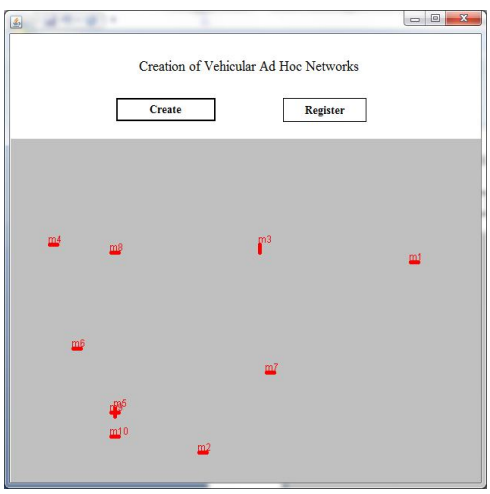
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

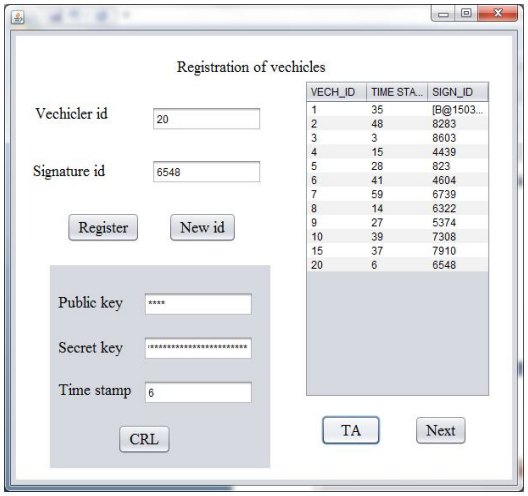
message without ignorance. The process can be performed by gathering the revoked OBU's secret key which is used secure communication and the hash value form the hash chain. Update both the secret key and the hash value and at last redistributed. The updated CRL is now distributed by the RSU to the all other OBUs.

v)Batch Verification: The destination vehicle verify the received message by using the SHA-1 algorithm. In existing the destination vehicle verify the integrity of the message one by one. But now the destination verifies the integrity of the message by the batch verification. It means the destination get all the data in a batch and verify all that at a same time by the sha-1 algorithm. It consumes less time.

V. EXPERIMENTAL RESULTS



(a)



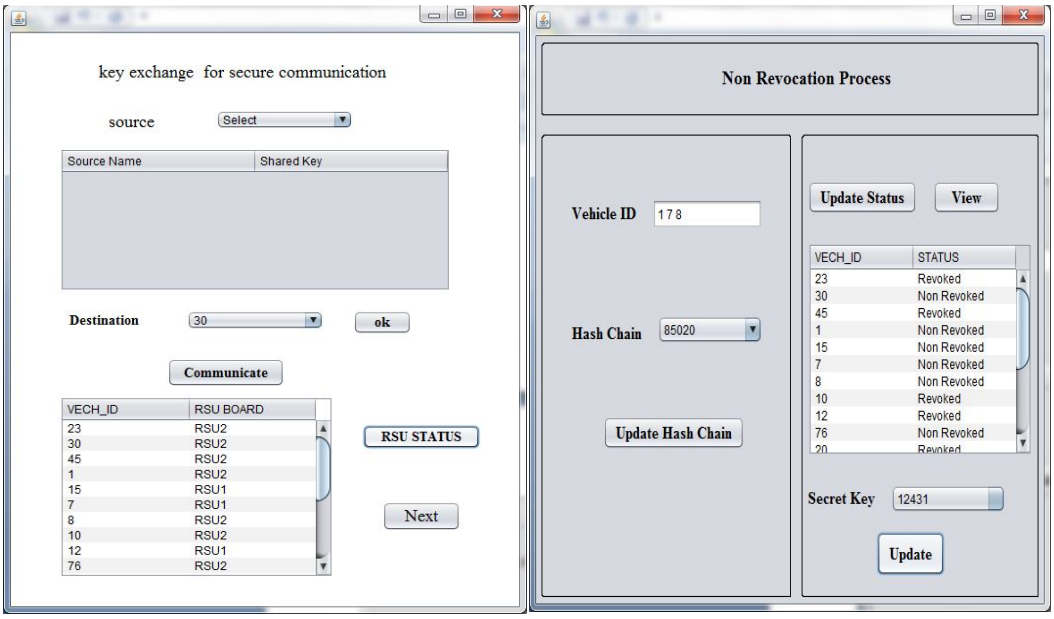
(b)

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014



(c) (d)

Figure 2 (a) to create a vehicle (b) registration of vehicles (c) communicating between source and destination vehicle (d) verifying the CRL process

VI. CONCLUSION

The technique has only one request reply message exchange.VANET reduces the bandwidth requirement and the total communication delay in the authentication process. Authentication process should be carried out in order to ensure whether the source vehicle has been revoked or not.CRL status should be listed and validation should be held. If the source vehicle is revoked then non revocation process should be held. Once the source node gets non revoked hash value should be updated similarly key which is used for communication should be updated. Message verification process will be carried out at destination phase, it verifies with the MAC code which has been generated by the source vehicle and performs batch verification process.

REFERENCES

[1] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets," IEEE Trans. Vehicular Technology, vol. 61, no. 1,pp. 86-96, Jan. 2012.

[2] Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[3] Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

[4] A.Wasef and X.Shen,"EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 9, pp. 5214-5224, Nov. 2009.

[5] P. P.Papadimitrators,G.Mezouur and J.ubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," Proc. Fifth ACM Int'l Workshop VehiculAr Inter-Networking pp. 86-87, 2008.

[6] 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.

[7] Wasef and X. Shen, "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks," Proc. IEEE GlobeCom, 2009

[8] Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs,"Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9, 2009

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

BIOGRAPHY

A.Masanam, received B.E (computer science) Degree from Periyar Maniammai University, Vallam and now pursuing M.E (computer science and engineering) in Parisutham Institute of technology and science, Thanjavur, Tamilnadu, India. Interested in mobile computing, networking.

S.Suganya, received B.E (computer science) Degree from Anna University, Chennai and now pursuing M.E (computer science and engineering) in Parisutham Institute of technology and science, Thanjavur, Tamilnadu, India. Interested in Cloud computing, Database management.

P.Rajipriyadharshini, received B.E (computer science) Degree from Anna University, Chennai and now pursuing M.E (computer science and engineering) in Parisutham Institute of technology and science, Thanjavur, Tamilnadu, India. Interested in mobile computing, networking.