ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Privacy Preserving Authentication for Security in VANET

[I]Mahalakshmi.R.S, [II]Alangudi Balaji.N
[I, II]Dept. of Computer and Communication Engineering
Sethu Institute of Technology, Virudhunagar, India

Abstract
With the present era of Vehicular Communication, a Vehicular ad-hoc network(VANET) is facing problem with vehicle anonymity and location privacy while communicating among the vehicle. To overcome that Vehicular Public Key Infrastructure(VPKI) has been used. Security becomes very important for VANET considering the criticality of safety application.In VANET authentication is a crucial security requirement to avoid attacks to both inter-vehicle and vehicle-to-roadside communication.Vehicles have to be prevented from the misuse of their private data and the attacks on their privacy. VPKI is the effective technique used for the security purpose and city road scenario with an assumption that each safety message carries the location information of the sending vehicle. In this paper, a distributed Vehicular Public Key Infrastructure is used to secure VC, and preserve vehicle location privacy and anonymity. To ensure security RSA key generation technique has been used. RSA is a open network environment technology, using public key cryptogram system.

Keywords
Vehicular Ad-hoc Network, PKI, Vehicle anonymity, Security, Privacy, RSA Algorithm

I. Introduction

Within the next decade, vehicles will be equipped with Dedicated Short Range Communication (DSRC) capabilities to provide a means for a Vehicular Ad-hoc Network (VANET) where vehicles On-Board Units (OBU) communicate wirelessly with other vehicles OBUs or Road Side Units (RSUs). VANET aims at enhancing driving safety through inter-vehicle or vehicle-to-infrastructure communications. Safe driving is the milestone application for VANETs. In general, a secure network should have the following attributes: (i) authentication (ii) non-repudiation (iii) confidentiality (iv) data integrity (v) access control (vi) availability.

The evolution of Vehicular Communications (VC) over the past years leads to extended investigations in collaboration with the Car-to-Car communication Consortium (C2C-CC) [4]. The importance of authentication in vehicular communication is to ensure that, when a connection is established between two entities without previous knowledge of one another, they are actually communicating securely with their intended destination entity and not an attacker in existence of Certification Authority (CA) [2]. Authentication is the most essential mechanism for network activity, because if the destination party is not authenticated, then establishing secure channels is not prudent. The important challenge for VANETs is to provide AAA for the offered services, while preserving vehicle anonymity and location privacy.

In this work, the implementation of VPKI is used, in order to secure VC using a privacy-preserving architecture according to the standards. The kerberized version of a VPKI is presented by using cryptographic tickets to enable AAA to the provided services. While preserving the privacy against the VPKI credential management is offered.

The anonymization schemas based on pseudonymous certificates and group signatures presented in [5]. A draft version of standards for secure VC appeared in the IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE) [3]. Other standardization and harmonization efforts by the Car-to-Car Communication Consortium (C2C-CC) [4] and European Telecommunications Standards Institute (ETSI) [6] also converged towards the usage of pseudonymous certificates for privacy-preserving vehicular applications.

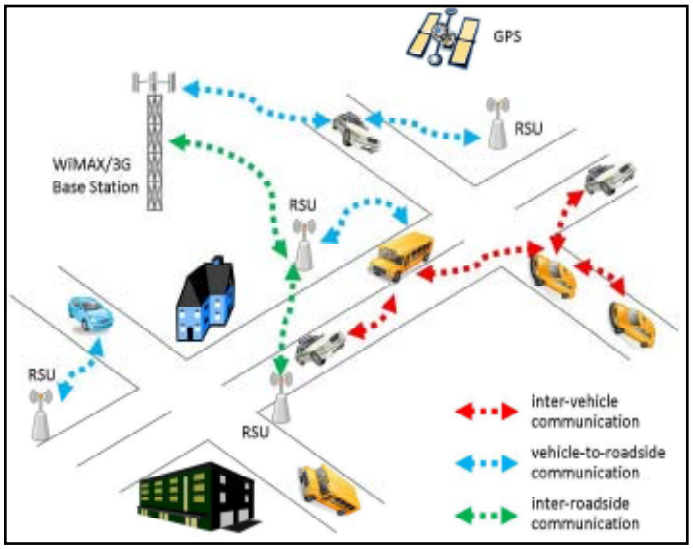

Fig. 1: VANET Structure

The European Project SeVeCom [7] defines the architecture for secure VC. In addition, it addresses aspects such as key management and distribution, vehicle certification and credential management. The effectiveness of pseudonyms in preserving anonymity and location privacy for VC is studied in [9]. The impact of security on safety beaconing has been presented in [10].

The current proposals for security and privacy depends on the implementation of a VPKI, this is the first work to provide efficiency results and considers a AAA solution. A resolution approach using cryptographic tokens issued by a trusted authority is presented in [13]. De-anonymization of the vehicles in case of user misbehavior is a requirement for safety applications in VC [2,4]. Therefore, PKI paradigms such as [13,15] cannot be employed since they do not provide revocation or anonymity, respectively.A detailed threat analysis and appropriate security architecture is presented in [5] here, the set of security protocols are provided to show that they protect privacy. Finally robustness and efficiency results are analyzed in [5].

In future vehicles will become significant mobile platforms, extending the digital life of individuals with an ecosystem of application and services. To secure these services and to protect the privacy of individuals VPKI based approach towards multi-

service security architecture is discussed in [8]. The paper [11] suggested to protect the network (VANET) from adversary and attacks still not enough, trying to reach a satisfactory level, for the driver and manufacturer to achieve safety of life and infotainment. The need for a robust VANET networks is strongly dependent on their security and privacy features. In this paper a various types of security problems and challenges of VANET been analyzed and discussed to solve these challenges and problems.

In [14] an efficient and spontaneous privacy-preserving protocol for vehicular ad-hoc networks based on revocable ring signature. The proposed protocol has three appealing characteristics: First, it offers conditional privacy preservation: while a receiver can verify that a message issuer is an authorized participant in the sstem only a atrusted authority can reveal the true identity of a message sender. Second, it is spontaneous: safety messages can be authenticated locally, without support form the roadside units or contacting other vehicles. Third, it is efficient by offering fast message authentication and verification, cost-effective identity tracking in case of a dispute and low storage requirements. Extensive analysis is used to demonstrate the merits of the proposed protocol and to contrast it with previously proposed solutions.

II. Existing System

A special kind of Mobile Ad-hoc Networks (MANETs) is the VANET. Here, the communications are taken by among the nearby vehicles. While communicating the vehicles the safety messages/packets are transferred between vehicles with the location information of that sending vehicle. Transmission of traffic, emergency alerts and routing related information is the essential task of VANET.

In existing system, each vehicle is equipped with a temper-resistant crypto-module. Packet authentication is not guarantee with this crypto-module. Using impersonation attacks, the attacker claims to have a legitimate identity and can fabricate messages or replay old packets. Attackers constantly change the content of packets to achieve erroneous or malicious behavior. Packet forgery is a serious attack in the previous system.

III. Proposed System

A distributed VPKI is used to monitor the network or malicious activities. It is an arrangement that binds public key with respective user identities by means of a certification authority. RSA key generation techniques has been used for security and authentication. RSA is an open network environment technology, using public key cryptogram system theory has implemented and supplied a universal security services, it has two main applications, include encryption and digital signature.In VPKI, the user identity must be unique within each CA domain.

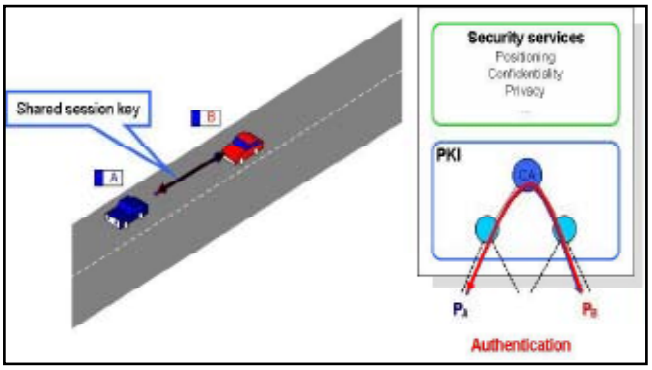

Fig. 2: PKI Authentication

A. Network Formation

VNAET is a technology that uses moving cars as nodes in a network to create a mobile network.It turns every participating car into a wireless router or node, allowing approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. The network architecture may have number of nodes and the simulated area is about 2km*2km. The node size, position and colors are initialized in the network.

B. Traffic Montoring

Traffic monitoring using GPS equipped vehicles raises significant privacy concerns, because the external traffic monitoring entity acquires fine-grained movement traces of the probe vehicle drivers. These location traces might reveal sensitive placesthat drivers have visited for example medical conditions, political affiliations, traffic violations, or potential involvement in traffic accidents. Traffic monitoring does not need to depend on individuals or personal information, only on the aggregated statistics from a large number of probe vehicles.

C. Virtual Trip Line

A virtual trip lines are geographical markers stored in the client i.e., vehicle which trigger a position and speed update whenever a probe vehicle passes.When a vehicle traverse the trip line its location update comprise time, trip line ID, speed and the direction of crossing.The trip lines are pre generated and stored in clients. To check any crossings, we set the sampling period of a single-chip GPS/A-GPS module and retrieve the position readings.

D. Algorithm Implementation

The RSA algorithm is an example of a public key algorithm. RSA is an open network environment technology, using public key cryptogram system. In a public key algorithm(PKA), pair of keys is used.One of the key is the private key, is kept secret and not shared with anyone. The other key is public key, is not secret and can be shared with anyone. Data is encrypted by one of the keys, it can only be decrypted and recovered by using the other key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key.

E. Performance Evoluation

It is easy to find the malicious node,avoids traffic signal and reduce delay during data transfer is reduced. Delay, packet overhead and packet deliveryratio are evaluated. Finally, vehicular communication in VANET is done with a data transfer in efficient manner.

1. DELAY

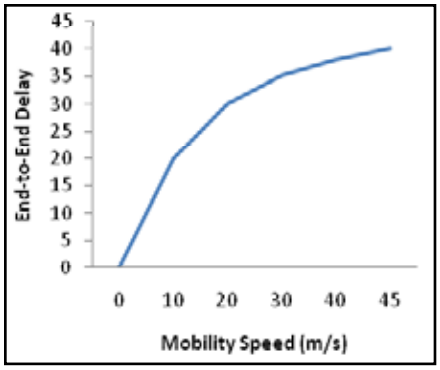

Fig. 3: Mobility Speed Vs End-to-End Delay

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

In Figure 3, the graph represents the packet delay to the node in the network. When mobility speed of the vehicle is increased the packet delay is also increased.

2. Packet Overhead

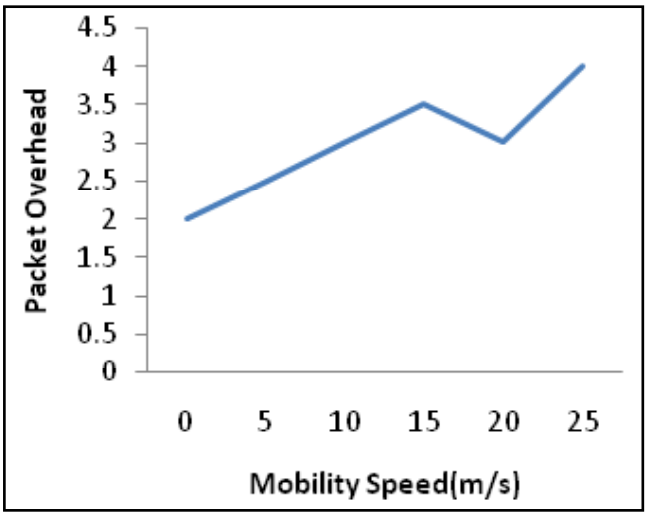

Fig. 4 Mobility Speed Vs Packet Overhead

In Figure 4, the graph represents the packet loss i.e., overhead to the node in the network. When the mobility speed in increased the packet loss is varied with the speed.

3. Packet Delivery Ratio

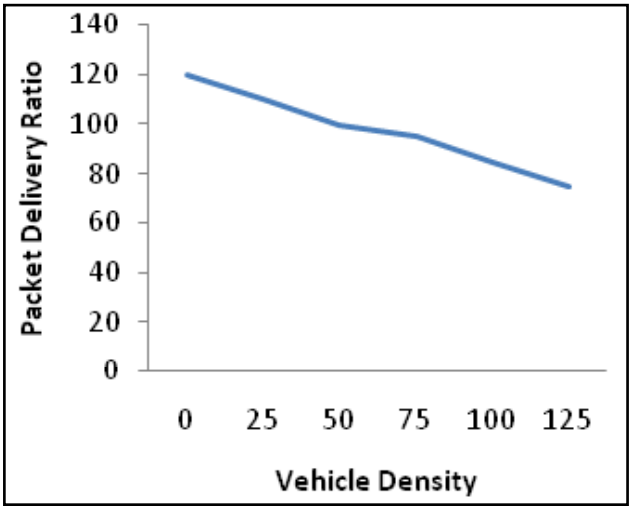

Fig. 5 Vehicle Density Vs Packet Delivery Ratio

In Figure 5, the graph represents the delivery ratio of the packet. When the vehicle density is increased in the certain region the delivery ratio will be less.

IV. Conclusion

This work is mainly used to provide a security with a location privacy preservation. The proposed approach utilizes a distributed VPKI architecture to provide security and privacy protection in VANETs. The packets are delivered between the vehicle with the location information. The generated tickets are used to guarantee unlinkability between consecutive vehicle requests for pseudonyms, when a new ticket is used for each request.

V. Future Enhancement

In future enhancement, presenting an anonymous authentication and verification schemefor the IEEE Wireless Access in Vehicular Environment(WAVE) based VANET. The polynomial encryption techniques are used for more security. The contribution includes vehicular message authentication and an efficient prioritized verification strategy for periodic road safety messages.

References

[1] *B.Parno and A.Perrig, "Challenges in Securing Vehicular Networks", Nov.2005.*
[2] *J.P.Stotz et al., eds. "Security Requirements of Vehicle Security Architecture". June2011.*
[3] *IEEE 1609.2 Draft Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages. Jan.2012.*
[4] *Car-to-Car Communication Consortium(C2C). Jan.2013.*
[5] *Jean-Pierre Hubaux and M.Raya, "Securing Vehicular Adhoc Networks" Journal of Computer Security,2007.*
[6] *ETSI TR 102 638. Intelligent Transport Systems(ITS); Vehicular Communications; Basic Set of Applications; Defintions. June2009.*
[7] *A.Kung, ed. "Security Architecture and Mechanisms for V2V/V2I". SeVeCom-Deliverable 2.1 Version 3.0. Feb. 2008.*
[8] *Nikolaos Alexiou, Stylianos Diskadis, Marcello Lagana, Panagiotis Papadimitratos, "Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture" pp-294-002, 2013.*
[9] *L.Buttyan, T.Holczer and I.Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs". In: Security and Privacy in Ad-hoc and Sensor Networks. Vol.4572. Lecture Notes in Computer Science.2007, pp. 129-141.*
[10] *F.Kargl et al., "Secure and efficient beaconing for vehicular networks". In:Proceddings of the 5th ACM International Workshop on Vehicular Ad Hoc Networks. New York, USA, Sept. 2008, pp. 82-83.*
[11] *Ghassan Samara, Wafaa A.H., R.Sures, "Security Analysis of Vehicular Ad-hoc Networks(VANET)" National Advanced IPV6 Center, 2010.*
[12] *Qianhong Wu, Virgali,, Bo Qin, "Distributed Privacy-preserving Secure Aggregation in Vehicular Communication", vol-11, 2011.*
[13] *F.Schaub et al., "V-Tokens for Conditional Pseudonymity in VANETs". In: Wireless Communications and Networking Conference(WCNC), 2010 IEEE. Apr.2010, PP. 1-6.*
[14] *Hu Xiong, Matei Ripeanu, Zhiguang Qin, "Efficient and Spontaneous Privacy-preserving Protocol for Secure Vehicular Communication", 2009.*
[15] *J.Gu et.al., "Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications". In: Information Security and Privacy. Vol. 2727. Lecture Notes in Computer Science. 2003, pp. 180-191.*
[16] *J.Camenisch et al. "How to win the clonewars: efficient periodic n-times anonymous authentication". In:Proceedings of the 13th ACM conference on Computer and communications security. CCS '06. Alexandria, Virginia, USA, 2006, pp. 201-210.*

Mahalakshmi.R.Sreceived her B.E. degree in Computer Science and Engineering from Anna University at Pandian Saraswthi Yadav Engineering College, Tamilnadu, India in 2011. She is currently pursuing her M.E., degree in Computer and Communication Engineering from Anna University at Sethu Institute of Technology, Tamilnadu, India.

Alangudi Balaji.N received his B.E. degree in Computer Science and Engineering from SIT, Tamilnadu, India in 1999. He has received his M.Tech. degree in Information Technology from VIT, Tamilnadu, India in 2005.He has 10 years of teaching experience in Engineering. He is currently pursuing his Ph.D degree in Anna University, Chennai. His research interests include Network Security and Vehicular Ad-hoc Network.