ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Review on Efficient Way of Authentication in VANET Through Public Key Cryptography

Gauri N. Dudhat[1], Karuna G. Bagde[2]

M.E Student (CSIT), H.V.P.M College of Engineering and Technology, Amravati, Maharashtra, India[1]

Associate Professor, Department of Computer Science& Engineering, H.V.P.M College of Engineering and Technology, Amravati, Maharashtra, India[2]

ABSTRACT: Vehicular ad hoc networks (VANETs) are the specific class of Mobile ad hoc networks (MANETs).In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers**.** In this paper, we investigate the authentication issues with privacy preservation and non-repudiation in VANETs. We propose a novel framework with preservationand repudiation (ACPN) for VANETs. In ACPN, we introduce the public-key cryptography (PKC) to the pseudonym generation, which ensures legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicles' real IDs. The self-generated PKCbasedpseudonyms are also used as identifiers instead of vehicle IDs for the privacy-preserving authentication, while the update of the pseudonyms depends on vehicular demands.

KEYWORDS: VANET, MANET,PKC,Pseudonyms**.**

I. INTRODUCTION

A Vehicular Ad-hoc Network (VANETs) is a technology, that makes nodes as routers and provides self-organized network for communication among Vehicles and Roadside Infrastructure. This communication is provided by Dedicated Short Range Communication,, that provides communication within 300 meters.. This communication provides both safety and non-safety applications to the users. Safety applications include messages like emergent braking, traffic jam in a certain locality or accident and the non-safety applications include location based services and infotainment services, which improve the comfort level of the users on road.[8]. The mobility of vehicles is constrained by predefined paths, node's speed limit or the congestion level. Advanced wireless technologies enable direct and instant communication among vehicles (Vehicle-to-Vehicle V2V) as well as between vehicles and the road infrastructure

II. LITERATURE REVIEW

Wireless sensor network (WSN) is a network of collection of tiny sensor nodes called as motes which are densely deployed over target area. The sensor are able to sense the data through events occurring in their coverage area and are able to either forward the data or process the data in some cases as . A sensor network node typically consists of Radio transceiver, a microcontroller and battery or typical form of an embedded type of energy source .There are many advantages of using wireless sensor networks. One of these advantages is reducing the cost of the applications by having many sensors with little cost communicate with each other and with the base station providing full network function.

In [6], The security and performance analysis show that our scheme can achieve efficient group signature based authentication while keeping conditional privacy for VANETs.

In [7], The security of VANET of the road condition information transferring system is crucial. For example, it is essential to make sure that life-critical information cannot be inserted or modified by an attacker. The system should be able to help establish the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers. In fact, there are very few academic publications describing the security architecture of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

VANETs. So integrate the characteristics of ad hoc network itself, concerned the security issues of VANETs from only a few aspects based on some referential papers and provide the appropriate solving measures.

In [8],The scheme suggested in this paper can be implemented on any network simulator and one such simulation reports that this approach for VANET authentication scheme efficiently overcomes Sybil and Impersonation attacks, a major crisis to authentication. As Identities are used, but not directly to authenticate on the go, it provides privacy which is also adaptive. Thus it makes a strong case for implementation on VANET.

III. SECURITY IN VANET

The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments. It is necessary that all transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. VANET packetscontains life critical information hence it is necessary to make sure that these packets are notinserted or modified by the attacker; likewise the liability of drivers should also be establishedthat they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security.These problems in VANET are difficult to solve because In terms of security implementation, there are several layers which are used in proposed protocols to deploy security policies but one of the most often-used levels is layer three for implementation security [12]. There are several methods to assure security in the network world which are also applicable in wireless networks.

IV. RELATED WORK

- AUTHENTICATION THROUGH PKC

PKC is based on asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it . Many existing PKC schemes are available to be utilized in the PKC-based pseudonym generation. Each vehicle c has a pair of cryptographic keys, i.e., a public encryption key pkc and a private decryption key skc. The cryptographic key pairs are generated by the RTA periodically, and the public keys are transmitted to every RSU in its service region through secure channels. Each key pkc is broadcast to all vehicles by the RSU, while the corresponding private key skc is known only to the RTA. In this way, a vehicle can obtain a public key pkc and generate the PKC-based pseudonym from the current public key, which can be decrypted only with the corresponding RTA's private key skc.

- Need ID based signature scheme for authentication:

For better authentication without any compromises at the initial phase of registration and faster verification of this authenticity on road, two different schemes are used. The first scheme identity Based Signature (IBS) makes use of the real world identity of the uses to authenticate itself with the RTA. The RTA in turn provide the user with parameters. In the second scheme, Identity Based Online / Offline Signature (IBOOS) two phases are employed. In the offline phase, using the RTA verified parameters, offline signature is generated and in the online phase, message is used in addition to the private key for generation of online signature (The process of verification in the online phase, makes use of online signature & message and hence less time consuming and efficient).

V. SECURITY ANALYSIS IN VANET

Authentication of message legitimacy is provided by the digital signature of the sender and the corresponding CA certificate. The only guarantee that this provides is that the message comes from a vehicle that was trusted, at least when the keys were issued. Availability can be totally guaranteed.[7]the ways in which an attacker can disrupt the network service are limited.outsiders can only mount jamming attacks. Starting from the initial assumptions we have the following facts: Vehicles cannot claim to be other vehicles since they only interact with their anonymous public keys vehicles cannot cheat about their position and related parameters if a secure positioning solution is used a vehicle

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

cannot deny having sent a message because it is signed by an anonymous key that belongs exclusively to the sender. Using these facts, the security of a VANET is more a certainty than an assumption.
In ACPN, the efficiency of authentication is estimated by the communication delay among vehicles, in which we focus on the computational delay consumed by using cryptographic techniques including IBS and IBOOS schemes
For ACPN:Inner-RSU-V2V, the computational delay of the V2V authentication Tinner is calculated as:.

Tinner = Tsender + Treceiver
whereTsender sign is the time of signing the online signature by the sender vehicle, and Treceiver verify is the time of verifying the online signature by the receiver vehicle, by using the IBOOS scheme

VI. CONCLUSION

In this paper, we prepared transportation scheme that uses the online road information in real time by the help of VANET. In addition to information sharing, co-operative driving, finding a shortest route to a certain destination, it provides authentication, privacy and security to the data.

REFERENCES

1. Jie Li, Senior Member, IEEE, Huang Lu, Member, IEEE, and Mohsen Guizani, Fellow, IEEE , "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs ",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.
2. F.R. Yu et al., "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks," IEEE Trans. Network and Service Management, vol. 7, no. 4, pp. 258-267, Dec. 2010Marcelo Bertalmio, LuminitaVese, Guillermo Sapiro, Stanley Osher, "Simultaneous Structure and Texture Image Inpainting", IEEE Transactions On Image Processing, vol. 12, No. 8, 2003.
3. Y. Sun et al., "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.
4. J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010
5. J. Choi and S. Jung, "A Security Framework with Strong Non- Repudiation and Privacy in VANETs," Proc. IEEE Sixth Consumer Comm. and Networking Conf. (CCNC), 2009.
6. **Deivanai.P, Mrs.K.Sudha , "** Privacy-Preserving and Priority Based Congestion Control for VANET" , International Journal of Computer Application Issue 5, Volume 1 (Jan.- Feb. 2015).
7. Mostofa Kamal Nasir, A.S.M. DelowarHossain, Md. SazzadHossain, Md. MosaddikHasan, Md. Belayet Ali, "Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network" , INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 4, APRIL 2013.
8. R.Nasreen Salma, N.AlangudiBalaji, Dr.R.Sukumar, " A Framework for Authentication in Vehicular Ad-hoc Network using Identity based approach", **IOSR Journal of Engineering (IOSRJEN)** Vol. 3, Issue 7 (July. 2013), ‖V3‖ PP 15-19
9. Pooja R K1, UdayKumar.N. Kalyane, "VANET BASED SECURE AND EFFICIENT TRANSPORTATION SYSTEM", IJRET: International Journal of Research in Engineering and Technology, Volume: 04 Special Issue: 05 | NCATECS-2015 | May-2015
10. J.M.D. Fuentes, A.I. Gonz_alez-Tablas, and A. Ribagorda,"Overview of Security Issues in Vehicular Ad-Hoc Networks,"Handbook of Research on Mobility and Computing, pp. 894-911, IGI Global Snippet, 2011.
11. J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9,pp. 287-296, 2010.