Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.178 – 181

Implementation of Authentication Framework for VANET with Conditional Privacy Preservation

Gauri Dudhat[1], Karuna Bagde[2]

[1]Department of Information Technology, H.V.P.M COET, Amravati, Maharashtra, India

[2]Department of Computer Science, H.V.P.M COET, Amravati, Maharashtra, India

[1] gauri.dudhat23@gmail.com; [2] karunabagde@yahoo.com

Abstract— In Vehicular Ad hoc NETworks (VANETs), authentication is a crucial security service for both inter-vehicle and vehicle roadside communications. On the other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy. In this paper, we investigate the authentication issues. Communications are becoming more wireless and mobile than ever. Thus, in the near future, we can expect that vehicles will be equipped with wireless devices, which will enable the formation of Vehicular Ad Hoc NETworks (VANETs). The main goal of these wireless networks will consist in providing safety and comfort to passenger. Vehicular Ad Hoc Networks (VANET) has mostly gained the attention of today's research efforts, while current solutions to achieve secure VANET, to protect the network 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 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 existing ID-based signature (IBS) scheme and the ID-based online/offline signature (IBOOS) scheme are used, for the authentication between the road side units (RSUs) and vehicles, and the authentication among vehicles, respectively.

Keywords— VANET, Authentication, PKC, IBS, IBOOS, RSU

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) are a subgroup of mobile ad hoc networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Because of the restricted node movement it is a feasible assumption that the VANET will be supported by some fixed infrastructure that assists with some services and can provide access to stationary networks. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, dangerous intersections or places well-known for hazardous weather conditions.

In VANETs, the user authentication is a crucial security service for access control in both inter-vehicle and vehicle-roadside communication. On the other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy, meanwhile, be capable of being investigated from accidents or liabilities for non-repudiation. Peculiarly, safety applications require a strong mutual authentication, because most of the safety related messages may contain life-critical information [12].Therefore in this paper, along with the development of the VANET technology based on advancing smart vehicles, and other undiscovered potential threats on security, we are committed to solving the issues of authentication

II. LITERATURE REVIEW

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 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.

Routing in Vehicular Ad Hoc Networks: A Survey

AUTHORS : F. Li and Y. Wang

Vehicular ad hoc network (VANET) is an emerging new technology integrating ad hoc network, wireless LAN (WLAN) and cellular technology to achieve intelligent inter-vehicle communications and improve road traffic safety and efficiency. VANETs are distinguished from other kinds of ad hoc networks by their hybrid network architectures, node movement characteristics, and new application scenarios. Therefore, VANETs pose many unique networking research challenges, and the design of an efficient routing protocol for VANETs is very crucial. In this article, we discuss the research challenge of routing in VANETs and survey recent routing protocols and related mobility models for VANETs.

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 packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that 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

A. *Attacks on authentication*: There are two kinds of attacks related to authentication in VANETs and are given as follows Impersonation attack: The attacker pretends to be another entity. The impersonation attack can be performed by stealing other vehicular entities' credentials for authentication. As a consequence, some warnings sent to a specific entity would be sent to an undesired one.

B. *Sybil attack:* The attacker uses different identities at the same time. In this way, e.g., a single attacker could pretend as a vehicle and reports the existence of a false traffic bottleneck.

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.

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 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.

VI. PERFORMANCE EVALUATION

A. *Authentication Efficiency*

In this part, the efficiency of mutual authentication among vehicles in VANETs is evaluated through theoretical quantitative calculations for UVC. 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. We design the performance evaluation considering the following two situations/scenarios for the V2V authentication of ACPN in VANETs, named ACPN:Inner-RSUV2V and ACPN:Cross-RSU-V2V, which have been introduced in the operation of ACPN in Section 4 as the inner-RSU V2V authentication and the cross-RSU V2V authentication, respectively:

Inner-RSU-V2V- In this situation, both the sender and the receiver vehicles are V2R authenticated to the current corresponding RSU within its communication range. Thus, the receiver owns the pseudonym and the POI set of the sender vehicle, and the sender vehicle can directly authenticate the receiver.

Cross-RSU-V2V- In this situation, the receiver vehicle does not have the current pseudonym and the POI set of the sender vehicle in its storage. Thus, the receiver has to query the corresponding RSU for the cross-RSU-V2V authentication.

VII. CONCLUSION

In this paper, a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs has been proposed, which utilizes the IBS and IBOOS schemes for the authentication.It achieves the desired authentication,

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, Luminita Vese, 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. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, 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.Alangudi Balaji, 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, Uday Kumar.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.

[12] M. Raya and J. Pierre, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007

[13] H. Dok et al., “Privacy Issues of Vehicular Ad-Hoc Networks,” Int’l J. Future Generation Comm. And Networking, vol. 3, no. 1, pp. 17-32, 2010. M. Gerlach and F. Guttler, “Privacy in VANETs Using Changing Pseudonyms—Ideal and Real,” Proc. IEEE Vehicular Technology Conf. (VTC-Spring), pp. 2521-2525, 2007.