Improving Privacy Preservation using IBS and IBOOS in VANET

J.Lavanya[1], Dr. S. Sivananaitha Perumal[2]

[1]P.G. Student (M.Tech-II Year), Department of Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, TamilNadu, India
[2]Head of the Department, Department of Information Technology, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur, TamilNadu, India

Abstract—*In Vehicular Ad hoc NETworks (VANETs), vehicles have to be protected from the misuse of their private data and the attacks on their privacy. Here the authentication issues with privacy preservation and non-repudiation in VANETs have been considered. The self-generated public-key cryptography PKC based pseudonyms are also used as identifiers instead of vehicle IDs for the privacy-preserving authentication, while the update of the pseudonyms depends on vehicular demands. 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. Authentication, privacy preservation, non-repudiation have been analyzed for VANETs. Typical performance evaluation has been conducted using efficient IBS and IBOOS schemes.*

Keywords— Vehicular Ad hoc NETworks, ID-based signature , ID-based online/offline signature, road side unit.

I. INTRODUCTION

A Vehicular ad hoc network (VANET) is a technology that employs moving vehicles as nodes in a network to create a mobile network to provide communication among vehicles, nearby fixed road side units (RSUs) and regional trusted authorities (RTAs) [1]. VANETs are utilized for a broad range of safety applications, and non-safety applications. 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, it should be capable of being investigated from accidents or liabilities for non-repudiation.

Authentication frameworks using the ID-based signature (IBS) schemes based on the ID-based cryptography (IBC) have been proposed to reduce the communication overheads. The IBS schemes can be adopted to the authentication service for VANETs, in which each vehicular identity is used as a public key for signing/verifying messages in communication. Using ID-based online/offline signature (IBOOS) is an attractive solution for authentication in VANETs, for alleviating the computation overhead of the IBS process. An IBOOS scheme increases efficiency of the pairing process by separating the signing process into an offline phase and an online phase, in which the verification is comparatively more efficient than that of IBS [2]. In this paper, different from the existing work, we propose an authentication framework by utilizing the IBS scheme in the V2R communication, and together with the IBOOS scheme in the V2V communication for better performance. In IBOOS for VANETs, the offline phase can be executed initially at RSUs or vehicles, while the online phase is to be executed in vehicles during the V2V communication

II. RELATED WORK

An ideal VANET should have a mechanism to validate the authenticated vehicles with privacy preservation while retaining message non-repudiation. In this paper, we propose a novel Authentication framework with preservation and repudiation (ACPN) for VANETs, by using the IBC for authentication and the pseudonym-based mechanism for conditional privacy preservation [3] and non-repudiation in urban vehicular communications (UVC). One of the advantages of ACPN is its reusability. Besides the solution by using the existing PKC, IBS and IBOOS schemes, ACPN can also be utilized with new schemes for security and performance improvements. The contributions of this work are as follows.

- The proposed ACPN provides the conditional vehicle anonymity for privacy preservation with traceability for the non-repudiation, in case that malicious vehicles abuse anonymous authentication techniques to achieve malicious attacks.
- In ACPN, we introduce the public-key cryptography (PKC) to the pseudonym generation, which ensures a legitimate third party to achieve

non-repudiation [4] of vehicles by obtaining their real IDs.

- We propose a PKC-based adaptive pseudonym scheme by using self-generated pseudonyms instead of real-world IDs in authentication for privacy preservation [5] and non-repudiation, in which the update of the pseudonyms depends on vehicular demands.
- In ACPN, we utilize the IBS scheme for the vehicle to roadside authentication and the roadside-to-vehicle (R2V) authentication, which is efficient in communication. In order to further reduce the computation overhead by IBS in authentication, the IBOOS scheme is used for the vehicle-to-vehicle authentication.
- We show the feasibility of ACPN with respect to the system analysis on the objectives, such as authentication, privacy preservation[6], non-repudiation, time constraint, independency, availability and integration.Moreover, the storage and computation overhead of ACPN is evaluated by quantitative calculations in the performance evaluation.

III. IBS AND IBOOS

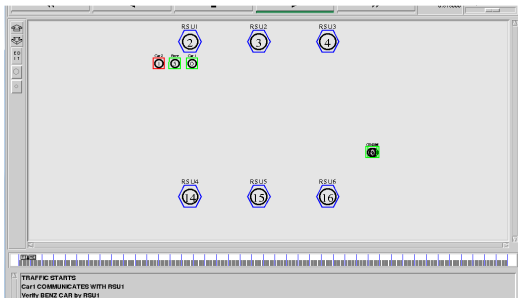
In [7] A.Shamir., uses IBS from IBC used in VANETs consists of four steps including setup, key extraction, signature signing and verification:

- Setup: The RTA computes a master key s and public parameters param for the private key generator (PKG), and gives param to all vehicles.
- Extraction: Based on an ID string, a vehicle generates a private key associated with the ID using the master keys.
- Signature signing: Based on a message M, time stamp t and a signing key u, the sending vehicle generates a signature SIG.
- Verification: Based on the ID, M and SIG, the receiving vehicle outputs “accept” if SIG is valid for verification, and outputs “reject” otherwise.

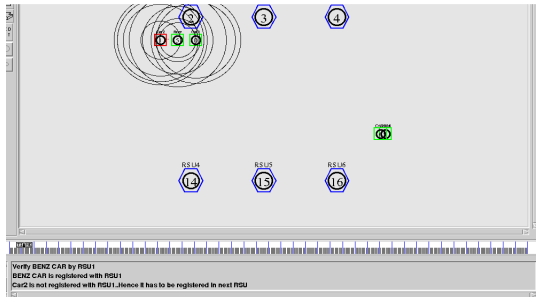
Similarly, in [8] Shamir., uses from IBC used in VANETs consists of five steps including setup, key extraction, offline signing, online signing and verification:

- Setup: Same as that in the IBS scheme.
- Extraction: The RTA generates a private key sekID associated with the ID using the master key s.
- Offline signing: Based on the ID and public parameters, the RTA/RSU generates an offline signature SIGoffline for each vehicle.
- Online signing: Based on the offline signature SIGoffline and a message M, the sending vehicle generates an online signature SIGonline ofM.
- Verification: Based on the ID, M and SIGonline, the receiving vehicle outputs “accept” if SIGonline is valid for verification, and outputs “reject” otherwise.

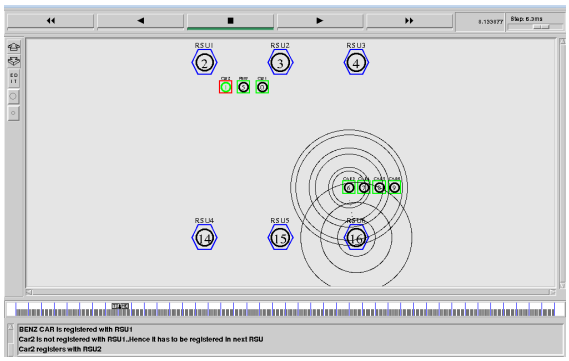
IV. EXPERIMENTAL RESULTS



(a)



(b)



(c)

Figures shows the simulation of the IBOOS and IBS schemes. Fig (a) shows the Initialisation. (b) is the image when it has not been registered (c) After registration of the vehicle

V. CONCLUSION

We have implemented an IBS and IBOOS technique from the simulation of vehicle. Our scheme successfully provides authentication, privacy preservation in VANETs. It provides

reusability i.e., it can also be utilised with other new schemes for security and performance improvements.

REFERENCES

[1] S. Zeadally et al., "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges," Telecomm. Systems, vol. 50, no. 4,pp. 217- 241, 2012.

[2] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. CRYPTO: Advances in Cryptology, pp. 263-275, 1990.

[3] 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.

[4] J. Sun, C. Zhang, and Y. Fang, "An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks,"Proc. IEEE Military Comm. Conf. (MILCOM), pp. 1-7, 2007.

[5] B. Hoh et al., "Preserving Privacy in GPS Traces via Uncertainty- Aware Path Cloaking," Proc. 14th ACM Conf. Computer and Comm.Security (CCS), pp. 161-171, 2009.

[6] 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.

[7] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. CRYPTO, pp. 47-53, 1985.

[8] A. Shamir and Y. Tauman, "Improved Online/Offline Signature Schemes," Proc. CRYPTO, pp. 355-367, 2001.