IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 7 (July. 2013), ||V3|| PP 15-19

A Framework for Authentication in Vehicular Ad-hoc Network using Identity based approach

R.Nasreen Salma, N.Alangudi Balaji, Dr.R.Sukumar
PG Scholor Sethu Institute of Technology Pulloor,Kariapatti, India
Assistant Professor Sethu Institute of Technology Pulloor,Kariapatti, India
Professor Sethu Institute of Technology Pulloor,Kariapatti, India

Abstract: - In Vehicular Ad-hoc Network (VANETs), security is a primary concern, as it affects traffic safety. Authentication in essence is an important security requirement to avoid attacks on vehicular communication. To provide authentication with some privacy to the users, we propose an authentication framework that uses pseudonyms, which are self-generated are used as key value in communication among vehicles. ID-Based Signature (IBS) Scheme and the ID-Based Online / Offline Signature (IBOOS) Schemes are used, which provides authentication for the basic three types of communication in VANET, namely the vehicle to vehicle (V2V) communication, Vehicle to Roadside (V2R) communication. and Roadside unit to Vehicle (R2V) communication. Simulation result demonstrate that the use of IBS/IBOOS has improved reduced packet delivery ratio and decreased storage latency and hence this approach proves to be very suitable for VANET architecture.

Keywords: – *Vehicular Ad-hoc Network, Identity Based Signature, Identity Based Online/Offline Signature.*

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.

VANET is basically a variant of MANET with the following properties to be considered essentially in the design of VANET architecture. Those properties include high mobility and rapidly changing topology., geographic position available, mobility modeling and predication, hard delay constraints and no power constraints. The nodes (vehicles) are capable of moving in the desired path which is. pre-determined, as roads are well established between every point or place. These nodes are similar to the nodes in Wireless Sensor Network (WSN), as they are capable of routing and sensing environmental conditions. So the design of a VANET Architecture is to consider all these properties.

Security issues are prominent in VANETs, because the network is publicly available and contains life-critical information which needs no alteration and hence supports the need of strong authentication is such a network.

There are certain requirements for providing authentication to the users in VANETs and they are computation overhead, (amount of cryptographic operations needed), control overhead (bandwidth overhead), latency (time for a response), Initialization time (time for initializing the system), strong authentication, scalable and support for the re-authentication and revocation procedures.

Authentication in general, can be done at various levels namely node level, group level, unicast, broadcast and multicast. In this project, our aim is to design a framework that provides authentication for each and every node, i.e., at node level using identity based approaches. These identities are the real world identities, that will be used only for wired communication and in the wireless media communication, authentication is provided by parameters that are not real world identities, but are certified by a Trusted Authority.

Basically, there are only three entities in the topology namely, Regional Trusted Authority (RTA), Road Side Unit (RSU) and vehicle. Among these, the vehicle is the only moving entity whereas the RTA and RSU are fixed. RTA is capable of verifying the real world identity and authenticating the vehicle, whereas RSU provides the vehicles with the required applications based on request-response mechanism.

The signing process is basically divided into two phases: an online phase and an offline phase. The offline phase is one in which the vehicle is not moving on-road and in the online phase, the vehicle is moving

on-road. This division enables faster and efficient way of authentication as highly computational initial signing is done in offline phase, this consists of vehicle registration with trusted authority, verification of identity and obtaining certified parameters. In the online phase, the vehicle has very few steps to be done before starting a secure communication, this consist of only verifying the certified parameters provided by the vehicle. The system will be evaluated based on throughput level, packet delivery ratio and storage latency.
The rest parts of this work is organized as follows. Section II provides those related work. In Section III, we provide an overall view of the system with the algorithm used. In Section IV, the proposed framework's implementation and methodology is described and in the last section, we conclude the paper.

II. RELATED WORK

In 2004 (1) Hubax et al., proposed two solutions to provide security and privacy in vehicular networks. In the first, Electronic License plate are used as certified identity. They have also discussed on dynamic pricing with an estimated toll price of choice and to identify misbehaving drivers, even if no vehicle is within its communicating range. In the second solution, Tamper-proof GPS and verifiable Multilateration are used for Location Verification. A challenge response based protocol with distance bounding property is to be used. The drawback is, it does not provide any specific solution to the problem.

In 2006 (5) and later in 2008 (6) Kamal et al. proposal an identity based cryptography based security framework for VANET. They insisted on the use short-lived pseudonyms for the purpose of being untracked by some adversary and elimination of certificate exchange. Every vehicle has its unique ID, a public certificate and a key pair. The Certificate Revocation List (CRL) is kept at the Base Station. But this framework, has an increased signaling overhead and potential abuse by the authority.

In 2007 Lin et al.(3), presented GSIS which deals with both privacy and security. It provides conditional privacy using group signature and Identity based signatures based on Bilinear pairing for efficient Bandwidth usage. The Security Scenario is divided into two each with its own protocol and assuming the infrastructure points are trusted; one between OBU and OBU for which group signature is used and the other between OBU and RSU where Identity Based Signature is used. The first protocol has five phases with membership traceability and the second protocol has three phases with private key for each entity. The tedious phase is their implementation.

In 2007 Sun et al (7), also proposed an ID-based framework that removes the need for certificates and provides authentication with privacy, non-repudiation, authentication, message integrity and confidentiality. The approach uses pseudonym-based and threshold-based techniques for defending against location tracking and user profiling respectively. For realizing non-repudiation, multiple authorities are distributed with identity revealing information. For authentication and integrity ID-based digital signatures are used. For Confidentiality, public or symmetric key encryptions are used.

In 2009, another ID-based solution DRTA (Dynamic Revocation with Threshold Authentication) is proposed in (8) by Sun and Jang. This approach uses threshold authentication technique, where the parameter k is the threshold beyond the AU-RSU(Authentication RSU) at the other end detect it and revoke the temporary certificate. They have not considered the time issues for the freshness of the certificates, as there is a possibility of misusing older certificates and only a framework is suggested without any protocols for implementation.

III. OVERVIEW

3.1 Description

This paper describes the mechanism of authentication is VANET using identity based approach. The vehicles initially register themselves to the Regional Trusted Authority (RTA) by providing it with the user's original information. They then start communicating with the Roadside Unit (RSU) or other vehicle. The RSU in turn checks the identity of this vehicle with the RTA and once if it is valid, it provides the vehicle with the needed data. Finally, the vehicles using the RSU can communicate with other entities in the topology in a more secure manner.

3.2 Existing System

Vehicles use their identity of the real world to register themselves with the RTA. As RTA is a trusted third party (TTP) and this communication takes place over a wired medium this communication is secure and can be time consuming since RTA has to check the authentically of the user by verifying all its identity. But when the vehicle is on road or moving, it is not at all possible for every entity in the topology to authenticate itself using real world identities. It is also time consuming and insecure hence these communications are over wireless medium, which are more prone to attacks.

3.3 Proposed System

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).

3.4 Algorithm

The general algorithm for IBS & IBOOS scheme is the same, but the parameters used varies. The five basic steps of this algorithm is summarized as follows.

1. Initial setup phase at RSU/RTA.
2. Extraction of parameters.
3. Generation of signature using IBS/IBOOS
4. Verification of signature
5. Secure Communication in the network

The Fig.1 shows how those vehicles with only registered certified parameters enter in to communication using IBOOS.

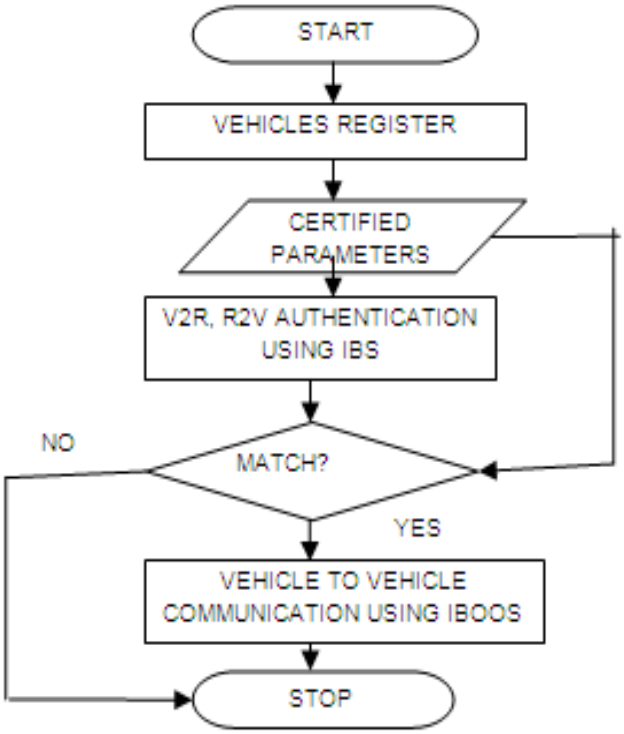

Fig.1: Signature Verification Process

3.5 Algorithm Description

In the initial setup phase, the vehicle registers themselves to the RTA using their real world identities, initially the RTA are assumed to be trusted authorities and are cross-certified in order to extend the use of parameters that are certified already and hence reduce the overhead of registering and verifying once again. The vehicles then attain certified parameters from the RTA, which are then extracted for signature generation. The signature is then verified to authenticate the users.

The signature verification process, takes place as in the fig.1, the certified parameters are extracted by the RSU on demand using IBS scheme, and are checked with those provided by the vehicles during the initial setup phase and if and only if, they correspond to one another, they are allowed to communicate among other vehicles in the topology, using only those certified parameters. The proceeding communications take place using IBOOS scheme.

IV. IMPLEMENTATION AND METHODOLOGY

4.1. Data Flow Diagram

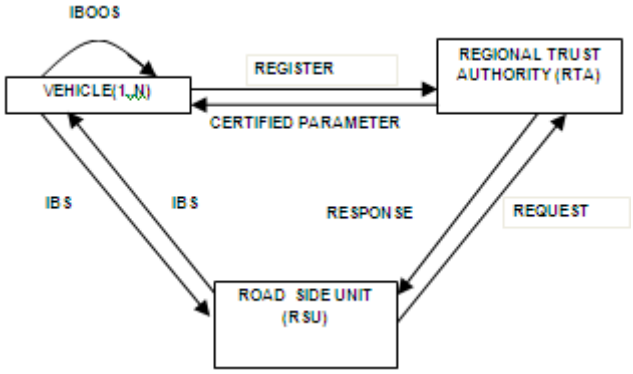

Fig.2: Vehicle Registration and Authentication Process

4.2. Module Description

4.2.1. Vehicle Registration

This initial phase of vehicle registration takes place, even before the vehicles start moving. Every vehicle must register itself to the Regional Trusted Authority (RTA) which are wide spread and are all cross authenticated. This can be done either by the manufacturer or owner of the vehicle by providing the real world identity of the vehicle.

4.2.2. Vehicle to Road Side Unit Authentication

The Road Side unit periodically broadcasts its information, so that the vehicles in that transmission range can obtain the RSU's information. When a vehicle wants to authenticate itself in the system, it initially sends a join request message to a RSU, which verifies the signature using IBS and accepts the vehicle as valid only if it is already authenticated by the RTA.

4.2.3. Vehicle to Vehicle Authentication

For ensuring authentication among one another, vehicles use IBOOS scheme. Initially, a vehicle generates its online signature which is based on its offline signature and time.

V. CONCLUSION

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.

REFERENCES

[1] J. P. Hubaux, S.C. Apkun, and J.Luo," The Security and Privacy of Smart Vehicles", IEEE Journal on Security and Privacy, Vol. 2, Issue 3, pp.49 -55, 2004.

[2] M. Raya and J. Pierre, " Securing vehicular ad hoc networks", Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[3] X. Lin, X. Sun, P.H. Ho, X. Shen," GSIS : A Secure and Privacy Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol. 56, Issue 6, pp. 3442- 3456, 2007.

[4] J. M. D. Fuentes, A. I. Gonz'alez-Tablas, and A. Ribagorda, " Overview of Security Issues in Vehicular Ad-hoc Networks", in Vehicular Technolgy conference, VTC 2007-Spring, 2007.

[5] P. Kamat, A. Baliga, W. Trappe, "An Identity Based security Framework for VANETs", VANET 06 Proceeding of the 3rd International workshop on Vehicular Ad-hoc networks, pp. 94-95, 2006.

[6] P. Kamat, A. Baliga, W. Trappe, "Secure, pseudonym and auditable communication in vehicular Ad-hoc networks", Security and Communication Networks, vol. 1, no. 3, pp. 233-244, 2008.

[7] J. Sun, C .Zhang, Y. Jang, "An Id-Based Framework Achieving Privacy and Non-Repudiation in vehicular Ad-hoc Networks", IEEE Conference Military Communications Conference MILCOM 2007, pp. 1-7, 2007.

[8] J. Sun, J. Fang, "Defense against misbehavior in anonymous vehicular ad hoc networks", Journal of Ad hoc Networks, Vol. 7, Issue 8. pp. 1515 - 1525, 2009.

[9] P. Barreto, H. Kim, B. Lynn, and M. Scott," Efficient Algorithms for Pairing-Based Cryptosystems", in Adv. in Cryptology – CRYPTO 2002, LNCS, vol. 2442, 2002.
[10] N. Gura, A. Patel, A. Wander, H. Ebrel, and S. C. Shantz," Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", in Cryptographic Hardware and Embedded Systems – CHES 2004, LNCS, vol. 3156, 2004.
[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen," An Efficient Identity Based Batch Verification Scheme for Vehicular Sensor Networks", in Proc. of IEEE 27th Conference on Computer Communications, INFOCOM 2008, 2008.
[12] A. Shamir and Y. Tauman," Improved Online/ .Offline Signature Schemes", in Adv. in Cryptology – CRYPTO'84, LNCS, vol. 196,1985.
[13] S. Even, O. Goldreich, and S. Micali,"On-Line/ Off-Line Digital Signatures", in Adv. in Cryptology – CRYPTO'89, LNCS, vol. 435, 1990.
[14] S. Zeadally, R.Hunt, Y.S.-Chen, A.Irwin and A. Hassun "Vehicular ad hoc networks (VANETs) status, results and challenges", Telecommunication Systems, pp 1-25, 2010.
[15] N.-W. Wang, Y.- M. Huang, and W.-M. Chen ," A novel secure communication scheme in vehicular ad hoc networks", Computer Communications, vol. 31, pp. 2827-2837, 2008.

AUTHORS PROFILE

R. Nasreen Salma**,** received her B.Tech, degree in Information and Technology from Raja College of Engineering and Technology, India, in 2011. She is currently pursuing her M.E. in computer and Communication engineering from Sethu Institute of Technology, India.

Her research interests include Network Security, Networks and Data Mining.

N.Alangudi Balaji is an Assistant Professor of Computer Science and Engineering in Sethu Institute of Technology, Virudhunagar. He has received his B.E, degree in Computer Science and Engineering from Sethu Institute of Technology, India in 1999. He has received his M.Tech degree from VIT, India in 2005. He is currently pursuing his Ph.D degree.

His research interests include Networks, Vehicular Adhoc Networks and Network Security.

R.Sukumar is a Professor of Computer Science and Engineering in Sethu Institute of Technology, Virudhunagar. He received his B.E degree in Electronics and Communication Engineering from Madurai kamaraj University, Taminadu, India, in 1992. He has received his M.E degree in Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli, India in 2005. He has received his Ph.D Degree from Anna University, Chennai, Tamilnadu, India in 2009.

His research interests include Cryptography and Network Security.