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. 3, March 2016, pg.676 – 681

A Survey on Privacy Preservation for Improving IBS and IBOOS in VANET's

Dr. Sohan Kumar Gupta[1], Bhavya.R[2]
[1]Professor, PG Co-ordinator, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India
[2]PG Scholar Software Engineering, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India
[1] hod_pg@newhorizonindia.edu; [2] bhavyagowda060@gmail.com

Abstract— In Vehicular Ad-hoc networks are networks of communication between vehicles and roadside units and inter vehicle units. It can be used to provide traffic management, route planning, and identifying roadside units using short-range wireless communication. This network has the potential to increase safety system and it can provide many services to drivers, but they also present risks to privacy and we can provide and protected from the misuse of private data attacks on their privacy, as well as to be capable of being investigated for accidents or liabilities from non-repudiation. The existing ID-based signature (IBS) schema and ID-based online/offline signature(IBOOS) schema are used to authentication between the road side unit(RSUs) and authentication among vehicles,respectively.In this paper ,we proposed on the authentication issues with privacy preservation and non-repudiation in VANETs.here we introduce the public-key-cryptography(PKC) to the pseudonym generation, the non-repudiation of vehicles by obtained vehicles real ID's to legitimate third parties to achieve this .its also identifiers instead of vehicles ID's for the privacy-preservation authentication, while the update of the pseudonyms depends on vehicles demands. We proposed to show ACPN is feasible and secure to be used efficiently in the VANET.

Keywords- Vehicular ad-hoc network, privacy preservation, non-repudiation, authentication framework, Identity based cryptography.

I. Introduction

The Vehicle Ad-hoc network is a technology that has moving vehicles as nodes in the network for creating a mobile network. Every network is using wireless nodes to access the vehicular networks.it is a term which is used to describe the ad-hoc network that is formed over vehicles moving on the roads. The vehicular networks are very fast emerging for deploying and developing new and traditional applications. This vehicular ad-hoc technology is moving vehicles as a nodes in a network to create a mobile network to provide communication among vehicles, and its fixed roadside units(RSUs) and using RTA(regional trusted

authorities). It allowing cars to connect to each other which are 100-300 meters apart and, in turn, create a wide range of network. As cars fall out due to signal range and drop out of the present network, other cars can join in to connect vehicles to one another so a mobile Internet can be created [1].

A VANET is considered as a variant form of a mobile ad hoc network (MANET). It turns every participating vehicle into a wireless router or node. The vehicles is constrained by predefined roads, the road speed limits or the congestion level in VANETs.here devices and wireless networks become increasingly influential in recent years, the demand for the vehicle-to-vehicle (V2V) communication and the vehicle-to-roadside (V2R) communication increases continuously[5].

In this VANETs system is having some types of communication. Vehicle to vehicle communication, vehicle to infrastructure communication and routing based communications. VANETs have stimulated the development of several interesting applications such as vehicle collision warning, security distance warning, cooperative driving, driver assistance, etc. VANET is composed of On-Board-Units (OBUs) mounted on the vehicles and Road-Side Units (RSUs) installed along sides of the urban roads/highways which facilitate vehicle-to-vehicle (V2V) communications and Vehicle to Roadside (V2R) communication. In Vehicle to roadside unit Message can communicate both vehicle and also the devices which are placed near the road or may in nearest building to road. In vehicle to vehicle units are messages can be send and receive through network devices installed in the vehicles. The vehicle engine provides enough power for communication and intensive data processing [7].

The Traffic in India is increasing day by day and increase in number of vehicles on the road ultimately should be increases the traffic. This increase the traffic leads to the traffic congestion. If the traffic is managed in right way then there will be no congestion. The traffic management in India is still followed by old methods. That is the traffic management is only depended upon traffic signals. But in the developed countries like USA, Japan and European countries they developed the VANET for traffic management and congestion control. In the VANET the vehicles can directly communicate with each other and with infrastructure which is an entirely new paradigm for vehicle safety and traffic congestion control. The VANET can be used for the traffic management, safety, efficiency, etc. Besides the traditional applications of VANET such as accident alert and traffic information exchanged in form of simple text messages, the scientific and industrial communities envisage video communication within vehicular networks to be of major benefit for traffic management and also to provide a value added entertainment advertising services. Certainly, in a road emergency, streaming a live video of the accident area allows vehicles approaching the scene, mostly official vehicles, to better understand the nature of the accident and take the right decision consequently[2][3].

II. Motivation

In VANETs, the user authentication is a successful security services for access control in both vehicle to vehicle and vehicle to roadside units communication. On the another side have to protected from the misuse of their private data and attacks on their privacy. The capable of being investigated from the accidents or liabilities for non-repudation. this is safety applications required a strong mutual authentication, because the most secured messages to send from the life-critical information cycle of the VANETs system.in this paper we authentication of the privacy preservation and non-repudiation in VANETs is based on covered all security data and secured messages and committee to solving good authentication issues[6].

The VANETs using some authentication issues like symmetric and Asymmetric key based authentication schemes are proposed for VANETs system. The Symmetric key cryptographies for the message authentication.in this symmetric key authentication is having some drawback to authenticate each other via trusted authorities; this is not suitable for large-scale vehicles communications in VANETs [7] [2].The Asymmetric key authentication is widely adopted because of the use separate keys used for encryption and decryption.in this Asymmetric key authentication is using two classes: the public key infrastructure (PKI) based authentication and Identity (ID) based authentication. But here have some drawback this is not feasible or still not persive, because it should be needed some communication to manage the vehicular certificates and certificate revocation lists(CRLs)that may cause heavy communication and computer overheads[7].

The Authentication using IBS and IBOOS schemes based cryptography structure. The IBS (ID-based signature) schemes have been proposed to reduce the communication overheads in which certificate management process has been simplified by using the digital signature schemes. The IBS schemes can be adapted to the authentication service for VANETs, each vehicular identity is used as a public key for signing/verifying messages in communication used ID based online/offline signature (IBOOS). 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.In this paper different from the existing work, we proposed here an authentication framework by utilizing IBS and IBOOS authentications. In IBS scheme is access vehicle to roadside units and roadside units to vehicles communication.in IBOOS for access only vehicles to vehicles communication each other. Using this technique to access the authentication framework for conditional privacy-preservation and non repudiation of VANETs data for reduce the communication overhead and ACPN for reusability and it should be provide more secure security for the message authentication for the ACPN[7][8].

The VANET was provided by the need to inform fellow drivers of actual or imminent road conditions, delays, congestion, hazardous driving conditions and other similar concerns. Now a day's accidents are the major cause of death in many cities or countries. so it is vary necessary to have a technology which can be used to minimized the road accidents and provide security to the peoples. To avoid the accidents the driver should be well aware of the traffic movements and congestion so that he can easily take the best optimal path to reach its destination[2].

The VANETs, usually vehicles drivers or users are not want to their private information such as vehicle names, positions, moving routes and user information to be revealed, in order to protect themselves against any illegal tracing and/or user profiling.in this will be identities should be supported for the privacy preservation in VANETs. Achieving anonymity by using vehicle pseudonyms is a superior solution for the privacy preservation which intimately links a real-world identity (ID) to the corresponding pseudonyms. In VANETs generated by the fixed RSUs or the vehicles itself, even can be downloaded from a trusted link from the RTA periodically [7].

On the other side we will identify the, when accidents or certain crimes occur, the vehicle anonymity should be conditionally retrievable, and the identify information should be revealed to legal authorities to establish the liability of accidents or crimes, which is called conditional privacy or conditional anonymity and the non-repudiation service in VANETs prevents a vehicle from denying previous actions. The pseudonymous authentication used in vehicular communications can provide the privacy preservation with an effective tracing mechanism, which is used only by the trusted authorities (e.g., the certification authority (CA)) to reveal the real identity of malicious vehicles. The vehicles to achieve malicious goals or escape from liabilities. various methods of using anonymous credentials are different in each proposal, which render these issues more important and more complex to be handled in VANETs[5].

III. Literature Survey

The past decades have some active safety systems will be realized by innovative applications of information available through wireless communication and information travel between vehicles to fixed infrastructure. The behavior of current active safety systems is reactive and is relies on real time feedback with small constants from autonomous sensors. VANET not only promise safety benefits to drivers and those in the surrounding driving environment, but also improves mobility, increased comfort, reduced environmental impact.

The Hang Dok, Huirong Fu, Ruben Echevarria, and HesiriWeerasinghe these all authors published privacy Issues of Vehicular Ad-Hoc Networks ,we proposed to combine a set of ability to provide privacy,VANET,Security,and Mix Zones.it has some feature Silent periods and Group signatures and drawback is choices are frequently more expensive than those of the cost-aware approach[6].

The PandurangKamat, AratiBaliga and Wade Trappe this authors introduced Secure, pseudonymous, and auditable communication in vehicular ad hoc networks, in this ,The biggest advantage of our framework comes from the efficiency of providing user-controlled privacy by allowing users to obtain pseudonyms as and when desired. Others have suggested ways to provide the same that are not as flexible or efficient and Cryptosystems based on elliptic curves enjoy a key size advantage over equivalent asymmetric cryptosystems that utilize conventional integer based operations. In this have some drawback The user needs to predetermine the frequency with which he will change temporary identifiers[5].

The Neng-Wen Wang a, Yueh-Min Huang a, Wei-Ming Chen this authors introduced A novel secure communication scheme in vehicular ad hoc networks.in this it has ability to provide VANET and some features of wireless, security. And have some drawbacks of this approach is that a vehicle needs to store a lot of key and certificate set[7].

The Hannes Hartenstein, Kenneth P.Laberteaux was introduced A tutorial Survey on vehicular Ad-hoc networks in this The VANETs researches and standardization would is benefits from improved provenance management for simulation models and results and due to this diversity, a requirements-benefits analysis must be done on a case-by-case basis. In this draw back is consider the specific challenges of VANET designs[8].

The Yipin, Rongxing Lu,Xiaodong Lin,Xuemin shen,jinshu su was introduced An Efficient pseudonymous authentication scheme with strong privacy preservation for Vehicular Communication ,in this from the viewpoint of revocation cost, the group signature based schemes have an advantage that the CRL size is linear with the number of revoked vehicles. In this drawback is large-scale wireless network scenario for public service and it faces serious security and privacy challenges[8].

The Huang LU and Jie Li,Mohsen Guizani was introduced on A novel ID-based Authentication Framework with Adaptive Privacy preservation for VANETs in this we show its reusability, which means that, it can also be reused with new IBS and IBOOS schemes for security and performance imporvements.in this drawback is frequently more expensive than those of the cost-aware approach[7].

The Fau Li and Yu Wang, university of North Carolina at charlotte was introduced on Routing in vehicular ad-hoc networks in this all applications will benefits from geocast routing.for example,a vehicle identifies itself as crashed by vehicular sensors that detect events like airbag ignition,then it can report the accident instantly to nearby vehicles.in this drawback is challenge related to routing is efficient data dissemination and data sharing in VANETs[4][3].

The Ahren studer, Fan Bai, Bhargav Bellur,Adrian Perrig was introduced Flexible,Extensible and Efficient VANET Authentication is this to take advantage of the shorter stored MAC,an attacker wants a smaller stored MAC to match the MAC

for an attacker selected message using a legitimate party's key. The drawback to waiting until x messages are successfully authenticate using TESLA++ before verifying a certificate is the delay between when a receiver first hears a message from a sender and the time when the receiver verifies the certificate[4].

The Sheralli Zeadally, , Ray Hunt, Yuh-Shyan Chen, Angela Irwin. Aamir Hassan was introduced Vehicular ad hoc networks (VANETS): status, results, and challenges in this it has ability to provide networking, VANET, protocols and Standards and has some feature routing, security, broadcasting, simulation.in this main drawback of such approaches is that the maintenance of unused paths may occupy a significant part of the available bandwidth if the topology of the network changes frequently[1].

The Jie Li,Huang Lu,Mohsen Guizani Senior members of IEEE was introduced ACPN:Authentication framework with conditional privacy-preservation and non repudiation for VANETs.this is IEEE transactions on parallel and distributed systems, in this mainly we are introducing ACPN reusability and reduce the communication overhead and provide more secure security for the communication between one node to other node[7][8].

IV. Design for VANETs Architecture

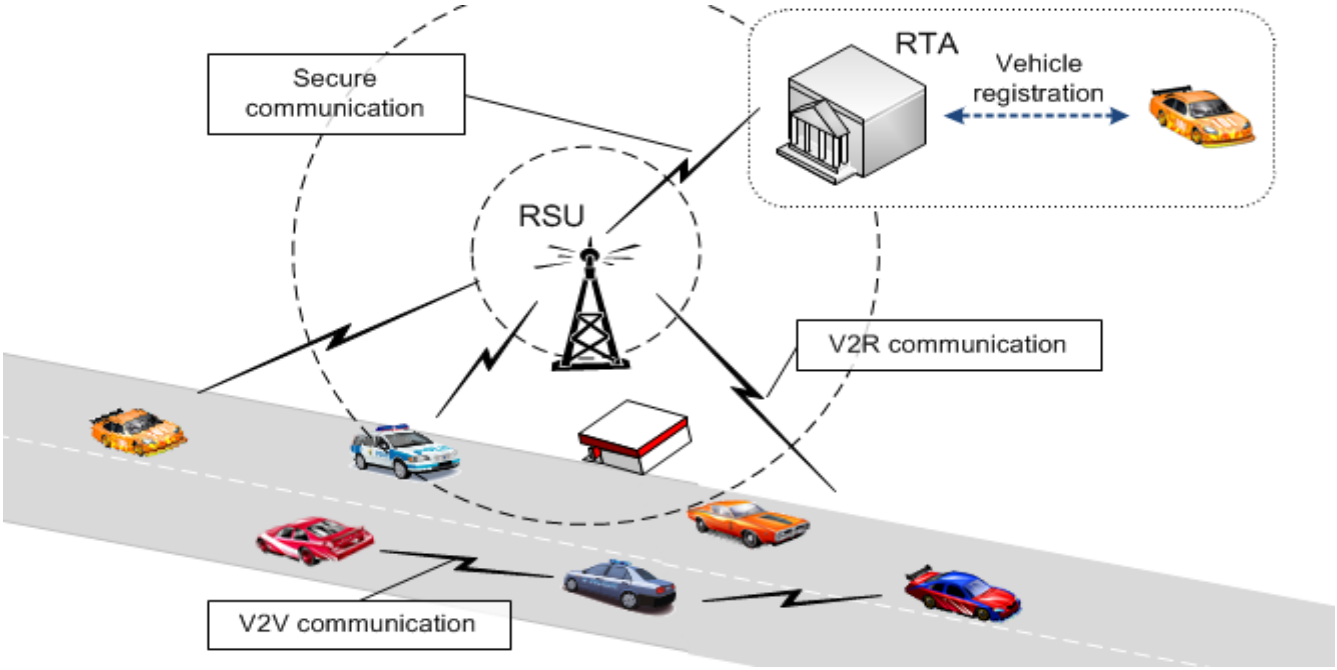

Figure 1. An Illustration of the VANET architecture.

The VANETs are separated by different regions like states ,and a RTA(regional trusted authority),RSU(road side units),V2V(vehicles to vehicles),V2R(vehicles to roadside units)communications. In RTA is a serves acts like individual regions, its acts as a certificate authority(CA) for security and it provides an authenticated recognition to each vehicles in a VANET .The road side unit assist the RTA in querying and tracking for certain vehicles of responsibilities. Using this we are going to increase continuously the V2R (vehicle to roadside units) and V2V (vehicle to vehicle) communications. In VANETs, vehicles do not want their private information such as name, position, moving routes, and user data to be revealed, against illegal tracing and user profiling. The anonymity of identity should be supported in VANETs.

On the other hand, when traffic accidents or certain crimes occur, vehicle anonymity should be conditional, and the identity information has to be established by the legal authority to establish the liability of accidents or crimes. In this case, non-repudiation is essential in VANETs to prevent a vehicle from denying previous commitments or actions. Concerning security in VANETs, We endeavour to construct an efficient authentication framework for security, by using the vehicular pseudonyms and ID-based key management for different kinds of communication in VANETs[9].

1. RTA

The RTA (regional trusted authority) is generated key materials for the RSU (road side units) and also acts with vehicle regions and delivers these keys to them over secure channels. If message sent by a vehicles to create a tangle on the road ,and the RTA is to blame for tracing and distinguishing the supply of the message resolve the dispute. The RTA is completely different region to communicate between RSU and vehicles infrastructure.

2. Vehicle Registration:

This initial section of vehicle registration takes place, even before the vehicles begin moving. Each vehicle should register itself to the Regional trusted Authority (RTA).This may be done either by the manufacturer or owner of the vehicle by providing the important world identity of the vehicle.

3. Communication process:

The communication between RTA to RSU and RTA to Vehicles and RSU to vehicles and Vehicles to Vehicles. An based on ID-based authentication framework will be used to access the privacy preservation has been projected for VANETs that utilizes IBS and IBOOS schemes for authentication, personal key cryptography for privacy preservation.one among the benefits of this framework is its reusability, which suggests that, it also can be reused with new IBS and IBOOS schemes for security and performance enhancements.

4. Vehicle to Road Side Unit Authentication:

The Road Side Unit sporadically broadcasts its information, in order that the vehicles in this transmission vary will get the RSU's information. Once a vehicle needs to evidence itself within the system, it at first sends a be a part of request message to a RSU, that verifies the signature victimization Identification based security(IBS) and accepts the vehicle as valid as long as it's already genuine by the RTA.

5. Vehicle to Vehicle Authentication:

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

6. IBS Scheme for VANETs

An ID-based signature scheme from IBC used in VANETs consists of four steps including setup, key extraction, signature signing and verification:

- **Setup**: The RTA computes a master keys and public parameters param for the private key generator (PKG), and gives parameter param to all vehicles.
- **Extraction**: Based on an ID string, a vehicle generates a private key sekID associated with the ID using the master key S.
- **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;

7. IBOOS Scheme for VANETs

An ID-based online/offline signature scheme from IBCused 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 sekID 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 of M.
- **Verification**: Based on the ID, M and SIGonline, the receiving vehicle outputs ―accept‖ if SIGonline is valid for verification and outputs ―reject‖ otherwise.

8. Public Key Cryptography

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.

In the VANETs, each vehicle 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.

Types of Communications in Vanet

1. Vehicle to vehicle communication

Using multi-hop/multi cast technique. It uses two types of broadcasting i.e.

- Naive broadcasting
- Intelligent broadcasting

2. Vehicle to infrastructure communication

- Have a high bandwidth link with vehicle and roadside equipment.
- Roadside units broadcast messages for communications.

3. Routing based communication

- Uses multiple hops and unicast device.

APPLICATIONS

- Real-time traffic management system process.
- Traffic Information Internet Access .
- Road Hazard Control Notification Cooperative Collision Warning .
- Co-operative Message Transfer Post Crash Notification.
- Digital map downloading of route diversions.

V. Conclusion

In this paper we present the implementation of the traffic signals to avoid the chances of collision between vehicles to vehicle and connection between the RTA to RSU and RUS to vehicles and message authentication of the vehicles and send secure messages from one to other units and it will be reduce the communication overhead between the unit sets . The ACPN is a very much reusability structure to access message authentication.

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. 2 .M. Raya and J. Pierre, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
3. X. Lin, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving," IEEE Trans. Wireless Comm., vol. 7, no. 12, pp. 4987-4998, Dec. 2008.
4. A Studer et al., "Flexible, Extensible, and Efficient VANET Authentication," J. Comm. and Networks, vol. 11, no. 6, pp. 574-588, 2009.
5. Y. Zhang et al., "Securing Mobile Ad Hoc Networks with Certificate less Public Keys," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 386-399, Oct.-Dec. 2006.
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. H. Lu, J. Li, and M. Guizani, "A Novel ID-Based Authentication Framework with Adaptive Privacy Preservation for VANETs," Proc. Comm. and Applications Conf. (ComComAp), pp. 345-350, 2012.
8. M. Riley, K. Akkaya, and K. Fong, "A Survey of Authentication Schemes for Vehicular Ad Hoc Networks," Security Comm. Networks, vol. 4, no. 10, pp. 1137-1152, 2011.
9. J. Li, H. Lu, and M. Guizani, "ACPN: a novel authentication framework with conditional privacypreservation and non-repudiation for VANETs," *Submitted to IEEE Transactions on Parallel and Distributed Systems,* undergoing major revision, 2013.

