VEHICULAR AD HOC COMMUNICATION SECURITY ENHANCEMENT

Er.Sushil Lekhi,[1]Er. Deepika Sharma[2]
[1]Assistant Professor, [2]Research Scholar
[1,2]Department of Computer Science and Engineering, Rayat Institute of Engineering and Information Technology College, Railmajra,SBS Nagar, (Punjab) India
[1]lekhi.engg@gmail.com,[2]ashu.gori.sharma@gmail.com

ABSTRACT:-**The large and rapid changes that know all the domains in the world not excluded the transport sector. Today, the fleet is growing; the roads are becoming more dangerous by the effect of congestion and increase the likelihood of collusion. Therefore, securing traffic becomes not only a necessity but also an obligation. The key challenge in Vehicular communications is how to combat with the high mobility of vehicles due to their different speed, as they communicate with each other via the Access Point (AP). Vehicles moving at high speeds have short opportunity to distribute data among each other, and this has to be within the shortest time; else there will be collision. . In this paper objective of our work is to make the secure communication possible in the VANETs environment. Various existing security mechanisms are already proposed but they need the sharing of private key which is not thought to be secure and efficient as it may need frequent change of private key to keep the communication visible only to authorized entities.To show our secure model we will simulate the VANET environment on NS-2 simulator. The network will be consisting of a number of RSUs and moving OBUs. The communication will be designed securely in C++.**

KEYWORDS:-**VANET (Vehicular ad hoc network), MANET (Mobile ad hoc network), RSU (Road side unit), Access Point, OBU(On-board units).**

I. INTRODUCTION

With the adoption of state-of-the-art wireless communication technologies, it is envisioned that vehicles are equipped with wireless communication devices, mostly named as on-board units (OBUs), to communicate with roadside units (RSUs) located at roadside or street intersection. Vehicles can also use OBUs to communicate among each other. Such a communication network is referred to as vehicular ad hoc network (VANET). VANET can be described into two types: vehicle-to-infrastructure (V2I) communication or inter-vehicle (V2V) communication.The basic application of VANET is that OBUs periodically broadcast information on their present states (e.g., the current time, position, direction, speed and traffic events) to other nearby vehicles and RSUs. For example, the traffic events could be accident location, brake light warning, change lane/merge traffic conjunction, emergency vehicle warning information, etc. After that, other vehicles may change their travelling routers and RSUs may inform the traffic control centre to adjust traffic lights for avoiding possible traffic congestion problems in the daily life. VANET offers various services and benefits to users, and thus deserves deployment efforts.[1] The security of message exchange plays a key role in VANET applications.Security issue is critical in VANETs because many different forms of attacks against VANETs may emerge due to the use of wireless devices in VANET communications. Such security attacks may lead to bad user experience (thus causing the loss of revenue for those value-added service providers) or create even morecatastrophic consequences such as the loss of lives due to the traffic accidents due to the failure of VANET communications.[2]Now these days, the security issue in VANETs has become a current hot topic, and then many researchers provide the Vechicle-2-infrastucture and Vechicle-2-Vechicle authentication mechanisms to protect valid users. However, the architecture for an efficient Vechicle-2-Vechicle authentication mechanism is more challenge than that for Vechicle-2-Infrastructure authentication mechanism in VANETs because the vehicle cannot be authenticated via the infrastructure directly in Vechicle-2-vehicle communications.[3] Each vehicle is equipped with a wireless communication device called an on-board unit (OBU) and at the road side location road-side units (RSU) are installed. The system is coordinated by a trusted third entity called, Central Authority (CA), which could be the department of transportation. Because of the important aspect of the information shared through the network, it is necessary to develop the security protocols to make its(VANET) applications are helpful. Especially,very sensitive information such asprivacy and location identity must be preserved through vehicular communications [4].Vehicular communication is of high importance to improve road safety by preventing hazardous situations and by providing information on the road state to make drivers aware of the existing environment. Vehicular Ad hoc Networks (VANETs) leverage communicating devices to construct a global awareness of the surrounding environment and vehicles intentions. The first concern of using such networks is to extend the driver perception which is generally limited to line of sight. This, in turn, guaranteed high information reach ability. In high speed environments such as highways and freeways, the reaction time must be reduced and consequently so must the information dissemination delay [5]. To enhance security points need to be in consideration:

a. The mobility Impact on the density of vehicles around the transmitter.
b. The transmitter's and receiver'sspeedsimpact on the system reliability.
c. The impact of channel fading by modelling the communication parameter as a random Variable.

d. The hidden transmission collisions andterminal problem from neighbouring vehicles.
e. Ensuring reliable messages transmission with respect to the delay constraint especially in highly dense environments.
f. Ensuring that a high broadcast load does not affect the network Performances especially close to channel saturation threshold.
g. Ensuring the 1000 meters dissemination distance barrier specified by the standard.

The security of VANETs has been receiving a valuableamount of attention in the area of wireless mobile networking because VANETs are easily vulnerable to malicious attacks.VANETs have attracted increasing attention from both industry and research communities within recent years. The focus of VANETs is to fulfil users‟ requested demands on the road and make their journey comfortable and safe.[6]

1.1 SECURITY REQUIREMENT IS FURTHER CLASSIFIED INTO DIFFERENT PARAMETERS THAT ARE:

We focus on security and privacy in VANET. A secure IBV scheme should satisfy the following security objectives: message authentication, identity privacy preserving, traceability, non-repudiation, unlink ability and replaying resistance etc. The detailed descriptions of the above requirements are listed as follows.

1) ***Message authentication***: Any RSU should be able to verify that a message is indeed sent and signed by a certain legitimate vehicle without being updated/changed or forged by anyone.

2) ***Identity privacy preserving:***The real identity of a vehicle should be kept anonymous from Road Side Units and anothervehicle. Any third party would not be able to reveal the vehicle's real identification by analyzing multiple messages sent by it.

3) ***Traceability****:* Although the vehicle's real identity should be hidden from Road Side Units and other vehicles, if necessary, Trust authority would have the ability to retrieve the vehicle's real identification. In addition, once the malicious vehicle wants to escape from its guilty of causing the accident or crime, Trust Authority still enable to trace its real identity from its message sent under the proposed scheme.

4) ***Non-repudiation:***A infected vehicle is unable to broadcast wrong messages to misinform an Road Side Unit and deny the behaviours when Trust Authority traces it by its message signatures.

5) ***Unlink ability:.***A infected vehicle or RSUs cannot successfully distinguish an anonymous entity by linking some of its message authorized signatures.

6) ***Replaying resistance:***A malicious vehicle could not collect and store a signature message and try to distribute it at a later time when the original message is invalid.

7) ***Efficiency:***In VANETs, the computational cost of vehiclesmust be as low as possible in order to achieve a real-time response.

8) ***Anonymity:***The anonymous authentication procedure verifies that an On-Board Unit does not use its real identification to execute the authentication proceeding scheme.

9) ***Privacy of Location:***An adversary collects the serial authentication messages of the OBU but it still failed to track the location of the vehicle.

10) ***Mutual authentication:***A mutual authentication procedureis implemented whereby the LE must verify that the OBU is a legal user and the OBU must ensure that the LE is not doubtful.

11) ***Message Integrity:***The message integrity means that data cannotbe changedimpalpably.[1,3]

Above are the main security requirements that we should keep in mind while communicating.

1.2 PROPOSED METHODOLOGY

Various existing security mechanisms are already proposed but they need the sharing of private key which is not thought to be secure and efficient as it may need frequent change of private key to keep the communication visible only to authorized entities.We propose a secure session key generation for each pair of communication entities in the network to keep the data confidential while making it bind only with authorized parties of VANETs. The communication may be between two OBUs or in between one OBU and one RSU. The proposed methodology will consist of the followingSteps:-

To show our secure model we will simulate the VANET environment on NS-2 simulator.

STEPS:

Step:-1 Install Ubuntu 12.10. Update Ubuntu using command Sudo-apt get update.

Step:-2 Study and Installation of ns-2 version NS-2.35, Install xgraph, Install Network Animator.

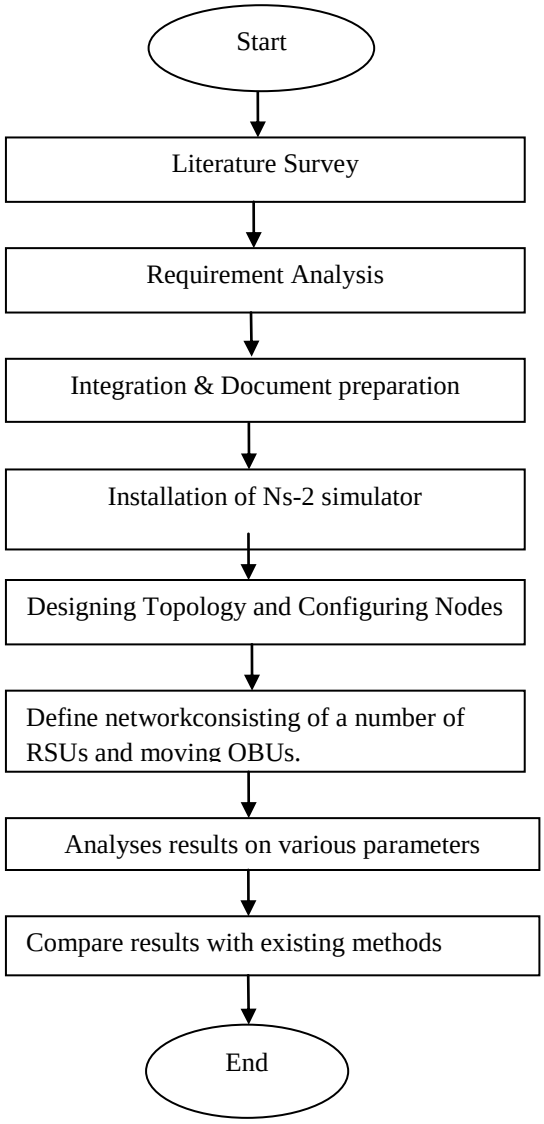
Step:-3 Designing Topology for communication.

Step:-4 Configuration of nodes in network.

Step:-5 Define network that will be consisting of a number of RSUs and moving OBUs.

Step:-6 Creating backend header file in C++ then integrate with NS-2 simulator.

Step:-7 Defining parameters for output that enhance security.



As per the security requirements defined in the 1.1 part and the topology we defined the output parameters will be defined.
The rest of the paper is organized as follows: Section II describes Related Researches: A Review on VANET Security Section III gives the conclusion and future scope.

II. RELATED RESEARCHES: A REVIEW

In this paper we have discussed various techniques used for the enhancementof security parameters in the vehicular ad hoc communication:

2.1 Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET.

Shiang-FengTzeng et al 2015:[7]Issues considered in the authentication schemes combine the level of security and computational efficiency and capacity in verification processes.Normally, authentication in vehicular ad-hoc networks (VANETs) uses PKI to verify the integrity of messages and the identity of message senders. Most existing schemes focus mainly on assuring the confidentiality and security of VANET information. However, these schemes mightnot work well in VANET.Because it is difficult for a Roadside Unit (RSU) to verify every vehicle's signature sequentially when a large number of vehicles emerge in the coverage areas of an RSU. To reduce the computational overhead of RSUs, we propose a Proxy Based Authentication Scheme is represented as PBAS using distributed computing. In this, proxy vehicles are used to authenticate multiple messages with a verification function at the same time.We also design an expedite key negotiation scheme for transmitting sensitive messages

2.2 A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs Computing.

Huang Lu et al 2012: [8]In this framework, the vehicles use pseudonym/signal to modify and to communicate of pseudonym depends on vehicles demands. The authors propose a novel ID-based authentication framework with adaptive privacy preservation for VANETs.

2.3 A Cooperative Message Authentication Protocol in VANETs

Yong Hao et al 2012*:*[9]The idea of this work is to alleviate vehicles computation burden during the authentication stage and reduce the number of safety messages that each vehicle needs to verify.A cooperative message authentication protocol in VANETs is supposed to implement.

2.4 A Pre-authentication Method for Secure Communications in Vehicular Ad Hoc Networks.

JaeHyu Kim et al 2012:[10]JaeHyu Kim and JooSeok Song propose a pre-authentication method to reduce the number of packets transmitted in the key request stage based on scalable robust authentication protocol (SRAP). They also try to use symmetric key encryption function to reduce calculation time.

2.5 Secure and Efficient Protocol for Position-based Routing in VANETs

JieHou et al 2012:[11]The proposed scheme improves the security of position-based protocol. The authors present a secure and efficient protocol for position based routing in VANETs.

2.6 ID-based Safety Message Authentication for Security and Trust in Vehicular Networks

SubirBiswas et al 2011:[12] In this paper the groupof people who all are performing a combine task is propose ID-based Safety Message Authentication for trust and security in Vehicular Networks. They incorporate an ID-based proxy signature framework with the standard ECDSA for VANETs road-side unit (RSU) generated for safety application messages. The proposed protocol is appropriate for authentication and trust management but may suffer of the traceability problem. Because, if an hacker intercepts the message exchanged by two OBUs and

if it contains the OBU location, then he could trace a vehicle in the network.

2.7 A Secure and Location Assurance Protocol for Location-Aware Services in VANETs

Youngho park et al 2011:[13] Youngho Park, Kyung-Hyune Rhee and Chul Sur present a secure and Location Assurance Protocol for Location-Aware Services in VANETs which is used to providesavoid illegal movement tracking and anonymous authentication of vehicles in VANET and with this the location assurance. The proposed scheme permits to the vehicle to have confidence and assurance that the received information originated from the vehicles that actually passed through the target location area. The attacker can intercept it and use it to threaten the life of drivers, violating confidentiality properties and authentication.

2.7 A Privacy-Preserving Trust Model for VANETs.

Aymantajeddine et al 2011: [14] It is designed on a static group of vehicles assigned off mood. This protocol doesn't give a better security algorithm because of dynamic topology and change in nodes in vehicular network. The authors propose a privacy-preserving trust model that attains the privacy of the users through groups and offers security through trust and reputation. The protocol permits to exchange secure messages among vehicles and helps them to attain the reliability of receiving message.

2.8 A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation

Bharti Mishra et al 2011:[15]The authors proposeda efficient and secure protocol for VANETs. Their scheme ensures both message and information authentication and privacy reservation. But a vehicle needs to communicate to road side unit before and after verifying the signature of a message it has received.

2.9 "Short-lived Key Management for Secure Communications in VANETs, Security and Applications"

Stefano Busaneli et al 2011:[16] The proposed algorithm is based on a couple of hash-chains generated from the master/primary key.An innovative scheme for generating series of-lived secret keys that are shared by all the subscribers of the service is presented.

2.10One-way-linkable Blind Signature Security Architecture for VANET

Baber Aslam et al 2011:[17] The proposed protocol doesn't require a tamper-proof-device (TPD) which reserves the vehicles communication keys. The creator present a security architecturewithout changing the complex or multi-transaction procedure scheme which helps achieve all the security attributes.

2.11 Securing Vehicular Ad-Hoc Network against Malicious Drivers: A Probabilistic Approch

Danda B. Et al 2011:[18]in this paper the authors designs an algorithm to provide security to vehicular communication and exchange of information among vehicle is based on a probabilistic approach is proposedtoidentify the trust level of vehicles communication messages and to verify the validity of the received messages.

2.12 REACT: Secure and Efficient Data Acquisition in VANETs

KhaleelMershad et al(2011:[19]The innovation of the authors is to started each vehicle user (driver and passengers) to communicate separately in the network. A Secure and efficient data acquisition method in VANETs is think to propose. The road side unit assigns to each user who is connected a pseudonym per packet to prevent attacks.

2.13PPAS: A Privacy Preservation Authentication Scheme for Vehicleto- Infrastructure Communication Networks

Ming –Chin et al 2011:[20]A privacy preservation authentication scheme for communication between vehicle and infrastructure in VANETs is proposed and designed. The scheme allows to a vehicle and a road side unit to authenticate among each other without returning to the trust authority. Although the proposed scheme justifies most of the security requirements, it can be used to a communication between vehicles.

2.14 Group based Secure Source Authentication Protocol for VANETs

You Lu et al 2010:[21]The results of this implementation can guarantee multicast source authentication and boost the efficiency of authentication for multicast communication in VANETs. Group-based Source Authentication protocol (GSA) proposed to handle the information authentication in VANETs. GSA makes use of group parameters as dynamic group key to protect data transmission in intra-group or different group communication.

2.15 "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network

C.I Fan et. al 2008: [22] The authors propose an efficient pseudonymor signal catching PKI mechanism based on bilinear mapping to improve the performance of the message authentication protocol, and permits certificate tracing and certification revocation.

2.16 Protocol of Change Pseudonyms for VANETs

Adetundji Adigun et al 2013:[4]Our protocol provides authentication, non-repudiation and privacy.We evaluate in this work, the bandwidth used by considering the vehicles speed in each approach.Our objectiveis to permit at least two vehicles to change their pseudonym or signal in the same time interval The supposed protocol is created on equidistant distribution of the road side unit and uses the average of speed allowed on the road to evaluate lifetime t of the communication's pseudonyms and certificates. The exchange of information or data is based on symmetric and asymmetric cryptography scheme and it uses hash function.

III. CONCLUSION AND FUTURE SCOPE

After studying the above mentioned surveys we try to overcome the shortcomings in the previous system in future we would propose a secure session key generation for each pair of communication entities in the network to keep the data confidential while making it bind only with authorized parties of VANETs. The communication may be between two OBUs or in between one OBU and one RSU.

ACKNOWLEDGEMENT

This work is supported and guided by my Research guideEr. SushilLekhi, Assistant Professor (IT) of RayatInstitute of Engineering and IT, Ropar. I am thankful to him for his continuous guidancewho made it possible.I am grateful for his continual support, encouragement, and invaluable suggestion

REFERENCES

[1] Shiang-FengTzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and MuhmmadKhurram Khan (2015) "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET" vt-2014-00658. doi 10.1109/tvt.2015.2406877, ieee.

[2] Yiliang Liu, Liangmin Wang and Hsiao-Hwa Chen (2014)"Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks." ieee transactions on vehicular technology, vol. xxx, year 2014.

[3] Ming-Chin Chuang and Jeng-Farn Lee (2014) "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks" ieee systems journal, vol. 8, no. 3, september 2014 749.

[4] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri (2013)"Protocol of Change Pseudonyms for VANETs" 978-1-4799-0540-9/13/$31.00 ©2013 ieee

[5] Omar Chakroun, SoumayaCherkaoui (2013) "Enhancing Safety Messages Dissemination Over 802.11p/DSRC" The 7th IEEE LCN Workshop on user mobility and vehicular networks (on-move 2013) 978-1-4799-0540-9/13/$31.00 ©2013 ieee

[6] Khalid Abdel Hafeez, Lian Zhao, Bobby Ma, Jon W. Mark (2013) "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications"ieee transactions on vehicular technology, vol. 62, no. 7, september 2013.

[7] Shiang-FengTzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and MuhmmadKhurram Khan (2015) "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET" vt-2014-00658. doi 10.1109/tvt.2015.2406877, ieee.

[8] Huang Lu, Jie Li and Mohsen Guizani, (2012) " A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs Computing", Communication and Applications Conference (ComComAp), pp. 345-350, 2012.

[9] Yong Hao, Tingting Han and Yu Cheng,(2012) "A Cooperative Message Authentication Protocol in VANETs," Global Communication ConferenceIEEE, pp. 5562-5566, 2012.

[10] JaeHyu Kim and JooSeok Song, (2012) "A Pre-authentication Method for Secure Communications in Vehicular Ad Hoc Networks," 8th International Conference on Wireless Communication, Networking and Mobile Computing (WiCom), pp.1-6, 2012.

[11] JieHou, Lei Han, Jiqiang Liu and Jia Zhao,(2012) "Secure and Efficient Protocol for Position-based Routing in VANETs", Intelligent Control Automatic Detection and High-End Equipment, (ICADE), IEEE International Conference, pp. 142-148, 2012.

[12] SubirBiswas, JelenaMisic and Vojislav Misic,(2011) "ID-based Safety Message Authentication for Security and Trust in Vehicular Networks", 31st International Conference on Distributed Computing System Workshops, pp.323-331, 2011.

[13] Youngho Park and Kyung-Hyune Rhee, Chul Sur,(2011) " A Secure and Location Assurance Protocol for Location-Aware Services in VANETs," 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.456-461, 2011.

[14] AymanTajeddine, AymanKayssi and Ali Chehab,(2010) "A Privacy-Preserving Trust Model for VANETs," 10th IEEE International Conference on Computer and Information Technologie (CIT 2010), pp.832-837.

[15] Bharati Mishra, Saroj Kumar Panigrahy, TariniCharanTripathy, Debasish Jena and Sanjay Kumar Jena, (2011) "A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation", Information and Communication Technologies (WICT), pp. 880-885, 2011.

[16] StefanoBusanelli, Gianluigi Ferrari and LucaVeltri, (2011) "Short-lived Key Management for Secure Communications in VANETs, Security and Applications" IEEE, pp.613-618, 2011.

[17] Baber Aslam and Cliff C.Zou, (2011) "One-way-linkable Blind Signature Security Architecture for VANET", The 8th Annual IEEE Consumer Communication and Networking Conference- Smart Spaces and Personal Area Networks, pp.745-750, 2011.

[18] Danda B. Rawat, Bhed B. Bista, Gongjun Yan and Michele C. Weigle,(2011) " Securing Vehicular Ad-Hoc Network against Malicious Drivers: A Probabilistic Approch", International Conference on Complex, Intelligent, and Software Intensive Systems, pp.146-151, 2011.

[19] KhaleelMershad and Hassan Artail, (2011) "REACT: Secure and Efficient Data Acquisition in VANETs," 7th International Conference IEEE, Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 149-156, 2011.