A Survey on Various Methods in VANET Based On Security and Privacy-Preserving Navigation System

Gowtham.I[1] Prabhu.K[2] Dr.L.M.Nithya[3]
[1,2]P.G. Scholar [3]Professor
[1,2,3]Department of Information Technology
[1,2,3]SNS College of Technology, Coimbatore, Tamilnadu, India.

Abstract— Vehicular ad hoc network (VANETs) is a promising and challenging approach to improve the traffic management and traffic safety with wireless vehicle-to-roadside and vehicle-to-vehicle communications. An efficient navigation scheme is employed based on the online road information gathered by VANETs to direct the drivers to corresponding destinations in a real-time and distributed manner. Major advantage of using real-time road situation is to estimate a better route and the information source that is appropriately authenticated simultaneously. In order to guard the privacy of the drivers, the destination and the driver who provides the query are assured to be unlinkable to any party. This idea can be attained by enhancing the anonymous credential. In this paper, various methods related to security and privacy related methods are surveyed for providing security for VANET. Each surveyed method briefly discusses the security and privacy related issues and solutions in VANET. At last, comparative measures of each method are presented which provides the significance and limitations for VANET Based Secure and Privacy-Preserving Navigation system.

Key words: Vehicular ad hoc network, Privacy-Preserving Navigation System, vehicle-to-vehicle

I. INTRODUCTION

In Vehicular Ad Hoc Networks (VANETs), vehicles are furnished with wireless communication devices and sensors which allow vehicles to effectively sense traffic and road environment, and notify other nearby vehicles concerning traffic jams and possible emergency situations. VANETs present challenging techniques to diminish the 43,000 traffic fatalities and $260 billion exhausted yearly on traffic-related health care in the United States. Besides helping for preventing accidents, VANETs also offers business services which improve an experience of driver's.

In VANETs, On Board Unit (OBU) of vehicles eventually communicates with other vehicles' OBUs and also with predetermined infrastructure known as Road Side Units (RSUs). In order to function reliably and securely a vehicle's OBU must verifies the messages shown by other RSUs and OBUs ; or else, an attacker can effortlessly insert bogus messages to interrupt the usual process of VANETs. To facilitate OBUs and RSUs to authenticate each other, efficient secured mechanisms need to be built.

In general a driver wants another system namely Traffic Message Channel (TMC) to learn about real-time road conditions, which has been implemented in various developed countries. Traffic Message Channel (TMC) employs FM radio data system which broadcasts instantaneous weather and traffic information to drivers. Special tool is needed to filter or decode the received information. However, special road conditions i.e. severe traffic accident is only broadcasted and a driver could not hold information like the common facility of a road from TMC.

Recently, VANETs popularly developed in several countries which turn out to be significant building block of the Intelligent Transportation Systems (ITSs). In traditional system of VANET, RSU and OBU are mounted along the roads. In addition to trusted authority (TA) some other application servers are mounted in the back end. The RSUs and OBUs are communicated by means of Dedicated Short Range Communications (DSRC) protocol over the wireless channel whereas the RSUs, application servers and TA are communicated by means of a secure fixed network by Internet. The essential application of a VANET is to permit random vehicles to broadcast safety messages to other nearby vehicles and to RSU frequently such that other vehicles may alter their travelling routes and RSUs might notify the traffic control centre to regulate traffic lights for evading potential congestion of traffic. Similarly, a VANET can also be inferred as a sensor network since the traffic control centre or various central servers can bring together plenty of valuable information about road situation from vehicles. It is natural to examine how to exploit the gathered real-time road conditions to offer useful applications.

The following literature surveys various methods for security and privacy related issues in VANET. In addition merits and demerits of each method is represented in the following comparative table.

II. SECURITY AND PRIVACY-PRESERVING METHODS IN VANET

A. Amoeba

In [1] Krishna Sampigethaya et.al presented AMOEBA, that presents location privacy by employing the vehicles group navigation. The presented method works in group concept by means of grouping vehicles to alleviating the location tracking of every target vehicle. In addition, this concept offers robust anonymous access to avoid the profiling of Location Based Service (LBS) applications used by every target vehicle. During navigation, in order to increase location privacy at opportune places, random silent period in join technique is facilitated for every target. Then a trade off between safety and location privacy is balanced by employing the solution offered by power control ability of vehicles. The presented method in this work dealt the location privacy risks that appear in VANET owing to unauthorized tracking of vehicles derived from their broadcasts in addition to the potential user privacy risks as a result of identification of LBS applications accessed from vehicle. Finally this method leveraged the group of vehicles to offer unlink ability among location of a LBS broadcast request and requested LBS application. The strength of the obtained anonymous access to LBS applications was used for several attacks by a global passive adversary.

B. RAISE- RSU-Aided Messages Authentication Scheme

In [2] Chenxi et.al presented RSU-aided messages authentication scheme (RAISE) for addressing the privacy and security problems in VANET. The presented scheme goal offers a considerable improvement in scalability and authentication efficiency for metropolitan-area inter-vehicle Communication (IVC).Unlike traditional message authentication schemes which only considered IVC, the presented RAISE discovers the exclusive features of VANETs by utilizing RSUs to aid vehicles in authenticating messages. With this fact, a metropolitan area might covered by RSU in which a vehicle that obtains a message does not required to be confirmed by the message throughout a traditional public key infrastructure (PKI) based system so as to leads considerable overhead. As an alternative, each inter-vehicle Communication message will be connected with a short keyed-hash message authentication (HMAC) code produced by the vehicle, and the resultant RSU in the series will authenticate these HMACs and broadcast the observation of authenticity to each vehicle. The notice message obtained is by the association of hash values of IVC messages. Since HMAC is performed using fast symmetric decryption, the short HMAC code connected with each IVC message, confirms the message authenticity in an extremely fast and efficient way.

C. Temporary Anonymous Certified Keys (TACKs)

In [3] Ahren et.al presented Temporary Anonymous Certified Keys (TACKs) to obtain the privacy and security characteristics essential for key management in Vehicular Ad Hoc Networks (VANETs). The presented method utilizes short-termed keys in On-Board Units to sign messages employed for VANET communication. These short-termed keys are authorized by Regional Authorities (RAs). While updating keys, RAs validate that the appealing OBU is a justifiable OBU that has not been cancelled by means of that RAs do not gain knowledge of the OBU's identity this permits a suitable OBU to obtain a certificate for a temporary key and protect the privacy of OBU's. As RAs' certificates are simply suitable in their local region, OBUs should update keys ahead while entering a new region. Once a set of OBUs comes in the region, every OBU update keys at the same time that avoids eavesdroppers from tracking drivers from key changes when a message is recognized to violence the VANET, the certificates can be traced by the authorities which can be request back to the signer respectively.

D. Identity-Based Security System

In [4] Jinyuan et.al presented Identity-Based Security System which includes pseudonym-based scheme, threshold signature-based scheme and privacy-preserving defence scheme for achieving user privacy in VANET. The scheme of pseudonym-based method guarantees vehicle user privacy and traceability. Then a threshold signature-based scheme is used to attain non-frame ability in tracing law violators. By using this scheme an innocent vehicle could not be mounted by a ruined law enforcement authority by reason of the role-splitting system. After that the privacy-preserving defence scheme is presented and used for leveraging threshold authentication. This scheme assures that if any added authentication other than the threshold is provided then this result in the cancellation of the misbehaving users. The uniqueness of presented scheme is that it provides flexibility in the revocation. Further the dynamic accumulators in the threshold authentication system assist each user to put extra restrictions other than threshold on former communicating users, which is considered an interesting feature to service providers.

E. Oblivious transfer (OT) based Private Querying (OPQ) scheme

In [5] Chim et.al presented OT-based Private Querying (OPQ) scheme for addressing the privacy-preserving and confidential issues in VANETs for querying services This scheme is based on the methods of indistinguishable credentials and pseudo identity. In order to utilize this service, first a driver has to be authenticated to a close to his/her RSU. After that the RSU surpasses his/her system parameter credentials, then estimates the performance of the presented system with the varies system performance. By employing the law of oblivious transfer (OT), the driver may not know which system parameter credentials are being passed to him which is originally passed by RSU. By using the system parameter credentials attained to a QSP, a driver can consequently issue its query. With this system all RSUs, and QSPs collude and no one can make connect a query with the actual identity of the queries. In addition with this, basic security issues like message integrity and confidentiality has also been addressed.

F. Dynamic privacy-preserving key management scheme (DIKE)

In [6] Rongxing et.al presented Dynamic privacy-preserving key management scheme (DIKE) t for achieving user's privacy preservation for vehicle by enhancing the key update efficiency of location based services (LBSs) in (VANETs).Particularly in DIKE, initially privacy-preserving authentication technique is utilized in which that not only offers the vehicle user's anonymous authentication but also facilitates double-registration detection. After that improved LBS session key update procedures are presented. This works by dividing the session of an LB into numerous time slots in order that each time slot contains a diverse session key; while no users of vehicle are departed from the service session in which each connected user be able to utilize a one-way hash function to originally update the recent session key for obtaining forward secrecy. In addition with this a new dynamic threshold technique is incorporated in conventional vehicle-to-infrastructure (V-2-I) and vehicle-to-vehicle (V-2-V) communications to attain the backward secrecy of session key's. This means that while a user of vehicle departs from the service session, additional number of joined threshold users can jointly update the new session key.

G. VANET-based Ambient Ad-Dissemination scheme (VAAD)

In [7] Zhengming et.al presented VANET-based Ambient Ad-Dissemination scheme (VAAD) for maintaining secure ad disseminations by means of pragmatic cost and effect control VAAD offers an incentive-centred framework for the concerned parties to swap their clashing needs with regards of ad dissemination. VAAD accepts a distance-based gradient ad dissemination algorithm to exploit the

attainable ad effect by emulating the ad-posting models in the real world for a given innovating marketing effect and cost requirements of service providers (SP). In order to assist vehicular nodes' participation in VAAD, privacy-preserved and secured induced cash-in is guaranteed to hold financial transactions in VAAD. Hence VAAD provides a comprehensive solution to secure ad dissemination in VANETs with appropriate cost and effect control appropriately.

H. Physical-Layer Location Privacy-Preserving Scheme

In [8] Sanaa et.al presented Physical-Layer Location Privacy-Preserving Scheme which prevents attackers from localizing users within VANET hotspots. The presented system comprises the fake point–cluster-based system which prevents physical-layer attackers and attains mobile network nodes (MNNs') location privacy for public hotspots of mobile public in VANETs. The fake point–cluster-based system location privacy of sender by maximizing the attacker's uncertainty while measuring senders' received signal strength (RSS). With this, the presented scheme is practically incorporated by reason of the high likelihood of containing two nodes which choose the identical fake point, and then it enhances the performance of network by means of requiring less routing delay rather than those necessary for earlier mobility management protocols.

III. COMPARATIVE TABLE

The following comparative table shows the points the merits and demerits of each surveyed method in VANET security and privacy preserving methods.

S.No	Author & Year	Method/Technique	Merits	De-merits
1	Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran-2007	AMOEBA	Robustness against active attacks on vehicle safety and liability is achieved	Intersection behaviour for the mobility of vehicle is not evaluated. Improved security over group protocols is not modelled.
2	Chenxi Zhang, Xiaodong Lin, Rong xing Lu, and Pin-Han Ho-2008	RSU-aided messages authentication scheme (RAISE)	Improved authentication efficiency and scalability for IVC is produced, Less computation and communication overhead is obtained	Verification is done for group communication in VANET. Time delay occurs.
3	Ahren Studer, Elaine Shi, Fan Bai, Adrian Perrig-2009	Temporary Anonymous Certified Keys (TACKs)	Prevents eavesdroppers, Maintains constant overhead, Fulfilled security and privacy is obtained.	Limitation occurs in space complexity, Result unrealistic with congested traffic at such high speeds.
4	Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang-2010	Identity-Based Security System	Achieves desired privacy, traceability, authentication, non repudiation, message integrity, and confidentiality.	Communication overhead is results in inefficient design.
5	T.W. Chim, S. M. Yiu, Lucas C. K. Hui T.W. Chim, S. M. Yiu, Lucas C. K. Hui -2011	Oblivious transfer (OT) based Private Querying (OPQ) scheme	Better efficiency is obtained in terms of processing delay, message overhead, and success rate	Querying vehicle needs to perform more processing on the credentials. The QSP needs to keep more information and, possibly, more complicated processing.
6	Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen -2012	Dynamic privacy-preserving key management scheme (DIKE)	Improved efficiency and effectiveness is achieved in terms of low key update delay and fast key update ratio.	Desirable levels of security and robustness is not obtained
7	Zhengming Li, Congyi Liu, and Chunxiao Chigan-2013	VANET-based Ambient Ad-Dissemination scheme (VAAD)	Provides secure ad dissemination. Provides trade offs for conflicting requirements	Malicious nodes detected in VAAD is not detected and alleviated
8	Sanaa Taha, and Xuemin (Sherman) Shen-2013	Physical-Layer Location Privacy-Preserving Scheme	Efficient result is obtained with less routing delay. Better performance in network is obtained.	High message routing delay is resulted while sending the transmitted messages via several home agents. High consumption of power is obtained.

Table 1: Comparison of Various Methods

IV. CONCLUSION

The present survey illustrates various methods used for security and privacy preserving issues and solutions for VANET. The presented methods in the above literature demonstrates their inspiration and characteristics of the VANETs routing problem primarily for vehicle to vehicle (V2V) communication and vehicle-to-roadside Communications by means of providing VANETs routing methods that exist in the last few years were investigated and showed. In addition to each surveyed methods, comparison between each method is shown in comparison table which summarized result of the merits and de-merits of each methods. Thus presented survey used various methods related to security and privacy related issues in VANET whose open issues and research challenges are investigated and represented, as such effective effort on research must have be taken to address these issues.

REFERENCES

[1] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[2] C. Zhang, X. Lin, R. Lu, and P.H. Ho, "RAISE: An Efficient RSU Aided Message Authentication Scheme in Vehicular Communication Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1451-1457, May 2008

[3] Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE Sixth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '09), pp. 1-9, June 2009

[4] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang," An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," Proc. IEEE Transactions on Parallel and Distributed Systems, vol. 21, NO. 9, September 2010
[5] T.W. Chim, S. M. Yiu, Lucas C. K. Hui T.W. Chim, S. M. Yiu, Lucas C. K. Hui," OPQ: OT-Based Private Querying in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 4, December 2011
[6] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen," A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs," IEEE Transactions on Intelligent Transportation Systems, Vol. 13, No. 1, March 2012
[7] Zhengming Li, Congyi Liu, and Chunxiao Chigan," On Secure VANET-Based Ad Dissemination with Pragmatic Cost and Effect Control," IEEE Transactions on Intelligent Transportation Systems, Vol. 14, No. 1, March 2013
[8] Sanaa Taha, and Xuemin (Sherman) Shen," A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs," IEEE Transactions on Intelligent Transportation Systems, Vol. 14, No. 4, December 2013.