Safe Geo Graphic Location Privacy Scheme in the VANETs - Survey Methods and Its Limitation.

Mr. S.A. Khandelwal, Dr. P. M. Jawandhiya

Abstract— Vehicular ad hoc networks (VANETs) are expected to enable a plethora of communication-based automotive applications including diverse in-vehicle infotainment applications and road safety services. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large-scale VANET with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative. Via inter-vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated. However, most of VANET researches focus on message transmission. Vehicle is extremely personal device; therefore, personal information, so-called privacy has to be protected. In proposed work in which analyze identity and location privacy threatening factors, problems, and solutions based on network model. The network model's transparency design goal and protect vehicle's real identity even revealing the vehicle's location. The result of this work could guide a way to design a privacy preserve solution and present a trend of existing solutions.

Index Terms— Vehicular networks, Security ,Privacy, IVC, MANET, Attacks.

1 INTRODUCTION

Recently, Vehicular ad hoc network (VANET) [1] can offer various services and benefits to VANET users and thus deserves deployment effort. Vehicular networks are very likely to be deployed in the coming years and thus become the most relevant form of mobile ad hoc networks. In recent years, the number of motorists has been increasing drastically due to rapid urbanization. The number of automobiles has been increased on the road in the past few years. Due to high density of vehicles, the potential threats and road accident is increasing. Wireless technology is aiming to equip technology in vehicles to reduce these factors by sending messages to each other. Critical traffic problems such as accidents and traffic congestion require the development of new transportation systems [2]. Intelligent Transportation Systems (ITS) [3, 4] are aimed at addressing critical issues like passenger safety and traffic congestion, by integrating information and communication technologies into transportation infrastructure and vehicles. They are built on top of self-organizing networks, known as a Vehicular Ad hoc Networks (VANET)[9], Vehicular communication systems facilitate communication devices for exchange of information among vehicles and between vehicles and roadside equipment.

Working in tandem with the fielded Intelligent Transportation Systems (ITS) infrastructure, VANET is expected to enhance the awareness of the traveling public by aggregating, propagating and disseminating up - to - the minute information about existing or impending traffic-related events. Even though vehicles are organized mostly in an ad hoc manner in the network topology, directly applying the existing communication approaches designed for traditional mobile ad hoc networks to large -scale VANETs with fast-moving vehicles can be ineffective and inefficient. To achieve success in a vehicular environment, VANET-specific communication solutions are imperative. Via inter - vehicle communications, drivers can be informed of crucial traffic information such as treacherous road conditions and accident sites by communicating with each other and/or with the roadside infrastructure. With better knowledge of traffic conditions, it is plausible that the problem of accidents can be alleviated. Traffic monitoring and management can also be facilitated by vehicular communications. In support of their mission, VANET communications, employing a combination of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [4,5,6] wireless communication are expected to integrate the driving experience into a ubiquitous and pervasive network that will enable novel traffic monitoring and incident detection paradigms[4]. It is widely known that, due to high-speed mobility [6], V2V and V2I communication links tend to be short lived. Thus, it is important to propagate traffic-related information toward a certain region of interest instead of sending to a particular vehicle; moreover, one of the best ways of propagating traffic-related advisories towards a particular region is some form of (controlled) broadcast transmission.

- ***Sumit A. Khandelwal,*** *Working As a Assistant Professor of the Department Computer Science & Engineering, DES's College of Engineering and Technology, Dhamangaon Rly,(MH), India. E-mail – sumit3khandelwal@gmail.com ,*
- ***Dr. P. M. Jawandhiya****, Working as a Head the Department Computer Science & Engineering, Jagdambha College of Engineering and Technology, Yavatmal,(MH). India. E-mail – pmjawandhiya@rediffmail.com*

Mobile nodes that are connected in a self-organized way without an underlying hierarchical infrastructure form mobile ad hoc network (MANET)[7]. The MANET is called a vehicular ad hoc network (VANET) in the special case where the mobile nodes are embedded in vehicles. The nodes of a VANET [1,8] are commonly divided in two categories: On-Board Units (OBU), that are radio devices installed on vehicles, and Road Side Units (RSU)[18], that constitute the network infrastructure. RSUs are placed along the roadside and are controlled by a network operator[2]. VANETs are expected to allow for transmission of information between vehicles or between vehicles and the roadside units (RSUs) [17] and, thus, to enhance the safety of both vehicle drivers and passengers [1].

2 Literature Review

Existing studies related to the security and authentication for VANETs are based on the use of an asymmetric algorithm (Dedicated Short Range Communications (DSRC); IEEE). The sender signs each message before sending it using the asymmetric algorithm and the receiver verifies the originality of each received message. For reasons related to achieving high safety levels of ground transportation, it is recommended that each vehicle broadcast at regular time intervals information disclosing location, speed and direction (IEEE) [15].VANET is developed to support Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [2,4] communication. For many years, global researchers and projects have been investigating VANET research issues: routing, security, address allocation etc. Based on these researches, some project group built a test bed and implemented programs on the vehicle for communication. The field test results of message exchange and network connectivity are satisfied. For an additional research, they focused on security and privacy issues on VANET.

2.1 Attacks on Privacy

Attacks on privacy [14, 19] over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

A) **Identity revealing**. Getting the owner´s identity of a given vehicle could put its privacy at risk. Usually, a vehicle´s owner is also its driver, so it would simplify getting personal data about that person.

B) **Location tracking**. The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver[16].

Mechanisms for facing both attacks are required in VANETs. They must satisfy the tradeoff between privacy and utility. In this way, security mechanisms should prevent unauthorized disclosures of information, but applications should have enough data to work properly.

Paolo Cencioni [10] proposed a VIPER a Vehicle-to-Infrastructure communication Privacy Enforcement pRotocol. VIPER[18] is inspired to solutions provided for the Internet—mix—and cryptography—universal re-encryption. The intuition behind this protocol is to have vehicles not to send their messages directly to the RSU [1], but to have vehicles acting as mixes; further, messages are encrypted via a public key crypto-system that allows re-encryption of messages. The mix is limited to nodes belonging to the same group, where a group is defined as the set of vehicles registered within a Road Side Unit. VIPER is resilient to the message volume attack because both the message and the batch size are fixed, while it is resilient to the timing attack thanks to the mix function carried out by the relay vehicles. By forcing vehicles to transmit and receive messages at fixed data rate, it is also impossible for a local eavesdropper to track a message using different transmission and receiving intervals. The protocol is to be resilient to traffic analysis attacks and analytical results suggest that it also performs well with respect to key performance indicators: queue occupancy, message path length and message delivery time. VIPER also performs well with respect to key performance indicators: queue occupancy, message path length and message delivery time that is the performances of VIPER are only marginally affected by an increase in the number of vehicles.

Lo-Yao Yeh [11] proposed a Portable privacy-preserving Authentication and Access Control Protocol, named PAACP, with the support of differentiated service access control. In addition, considering stringent time requirement in transmission delay, PAACP eliminates the communications between the roadside units (RSUs) and service providers (SPs). In a conventional access control scheme, SPs are usually responsible for determining the validity of the access requests. To get rid of the communication with SPs, we propose a novel portable access control method to store a portable service right list (SRL) into each vehicle, instead of keeping the SRLs in the SPs. In order to assure the validity and privacy of an SRL, we also propose a novel attachable blind signature. Based on the attachable blind signature, vehicles (OBUs) cannot tamper the SRL. Therefore, PAACP can prevent privilege elevation attacks. As for privacy protection of users, the SP cannot trace the current location of the requesting vehicle, due to the attachable blind signature and the no need of any verification by SP. In addition, PAACP is more efficient than conventional access control schemes since RSUs can verify the correctness of an SRL without backend communications with SPs. As a result, PAACP is desirable for large scale VANETs. PAACP achieves the following properties: (1) mutual authentication between the requesting vehicle and RSU, (2) dynamic session key establishment for the subsequent communications, (3) privacy preservation of the vehicle's information, (4) data confidentiality and integrity, (5) differentiated service access control, and (6) better scalability.

Sun et al [12] proposed a privacy-preserving defense scheme against misbehavior in leveraging threshold authentication technique. This pseudonym-based scheme to assure vehicle user privacy and traceability and preserve user privacy, and simultaneously provide traceability (i.e., tracing law violators by enforcement authorities and tracing misbehaving users by network authorities. The major differences between these schemes are the different technical realizations of the privacy and traceability schemes, due to the different application scenarios and detailed security requirements. Communication costs in systems are mainly induced by broadcasts. Each message broadcast by vehicles consists of a pseudonym (22 bytes), a plaintext message (disregarded in the comparisons), and a signature. Each broadcasted message in ID-based cryptosystem yields 65 bytes. If the RSA-based PKI is adopted, each broadcasted message will induce up to 1.1 K bytes communication overhead. The broadcast of partial threshold signatures by participating authorities for non-frame ability takes place infrequently due to the rare case of escaping from the crime scene, as argued in the storage analysis.

LU *et al.*[13] proposed Dynamic Privacy-Preserving Key Management Scheme each vehicle user can be privacy-preserving authenticated before joining a Location-Based Services (LBS) and can also use a pseudo-ID to conceal its real identity during a service session; meanwhile, the service session key, which is used to secure service contents' distribution, can be fast and efficiently updated for achieving forward secrecy, backward secrecy, and collusion resistance. a privacy-preserving authentication (PPA) mechanism, which is derived from an efficient group signature, and can not only achieve vehicle user's privacy preservation but also restrict the possible vehicle user's double registration. Also, present efficient service session key update procedures, particularly for sparse VANET environments. Specifically, divide a service session into several time slots, and each time slot holds a different session key. When no vehicle departs from the service session, each joined user can use the forward-secrecy technique to autonomously update, the new session key to reduce the key update delay (KUD).

3 Limitation and Scope of research

Author [10] focus on not time-constrained communications that are usually involved in applications like automatic tolling, traffic information diffusion, and entertainment[2]. VIPER in terms of extra it's required, computations, time delay and number of dummy messages sent. VIPER introduces negligible overhead and it scales well with the dimension of the network as well as with increasing requirements on the security of the underlying mechanisms.

A Portable privacy-preserving Authentication and Access Control Protocol (PAACP) [11] for non-safety applications in VANETs. Considering the stringent time requirement in VANETs, The speed of a vehicle could be more than 140 km/h. The communication delay in IVCs or RVCs should be short enough to meet stringent time requirement Due to the portability of authorized service right lists, roadside units can verify the validity of access privileges without the aid of service providers. Moreover, In general, with an inter-vehicle distance of 70 m, there are some 70 vehicles within a radius of 1 km around a given car. During a traffic jam, with an inter-vehicle instance of 5 m, there can be more than 1000 vehicles within the same region. Therefore, VANETs will be large scale networks When a vehicle tries to access a non-safety service via an RSU, the RSU must pass the signature sent from the requesting vehicle to theproper SP(Service Provider) for verification, whereas the SP may be located in a distant network. The speed of a vehicle may be extremely high. It is possible that the response sent from the SP has not arrived yet, but the requesting vehicle had passed the transmission range of the RSU. In this scheme privacy protection of users, the SP cannot trace the current location of the requesting vehicle, due to the attachable blind signature and the no need of any verification by SP.

Author [12] VANET systems determine that communication efficiency is the foremost performance indicator, among all the efficiency concerns. The reason is that vehicles, as the mobile devices in VANETs, are capable of intensive data storage and complex computation tasks, rendering the requirements for storage and computation efficiency less stringent. Moreover, limiting most communications to local interactions and not relying on pervasive infrastructure give rise to more affordable communication costs in proposed VANET system.

Author [13] a VANET is usually implemented in a civilian environment, where the locations of vehicles are tightly related to the vehicle users, if LBS in VANETs disclose privacy information of vehicle users, i.e., identity privacy and location privacy, the LBS cannot be widely accepted by the vehicle users. Therefore, when designing an efficient key management scheme, the vehicle user's privacy preservation should be taken into consideration, which makes the design of key management more challenging.

4 Challenges in Vehicular Ad-hoc Network

The motivation for future network will need to manipulate precious information, with a possible impact on driver behavior and even on human life. Therefore, any solution needs to be thoroughly tested before integration in a real system. Field tests require not only implementation of the solution on real hardware, but also dedicated road infrastructure and equipped vehicles. These high costs have, until now, limited the size of these experiments at no more than 10–20 cars. Even the large-scale deployment scenarios that are currently prepared will only have the capacity to test a minor proportion from the proposals made by the vehicular ad-hoc networks (VANET) research community. On the other hand, the vehicular environment is highly complex and analytical models need to take into consideration not only the network, but also the properties of the vehicles and the behavior of the drivers simple traffic models are inappropriate for road traffic simulation, the impact of IVC on road traffic can be directly evaluated. The proposed research fulfill the requirement of privacy technique for location based and working for RSU unit. However, these solutions still require precise topological information, like building location. VANET simulation is the large number of nodes that need to be modeled. This is because in a wireless simulation, the receivers need to be searched among all the other entities. In the case of V2V networks, every node is also a source, therefore the number of communications is not constant and the resource consumption grows in this case with the square of the number of cars. proposed protocol is not only provides conditional privacy, a critical requirement in VANETs, but also able to improve efficiency in terms of the number of keys stored at each vehicle, and identity tracking in case of a dispute. Meanwhile, our proposed solution can be deployed easily: does not require support from the roadside infrastructure or the OBUs is secure against adversary.

5 Conclusion

Vehicular Ad-hoc Networks (VANETs) will start becoming deployed within the next decade. Among other benefits, it is expected that VANETs will support applications and services targeting the increase of safety on the road, and assist in improving the efficiency of the road transportation network. However, several serious challenges remain to be solved before efficient and secure VANET technology becomes available, one of them been efficient authentication of messages in a VANET. There is a significant body of research work addressing this issue, however, while progress has been made, the challenge is still far from having been resolved and reliable and secure systems ready for deployment becoming available. Form the above limitations discussed; there is a scope for further research to address various issues in the design and implementation of privacy system and its application for the VANET outdoor environment, in general, and more specifically to the efficient and multi-level privacy-preserving communication protocol scheme for VANET

Reference

[1] Ho Ting Cheng, Hangguan Shan, Weihua Zhuang, Infotainment and road safety service support in vehicular networking: From a communication perspective, Mechanical Systems and Signal Processing 25 (2011) 2020–2038, journal homepage: www.elsevier.com/locate/jnlabr/ymssp

[2] Josiane Nzouonta, Neeraj Rajgure, Guiling (Grace) Wang, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009

[3] Razvan Stanica , Emmanuel Chaput, André-Luc Beylot, —Simulation of vehicular ad-hoc networks: Challenges, review of tools and recommendations Computer Networks, journal homepage: www.elsevier.com/ locate/comnet2011.

[4] C. Sommer, Z. Yao, R. German, and F. Dressler, "Simulating the Influence of IVC on Road Traffic Using Bidirectionally Coupled Simulators," Proc. IEEE INFOCOM: Mobile Networking for Vehicular Environments (MOVE '08), Apr. 2008.

[5] M. Bakhouya , J.Gaber , P.Lorenz, "An adaptive approach for information dissemination in Vehicular Ad hoc Networks" Journal of Network and Computer Applications, journal homepage: www.elsevier.com/locate/jnca

[6] Razvan Stanica , Emmanuel Chaput, André-Luc Beylot," Simulation of vehicular ad-hoc networks: Challenges, review of tools and recommendations", Contents lists available at ScienceDirect Computer Networks journal homepage: www.elsevier.com/ locate/comnet

[7] A. Shastri, R. Dadhich, Ramesh C. Poonia, "Performance Analysis Of On-Demand Routing Protocols For Vehicular Ad-Hoc Networks" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011 DOI : 10.5121/ijwmn.2011.3407

[8] Yasser Toor And Paul Mühlethaler, Inria "Vehicle Ad Hoc Networks: Applications And Related Technical Issues" **IEEE Communications Survey,** 3rd Quarter 2008, Volume 10, No. 3 www.comsoc.org/pubs/surveys

[9] Hannes Hartenstein, University of Karlsruhe Kenneth P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks" Toyota Technical Center.

[10] Paolo Cencioni a, Roberto Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication" Computer Communications 31 (2008) 2790–2802, www.elsevier.com/locate/comcom

[11] Lo-Yao Yeh , Yen-Cheng Chen , Jiun-Long Huang, "PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks" Computer Communications 34 (2011) 447–456, Contents lists available at ScienceDirect Computer Communications journal homepage: www.elsevier.com/locate/comcom

[12] Jinyuan Sun, Chi Zhang, Yanchao Zhang, Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010.

[13] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, 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.

[14] David AntolinoRivas , Jose´ M. Barcelo´ Ordinas, Manel Guerrero Zapata,Julian D.Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation" Journal of Network and Computer Applications 34 (2011) 1942–1955, Contents lists available at ScienceDirect journal homepage: www.elsevier.com/locate/jnca

[15] Bidi Ying , DimitriosMakrakis , HusseinT.Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs" , Contents lists available at SciVerse ScienceDirect journal homepage: www.elsevier.com/locate/jnca

[16] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang, Yuguang Fang, "RescueMe: Location-Based Secure and Dependable VANETs for Disaster Rescue" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011

[17] Ahren Studer, Elaine Shi, Fan Bai§, & Adrian Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs" CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office.

[18] Paolo Cencioni , Roberto Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication" Computer Communications 31 (2008) 2790–2802 , www.elsevier.com/locate/comcom

[19] Levente Butty´an, Tam´as Holczer, and Istv´an Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs" F. Stajano et al. (Eds.): ESAS 2007, LNCS 4572, pp. 129–141, 2007. c_Springer-Verlag Berlin Heidelberg 2007

[20] Dandan Ren and Suguo Du, Haojin Zhu, "A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs", IEEE ICC 2011 proceedings, 978-1-61284-231-8/11/$26.00 ©2011 IEEE.