Future Challenges Facing Location Privacy Issues in VANET

Bhawna Chaudhary[1] Om Dukiya[2]
[1]School of Computer Systems and Sciences, Jawaharlal Nehru University, Delhi, India [2]Jagannath Institute of Technology, Jaipur, Rajasthan, India

Abstract— Vehicular ad hoc networks (VANET), a part of Intelligent communication systems are on the edge of real-time deployment. Nevertheless, their routing, appropriate count of RSU, security and privacy protection are the problems that have been identified only recently. This paper discusses one of the main challenges in VANET i.e. location privacy. The applications offer by VANET demands precise information of the nodes to run the network successfully. The information routing in the network can be used by an adversary to harm a specific target. This paper unfolds the current issues need to be considered for preserving location privacy, misapprehension between security and privacy and possible challenges can occur in future research.

Key words: VANET, privacy, location privacy, LBS

I. INTRODUCTION

In 1991, Department of Transportation in America has come up with the idea of implementing the Intelligent Transport System (ITS) to cope up the problem of increasing number of road fatalities every year. The main objectives considered during designing were efficiency, safety, and convenience. Though, the whole idea of ITS rely upon currently available internet technologies, which can create the disaster in a networking by opening opportunities from the remote user or to the nodes may be present in the system. This involvement of the internet as a significant part of the system create a WiFi environment in WiFi city with the advance facility provides road information. This type of network is known as Vehicular Ad hoc Networks, comprise of moving nodes (cars, truck, Buses, two wheelers etc) all of them equipped with wireless transmission capacity approximately 100 to 300 meters of each other to connect and create a network with a wide range. Any vehicle with such capacity can join the network and those moves out of signal range leave the network.The VANET communication has been classified into two types:

A. Vehicle to Vehicle Communication (V2V):

In V2V type of communication, a vehicle communicates with another vehicle to exchange the useful information about road conditions, traffic clogging, route diversion and weather changes etc.

B. Vehicle to Road-Side Communication (V2R):

In the V2R type of communication, a vehicle communicates with fixed infrastructure known as Road-Side Unit (RSU). RSU provides available information and internet facility to the users, so they can access the required information. Apart from these two types of communications other types have been suggested by some authors known as Hybrid communication, which combines the above-mentioned methods. Another one is Vehicle to Pedestrian Communication (V2P), in which a vehicle can also communicate with a person who has a mobile device to ask any queries or a person can ask vehicle for the carpooling service [1].The whole communication in VANET is performed by continuously exchanging a beacon message in the network which includes location information of a vehicle to gain better functionalities. However, improper usage of location information may trade-off the security and privacy of a vehicle or multiple vehicles in a network.

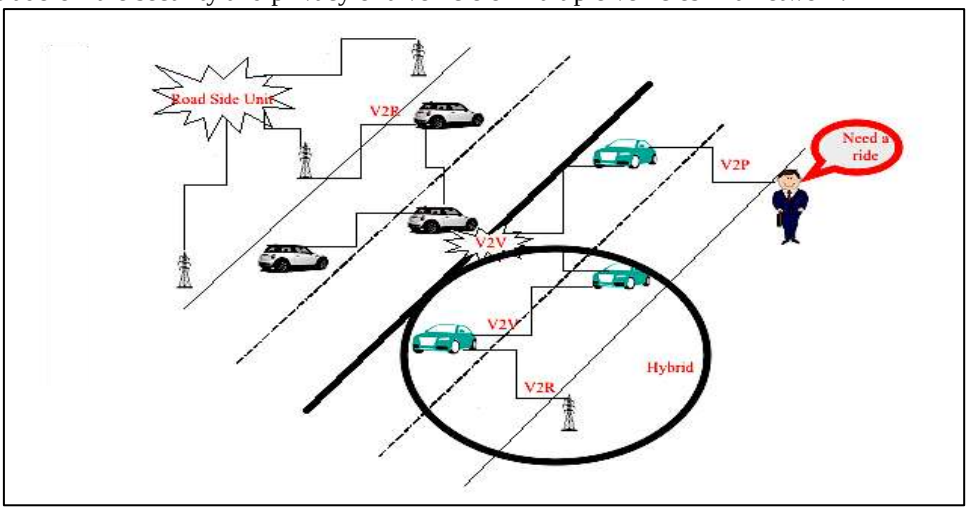

Fig. 1: Vehicle to Road-Side Communication (V2R)

II. WHAT IS PRIVACY?

Privacy cannot be generalized, it applies in different ways to different theories. Therefore, defining a standard definition of privacy is an extremely difficult task. So far definitions of privacy, a) "Hide yourself from other" explains that hide your all credentials from unknown or unauthorized activities.b) Danez [2], describes that privacy can be categorized into two types, hard privacy, and soft privacy. Hard privacy focuses on the goal of data protection by minimizing the size of data, whereas soft privacy aims at providing data security and privacy with security and privacy with specific purpose and consent by means of policies, access control and audit [2]. Another point that is to understand is that privacy is not a subset of security, both are entirely different concepts and inversely proportional to each other. To achieve a secure environment privacy preservation is not necessary, on the other hand, to preserve privacy sustaining security is essential. In [3], security is described as a condition, privacy is a prognosis.

Most of the applications of VANET are close to being set up in the real world while some are already functioning, there is more pressure to develop an adequate and comprehensive protection framework for the security and privacy. While a number of researchers are giving importance to the another issue like secure routing, RSU deployment, security and its attack, the area of privacy is far from understand. This paper lights the necessity to consider privacy uniformly and also presents the impact on the human if privacy is compromised.Moreover, Personal privacy is categorised into different categories.Such as:

A. Physical Privacy:

Also referred as bodily privacy. It includes physical encounters and concepts related to personal space, walls and doors etc. which separates the physical boundaries [3,4].

B. Information Privacy:

It can be described as the privacy, applies to data about people like passwords of their account, personal identification numbers etc [4].

C. Territorial Privacy:

This includes protection of one's personal belongings like house, vehicles etc. This type of protection generally requires registered space or some legal document that can verify the name of their owners [4].

In some scenarios, these categories may overlap each other and demand mechanisms that can take actions as per the laws. But our work is limited to discuss the privacy for secure communication in vehicular ad hoc networks.

D. Location-Based services (LBS):

LBS are a special type of promising and value-added applications in ad hoc networks, in which a service provider (SP) is responsible for providing various services through the ad hoc network and by utilizing the ability to make use of the location of requesting a vehicle. In this way, it can help those users who share common interest with their virtual friends while moving on the road. However, LBS's offers attractive features to VANET user's still requires strong management for the challenges concerned with the privacy preserving issues.

E. Location Privacy:

Location privacy is precise form of data privacy, it protects other adversaries to learn one's current and past location. It can be further divided into two levels: a) First is Personal subscriber level privacy that covers rights and options to individuals to control when, why and how their location is used by any application. b) Another one is Corporate-Enterprise level privacy, in which a corporate manager decides when, why and how mobile location capabilities provide application benefits to the whole organization, this is required in companies to preserve their corporate secrets and maintain a competitive edge.

III. SOLUTION PROPOSED TO ENSURE PRIVACY

To protect the identity of the user, many research solution projects and studies have been conducted regarding privacy of VANETs.

In [5], Papadimtratos et al proposed the idea, use of pseudonyms can be used to enhance the level of privacy in VANETs to make communication unidentified. In a region, a certification authority (CA) is responsible for management of the vehicle's identity. Each node either vehicle or RSU has assigned a unique identity with a pair of private and public cryptographic keys.Each private node has a set of explicit certified public keys as pseudonyms and appends the pseudonym to a message. These pseudonyms need to be changed after a specific lifetime span. Cheng et al propose a solution which states that how should be sender's identity security kept and also explains the different levels of location privacy for range location[6]. Raya et al [7] have given the concept of usage of a set of anonymous keys that should be changed frequently depending on the driving speed of the vehicle. The keys are available in Tamper Proof Device (TPD) and will change during visits to CA. CA certifies each key which has a short lifetime. The real identity of the vehicle can only be revealed by the concerned authority.

Dotzer[8], proposed a three-phase approach, first is initialization phase, which consists of matching the identity of a node with a set of pseudonyms in front of an authority. These pseudonyms will then be used to provide different services from car manufacturers that will map each pseudonym with a set of credentials.Second, the operational phase occurs when the node chooses one of the given pseudonyms to sign its message and participate in communication with other vehicles. The third phase is credential revocation phase, in which credential provided by the sender will be first verified by the other

vehicles to ensure the authenticity of the node. If the data sent by a authentic node is corrupted than this phase is applied. Lu et al [9,10], presents a privacy preserving protocol using Elliptic Curve method in VANETs for anonymous authentication. The protocol uses short-time anonymous key for communication between OBU and RSU. The reason for introducing anonymous key is, it needs minimum storage to avoid losing the security level. The network architecture comprises of TA , Fixed RSU and Mobile OBU installed in the moving vehicles. OBU is bound not to reveal its identity in the network.

Zhang et al [11] propose a decentralized group-authentication protocol, in which groups are maintained by each RSU unlike by centralized authority in other works. The vehicles in the group communicate via Vehicle to Vehicle messages that can be immediately verified by the vehicles of the same group.The vehicle desires each other a secret member key and verifies messages from the vehicles that are moving in the vicinity of at the same RSU. This protocol avoids the overhead of certificate management because protocol assumes that RSU's are densely deployed on the roadside.

Zhang et al [12] introduce an authentication protocol referred as APPA to trust the vehicular communication and privacy of vehicles. This protocol follows identity-based cryptography by involving aggregate signature and one-time signature.If a vehicle retrieves a secret key i.e. associated with the vehicle's id, from a trusted authority it can sign messages. The signature on a message uses the vehicle's identity i.e. one-time pseudonym. Aggregate signature i.e. n signature on n messages by n signers can be verified as if it had been generated by a single signer.

Liqun et al [13] give a solution for reliability, privacy and audibility feature together in Vehicle to Vehicle (V2V) communications.At the time of manufacturing, the vehicle is equipped with a black box that has a public key and able to perform cryptographic operations securely. A k-time anonymous signature scheme can reveal a signer's identity if he signs the same message more than k time. Various protocols are available to sign, verify and check if a message has been signed by a certain number of independent users, show whether two anonymous signatures on the same message are from the same source[14].

So far solutions proposed to ensure privacy, use pseudonyms on Vehicle and CA's are liable for the management of vehicle's certificates generation, distribution, and revocation. Also, many schemes assumed public keys and pseudonyms are preloaded in vehicles which create overhead for practical applications.However privacy has been identified as a serious problem by the Car to Car Communication Consortium[15], the relevant technologies and architectures still are in its infancy stage and need to be developed in order to solve the user's privacy problems.

IV. SYSTEM ARCHITECTURE AND ITS DEMAND FROM DEPLOYER

This section highlights some of the important issues regarding the formation of the logical architecture of the vehicular communication and its interactions with physical resources. Due to dynamic nature of nodes in VANET, we require an interface that can deal with computing, sensing, communicating and organizing structures enable autonomy and authority. The architectural design of VC includes different challenges regarding the formation of the logical structure of the VC and its interaction with physical resources such as roadside units. Hence demands of managing the mobility of the vehicles and diversity should be recognised for the computational purpose, communications and other changes in interest or location, resource failure or denial [16]. While designing the framework we need to follow few aspects:

A. Flexibility:

By the reason of unpredictability of the size of the network(any number of vehicles may present at given time), we need a flexible architecture that is able to fulfillfluctuating application requirements and resource accessibility on the move. The protocol architecture requires for support must be developed.

B. Robust in nature:

The fundamental building blocks and structure that composed privacy should be engineered and designed to face the uninvited stress of the unstable working situations.

C. The capability of extension:

Vehicular communications are still in growing phase and will take some time to settle in the real-time environment. On the other side, mobile technologies that play crucial role in VC are upgrading day by day which highly claims the architecture to add on services in future.

V. CURRENT PRIVACY ISSUES

Generally, privacy is recognized as a merely legal concern and is regulated by laws that will apply in a given country under a given set of conditions. We must know the establishment motives the availability of resource metrics, the rules and regulations of VC to operate unbiased in a decision support system, a central control structure and a body of the management system. Such as Personal Information Protection and Electronic Document Act (PIPEDA) was established in 2000 April in CANADA to protect data privacy, regulates how private sector organizations collect, use and disclose personal information in the course of commercial business. The metrics are required to estimate economic models for realistic pricing and billing of different VC services and features (Toll collection and public parking payment systems). Information privacy laws are present in almost every part of the world and vary from country to country, each have different laws if any breach of privacy occurs, Still, require more expedition in the area of Ad hoc networks perspective. Our motive is to protect user's information

and location privacy, compromising of any of these may lead to unexpected situations. Hence, we should give attention to the following factors:

Guarantee of trust management: In some situations, the VC may demand to have an authority which is capable of making decisions and accordingly takes local actions apart from a central authority. situations are like when the traffic jam occurs, or an ambulance is stuck in the traffic and needs rapid dissipation of congestion. Hence, the existence of trust management in VC can be useful for electronic authentication of actions.

Fundamental functional policies: In LBS, user's query a public server for nearby point of interest like petrol pumps or gas station, hospitals or cafeteria etc, but they may not be interested in revealing their locations to the service provider. Sharing private information unreliable service provider results in the violation of user privacy. To preserve the information of the user's, we need effective operational policies for inter-operations, decision support system, implementing accountability metrics, standardization and regulations.

A. Adaptive Privacy:

In general, privacy is a user-specific concept and a good mechanism should allow a user to select the type of privacy that they wish to have. A higher-level of privacy drives high computational overhead. Some users don't bother to reveal their personal information and doesn't wanted to pay for it. On the other hand, a different category of user's (Government officials/ Celebrities etc) may demand the higher level of privacy and ready to pay for it. we need to design a flexible and user-centric system.

B. Compatibility:

Another important question that must be answered beforehand, is how do we design the protection approaches that can work with existing infrastructure and established services in the industry. The practical implementation of the proposed approaches into the existing LBS approaches should be tested before deployment.

VI. FUTURE RESEARCH CHALLENGES

Understanding the depth of implementing privacy in VANET is one of the greatest challenges till the date. On one side VANET demands complete information of the users such as the identity of the driver, his interests etc. for the communication while on the other hand such information can be misused and become a life-threatening issue if accessible by adversaries. Now the main question arise is" how can we protect user's privacy while fulfilling the basic requirements of the network simultaneously?" The system must ensure anonymity in the communication exchanged while respecting the trusted authorities of VANETs. Another challenge is, this technology can be helpful to the police department in tracking the malicious persons like wanted criminals or terrorists by tracing their electronic license plate identity. Similarly, terrorists may use some advanced technologies to retrieve the information of target driver's vehicle (Minister of a state or VIP) and trace the vehicle to complete their motives. That's why the implementation of VANETs in incomplete stage works as a double edge sword and can create havoc if deployed before designing privacy measures.

VII. CONCLUSION

This paper provides an insight into the requirement to protect the privacy of its users and contribute a fine difference between security and privacy w.r.t. intelligent network systems. The definition of location privacy, certain amendments in existing architecture were suggested and the main challenges may occur at the time of deployment are explained, as well as research techniques proposed till date have been discussed. It is understood that achieving complete privacy is an impossible task but efforts must be made to reach the higher level of privacy protection for location based services.

REFERENCE

[1] N Liu, M. Liu, J. Cao, G. Chen and W. Lou, "When transportation meets communication: V2P over VANETs." IEEE 30th International conference on distributed computing systems, pp. 567-576, 2010 June.
[2] M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Josen, "A privacy threat analysis framework: supporting the election and fulfilment of privacy requirements." Requirement Engineering, Vol.16, Issue 1, pp. 3-32, Springer,2011.
[3] A.K. Tyagi and N. Sreenath,"Future Challenging Issue in Location based Services." International Journal of Computer Applications 114.5, 2015.
[4] T. Annkosa and S. Marsh, "Privacy representation in VANETs." Proceedings of the Third ACM International symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, pp. 39-44, Springer, 2013.
[5] P. Papadimitros, L. Buttyan, J. P. Hubaux, F. Kargl, A.Kung and M.Raya, "Architechture for secure and private vehicular communication." In 7th International conference on ITS Telecommunications, ITST'07, pp. 1-6, IEEE, 2007.
[6] H. T. Cheng, H. Shan and W. Zhuang, "Infotainment and road safety service support in vehicular networking: from a communication perspective." Mechanical System Signal Process, Vol.25, Issue 6, Elsevier, 2010.
[7] M. Raya, P. Papadimitratos and J. P. Hubaux, "Securing vehicular communications.", IEEE Wireless Communication Magazine, Special Issue on Inter-Vehicular-Communication (LCA-ARTICLE-2006-015), pp. 8-15, 2006.
[8] F.Dotzer, "Privacy issues in vehicular ad hoc networks." International Workshop on Privacy Enhancing Technologies, pp. 197-209, Springer, 2006.

[9] R.Lu, X.Lin, H. Zhu, X.Shen and P.H. Ho, "Efficient conditional privacy preservation protocol for secure vehicular communication." In 27th Conference on Computer Communication, INFOCOM, IEEE, 2008.
[10] G. Calandriello, P. Papadimitratos, J. P. Hubaux and A. Lioy, "Efficient and robust pseudonymous authentication in VANET." In Proceedings of the Fourth International Workshop on Vehicular Ad Hoc networks, ACM, 2007.
[11] L. Zhang, Q. Wu, A. Solanas and J. Domingo, "A scalable robust authentication protocol for secure vehicular communications." IEEE Transaction on Vehicular Technology, Vol.54, Issue 4, pp. 1606-1617, 2010.
[12] L. Zhang, Q.Q. Wu, Bo and J.Domingo-Ferrer, "APPA: aggregate privacy-preserving authentication in VANET." International Conference on Information Security, Xi'an, China, 2011.
[13] C. Liqun, N. Siaw-Lynn and W. Guilin,"Threshold anonymous in VANETs." IEEE Journal on selected areas of Communications, Vol.29, Issue 3, pp. 605-613, 2011.
[14] K. Priya and K. Karuppanan, "Secure privacy and distributed group authentication for VANET." International conference on Recent Trends in Information Technology, pp. 301-306, IEEE, 2011.
[15] C2C-CC,Car to Car Communication Consortium, http://www.car-to-car.org.
[16] R.G. Engoulou, M. Bellyache, S. Pierre and A. Quintero, "VANET Security Surveys." Computer Communication, Vol.44, pp. 1-13, Elsevier, 2014.