International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 17 (2018) pp. 12991-12994

An Insight Analysis of Economic and Legal Challenges in VANET

Bhawna Chaudhary[1], Sheetal Singh[2]

School of Computer Systems & Sciences, Jawaharlal Nehru University, Delhi, India.

[2]Ramanujan college, University of Delhi, India.

Abstract

Vehicular networks is an emerging technology which promises to decrease the road traffic and increase road safety and presents captivating applications for the users. This emerging technology is on the verge of being deployed globally. In this paper, we present briefly the requirement, features offered by VANET, and also security issues. Furthermore, we present the importance of market introduction problem and legal aspects which need to be considered before VANET can be introduced into the real world.

Keywords: VANET; Security issues; Economic challenges; Legal implications;

INTRODUCTION

The ever increasing intensity of traffic snarls has become a major concern for every metropolitan city around the globe. This leads to a large section of people ending up wasting two to three hours on an average in commuting in their vehicles. Thus, to make this daily ordeal less harassing and more comfortable, the car manufacturers are providing in-vehicle facilities such as audio/video players, gaming consoles ,radio, Bluetooth connectivity etc.. Apart from these entertaining features, it is important to create a safe and efficient environment for vehicles, which helps in reducing number of road fatalities. To fulfill such requirements vehicular ad hoc network is designed which offers both safety and non-safety applications by communicating in three different architectures. These architectures includes V2V(vehicle to vehicle),V2I(vehicle to infrastructure), and hybrid architecture(includes both V2V and V2I). Lately one more architecture V2P(vehicle to pedestrian) is being discussed which can be considered as fourth possible architecture.[1,13]

V2V communication can be considered as an important component of the ITS, as it enables a vehicle to communicate with other vehicles present in its vicinity, depending upon the protocol which decides how many hops a message can travel. This scenario does not include any other than vehicle. In V2I, communication takes place by exchange of information/data between vehicles and infrastructure placed on the road side known as road communication is deploying minimum number of road side units along with providing the maximum level of safety applications[2]. Hybrid architecture simply integrates the features of the above two discussed V2V and V2I architecture together.

The newly introduced V2P communication permits a direct, instant and flexible communication between moving vehicles and roadside passengers[3].By using their Smartphone's (having wireless capability) passengers can easily join the VANETs in the form of RSU's and may express their willingness to demand travel applications like carpooling or answer the queries of driver. This architecture adds additional challenges to the growing vehicular ad hoc networks.

OVERVIEW OF VANET

A. VANET Characteristics

As we usually call VANET is a subset of MANET but it has its own unique characteristics, including:

(i) *Providing safe driving, increasing passenger comfort and improving traffic efficiency*: VANET provides direct communications among vehicles moving in the same or in opposite direction(if comes under range), thus allowing a set of applications, requires direct communication between nodes to be applied over the network. These applications can help the drivers travelling in the same direction by sending warning messages about accident, or about the need of sudden hard braking, also helps the drivers in decision making by giving them a broad picture of the road conditions ahead. Additionally, different kinds of application could be applied via this type of network in order to increase the passengers comfort level and to improve traffic condition by disseminating information about the weather, traffic flow and point of interest information such as nearest patrol pump/gas station, shopping malls/ chemist and fast food[5].

(ii) *Unlimited power supply*: As we know this is one of the biggest challenge in MANET , on the other hand VANET has capability to provide uninterrupted power to the OBU because space is not an issue in vehicles[6].

(iii) *Greater computational capacity:* In VANET, nodes are vehicles which can be equipped with a adequate number of sensors and computational units; such as processors, sufficient memory storage, advanced antenna technology and GPS localization. The presence of these resources raise the computational capacity of each node which helps in achieving the vision of reliable wireless communication and obtaining correct information regarding its current position, velocity, and direction[8,9].

(iv) *Variable network density*: The network density depends on the number of vehicles present at the same time on the road, which can be very high during peak hours in cities and can be low in highway scenario[7].

(v) *Predictable mobility*: In VANET, nodes move in random manner , because vehicles have to follow road topology, traffic rules regulated by the government and also requirement to obey signals and road signs and to respond to other moving nodes leading to predictability in term of their mobility[4,5].

B. Security Requirements in VANETs

Like other networks VANET security demands authentication, data integrity, and in some special cases confidentiality, protection against unauthorized injection of a message, zero tolerance for message alteration and guarantee of no eavesdropping. To achieve authentication in VANET, digital signature is considered as building block for both types of communication. Whether it is through infrastructure or without infrastructure, message from only genuine senders will be considered. Digital signature can also be used for data integrity. An alternative method on which we can rely is MAC(message authentication code), where a secret key is required to be shared by both communicating entities. For message confidentiality, we can send safety/warning messages without encryption as they do not carry any sensitive information (contains information for public interest). Therefore, the exchange of safety messages requires authentication but not encryption[9]. But non-safety or often called infotainment messages which set up connection with road side units to take benefit of internet services may require some encryption mechanisms. In addition to the basic security requirements, we need to pay serious attention for some other aspects, such as:

- Identity theft, unique identity is required.
- Location privacy preserving schemes against unlawful tracing.
- Traceability by trusted authorities if any misbehavior is noticed by higher authorities.
- Suitable routing protocols that can work in real time environment and incorporates with the dynamic nature of the network.
- Non-repudiation, if any accident or crime happens and law enforcing authorities need to identify information for investigation.
- Efficiency and scalability of the security system.
- Signal fading, especially in urban areas where buildings are too tall and other vehicles act as obstacles in between two communicating vehicles.
- Introduction of new laws(country specific) that can deal with, if any, misbehavior is noticed by monitoring authorities.

Many schemes are present for the above mentioned requirements. But our very concern is to light the economic and privacy(legal) aspects of the VANET.

ECONOMIC CHALLENGES

In the imminent future, we can expect the vehicles to be equipped with ,and using beneficially, VANET technologies consisting of all the features that we have discussed albeit the large scale modification of the vehicles required by this technology. To implement this with efficacy, we need to embed all the software and hardware systems in our vehicles which directly results in at least 50% increment in the actual cost of the vehicles[10]. This increment may affect the purchasing capacity and hence the attractiveness of such vehicles to the end-user. Also, persuading end-user to buy such an expensive product, and that too, which reveals consumer identity (if required) is an issue. Apart from all the technical challenges in implementation, these issues have their own significance. So before implementing such a challenging ,and expensive technology in a big bang manner, the solution of its market introduction problem should be available beforehand. The solutions suggested so far are:

- To start with, introducing it on a pilot basis in few selected countries (which have higher degree of acceptance of new ideas and innovations among citizens) in specific cities. Once the technology is successfully implemented in these cities and thus gains popularity and acceptance among citizens, it can be scaled-up to be implemented in other cities and countries. It will also give leeway to car manufacturers and policy implementers to improvise the technology to suit other cities and also incorporate the lessons learnt during first phase.
- Making it compulsory for every citizen by introducing new regulative in legislations of those countries which are ready to accept these changes. These regulations will force the customer to buy such vehicles.

This idea of introduction of the new regulations is not possible till the data on the effectiveness of the VANET is not proven. This is so because we cannot make changes to the existing system only the basis of promised safety and traffic-condition improvements. Hence , the only solution left is to introduce the product in the target market(after surveying) first and then observe the results, and if the review proves that new technology is able to fulfill its promised features and helps in improving road safety ,then only we can consider bigger level changes in our existing system. Even for this option , an initial challenge will be to convince the customers in these few selected cities. For this reason, it is better to introduce V2 R architecture first as ,generally, people will trust infrastructural network easily rather than direct communication among vehicles. A well known example is- people do connect to the network (Wi-Fi and hotspot) available in their range but they do not connect immediately with unknown mobile users. Additionally , the cost of vehicles with this technology installed can be kept at attractive prices. This can be achieved by government subsidies or by appealing to international institutions working to make the road travel safer for people.

Although so many problems exist, there is a potential requirement of the successful introduction of VANET in the market. It needs that all interested peers coordinate with each

other so that they can set up their concept on the VANET platform and also participate in market redemption. This strategy should be applicable as soon as possible.

PRIVACY IMPLICATIONS

As we know, VANET and its applications are on the edge of being deployed worldwide, the pressure of designing a suitable and comprehensive protection framework for the data generated and stored by the system is increasing. Most of the research work done concerns solving security issues in VANET [9,11] but the preservation of privacy still has some unfolded issues that need to be solved. But before explaining further, first we need to understand the concept of privacy. Privacy has different meanings in different areas. We can categorize privacy in three forms[12]:

- ➢ Physical
- ➢ Informational
- ➢ Territorial

Physical privacy covers the notions of personal spaces and sexual encounters. For the protection of such privacy ,we need to include physical boundaries like walls, doors or clothing(physical things).Informational privacy concerns with the privacy of data about people. Protection of informational privacy is present in many forms like laws, passwords or locks. whereas territorial privacy covers how privacy can be achieved for personal belongings like lands or vehicles. Protection includes limits on defined spaces, registered papers by some governing authority. These categories overlap each other in some or the other way, so we need laws and authorities that can handle them altogether. For preserving physical privacy we have established privacy programs that include, an identified responsible person; budget; training and communication equipments; policies and procedures; standards; and incident management techniques.[9,12].

Most of the people consider that privacy is a part of security and if security is achieved ,then we do not need to worry about privacy. But there is a very fine distinction between security and privacy. Security means achieving the "confidentiality, integrity and availability", often known as CIA triangle. Data security refers to the data being stored safe from unauthorised access, ensuring that data is authentic and is always available when needed. But on the other hand, privacy refers to the use of information, it is the basic human right, or it can be expressed as informational self-determination ;the ability to decide what information about an individual can be accessed and by whom . In terms of their relationship with one another ,security measures are made to protect the individual privacy. Security is the ends to a means-privacy.

In VANET , balancing privacy concerns with the existing security needs will demand significant societal and practical attention. Most of the countries including INDIA have widely conflicting laws concerning their citizens right to privacy. In India, Right to privacy is defined in Article 21 in which term privacy means that "right to be let alone", "the right of a person to be free from unwanted publicity" ; or in other words right to live without any unwanted interference by public in matters with which the public is not concerned. Similarly UK legislation has Article 8(1), which deals with an individual's legal right to informational privacy and says that" everyone has the right for his private and family life, his home and his correspondence". The legal aspects of VANETs are related to the over-lapping areas of existing law and intelligent transportation system(ITS).We need to modify the current transportation laws or redesign them to enhance the development in transportation industry by interlinking with other fields like academics and professionals. Traffic law system is considered as a important part of the intelligent transport system's body. Legislative requirements might force VANET to provide effective security and privacy solutions. We need to develop a system which will be able to handle the fundamental right to privacy of a citizen and also ,at the same time ,can deal with privacy requirement in VANET without violating the human rights.

As VANET develops, many new legal policy issues will emerge for which we need an authority which can act as dispute revolution mechanism on these cases. An official surveillance for those accused who do not obey laws, an imposition of legal sanctions against those found guilty in any misconduct is required. Deployment of VANET will raise many peculiar and challenging issues for the transportation lawyers. It will require the development of new strategies and new approaches to achieve the goals of our transportation system.

CONCLUSION

While there is significant amount of work which has been done to secure the VANET, the field of privacy preservation, legal aspects to be considered is still at its nascent stage. In this paper, we have discussed the ideas as to how can we introduce this technology effectively and legal sanctions can also be applied. This technology cannot become successful until we don't have the solutions of these issues beforehand, though it is a challenging task, required modification can be done after deployment.

REFERENCES

[1] M.S. Kakkasageri and S.S. Manvi,"Information management in vehicular ad hoc networks: A review, "*Journal of Network and Computer Applications*, Volume no.39, June,2013, pp. 334-350.

[2] V. Kone et al.,"On Infostation Density of Vehicular Network," *In Wireless Internet Conference (WICON)*, March 2010, pp.1-9.

[3] N.Liu et al.,"When Transportation Meets Communication V2P over VANETs,"*Proc. 30th Int'l Conf. of Distributed Computing, IEEE, Italy, June 2010*, pp. 567-576.

[4] F.Li, Y.Wang,"Routing in Vehicular Ad-Hoc Networks: A Survey,"*Vehicular Technology Magazine*, IEEE, Volume no.2, June 2007, pp.12-22.

[5] J.Jakubiak and Y. Koucheryavy,"State of the Art and Research Challenges for VANET,"*5th IEEE Consumer Communications and Networking Conference*, CNCC 2008, pp.912-916.

[6] S.Yousefi, MS Mousavi, M.Falhy,"Vehicular Ad-Hoc Networks (VANETs): Challenges and Perspectives, "*Proc.Int'l Conf. on ITS Telecommunications*, 2006, pp. 761-766.

[7] M.Nekovee,"Sensor Networks on the Road: The Promises and Challenges of Vehicular Ad-Hoc Networks and Grids,"*Proc.Int'l Wksp. on Ubiquitous Computing and E-Research*,Edinburgh,UK, May 2005,pp.30-39.

[8] K.Ibrahim and MC.Weigle,"Optimizing CASCADE Data Aggreation for VANETs,"*Proc. 5th IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Systems*, 2008,pp.724-729.

[9] M.Raya and J.P.Hubaux," Securing Vehicular Ad-Hoc Networks*," Journal of Computer Security*, No-15,2007,pp.39-68.

[10] Weiberserch

[11] Y.Liu,J.Bi and J.Yang," Research on Vehicular Ad-Hoc Networks,"*In Control and Decision Conf.*,IEEE, 2009,pp.4430-4435.

[12] T.Kosa,S.Marsh and K. el-khatib," Privacy Representation in VANETs",*Proc. 3th Int'l Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*,ACM,Newyork,NY,USA,2013,pp.39-44.

[13] G.Karagiannis et al.," Vehicular Networking: A Survey and Tutorial on Requirements,Architecture, Challenges, Standards and Solutions,"*Communications Surveys and Tutorials*, IEEE 13,no.4,2011,pp.584-616.