International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31107-31113

http://www.ripublication.com

A Review on Vehicular Networks (VANETS) and Security Related Issues

[1]M.Thanjaivadivel

Asst. Professor Dept. of CSE Vel Tech University
thanjaivadivel@gmail.com

[2]M.Viswanathan

Asst. Professor Dept. of CSE Vel Tech University
viswamtech19@gmail.com

[2]G.S.Raj

Asst. Professor Dept. of CSE Vel Tech University
gsraj1982@gmail.com

[2]N.Bindhu

Asst. Professor Dept. of CSE Vel Tech University
bindhu2424@gmail.com

ABSTRACT

VANET (Vehicular Ad-Hoc Networks) plays a vital role between Ad-Hoc and vehicles. The main characteristic of VANETs is to increase traffic safety, efficiency and also increase the environmental friendliness, high mobility, rapidly changing network topology, unbounded network size, frequent exchange of information, time critical, better physical protection. It is a subtype of the MANET. It's also provide a variety of services like passenger safety, avoiding traffic congestion by mounting the environmental information and communication technologies. The VANET can send the information between the vehicles using simplex mode is known as "One Hop Communication". In other way, the vehicles shares and retransmit the information using full duplex mode is known as "Multi Hop communication" with the help of vehicles and road side unit.

The Road side units also act as gateway and, thus, collect the stored information and processed in cloud environment. In this paper we survey

some of the application for vehicle safety communication and security challenges.

Keywords— VANET; Safety Applications; Road side Unit, EEBC, FCW, BSW, LCW, DWPW, IMA and CLM.

I. INTRODUCTION

In recent years, the number of vehicles usage rate has been increasing day by day, when compare to previous decade with the effect of these critical traffic problems like accident, traffic congestions are occurred. In order to avoid this critical problem the Intelligent Transportation System (ITS) has been introduced to improve the coverage and robustness of communication. The main features of ITS is road safety and traveler safety application. It gives alert message for types of communication 'One Hop (V2V)' and 'Multi Hop (I2V)' communication. There several applications are encountered to address the crash scenarios [3]. Those applications are EEBC, FCW, BSW, LCW, DWPW, IMA and CLM.

The way of communication and information sharing used here is Vehicle to Infrastructure (V2I) in which peer mode through ADHOC communication. In other hand vehicle to vehicle (V2V) and vehicle to Roadside unit (V2R) provides flexible communication and content sharing.

According to the National Crime Records Bureau (NCRB) report every year, more than 135,000 occurs due to traffic collision-related deaths in India in 2010. In UN declared 2011-2020 as `Decade of Action for Road Safety`. But in India not even a single steps have been initiated regarding road safety. This shows our seriousness about the issue,"

Vehicular network is a kind of wireless Ad Hoc Network. These networks have maximum similarity for mobility or movement and self organizing of nodes and also they have some different. VANET have high mobility and unreliable channel condition. VANET have many challenging research issues such as data dissemination, beaconing, security issue etc., In addition to energy consumption more compare to MANET and also no battery constrains for VANET is suitable for long communication through vehicle [1].

The security challenges in VANET are Denial of Service (DoS), Message Suppressions attack, timing attack, Sybil Attack, ID Disclosure, Sending false information etc., the necessary Safety application must be protected from intruder. Compromising safety application is lead to loss human life [6].

2. VANET SAFETY RELATED APPLICATIONS

Nowadays VANET has gained lot of popularity among research and industry for improving the efficiency and safety for future transportations. The Generation of mobile communication has been emerged from first generation to third, fourth and fifth generation (5G) [12]. Here we have classified VANET applications three broad categories. They are safety related, Internet connectivity related and user based.

- **Safety Related:** These application are used improve the road safety on the roads. These applications taken care of collision avoidance. According to National Crime Records Bureau (NCRB) 70% of accidents can be avoided driver. If a driver receive warning message prior to the collisions [12]. Then cooperative driving in these driver receive signals related to road conditions warning like curve speed warning,lane change warning, forward collision warning etc., and also optimize the traffic by the use of sending signals like jams, accident, snow fall in road etc.,
- **Internet Connectivity Related**: The way of communication and information sharing used here is Vehicle to Infrastructure (V2I) in which peer mode through ADHOC communication. In other hand vehicle to vehicle (V2V) and vehicle to Roadside unit (V2R) provides flexible communication and content sharing.

There several applications are encountered to address the crash scenarios in V2V safety application. Some of these applications are :

- ❖ Lane Change Warning (LCW),
- ❖ Do Not Pass Warning (DNPW),
- ❖ Forward collision warning (FCW),
- ❖ Interaction Movement Assist (IMA),
- ❖ Blind Spot Warning (BSW)
- ❖ Control Loss Warning (CLW) and
- ❖ Emergency Electronic Brake Lights (EEBC).

Table 2.1. Mapping of V2V Safety Application

Crash Scenario	V2V Safety Application						
	EEBL	FCW	BSW	LCW	DNPW	IMA	CLW
Lead vehicle stopped		x					
Control loss without prior vehicle action							x
Vehicle turning at blind spot(curve)						x	
Unexpected deceleration of your Vehicle(Eg., Run out of gas, Over Heating etc.,)	x	x				x	
No Entry for vehicle(s)					x		
Changing lanes – same direction			x	x			
Non signalized junctions						x	

In Infrastructure to Vehicle application gives a solution distanced vehicular networks and also it make use of already available network infrastructure E.g., Road side Units (RSUs). This application warns the driver, when the driver violates the rule.

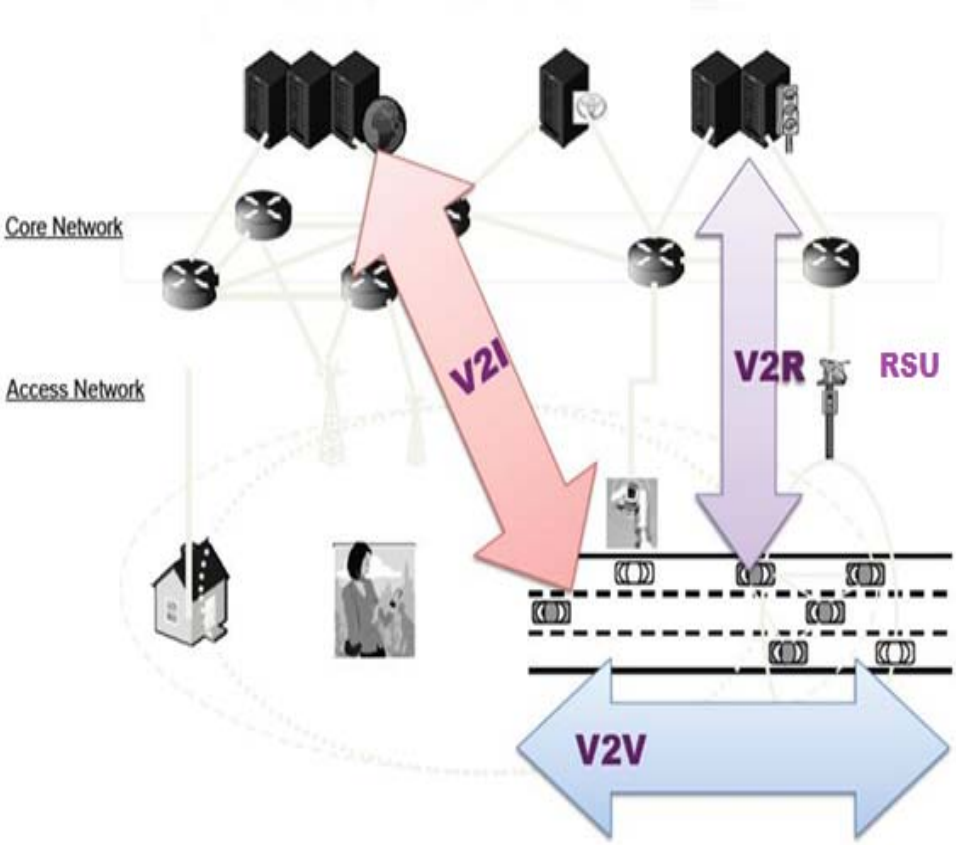

Fig 2.1 VANET ARCHITECTURE

- User Based Application: This application provides the user based information. It shares information among vehicles. It also collect and locate information related toll taxes, restaurant, nearest fuel station etc.,

3. SECURITY REQUIREMENTS IN VANET

The security challenges in VANET are high mobility, frequent disconnection, anonymity of support, Limited bandwidth, Limited transmission power, Energy storage and computing etc., The security system in VANET should satisfy following requirements[4], [5].

- **Authentication**: It ensures that the information has been received or sent by authorized user or not. In VANET, the vehicle or RU reacts upon the information came from the other vehicle or RUs, it acts accordingly.
- **Availability**: the context information must be available to all the authorized users. The network must aware attacks else it will make network down and information can't be shared. When attacker causes network availability. It can be protected by interconnection of public and private keys between RSUs and vehicles.
- **Confidentiality**: To avert the information from the unauthorized users and disclosure the information to the legitimate users. It's also broad concept of data privacy, so that it limits the individual personal information. It requires message delay attacks.
- **Integrity**: The legitimate user must ensure that that data has not been altered wrongly, whether by accident or deliberately slander activity. It also ensures the message actually came from the intended user.
- **Non Reputation:** The sender and receiver parties cannot deny that the sending and received message as accident or unauthorized ones.

4. ATTACKS ON VANET

The attacks on VANET are classified in three broad categories. They are threat to availability, threat to authenticity and threat to confidentiality.

4.1. CLASSIFICATION OF ATTACKERS

The attackers are classified according to their behavior of attack. Some of them are discussed below:

1. If the attacker is a member of node and he communicates the other node of same network, called as insider attack. Otherwise the attacker who is not authenticated to communicate directly the node of a other network, called as outsider attack.
2. An attacker directly damages a network or message is considered as active attack and generates a new packet. If the message is eavesdrop the channel, but it cannot generate new packet is considered as passive attack.
3. If the attacker affect or disrupts the network without any personal intention. These attacks called as Malicious. On other way, if he/she tries to find any benefit and intentionally attack the network. These attacks are known as rational.
4. If an attacker launches an attack with a limited scope and the attack is restricted to a particular area, it's known as local attack. If an area of attack is extended with several entities and distributed across the network is known as extended attack.

4.2. TYPES OF ATTACKS

There are several types of Attacks are available and identified on the basis of layers [8], [9].

Denial of Service (DOS): The main objective of DOS is to attack the communication medium. It causes the channel jam or to create problem to access network. The On board Unit (OBU) and RSU is unable to access the network or channel with the effect of this deviation, eaves dropping and overtiredness of network or nodes.
DDOS: It is more harmful than DOS attack. The attackers use different location to inject the false information. The main objective of DDOS is to down the network or make the network unavailable to vehicular network.
BOGUS INFORMATION: The bogus information may insider or outsider. The attacker broadcast false information in OBUs and RSUs to deviate the vehicular network. E.g., a vehicle may intimate traffic jam or an accident in the road to preventing the other vehicles choose the alternate route.
SPAMMING: It consumes bandwidth and increase the transmission latency and also attacker sends spam message. It also disseminates spam message to group of user.
BLACK HOLE: In this problem when a node refuses to participate in network or at a group of users it continuously drops the node and also the traffic has been redirected to particular network or node.
MALWARE: In this problem a node or a network has been injected with virus. It has been infected by software. Mostly this attack will occur at malicious (insider) rather than outsider.
SYBII ATTACK: It forges identities of vehicles with effect of this it create illusion to the vehicle on the road [10].
MESSAGE SUPPRESION: It is similar to black hole attack in addition to that it holds the critical information of the receiver. For example particular network or node as congestion alerts it refuses to remove this alert even after the congestion has been removed [10]. It may leads to unnecessary traffic jam or network has been over loader. So the node has been forced to choose the alternate path.
SOCIAL ATTACK: Basic idea of this attack is to disturb the network or legitimate user with an unethical and unmoral message. The Legitimate user reacts to it. It leads to create unnecessary network traffic.
ID DISCLOSURE: It is kind of passive attack. In this attack, the attackers send malicious code to the network and get the useful information. It gets information about targetID and its location.

CONCLUSION

In this paper we have analyzed about safety related application and various attacks in VANET. The table provides the mapping information of vehicle to vehicle (V2V) along with few crash scenarios. This safety related application used to improve the safety of vehicles and users. Then we have discussed about security requirements in VANETs and attacks on VANET. We expect that the above attacks may helpful to identify various attacks and attackers.

REFERENCES

[1]. Durech, J. ; Hrubos, M. ; Franekova, M. ; Janota, A. "Implementation of data from the mobile measurement platform to VANET application" in ELEKTRO, Page(s): 430 - 434, 2014.

[2]. Rajesh, K., Karthick, R.V., Raj, G.S." A new scalable reactive location based ad hoc routing protocol for VANETs" in 2014 International Conf. on Information Comm. and Embedded Systems, ICICES 2014.

[3]. Dobre, C. ; Fratila, C. ; Iftode, L. "An approach to evaluating usability of VANET applications" in Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, Page(s): 801- 807, 2011.

[4]. Mohammadi, A.A., Raj, G.S., Vimal Karthick, R. "GCTAR: A stout approach for increasing efficiency and fairness for city environment in VANET" in 2013 Source of the Document Proceedings of the 2013 International Conference on Green Computing, Communication and Conservation of Energy, ICGCE 2013, pp. 816-821, 2013.

[5]. Vinh Hoa LA, Ana Cavalli "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY", International Journal on AdHoc Networking Systems Vol. 4, No. 2, April 2014

[6]. Xiaodong Lin ; Rongxing Lu ; Chenxi Zhang ; Haojin Zhu ; Pin-Han Ho ; Xuemin Shen, "Security in vehicular ad hoc networks", IEEE Vol. 46, Issue: 4, Page(s): 88- 95, 2008.

[7]. Jie Luo et.al "MI-VANET: A New Mobile Infrastructure Based VANET Architecture for Urban Environment" in Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd page(s) 1-5, 2010.

[8]. Mohammadi, A.A., Raj, G.S., Vimal Karthick, R. "ABSTAR: Improves Qos for city environment in VANET "2013 5th International Conference on Advanced Computing, ICoAC 2013, pp. 458-462

[9]. Shuhaimi, N.I. ; Juhana, T., "Identity-based security systems for vehicular ad-hoc networks", in Telecommunication Systems, Services, and Applications (TSSA), 2012.

[10]. Alshaer, H, "Securing vehicular ad-hoc networks connectivity with roadside units support", in GCC Conference and Exhibition (GCCCE) pp 1 - 6, 2015.

[11]. Rakhshan, A. ; Pishro-nik, H. ; Nekoui, M. "Driver-based adaptation of Vehicular Ad Hoc Networks for design of active safety systems", Information Sciences and Systems (CISS), 2015.

[12]. http://ncrb.gov.in/.