Security Challenges and Issues in Vehicular Ad-Hoc Network (VANET): A Review

Chirag Saxena1, Danish Ather2

1Student, Teerthanker Mahaveer University, Moradabad U.P.

2Associate Professor, Teerthanker Mahaveer University, Moradabad U.P.

1saxenaji.chirag@gmail.com

2danishather@gmail.com

Abstract—**there is a rapid increase in road accident. New technology VANET has been introduced which is now become an emerging technology which provide security and safety to passengers as well as drivers in this paper , we review the concept of VANET along with its applications and characteristics. We have also discussed various threats and security challenges and issue related to Vehicular Ad-hoc Network(VANET). It also gives a review about how the vehicles communicate in a VANET.**

Keywords— Vehicular Ad-hoc Network (VANET), Mobile Ad-hoc Network (MANET), Road Side Unit (RSU), Vehicle -to-Vehicle (V2V), Vehicle to infrastructure (V2I).

I. INTRODUCTION

In the present scenario, the rapid increase in road traffic is affecting efficiency and safety of the environment .According to a survey around 1.2 million people are killed each year in a road accident that is why road safety is becoming an important issue of traffic management now a days. One of the most incident factor of traffic safety is driving. There is need to make it safer to do this we have to give warning of upcoming dangers for this a different type of technology called as VANET (vehicular ad-hoc network) is introduced.

VANET is said to be a type of MANET in which moving automobiles form the node of network. VANET are usually introduced for fire brigades, ambulance and police vehicle that are within a range of 150 to 300 metres in the network. VANET do not have infrastructure.

VANET can be considered as a subset of MANET with some differences. Different application of VANET can be applied peer-to-peer communication or via multi hop communication. VANET is also known as IVC Inter vehicle communication or V2V vehicle to vehicle communication. As per the configuration network VANET can be subdivided into 3 categories namely wireless wide area network, Hybrid wireless architecture, Ad hoc V2V communication.

Through VANET we can manage road safety because with the help of VANET we are able to communicate with the other moving vehicles. By communicating with different vehicles we can easily came to know that we are how far away from a collision. So, after knowing the exact distance one can put on break to avoid collision thus reducing the chances of road accidents.

VANET use car as a node to develop a mobile network. The main motive of VANET is to increase and provide safety to our road users. It also provide communication between vehicles.

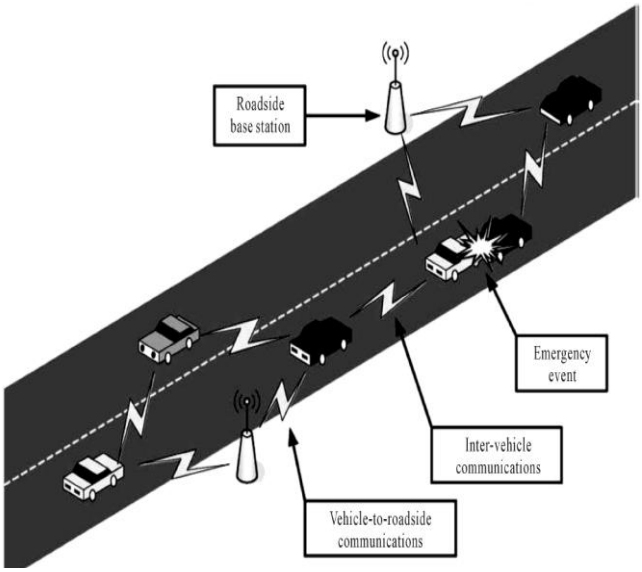

Fig 1.VANET consists of vehicle, roadside stations that exchange messages to help drivers.

II. CHARACTERISTIC OF VANET

- *Rapid changing network topology:* The speeds of moving vehicles (nodes) vary and position of node change rapidly causing the network topology to change frequently in VANET.
- *Unbound network size:* Network size of VANET does not relate to a particular city so VANET is said to be geographically limitless.
- *High mobility*: vehicles moves at very high speed that makes it difficult to determine a node position
- *Frequent exchange of information:* Information is being exchanged between vehicles and roadside unit RSU making the information exchange more Frequent and updated.
- *Time critical:* Every information packet which is sent or received has a time limit. This provides delivering the information at correct time without any unwanted delay.
- *Sufficient energy:* vehicles have their own batteries so there is sufficient power supply for component to function properly.

III. SECURITY THREATS IN VANET

There are number of security threats and attacks for VANET due to its wireless nature. In VANET human lives are involved so safety becomes our first priority. These problems are not easy to solve due to the network size, geographic positions and variations in speed of vehicles

Security issues, threats are subdivided into 3 group namely authencity, availability, confidentiality.

3.1 THREATS TO AVAILABILITY

- *Denial of Service*:
  Such kind of attacks is carried out by an insider or outsider in the connected network. This causes that the network will be unavailable to the authentic user.
- *Broadcasting Tampering*:this type of attack to the security is carried out by an insider. Input of wrong safety messages into the VANET. To did harm to read users when anyone manipulate traffic over a specific route then there are chances of accident arise.
- *Spamming:*Spamming of messages over VANET lead to rapid increase in transmission inactivity. it is difficult to control because there is no centralized administration.
- *Black hole attack:* this is caused by nodes refused to participate in the network. When this happens all the communication and link to it has been broken.

3.2 THREATS TO AUTHENTICITY

We have to protect the node from attackers "insider" or "outsiders" who infiltrating the network with fake identity these threats are:

- *Global Positioning System Spoofing:* GPS has a location table (geographical)of all vehicles and their identity. A attack can be carried out by GPS Spoofing by creating a false location on GPS system in the network.
- *Position Faking:* In VANET, this is the responsibility of the vehicles for their own positions. unsecured communication link creates a blind spot where the attackers easily modify their positions or of the other vehicles.
- *Message Tampering:* In the message tampering, the attacker alter or modifies the message that has been sent from the sender to receiver and vice-versa.
- *Tunnelling*: an attacker utilizes the loss positioning system when it goes through a tunnel. Before resurfacing on the other side to receive its positioning information. the attacker quickly inject false positioning information or data into the node.

3.3 THREATS TO CONFIDENTIALLY

Messages exchanges between nodes are open in VANET to confidentiality or attack with

illegitimate collection of message through passive attacks

IV. APPLICATION OF VANET

Application of VANET are classified into 2 categories i.e. safety and user based application.

A. *USER BASED APPLICATION:*

- *Peer to peer*: these applications provide music, video sharing among the vehicles.
- *Internet Connectivity:* People want to connect to the Internet .VANET provides the connectivity of user with internet.
- *Other services:* VANET can be used in other user based applications like payment service .

B. *SAFETY RELATED APPLICATIONS*

These applications are being using to increase safety on the road. So it contains collision avoidance, cooperative driving and traffic optimization.

- *Collision avoidance:* In this a signal is generated so that warning is given to the other node to avoid collision.
- *Cooperative driving:* Safe journey can be achieved by following traffic related warning like lane changing, speed limit. Many accidents take place because driver didn't cooperate with each other.
- *Traffic optimization:* In VANET, vehicles are data collectors. So a signal like jam, accident should receive signal regarding that jams, accidents so that the user can take alternative path for it.

V. COMMUNICATION PATTERN IN VANET

1) *V2V warning propagation:* Some situations are there when it become necessary to send message to other vehicle. For example, when a road accident occurs, a warning should given to the upcoming vehicle to provide traffic safety.

2) *V2V group communication:* In this pattern, vehicles with some features can communicate. Features may be Static or dynamic.

3) *V2V beaconing:* Messages are sent on a regular intervals which contain heading, breaking and current speed. Such messages are useful to raise neighbour awareness.

4) *I2V/V2I warning:* In message sent by vehicle or infrastructure when there is a danger. Suppose when a vehicle is nearby any intersection then a warning message should be sent to all vehicles which are nearby the intersection.

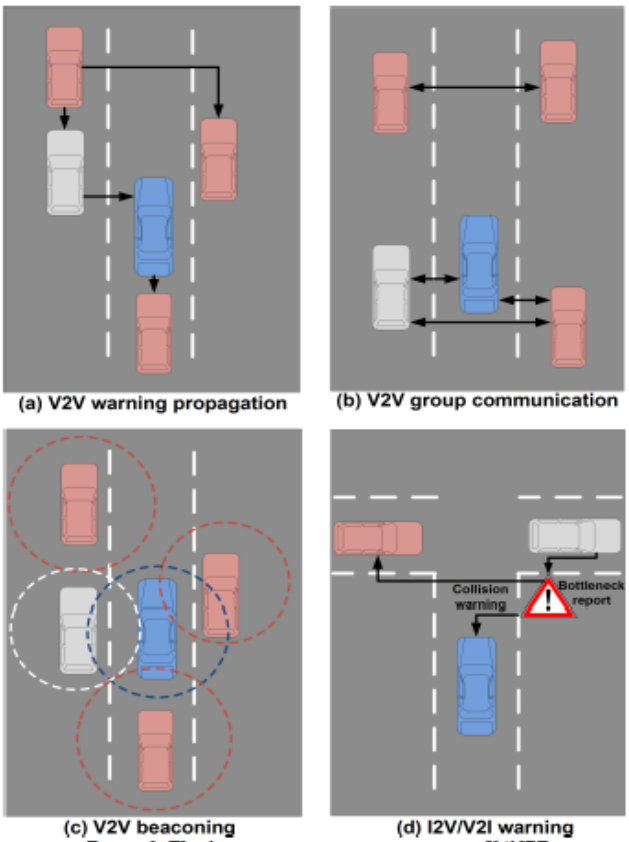

Figure 2. Wireless communication patterns in a VANET

VI. CONCLUSIONS

VANET is a new emerging technology which is developing rapidly. Several vehicles are enabled with this technology, which help in road safety but as we know each and every technology has pros and cons. There is lot of work done over this technology

but there is lot more to be done for security aspects. Above we have reviewed various security challenges and issue. Security in VANET is to be improved on various parameters. If security in VANET is improved then it should be very useful and prevent damage to the vehicles and rate of road accidents will decrease.

REFERENCES

[1] *Kadum, A. (2013) A Survey on Vehicular Ad Hoc and Sensor Networks (VASNET).*
[2] *Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security*
[3] *Mechanism. International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 3, 79-94.*
[4] *http://dx.doi.org/10.5121/ijasuc.2012.3306*
[5] *Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. International Journal of*
[20]
[21] *Sivasakthi, M. and Suresh, S. (2013) Research on Vehicular Ad Hoc Networks (VANETs): An Overview. Journal of*
[22] *Applied Sciences and Engineering Research, 2, 23-27.*
[23] *Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation*
[24] *for Network Layer Attacks. Transactions on Networks & Communications, Society for Science and Education,*
[25] *United Kingdom, 2, 1-6.*
[26] *(2011) Vehicular Ad Hoc and Sensor Networks—Principles and Challenges. International Journal of Ad Hoc, Sensor*
[27] *& Ubiquitous Computing (IJASUC), 2.*
[28] *Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. IEEE Vehicular Technology Magazine,*
[29] *Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad*
[30] *Hoc Networks. International Journal of Science and Advanced Technology, 2, 188-191.*
[31] *Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. IEEE of Vehicular Technology Magazine,*
[32] *2, 12-22. http://dx.doi.org/10.1109/MVT.2007.912927*
[33] *[10] Saha, A.K. and Johnson, D.B. (2004) Modelling Mobility for Vehicular Ad Hoc Networks. ACM International Workshop*
[34] *on Vehicular Ad Hoc Networks, Philedelphia, 91-92.*
[35] *Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. International*
[36] *Journal of Communications, Network, and System Sciences, 7, 365-372.*
[37] *http://dx.doi.org/10.4236/ijcns.2014.79038*
[38] *Manvi, S.S., Kakkasageri, M.S. and Mahapurush, C.V. (2009) Performance Analysis of AODV, DSR, and Swarm Intelligence*
[39]
[6] *Communications, Network and System Sciences, 8, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003*
[7] *Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 5th International*
[8] *Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), Madrid, 5-7 June 2013,*
[9] *334-337. http://dx.doi.org/10.1109/cicsyn.2013.79*
[10] *Bernsen, J. and Manivannan, D. (2008) Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of*
[11] *Service. The 4th International Conference on Wireless and Mobile Communications, Athens, 27 July-1 August 2008,*
[12] *1-6. http://dx.doi.org/10.1109/icwmc.2008.15*
[13] *Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N. and Nemoto, Y. (2007) A Stable Routing Protocol to*
[14] *Support ITS Services in VANET Networks. IEEE Transactions on Vehicular Technology, 56, 3337-3347.*
[15] *http://dx.doi.org/10.1109/TVT.2007.906873*
[16] *Sari, A. (2014) Economic Impact of Higher Education Institutions in a Small Island: A Case of TRNC. Global Journal*
[17] *of Sociology, 4, 41-45.*
[18] *Hartenstein, H. and Laberteaux, K.P. (2008) A Tutorial Survey on Vehicular Ad Hoc Networks. IEEE Communication*
[19] *Magazine, 46, 164-171.*