# Vehicular Ad-hoc Network, A Review

[1]Ms. Iqbaldeep Kaur, [1]Ms.Nafiza Mann, [1]Ms. Tanisha, [1]Ms.Gurmeen, [2]Ms.Deepi
*Associate Professor, Assistant Professor, Assistant Professor, Assistant Professor, Assistant Professor*
*[1]Department of computer Science and Engineering, [2]Department of Electronics and Communication and Engineering Chandigarh Engineering College, Landran, Punjab, India*

***Abstract*--**This paper includes VANETs that is vehicular Ad-hoc network. It is a sub class of mobile ad hoc network (MANET). It is self-configuring network which do not have any fixed infrastructure. In this the vehicles are act as nodes to create mobile network. It is also called as intelligent transportation system. There are various attacks in VANET's like DOS attack, prankster attack, fabrication attack, alteration attack, sybil Attack. In our research we are describing prankster attack in case of selfish driver.

***Keywords*** **–** VANETs, MANETs, vehicle-to-vehicle communication, vehicle-to-roadside communication, ITS, DOS.

## I. INTRODUCTION

During the past decades researches on ad hoc networks has focused on a large and different variety of applications, most of them working for MANET's i.e. mobile ad-hoc networks and other one is VANET's i.e. vehicular ad-hoc network. It is also called as "Network On Wheels". (VANET) is sub class of mobile ad-hoc network (MANET). MANETS are type of ad-hoc networks that can change position and configure itself. As the MANETS are mobile that is changing their location so they use wireless connection to connect to the network like Wi-Fi connection, satellite or cellular transmission[4]. A VANET is type of MANET that allows vehicles to communicate with roadside equipment. The vehicles may not have a direct Internet connection; the wireless roadside equipment may be connected to the Internet that allowing data from the vehicles to be sent over the Internet. Because of the dynamic nature of MANETs, they are not very secure, so it is important to be take care what data is sent over a MANET.

The key advantages are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. Researchers in communications engineering and traffic management systems are engaged for more than a decade to develop suitable Vehicular Ad hoc Networks (VANET) for traffic safety systems[3]. VANET is self- configuring like MANET. It is infrastructure less network of mobile devices connected by wireless. Each device is free to move in a VANET in any direction but within its link. A vehicular ad hoc network (VANET) uses moving cars as nodes in a network to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing to connect with each other with a range between 100 to 300 meters. As vehicles goes out of the signal range and drop out of the network, other vehicles can join in, vehicles are connecting to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purpose.

## II. LITERATURE REVIEW

Ghaleb F**.** et.al. proposed " Security And Privacy Enhancement In VANETs Using Mobility Pattern"(2013). This paper is presenting a mobility pattern based misbehavior detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehavior), such as modify, fabricate, drop the messages in addition to, impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse ordenial of the communications among VANET's nodes. Misbehavior in VANETs can be viewed two perspectives:(i) physical movement and (ii) information security perspectives. Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network which relies on the location information and corresponding time. This paper includes algorithms by which the misbehavior can be detected.

Sharma G. et.al proposed "Security Analysis Of Vehicular Ad Hoc Network(VANET)"(2010) . In this paper various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU(On Board Unit).this unit connects vehicles with RSU via DSRC. and another device is TPD(Tamper Proof Device),this device hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc. Various attacks discussed are DOS, Fabrication Attack, Alteration Attack, Replay Attack and various attackers are Selfish Driver, Malicious Attackers, Pranksters. According to this paper Various vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability,

Network Scalability and various security requirements are Authentication, Availability, Non repudiation, Privacy, Integrity , privacy, Confidentiality.

Seuwou P. et.al. proposed " Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".He stated vanet as technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst themselves (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. He discussed various attacks in vanet , according to him the attacks are classified into two broad categories first one is physical attack and other is logical attack[1].

Sumra A.I. et.al.proposed "Trust Levels in Peer-to-Peer (P2P) Vehicular Network"(2011). According to this paper trust is key component of security in vehicular application if any component behave unexpectedly then it would be harmful for other users of the network. In this paper, they are proposed three different trust levels in peer to peer vehicular network .According to this paper trust is combination of expectancy, belief in expectancy and willingness to be vulnerable for that belief. This paper divide trust in three levels which are: zero trust level, weak trust level, strong trust level and also the attacker's behavior is of two type a. Positive Behavior b. Negative Behavior.

## III. VANETs

VANET is self- configuring like MANET. It is infrastructure less network of mobile devices connected by wireless. Each device is free to move in a VANET in any direction but within its link. A vehicular ad hoc network (VANET) uses moving cars as nodes in a network to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing to connect with each other with a range between 100 to 300 meters. As vehicles goes out of the signal range and drop out of the network, other vehicles can join in, vehicles are connecting to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purpose.

### *1.1 Routing Control*

Routing control in Vehicular ad-hoc network is also called as intelligent transportation system (ITS). In this the vehicles communicate with each other called vehicle to vehicle communication (V2V) or inter vehicular communication and vehicles communicate with the road side equipments called as vehicle to road communication (V2V). In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. Each vehicle broadcast the message to another ones[2].

**Inter vehicular communication:**

It is the communication between vehicles. In inter vehicular communication there are two types of message forwarding: Naïve broadcasting and intelligent broadcasting [2]. **In naïve broadcasting**, vehicles send broadcast messages periodically and at regular intervals. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. The dis-advantage of this method is that the large number of message broadcasting are generated due to which the message collision occurs and the message delivery rate become slow[10]. **In intelligent broadcasting,** if the vehicle detecting that they receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles[2].


Fig.1: Inter vehicle communication

**Vehicle to roadside communication:**

The vehicle-to-roadside communication configuration represents a single hop broadcast where the roadside equipment sends a broadcast message to all equipped vehicles in the surrounding area. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside equipments. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside equipment will determine the appropriate speed limit according to its internal timetable and traffic rules. The roadside unit will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the surrounded area. If a vehicle violates the desired speed limit, a

broadcast will be delivered to the vehicle in the form of an auditory or visual warning, requesting driver that they should reduce their speed.[2][10]

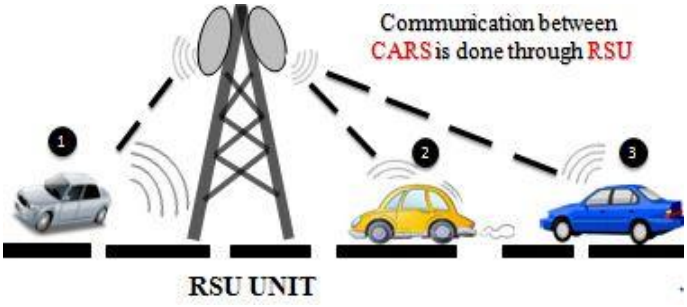


Fig.2: Vehicle to roadside communication

**1.2 Various attacks in VANET's**

In spite of various advantages there are many attacks in VANET.

**a. Prankster Attack**

Prankster Attack is when some hacker causes a false virtual traffic information and forces the vehicles to move into another direction from their pre-decided path. Selfish driver or Terrorist can propagate false information in the VANET and then as a result the vehicle will change their lane or direction, which can cause a traffic jam, unexpected turn or accident.

**b. Denial of service attack.**

This attack arises when attacker take control over vehicle's resources or creating jam over communication channel, so it prevent critical information from arriving. For instance if a attacker want to create a massive pile up on the road, it can make an accident and use the DOS attack to prevent the warning from reaching to the another vehicles.

**c. Alteration Attack**

This attack arises when attacker alters an existing data. It includes delaying the transmission of information, replaying earlier transmission, or altering the actual entry of data transmitted. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested.

**d. Replay Attack**

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending.

**e. Fabrication Attack**

An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else. This attack include fabricate messages, warnings, certificates, identities.

## IV. NEW PROPOSED SCHEME

In this research, we are addressing the issue of a prankster object propagating false information into the VANET cluster which may be used to cause an accident, traffic jam or terrorist activities. This paper is addressing the issue of prankster object in case of automatically driven vehicles in a VANET cluster. Vehicles prevent the addressed security threat by communicating with each other. No RSU (Road side units) are utilized in this scenario, hence, this method can be applicable anywhere without respect to the RSU network. The prankster object is the one, who propagates false information related to its position, drive direction or self collision indication. Prankster technique in VANETs can be used by selfish drivers or terrorists. Selfish drive launches prankster attack because he wants to make his way clear to reach his destination without any hurdle. Terrorist may use this attack to create a traffic jam to cause the maximum number of causalities.

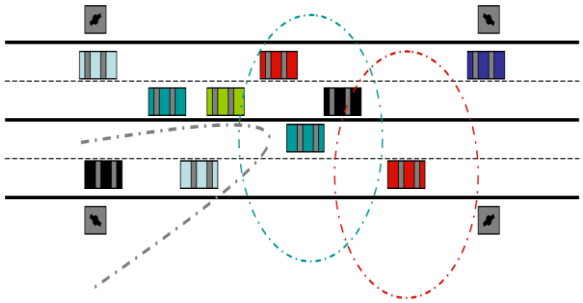

Fig.3: A simple VANET in action

There are two major problems of prankster attack has been addressed in the case of prankster attack i.e. false location information and false driving direction information. In this scenario, we assume that all of the vehicles are GPS aware objects and can also monitor their coverage/transmission area (Near-field communications) with respect to the GPS coordinates. Simplifying, a node is aware about its own location by knowing location GPS coordinates, and can relate coverage area of its TR-antenna with GPS coordinates around itself within the range of VANET antenna.

There will be required two perfectly working and GPS aware ordinary VANET nodes within range to handle a prankster object. The nodes are assumed to be automatically driven vehicles, which depends upon the GPS coordinates and neighbor nodes to take a ride. To prevent the prankster attack, Location-Aware/GPS-Aware VANET nodes will be aware of their coverage area in perspective of the GPS coordinates. Hence, if the vehicle (Assume CAR-X) travelling in their area

will propagate its false location, which is out of the coverage area of the VANET node, it will detect the false information. Then, discard the false information, and broadcast a message in the network that CAR-X is a malicious vehicle. The VANET nodes will communicate with each other in the cluster. Assume that VANET nodes A, B and C are travelling from west to east respectively. So if a vehicle will enter at first, in the coverage of node A and then, node B, it is detectable that vehicle is moving into the west direction and vice versa. So our method will also be able to detect the correct direction of movement of the vehicle. Hence, a vehicle will not be able to propagate the false information about the direction of its movement. We will start our research project by conducting a detailed literature review on the prankster attack in case of selfish driver in VANETs to know the problem in detail. Then, a detailed security mechanism would be designed to prevent the prankster attack in VANETs. The simulation would be implemented using Network Simulator (NS2). The obtained results would be examined and compared with the existing security mechanism to address the similar issues. Waterfall development method is ideal for projects with clear task formalization and fixed scope of work like this research work, i.e. for small and medium-size projects. Waterfall methodology comprises the following steps:

- working out system requirements, drawing up and approving the specification;
- design and prototyping;
- development;
- delivery;
- analysis and finalization.

## V. CONCLUSIONS AND FUTURE WORK

In research it has been concluded that VANETs are very efficient way of communicating between different travelling nodes but have some security problems in it, so by using GPS aware system will be a solution to eradicate this problem defined in paper and then this network will sooner become a futuristic network. During this whole research we have concluded that VANET is a newer topic for research purpose and it still have many flaws in its real time working scenario, this network can be use anywhere if its problems are being eliminated day by day. We have also concluded that in scenarios like VANET more attacks are liable to happen so there is a need to make it more secure such that its message privacy should be more and identity will be hidden.

## VI. REFERENCES

[1]. Fuad A. Ghaleb, M. A. Razzaque, Ismail Fauzi Isnin "Security and Privacy Enhancement in VANETs using Mobility Pattern" (IEEE,2013).

[2]. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" (IEEE,2010).

[3]. Muhammad a. Javed and jamil y. Khan "a Geocasting Technique in an IEEE802.11p basedVehicular Ad hoc Network for Road Traffic Management". IEEE 2010.

[4]. Chia-Chen Hung, Hope Chan, and Eric Hsiao-Kuang Wu "Mobility Pattern Aware Routing forHeterogeneous Vehicular Networks" IEEEWCNC 2008.

[5]. João A. Dias, João N. Isento, Vasco N. G. J. Soares, FaridFarahmand, and Joel J. P. C. Rodrigues "Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" 2011 IEEE pp.51-56.

[6]. Steffen Moser, Simon Eckert and Frank Slomka "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks" 2012 IEEE pp.36-41.

[7]. Irshad Ahmed Sumra, HalabiHasbullah, J.AbMananMohsanIftikhar,Iftikhar Ahmad, Mohammed Y Aalsalem "Trust Levels in Peer-to-Peer (P2P) vehicular network" 2011 IEEE pp.708-714.

[8]. Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Networks (VANET)", 2010 IEEE pp.55-60.

[9]. Irshad Ahmed Sumra, HalabiHasbullah, Jamalul-lailAbManan, "VANET Security Research and Development Ecosystem", 2011 IEEE.

[10]. Lu Chen, Hongbo Tang, Junfei Wang, "Analysis of VANET Security Based on Routing Protocol Information", 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China pp.134-138.