International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

VANET, its Characteristics, Attacks and Routing Techniques: A Survey

Manjyot Saini[1], Harjit Singh[2]

[1]Student, Guru Nanak Dev University, RC Gurdaspur

[2]Assistant Professor, Guru Nanak Dev University, RC Gurdaspur

Abstract: ***VANET vehicular ad-hoc network or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. In this paper various attacks and approaches in vanet are briefly defined.***

Keywords: VANET Scenario, Bandwidth, AODV, DSR, fuzzy

1. Introduction

1.1VANET

VANETs are vehicular ad hoc networks is a collection of wireless node that forms a momentary network to communicate between vehicles. The main use of VANETs is for safety and comfort application. The moving vehicles in the roadside are considered as nodes and these nodes can communicate with each other. These vehicle nodes are equipped with wireless devices to connect with the other devices fitted in the vehicles. During the communication, the vehicle communicate and transfer many useful on information .Reliability value is calculated by collecting some information like node location, direction and the velocity of the node. VANETs are different from other wireless networks in a way that they have high transmission power, high computational capability.[1] Vehicular Ad Hoc Networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) - the spontaneous creation of a wireless network for data exchange - to the domain of vehicles. They are a key component of intelligent transportation systems (ITS).[1]

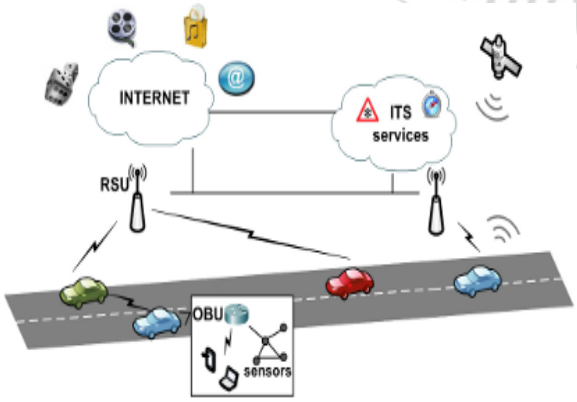

Figure 1.1: VANET [www.google.com]

1.2 Characteristics of VANET

VANET is an application of MANET but it has its own distinct characteristics which can be summarized as:

- **High Mobility:** The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy [2]. Rapidly changing
- **Network topology:** Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.
- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.[1]

Wireless Communication: VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication. Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

Sufficient Energy: The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.

Better Physical Protection: The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack.

1.3 Routing in VANET

For communication Ad-hoc networks are used. Ad-hoc Network is initially used for the MANETs but now they are used for the VANETs also. VANET utilizes these location based and topology-based steering conventions obliges that each of the partaking hubs be allocated a novel location. This intimates that we require an instrument that can be utilized to appoint interesting locations to vehicles yet these

conventions don't promise that the copy locations are doled out in a system or not. Consequently, existing circulated tending to calculations utilized as a part of versatile specially appointed systems are significantly less suitable in a VANET environment. Particular VANET-related issues, for example, system topology, portability designs, thickness of vehicles at diverse times of the day, fast changes in vehicles arriving and leaving the VANET and the way that the width of the street is regularly littler than the transmission run all make the utilization of these routine specially appointed directing conventions lacking.

1.3.1 Protective routing protocol

Proactive steering conventions utilize standard separation vector directing methodologies (e.g., Destination-Sequenced Distance-Vector (DSDV) steering) or connection state directing techniques (e.g., Optimized Link State Routing convention (OLSR) and Topology Broadcast-focused around Reverse-Path Forwarding (TBRPF)). They keep up and overhaul data on directing to all hubs that being said additionally when the way is not utilized. Course overhauls are occasionally performed paying little heed to system load, data transmission imperatives, and system size.

1.3.2 Reactive routing protocol

Touchy directing conventions, for example, Dynamic Source Routing (DSR), and Ad hoc On-Demand Distance Vector (AODV) steering execute course determination on an interest or need premise and keep up just the courses that are right now being used, in this manner lessening the load on the system when just a subset of accessible courses is being used and this breaking point the data transfer capacity wastage.

1.3.3 Position-based routing

Position-based directing conventions oblige that data about the physical position of the taking part hubs be accessible. This position is made accessible to the immediate neighbors as intermittently transmitted reference points. A sender can ask for the position of a recipient with the assistance of an area administration.

1.3.4 Forwarding

A geographic uncast transports bundle between two hubs through various remote jumps. At the point when the asking for hub needs to send a unicast parcel, it discovers the position of the goal hub by taking a gander at the area table. An avaricious sending calculation is then used to send the bundle to the neighboring vehicle or hubs, rehashes enumerating the base remaining separation to the end of the line vehicle and this methodology at each vehicle along the sending way until the parcel achieves its goal.

1.3.5 Protocols for dedicated short-range communication (DSRC)

Traditions, particularly Coordinated External Peer Communication (CEPEC) and Communications Architecture for Reliable Adaptive Vehicular Ad Hoc Networks .(CARAVAN) use mapping and timeslot designation to minimize the occasion of difference of organization ambushes or attacks that inconvenience the compelled move pace show in vehicular frameworks. Correspondences in a vehicular framework are weak to difference of organization strikes by staying the correspondence medium or saddling the confined remote information transmission that is open. These ambushes are happen due to the DSRC standard specific that a vehicle simply send data when it employees that the channel is impeccable, permitting a toxic vehicle to always transmit racket to keep transmission from inside sensing extent of the aggressor vehicles.

1.4 Attacks

There are various kinds of attack that can affect the entire system or can degrade the performance of system. The attacks can be categorized into following types.

a) Denial of Service attack

This strike happens when the aggressor increments control of a vehicle's benefits or jams the channel of correspondence utilized by the Vehicular Network, so it makes tangle to send separating information to its end of the line. It additionally expands the threat to the driver, on the off chance that it needs to rely on upon the application's data. For example, in the event that a malignant needs to make a colossal load up on the roadway, it can make a disaster and use the Dos strike to keep the forewarn from landing at to the approaching vehicles. Creators in talked about an answer for Dos issue and saying that the current arrangements, for example, bouncing don't totally tackle the issue, the utilization of different radio handsets, working in disjoint recurrence groups, can be a conceivable approach yet even this course of action will oblige adding new and more apparatuses to the vehicles, and this will oblige more sponsors and more space in the vehicle. The inventors in proposed an answer by trading between assorted channels or even correspondence progresses (e.g., DSRC, UTRA-TDD, or even Bluetooth for short ranges), in case they are open, when one of them (routinely DSRC) is chopped down.

b) Message Suppression Attack

An assailant specifically dropping packets from the system, these bundles may hold discriminating data for the beneficiary, the aggressor stifle these parcels and can utilize them again as a part of other time. The objective of such an assailant would be to keep enrollment and protection powers from looking into crashes including his vehicle and/or to abstain from conveying crash reports to roadside access focuses. Case in point, an aggressor may smother a blockage cautioning, and use it in an alternate time, so vehicles won't get the cautioning and compelled to hold up in the activity.

c) Fabrication Attack

An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personalities.

d) Alteration Attack

This assault happens when aggressor modifies current information, it incorporates deferring the transmission of the data, replaying prior transmission, or changing the genuine section of the information transmitted. For example, an

aggressor can modify a message telling different vehicles that the current street is clear while the street is congested.

e) Replay Attack
This assault happens when an aggressor replay the transmission of a prior data to exploit the circumstances of the message at time of sending.

f) Black hole Attack
When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node.

g) Grey hole Attack
This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcast.

h) Sybil Attack
In this attack, attacker generates multiple identities to simulate multiple nodes. Each node send messages with multiple identities, in this way other nodes realize that there are many nodes in the network at the same time. This attack is very dangerous because a bone node can give its various locations at the same time and this creating security risk.

2. Review of Literature

Ducourthial, B. et al [1] "Conditional Transmissions: Performance Study of a New Communication Strategy in VANET" Many solutions have been developed for routing messages in ad hoc networks. However, few of them are efficient when the network is highly dynamic. Indeed, building a routing table, discovering and maintaining a route, or localizing a node is a great challenge when the dynamic is high. This topic is currently attracting attention with vehicular ad hoc networks (VANETs), which are a special case of highly dynamic networks. VANET may allow us to enhance road safety and to develop new driver-or passenger-oriented services. In this paper, we present a novel approach for routing in highly dynamic networks, relying on condition-based communication. Instead of transporting addresses (or positions), a message is sent with some conditions used for retransmission or reception. Owing to the dynamic evaluation of the conditions, we show that this solution can efficiently support the high dynamic of vehicular networks.

Campolo, C. et al [3] **"**Modeling Broadcasting in IEEE 802.11p/WAVE Vehicular Networks" IEEE 802.11p/WAVE (Wireless Access in Vehicular Environments) is an emerging family of standards intended to support wireless access in Vehicular Ad Hoc Networks (VANETs). Broadcasting of data and control packets is expected to be crucial in this environment. Both safety-related and non-safety applications rely on broadcasting for the exchange of data or status and advertisement messages. Most of the broadcasting traffic is designed to be delivered on a given frequency during the control channel (CCH) interval set by the WAVE draft standard. The rest of the time, vehicles switch over to one of available service channels (SCHs) for non-safety related data exchange. Although broadcasting in VANETs has been analytically studied, related works neither consider the WAVE channel switching nor its effects on the VANET performance. In this letter, a new analytical model is designed for evaluating the broadcasting performance on CCH in IEEE 802.11p/WAVE vehicular networks. This model explicitly accounts for the WAVE channel switching and computes packet delivery probability as a function of contention window size and number of vehicles.

Azogu, I.K. et al [4] "A new anti-jamming strategy for VANET metrics-directed security defense " As Vehicular Ad-hoc Network (VANET) becomes a critical infrastructure for road safety and traffic efficiency, its standardization and deployment face serious security challenges. The nature of VANET hinders ineffective most of existing defense schemes for wireless/mobile networks. This paper studies the impact of jamming on 802.11p, the standard of vehicle-to-vehicle (V2V) communications. Jamming, a category in Denial-of-Service (DoS) attack, is a legacy in wireless communications. Although some detections and countermeasures of jamming-style DoS attacks have been proposed for generic 802.11 wireless local area networks, few is tested for 802.11p. Specifically, retreat strategies fail to mitigate jammers in VANET as geography may prohibit escaping from a jammed area, and the only one control channel for safety critical messages in 802.11p excludes channel hopping. Likewise, competition strategies such as tuning the carrier sense threshold does not respond fast enough to high-speed mobility. This work proposes a hideaway strategy, suitable for anti-jamming in VANET. The new strategy is perceived with a novel security metrics to measure the effectiveness of jammers, directing the design of defense mechanisms.

Kumar, A. et al [5] "An efficient group-based safety message transmission protocol for VANET" Vehicular Ad-hoc Network (VANET) is a type of mobile communication in which topology changes dynamically due to high mobility of vehicles. Vehicles use two types of messages to update their status and to communicate with other vehicles. First is Periodic Safety Message (PSM) which gives us information about position, speed etc. and second is Event Driven Safety Message (ESM) which occurs when emergency situation like hard breaking, sudden lane change, etc. When vehicle movement is abnormal either due to change in speed or direction, vehicles generate eventdriven safety alert messages. Safety alert messages are needed to be very fast and reliable for VANET applications. In this paper, we propose a novel approach to improve safety alert message communication in VANET using grouping of vehicles. Firstly, vehicles form a group and select their Group Leader to communicate with other Group Leaders. Secondly, we send the safety alert message by using priority in the messages and context-based communication. The priority is set according to various types of accidents and by using context-based communication the ESM messages are send to those groups which are endangered by the accidents. Simulation of proposed scheme is performed on multi-lane roads by considering vehicles movement in a single direction.

3. Approaches Used

3.1 AODV ROUTING

AODV is a well known topology routing protocol which has a very high packet delivery ratio and low routing overhead. AODV works as follows Whenever a node wants to communicate with another node, it checks in local routing table to find an available path to the destination node. If there is no path available, then it broadcasts a route request (RREQ) message to its neighbourhood. The node that receives RREQ looks its table for a path leading to the destination node. If there is no path then, the RREQ message is re-broadcasted and a path to the originating node is formed that has sent RREQ message. This helps in establishing the end to end path when the same node receives route reply (RREP) message as shown in Fig 2.All the node in the network follows this process until this RREQ message reaches a node which has a suitable path to the destination Node. At the end of this request-reply process a path between source and destination node is created and is available for further communication. In this way, the originating node that generated RREQ receives an RREP message as shown in fig 1.

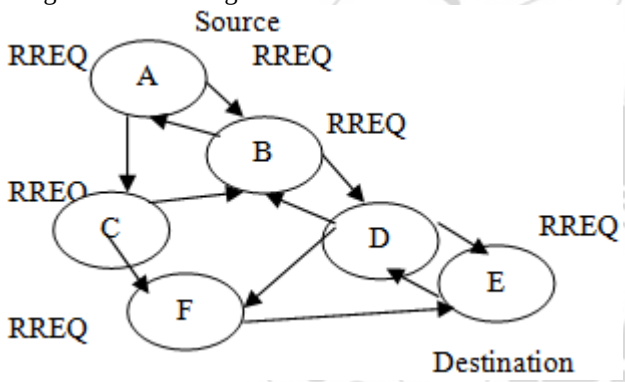

Figure 1.2: Message routing

To maintain a connection with the sink node is a crucial issue to collect data from networks without any interruption. While networks are typically deployed in abundance, losing the connectivity with the sink node due to frequent path break eventually reduces the quality and efficiency of the network operation

3.2 GPSR (Greedy Perimeter Stateless Routing)

GPSR is one of the popular geographic routing protocols which can be used for Vanets. GPSR [18] assumes that each node in the network has a local table which maintains the ID and position of all the neighboring 267 nodes.A correct forwarding decision can be made with the help of wireless routers position and the position of the packets destination. There are two methods of forwarding the packets:

3.2.1 Greedy algorithm in GPSR

Let (XLF, YLF) and (XLD, YLD) respectively denote the locations of the forwarding node F and the destination node D that has the data packet addressed to the destination node D. The forwarding node F calculates the distance between itself and the destination node D. And it also calculates the distance between each of forwarding nodes neighbour nodes and destination node D. After calculating the distance parameter, the neighbour node that lies nearby to the destination is selected as the next forwarding node to forward the data packet. If the forwarding node F could not find a neighbour node that lies closer to the destination node D than itself, then the node switches to perimeter forwarding. The pseudo code for the greedy algorithm used at a forwarding node in the traditional GPSR is shown below.

Begin GPSR Greedy Forwarding Algorithm
Input: Forwarding Node F, Destination D, Neighbours-List (F)
Auxiliary Variables: Progress (F, I) where I∈Neighbours-List (F) Maximum-Progress
Output: Next-Hop-Node // if Greedy forwarding is successful NULL // if Greedy forwarding is not successful and Perimeter forwarding is needed
Initialization: Next-Hop-Node = NULL Maximum-Progress← 0.0
Begin GPSR Greedy Forwarding Algorithm

$$\text{Distance} = F.D\sqrt{(X_{li} - X_{ld})2 + (y_{li} - y_{ld})2}$$

3.3 Dynamic Source Routing (DSR)

Protocol DSR is a reactive routing protocol as send the packet to destination to discover address of route. This routing needs source route maintenance, while the use of route, it is needed to monitor the process of the route and notify the sender of any mistake [11]. It is weak against wormhole attack and DoS attack could be occurred at the destination. This routing protocol needs to forwarding of only the first RREQ packets received by it and will drop other RREQ packets for the same route. This RREQ packet includes some information about intermediate nodes and the hop count. The route used to send data packet, when the route discovered. According to wormhole attack, that uses fast channel for forwarding the message, the RREQ packet through them will receive to destination faster than other paths. This result will be from a wormhole route to be discovered as the route to destination nod. The packet may be selectively or fully dropped by the wormhole attacker resulting permanent DoS attack at the destination node.

4. Conclusion

VANET is extension of MANET that deals with vehicles for communication of auto driven system. In this approach the nodes have been approved as vehicles that connected to read side units available in the communication area. RSU available are concerned for transmission of information about traffic density, collision, position & speed of the nodes. The RSU transmit the safety message over the communication range for reliable communication by avoiding collision b/w he nodes. Various protocols had been utilized for reliable communication & transmission of safety message. In VANET on-demand/ Proactive protocol had been used for communication that computes the routing path dynamically at the time of transmission. Reactive protocol choose shortest path for communication but the shortest path does not guarantee of delivery of safety message. In the base paper other factor like Delay, probability of collision; Bandwidth had been considered to develop surgery construct

rules for communication. This causes problem for communication due to selection of rules. To overcome this fuzzy constant must include number of intermediates nodes & number of hopes used for transmission of safety message.

References

[1] B. Ducourthial, Y. Khaled, and M. Shawky, "Conditional transmissions: Performance study of a new communication strategy in VANET," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3348–3357, 2007.
[2] S. R. Kolte and M. S. Madankar, "Adaptive congestion control for transmission of safety messages in VANET," 2014 Int. Conf. Converg. Technol. I2CT 2014, pp. 1–5, 2014.
[3] C. Campolo and a Vinel, "Modeling broadcasting in IEEE 802.11 p/WAVE vehicular networks," … Lett. IEEE, vol. 15, no. 2, pp. 199–201, 2011.
[4] I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," 2013 IEEE Globecom Work. GC Wkshps 2013, pp. 1344–1349, 2013.
[5] A. Kumar and R. P. Nayak, "An efficient group-based safety message transmission protocol for VANET," Int. Conf. Commun. Signal Process. ICCSP 2013 - Proc., pp. 270–274, 2013.
[6] S. Roselinmary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)," 2013 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2013, pp. 237–240, 2013.
[7] J. Copeland, F. Khan, K. Sanil, and F. Elahi, "Recovering VANET safety messages in transmission holes," Glob. Inf. Infrastruct. Symp. GIIS 2013, pp. 0–4, 2013.
[8] Y. B. Jinila and K. Komathy, "a Privacy Preserving Authentication Framework for Safety Messages in Vanet", Fourth International Conference on Sustainable Energy and Intelligent Systems, pp. 456-461, 12-14 Dec 2013 - K.C.G College of Technology – Chennai
[9] K. Verma and H. Hasbullah, "IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET", International Conference on Computer and Information Sciences (ICCOINS), pp. 1-6, 3-5 June 2014.
[10] S. Verma, "Impact of Gray Hole Attack in V ANET", 1st International Conference on Next Generation Computing Technologies (NGCT-2015), pp.127-130, 4-5 September 2015.
[11] G. M. Valantina and S. Jayashri, "Q-Learning Based Point to Point Data Transfer in Vanets," Procedia Comput. Sci., vol. 57, pp. 1394–1400, 2015.