Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Different Approaches of Safety Message Transmission in VANET

[1] Harjit Kaur, [2]Kamal Jeet Kaint, [3]Rakesh Kumar
[1] Research Scholar, [2, 3] Asst. Professor
[1, 2, 3] Computer Science and Engineering, Sachdeva Engineering College for Girls, Gharuan, Punjab, India

Abstract-the 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, creates a network with a wide range. in this paper learn various protocols used to VANET and evaluating high performance using different parameters.

Keywords: VANET, QOS, vehicles, GPSR.

I. INTRODUCTION

1.1 VANET

VANET uses cars as moving nodes in a MANET to create a mobile network. A VANET turns participating car into a wireless router or node which allowing cars 100 to 300 meters of each other to join and create a network with a broad range. As cars fall out of the signal range and fall out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is predictable that the first systems that will be this technology are law enforcement and fire vehicles to communicate with each other for the purpose of security [1].

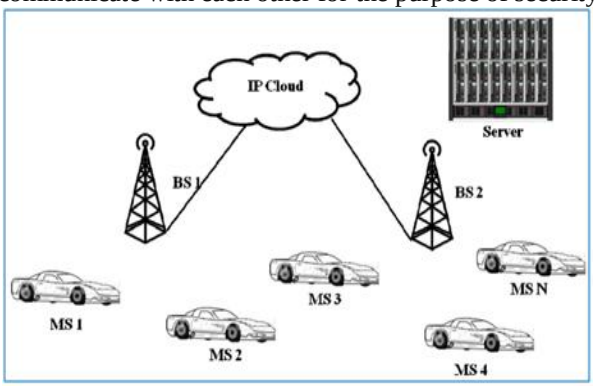

Fig 1.1 VANET

The connectivity is done among one vehicle to other vehicle and vehicle to road side infrastructure and vehicle or road side infrastructures to the central authority in charge for the network maintenance.

The basic tool for message transfer is the short range radios that are being installed in any of the nodes. The short transmission node is used by vehicular node. RSU's are extended at irregular intervals or regularly depending on the deployment of the network in any particular region. In actuality spread at irregular intervals. They act as an intermediary node between the Central Authority (CA) and Vehicular Node (VN).VANET-Vehicular Ad-Hoc Network is the network in which communication has been done between road side units to cars, car to car in a short range of 100 to 300 m. Existing authentication protocols to secure vehicular ad hoc networks raise challenges like as certificate allocation and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper proof devices

The number of vehicles owned by people is rapidly rising with the development of economy and society. The security problem in transportation is increasingly exceptional. It brings a serious risk to humans' life and goods. As we all known, safe-driving is always one of the most important topics in vehicle engineering. In order to reduce traffic accidents, the intelligent vehicle emerges as the times require. It is a complex system equipped with complex technologies such as the artificial intelligence, automatic control, computer, and communication.

1.2 Characteristics of VANET

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

1.2.1High Mobility: The nodes in VANETs regularly are moving at high speed. This makes harder to predict a node's position and making security of node privacy [2] rapidly changing

2.2.2 Network topology: Due to high node mobility and casual speed of vehicles, the position of node changes regularly. As a result of this, network topology in VANETs tends to change regularly.

1.2.3 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.

1.2.4 Frequent exchange of information: The ad hoc nature of VANET boost up the nodes to get together information from the other vehicles and road side units. Hence the information replace among node becomes frequent.

1.2.5 Wireless Communication: VANET is intended for the wireless environment. Nodes are connected and swap their information via wireless. So 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 choice can be made by the node and perform action for that reason.

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

1.2.7 Better Physical Protection: The VANET nodes are physically improved protected. Thus, VANET nodes are harder to compromise physically and reduce the effect of infrastructure attack.

1.3 Challenges in VANET'S:

A Speed-based Shortest Path Trip generation has been added. Accordingly, we can modify a threshold between high speed street segments and distance to the destination, which may create a longer but faster path. Street Segments includes a speed limitation attribute. For tiger files, we create default values based on the State of California present regulations, or let the user define them in an external file decoupling the multi-lane feature from the lane changing characteristic. When several lanes are available, every car chooses one lane and keeps it for the complete trip New Randomized Dijikstra direct path algorithm. The original Dijkstra's algorithm, given a start and an finish point, always selects the same pathway, even in presence of multiple available paths with same weights. For traffic balancing, cars should be able to select dissimilar direct paths.

1.4 Security Requirements of VANET'S

1.4.1 Authentication

Authentication is a main requirement in VANET as it ensures that the messages are sent by the real nodes and hence attacks done by the greedy drivers or the other adversaries can be reduced to a better extent

1.4.2 Message Integrity

This is very much requires as this ensures the communication is not changes in transit that the messages the driver receives are not fake.

1.4.3 Message Non-Repudiation

In this safety based system a sender cannot deny the fact having sent the message. But that doesn't mean that everybody can recognize the sender only exact authorities should be allowed to recognize a vehicle from the authenticated messages it sends.

1.4.4 Entity authentication

It ensures that the sender who has generated the message is still within the network and that the driver can be assured that the sender has send the message within a very short time.

Access manage it is necessary to ensure that all nodes function according to the roles and privileges authorized to them in the network.

1.4.5 Message confidentiality

It is a system which is necessary when certain nodes want to communicate in private. But anybody cannot do that. This can only be completed by the law enforcement authority vehicles to communicate with each other to put across private information. An example would be, to find the place of a criminal or a terrorist.

1.4.6 Privacy

This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information Third parties should also not be able to track vehicle movements as it is a violation of personal privacy.

1.4.7 Real time guarantees

It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met.

1.5 Routing Protocols

In VANET, the routing protocols are classified into five categories: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Broadcast routing protocol, Geocast routing protocol.

1.5.1 Topology based routing protocol

These routing protocols use link information that exists in the network to perform packet forwarding.

They are additional classified as Reactive and Proactive routing protocol.

1.5.2 Proactive routing protocols

The proactive routing means that the routing information from source to destination is readily accessible irrespective of the communication requests. The packets are constantly flooded among nodes to maintain the path and a routing table is constructed and maintained within a node which tell next hop node towardsa destination. The main advantage in these routing protocols is so as to there is no need for route discovery methods, since the destination route is stored in the

background. But it give low latency for real time application [5], it maintains unexploited data paths without cause, which causes the decrease in the available bandwidth. [6] This is measured as the main disadvantage.

1.5.3 Reactive routing protocolsA protocol which tries to locate routes from source to destination only on-demand fashion. In the Reactive routing protocol, a connection between two nodes is created, only when there is a demand from the source. A route is established and it is kept by a route maintenance technique in anticipation of the destination no longer exists. In reactive, when a node wishes to send a packet to a particular destination, a route discovery procedure is initiated in order to find the destination. The key for packet routing provided by the reactive routing protocol is cost efficient. However, when routes are requested, nodes want to send out a route request into a large part of the communication network, which could lead to low latency of route response and potentially a large penalty in network resources. A situation like this causes throughput loss in high mobility scenarios, because the packets get lost rapidly due to unstable route selection. 265

1.5.4 Position based routing protocol Position based routing made of set of routing algorithms. They use the property by using geographic positioning information in order to select the path from source to destination. Without any map information the packet is sent to the one hop neighbor who is adjacent to the destination node. Place based routing is advantageous since no global route from source node to destination node need to be created and maintained. Position based routing is usually classified into two types: Position based greedy V2V protocols, [5] Delay Tolerant Protocols.

1.5.5 Cluster based routing protocol In Cluster based routing protocol the nodes of a wireless network are separated into several disjoint or overlapping clusters. Each cluster elects one node as the head which is called the cluster head. The cluster heads are responsible for the routing course. Cluster heads are able to communicate with each other using gateway node [11]. A gateway is a node that has two or more cluster heads as its neighbors' or when the clusters are disjoint, there should be at least one cluster head and another should be a gateway node [7]. The routing process itself is performed as source routing by flooding the network with a route request packet. The routing overhead in this case is condensed because the communication is done by only cluster heads in its place of all the nodes.

1.5.6 Geocast Routing Protocol Basically Geocast routing is a place based multicast routing. The main aim of Geocast routing is to effectively deliver the packet from source node to all other nodes within a specified geographical area (Zone of Relevance ZOR). Vehicles external to the ZOR are not alerted, to keep away from redundant hasty reaction [8]. Geocast routing is considered as a multicast service inside a specific Zone of Relevance. Usually a forwarding zone is defined, where it directs the flooding of the packets in arrange to reduce message overhead and network jamming caused by simply flooding packets in the network.

II. REVIEW OF LITERATURE

Alwakeel, S et. al. [1] "A virtual P-Persistent bandwidth partitioning manager for VANET's broadcast channel" In VANET'S Safety messages is very much significant so that it must have the highest guarantee of delivery. But security message can be discarded due to its low bandwidth. In this message we implement a approach to block minimum numbers of safety messages. But if you kept non safety message it can be penalized you. Through virtually partitioned VANET's bandwidth and by applying P-Persistent scheme to reduce message congestion an improved performance of message dissemination in VANETs can be achieved.

Varshney, Neerajet. al. [2] "Security protocol for VANET by using digital certification to provide security with low bandwidth" Author introduced a algorithm to conquer these network attacks via low message passing and try to reduce the bandwidth at the time of authentication, message passing. For analysis and check the safety of our protocol author have analyzed the proposed protocol with the existing protocol based on computational price and presentation time

Ghosh, T. et. al. [3] "Congestion control by dynamic sharing of bandwidth among vehicles in VANET" For the safe transmission of message author use the control channel and service channel is use for the transmission of insecure message. Each node computes its own priority depending upon the number of coming up messages in control queue and service queue. Every node reserves a part of control channel and service channel dynamically depending upon the number of waiting messages in its queue. The insecure messages at a node may also be transmitted by means of control channel provided the control channel is free and service channel is overloaded which helps to reduce the defeat of unsafe message at a node which in turn reduces the congestion level of a node and also improves its quality of service

Gandhi, U.D et. al. [4] "Request Response Detection Algorithm for detecting DoS attack in VANET" The sub category of MANET is VANET which is used to create a mobile network that is based on mobile vehicles. It allows every participating vehicle into a wireless node, allowing it just about 100 to 300 meters of each other to connect and in turn, create a wide range network. Vehicle can link one another between these ranges. It is used for ITS (Intelligence Traffic System). Very well-known automotive companies like BMW and Ford promote this term. The mobile nodes are well prepared with ORT (On board Radio Transponder) that is helpful in communication with other nodes in a network. In order to establish communication among the vehicles VANET comes with communication points by road infrastructure. Lot of security attacks happen in VANET like Sybil attack, selfish driver attack. In this paper we proposed a Request Response Detection Algorithm (RRDA) which is used to detect DOS after APDA response Time and Security Increase.

Meriam, E. et. al. [5] "VANET adaptive and Reliable Broadcast protocol", security is most important in VANET. A major application of VANET is safety warning. Broadcasting of safety messages requires an effective broadcast mechanism. Selection of the probe node is the major problem in VANET broadcasting. The process of the probe node collection and broadcasting of safety messages must be achieved in a limited time. Meanwhile, the transmission reliability must also be preserved. Multi behavior and Reliable Broadcast (MRB) protocol is especially designed for an optimum performance of safety applications and addresses these constraints.

III. APPROACHES USED

3.1 AODV (Ad hoc On-Demand Distance Vector):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 needs to communicate with another node, it checks in local routing table to locate an available path to the destination node. If there is no path available, then it broadcasts a route request (RREQ) message to its region. The node that receives RREQ looks its table for a path leading to the aim 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 similar 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 additional communication.

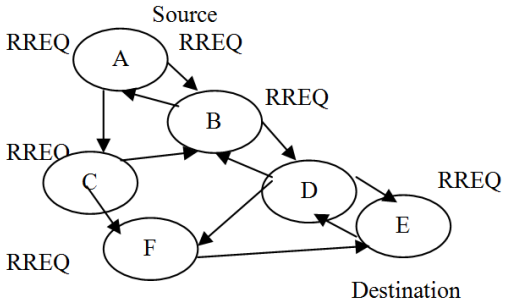

Fig 1.2 Message routing

To maintain a connection with the sink node is a critical issue to collect data from networks without any interruption. While networks are typically deployed in large quantity, 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 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 choice 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:

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 target 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, after that 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

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

3.3 Dynamic Source Routing (DSR):

DSR is a reactive routing protocol as send the packet to destination to find out 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. It is weak against wormhole attack and DoS attack could be occurred at the destination. This routing protocol wants 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 information packet, when the route exposed. According to wormhole attack, that uses speedy channel for forwarding the message, the RREQ packet through them will receive to destination quicker than other paths. This result will be from a wormhole route to be exposed 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.

3.4 Predictive Unicast Multipath Algorithm (PUMA):

PUMA is an ad-hoc routing functionality (atthe IP layer) for wireless mobile unmanned sensor networks. An ad-hoc network is a compilation of mobile nodes dynamically organizing themselves for communication in the absence of existing infrastructure, which requires routing between mobile nodes. Routing in ad-hoc networks enables each mobile

node to operate not only as an endpoint but also as a switch that has the functionality to forward data over the next hop. Two causes of connection disturbance are addressed, node mobility, where communicating nodes shift out ofone-hop range of each other; and link outage caused by such events as terrain or characteristic masking and node failure (e.g., destruction, compromise, battery depletion).

IV. CONCLUSION

VANET is vehicular Ad-hoc network which is used for intelligent transport system for the drivers the ad-hoc network is used to transmit various types of message over the network. Safety message has to transmit for the security reasons on the vehicle and road transportation.V2V is vehicle to vehicle communications and V2R is vehicle to roadside communication. In various scenarios message transmission is done according to vehicle density available on the road. Based on the real time road density vehicle establish reliable route for the communication on packet delivery. The main issue of road density is due to high load on road message communication get overhead due to less amount of network bandwidth to overcome this issue cognitive radio bandwidth can be utilize for data transmission by channel sensing and message can be transmit through cognitive radio channels.

REFRENCES

[1] Alwakeel, S "A virtual P-Persistent bandwidth partitioning manager for VANET's broadcast channel", International conf. on Multimedia Computing and Systems (ICMCS), 2014, PP 1212 – 1215,.

[2] Varshney "Security protocol for VANET by using digital certification to provide security with low bandwidth", International Conf. on Communications and Signal Processing (ICCSP), 2014, PP 768 – 772.

[3] Ghosh, T. "Congestion control by dynamic sharing of bandwidth among vehicles in VANET", International Conf. on Intelligent Systems Design and Applications (ISDA), 2014, PP 291 – 296.

[4] Gandhi, U.D "Request Response Detection Algorithm for detecting DoS attack in VANET", International Conf. on Optimization, Reliabilty, and Information Technology (ICROIT), 2014, PP 192 – 194.

[5] Meriam, E. "VANET adaptive and Reliable Broadcast protocol", International Conf. on Wireless Communications and Mobile Computing Conference (IWCMC), 2014, PP 237 – 243.

[6] Wu, Sau-Hsua "A conceptual model and prototype of Cognitive Radio Cloud Networks in TV White Spaces", IEEE Conf. on Wireless Communications and Networking Conference Workshops, 2012, PP 425 – 430.

[7] Wu, Sau-Hsuan "A cloud model and concept prototype for cognitive radio networks", IEEE Conf. on Wireless Communications ISSN 1536-1284, PP 49 – 58, IEEE, 2012.

[8] Wu, Sau-Hsuan "A conceptual model and prototype of Cognitive Radio Cloud Networks in TV White Spaces", IEEE Conf on Wireless Communications and Networking Conference Workshops, 2012, pp 425 – 430.

[9] Selvakanmani, S. "CRCN CORMEN — an on demand opportunistic routing protocol for mobile cognitive radio ad hoc networks", IEEE Conf. on Computer Communication and Systems, 2014, pp 265 – 270.

[10] Xing Fu "Cache-Aware Utilization Control for Energy Efficiency in Multi-Core Real-Time Systems", IEEE Conf. on Real-Time Systems (ECRTS), 211, pp 102 – 111.

