International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Vehicular Ad-hoc Networks: Address Configuration and Routing Protocols

Shilpa Sharma[1], Harpreet Kaur[2]

[1]P.G Student, Department of Electronics and Communication Engineering, Chandigarh University Gharuan, Mohali

[2]Assistant Professor, Department of Computer Science Engineering, Chandigarh University Gharuan, Mohali

Abstract: ***The goal of Vehicular Ad-hoc network (VANET) is increasing the road traffic efficiency. Due to the unique property of VANET such as high movability of nodes, dynamic change in topology, routing in VANET is a very difficult task. It is a challenge to certify a reliable, continuous and consistent communication of vehicles having very high speed [1], so we study some of the routing protocols and the address configuration schemes in the VANETs.***

Keywords: VANET, Address configuration, Routing protocols

1. Introduction

A Vehicular Ad-hoc Network (VANET) is basically a class of Mobile Ad-hoc Networks (MANETS) in which nodes are communicating with each other and these nodes are vehicles which have a very high movability.It uses North American Direct short-range (DSRC) standard which uses the IEEE 802.11p standard for wireless communication [2].Typically, vehicles can communicate with each other within the range of 100 to 900 meters[3]. Modish vehicles are often designed as local area networks which have the ability to connect with other vehicles as well as themselves via numerous wireless connections. The VANET is being used in many applications such as giving information to vehicles regarding routing, providing information regarding traffic to the drivers, road condition, etc. To observe the network conditions VANET uses some sensor devices. These sensors are capable of collecting information and providing relevant information to vehicles.

A reference architecture of vehicular networks consists of three regions such as:In-vehicle region which is defined as a local network inside each vehicle which is composed of an on-board unit and one or more application units .The Ad-hoc region which is composed of OBUs and road side units (RSU) or referred as access routers. Every vehicle has a different OBU and these OBUs form a mobile ad-hoc network and OBUs are equipped with communication devices. These OBUs are the nodes of ad-hoc networks, which are free to move and RSUs can be stationary nodes.These RSUs is connected within an infrastructure which in succession connected to the internet.

The rest of the paper is organized as follows: In section1 some of the routing protocols of VANETs are discussed, in Section2 IP addressing. For vehicular networks is discussed and in Section 3 possible attacks in VANETs are discussed.

2. Routing Protocols of VANET

2.1Topology based routing protocols

It uses the global information of network topography and the links used in routing. These protocols use two approaches for routing, which are proactive approach and reactive approach. Proactive approach maintains the information of all the nodes, whether they are participating in communication or not. The every node has a table representing the entire network topology and these tables are updated regularly. Whereas the reactive approach determines the routing only when it is needed to the current communication. Examples of proactive protocols are Distance Vector protocol (DV), Optimized link state routing protocol (OLSR), Destination-sequenced distance vector (DSDV). These create a routing table which is distributed throughout the network. Dynamic source routing and ad-hoc on demand distance vector (AODV) protocols are the examples of reactive approach. AODV support both unicast and multicast routing, it contains the destination sequence number for every route so that the counting to infinity problem is solved.

In VANET, topology based routing protocols do not work well due to the overheads and maintenance of the route because of high mobility.

2.2 Position-based Routing Protocols

In this we need the geographic position of the vehicles. It requires location based services so that we can find the position of the destination. Some of the location services which are commonly used are Global Position System (GPS), DREAM location Services (DLS). In position based routing protocol the packets are sent to their one-hop neighbour, which is very close to destination without any knowledge of digital maps. In VANETs position based routing protocols are used since there is minimum delay in creating the route and high delivery ratio than topology based routing protocols.

2.3 Cluster based Routing Protocols

Clustering in VANETs can be defined as the division of the dynamic nodes into various groups. Cluster-head is responsible for routing, channel assignment. The cluster members do not take part in the routing.[1]

2.4 Hybrid Protocols

In hybrid protocols, the network is divided into two layers.The inner layer is responsible for maintaining and updating the details all the times in the network means this layer is proactive. The outer layer is responsible for on-demand path determination so it is reactive.Hybrid routing protocols use the advantages of proactive and reactive approaches.

3. Configuration of IP Address in Vehicular Networks

With the growth in the technology of vehicular networks and the expansion of new applications, it becomes very necessary for vehicular networks to connect with the internet.Each device has its unique address which is called internet protocol address (IP address).There are two types of versions which we used in internet protocol: one is IPv4 which refers to Internet Protocol version 4 and second is IPv6 which refers to Internet Protocol version 6.Version 4 is 32-bit address and version 6 is 128-bit address, so due to the growth of internet version 6 is used and more number of vehicles are connected to the internet as compared to version 4.In this section we discussed address configuration of address in vehicular networks.

The mobility of vehicles are very high so the protocols which are used to configured the IPv6 address cannot work in efficient manner in vehicular networks [7]. When version 6 is combined to vehicular networks following three types of issues can occur.

1) The configuration of IPv6 address in vehicular networks.
2) The movability of vehicles.
3) The communication problem in vehicles.

In this section, we discussed that how the address can be obtained within VANET. In[4] the address configuration scheme classifies OBUs into two types: normal OBU and leader OBU. Leader scope has a scope parameter and dynamic host configuration protocol (DHCP) server is equipped with it, that enables the server to automatically assign an IP address to vehicles from a defined range of number (scope) in the network.If the normal OBU is moving out from the leader OBU, it inherits the IP address from the leader OBU and acquired a new address in case it is out of scope. As a normal OBU's speed does not match with that of the leader OBU's speed, so it is not possible for a normal OBU to remain in a leader OBU's scope. Resultingly, a normal OBU will change its IP address often. However, if normal OBU is not in the range of leader OBU, it cannot get an IP address.

In [5], when a vehicle is moving out from one region and shifting to the boundary of the other region, it obtains a new address from the neighbouring vehicle, but if the crowdedness of the vehicles is very less than this scheme does not work.

To make the scheme better, Chen et al. [6] propose an addressing scheme in which when a vehicle is leaving its communication region it passes its IP address to the intermediate vehicle in order to increase the lifetime of address. During this lifetime if in the serving communication region, a vehicle is entered, it can acquire an address from the intermediate vehicle.But if the vehicle cannot get the IP address from the intermediate vehicle, then it gets its IP address from the server.In this type of case, the configuration of address is elongated.

To solve this problem, Wang et al.[7], propose a scheme in which the stateless address configuration scheme is combined with stateful one.

In the stateless address configuration mechanism, the address of the target is broadcasted between the neighbours (DAD) to guarantee its uniqueness. Since the count of vehicles is very high, thereby increasing in cost and delay which is compensated stateful address configuration because in this mechanism without using DAD the assigned IP address's uniqueness can be guaranteed. However, the stateful address configuration has some drawbacks:

1) The states of the address must be sustained.
2) The space of the address released must be sustained.

But in the stateless mechanism, these drawbacks are not existing. In the proposed stateless mechanism the DAD is not performed in the network, whereas it is performed on the road side domain, so the cost and delay are significantly decreased. In this way these both schemes are combined and purpose is to make use of their advantages.

4. Possible Attacks in VANETs

There are a number of attacks in VANETs and the focus of these attacks is to create a hurdle for users or spoofing some information.There are some of the following:

Denial of service: The attackers attacks on the nodes or the communication medium, so that the vehicle is not able to access the network and the result in the wreckage of the nodes and network's resources[8].

Message suppression attack: Attackers selectively discard packets from the packets and compress them and used them again for another purpose. The aim of these attackers is to hide any information from roadside access regarding the collision. [9]

Time critical: The information among the vehicles must be delivered within the time limit so that there can be an effective communication and the decision can be made and performed accordingly.

Routing Attack: In this attacker disturbs the routing process of the network.

Sybil Attack: In this attack the attackers creates a large number of pseudonymous and force other vehicles to take an alternate route[10]. In this each node sends their packets with multiple identities so that other nodes notice that there are many locations of that node in the network at the same time and so that create the risk of security.

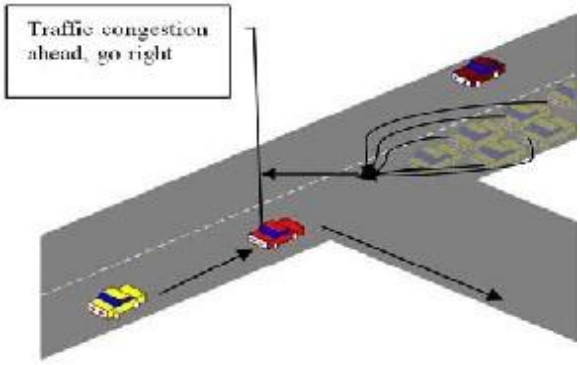

Figure 1[10]

5. Conclusion and Future Scope

In this paper, we discussed the routing protocols of VANETs and see how IP address is obtained by vehicles by reducing the cost and delay and study about some attacks in VANETs. In future we can work on the communication problem occur in vehicular networks and we can improve the range of the vehicle-to-vehicle communication and focus on the security of VANETs.

References

[1] Venkatesh, A. Indra, R.Murali: Routing protocols for vehicular Ad-hoc networks(VANETs): A review, Journal of emerging trends in computing and information sciences, Vol. 5, No. 1 January 2014
[2] D.Bhattacharyya,A.Bhattacharyya:Architecture of vehicular networks
[3] M.S.Anwer, C.Guy: Survey of VANET Technologies, Journal of Emerging Trends in Computing and Information Sciences, Vol.5, No.9 September 2014.
[4] Fazio, M., Palazzi, C.E., Das, S., Gerla, M.: Automatic IP address configuration in VANETs, In Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, pp. 100–101. ACM (2006)
[5] Chen, Y.S., Hsu, C.S., Yi, W.H.: An IP passing protocol for vehicular ad hoc networks with network
[6] Chen, Y.S., Hsu, C.S., Cheng, C.H.: Network mobility protocol for vehicular ad hoc networks. Int. fragmentation. Comput. Math Appl. 63(2), 407–426 (2012)
[7] X.Wang, D.le, H.Cheng:location-based IPv6 Address configuration for Vehicular networks, Springer science+Business Media Newyork 2015 J. Commun. Syst. 27(11), 3042–3063 (2013)
[8] A.Phutela,T.Mehta: Vehicular Ad-Hoc Networks (VANETs): A Survey International Journal of Computer Science And Technology, Vol. 6, Iss ue 1 Spl- 1 Jan-March 2015
[9] B.Parno,A.Perrig: Challenges in Securing Vehicular networks, Proc. Of HotNets- IV,2005
[10] J.Douceur: The Sybil Attack,First International Workshop on Peer-to-Peer Systems.