Comparative Study of the Routing Protocols based on Vehicular ad-hoc Network (VANET)

Mamta Devi[1], Dr Rakesh Kumar[2], Er Nidhi Bhatla[3]
[1]*Research Scholar, CSE Department*
[2]*Professor& Principal, CSE Department*
[3]*Head of Department, CSE Department*
SECG, Mohali

Abstract: -VANET (Vehicular Ad-hoc Network) is a new technology which has taken enormous attention in the recent years. Due to rapid topology changing and frequent disconnection makes it difficult to design an efficient routing protocol for routing data among vehicles, called V2V or vehicle to vehicle communication and vehicle to road side infrastructure, called V2I (vehicle to infrastructure). Routing in Vehicular Ad hoc Networks is a challenging task due to the unique characteristics of the network such as high mobility of nodes, dynamically changing topology and highly partitioned network. It is a challenge to ensure reliable, continuous and seamless communication in the presence of speeding vehicles. The performance of routing protocols depends on various internal factors such as mobility of nodes and external factors such as road topology and obstacles that block the signal. This demands a highly adaptive approach to deal with the dynamic scenarios by selecting the best routing and forwarding strategies and by using appropriate mobility and propagation models. In this paper we have reviewed the existing routing protocols for VANETs and categorized them into a taxonomy based on key attributes such as network architecture, applications supported, routing strategies, forwarding strategies, mobility models and quality of service metrics. Protocols belonging to unicast, multicast, geocast and broadcast categories are discussed. Strengths and weaknesses of various protocols using topology based, position based and cluster based approaches are analyzed.

Keywords:VANET, Proactive, Reactive, Hybrid routing protocol.

I. INTRODUCTION

Wireless communication has enabled many of the convenience in our lives and also increased our day to day output. VANET is also a wireless network & has tremendous impact on the area of inter-vehicle communication i.e. V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure) communication & VANET. VANET are self-organized networks built up from fast moving vehicles. VANET is also part of MANET and like it, it is also based on multi-hop relaying but high mobility of nodes, frequent network partition, restraints on roadways etc. impose high technical tests to implement a high performance in VANET. VANET is a vehicle-to-vehicle or vehicle-to- road side units (RSU) network style that can deployed lacking relying on network infrastructure. The promising applications and cost effectiveness of VANETs constitute major encouragement behind growing interest in such networks [1]. Topological structure of VANET is extra dynamic when compared to MANET, where an end-to-end connection is usually assumed. Vehicular Networks are frequently disconnected depending upon vehicles density & speed of the nodes. The movement of vehicles is restricted on the layout of roads, which renders many topological holes in the network. These features make the classical MANET routing algorithms such as AODV & GPSR are inefficient for vehicular networks [2]. These protocols do not solve the problems caused by the high speed vehicles & radio obstacles as well.

II. RELATED WORK

Rifaqat Hussain et al., 2012 [3] In this paper, they put forth the classification of VANET based on cloud computing. It was, to the best of information, the first effort to define VANET Cloud architecture. Moreover they have divided VANET clouds into three architectural outlines named Vehicular Clouds, Automobiles using Clouds, and Hybrid Vehicular Clouds. They also outline the unique security and privacy subjects and research experiments in VANET clouds. Baldini Gianmarco et al., 2013 [4] Examined the application of individuality based cryptographic scheme in particular, signature schemes to provide better security and discretion for VANET. Along with an exhibition of the state-of-the-art in this zone, this paper present a safety framework for car-to-car VANETs based on a protocol for the distributed group of signing keys that overcome key escrow issues. Li Wenjia et al., 2015 [5] An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks Planned trust management subject is appropriate to a wide range of VANET applications to progress traffic safety, mobility, & recyclable protection with heightened trustworthiness. Wei, Wei, et al., 2013 [6] Distributed systems without trusted identities were particularly vulnerable to Sybil attacks, where an adversary creates multiple bogus identities to compromise the running of the system. They presented Sybil Defender, a Sybil defense mechanism that leverages the network topologies to defend against Sybil attacks in social networks. Based on performing a limited number of random walks within the social

graphs, Sybil Defender is efficient and scalable to large social network .results of our facebook application show that the assumption made by previous work that all the relationships in social networks are trusted does not apply to online social networks, and it is feasible to limit the number of attack edges in online social networks by relationship rating.

III. NEEDS OF VANET

There are various needs of VANET such as:

- Lack of connectivity: There is need of connectivity between the fast moving vehicles as there is disconnection on high speed of vehicles.
- Fast communication: There is need of fast data communication while travelling ranging from safety to non-safety.
- Safety: There is need of safety on roads while travelling & to keep track of predecessor & the succeeding nodes to avoid accidents and track of their movement on the roads. This will help in the proper safety on roads related to driving.
- Infotainment: This consist of all sorts of activities related to other than security such as online gaming, data sharing related to music and other kind of activities in the day to day life.

IV. APPLICATIONS OF VANET

The two main applications of VANET are [7-9] :-

- Safety: These include those issues that are directly related to safety of passengers and drivers. These mainly include cooperative driving, accident avoidance, etc.
- Non-Safety: These are those issues which are directly related to entertainment and information. These mainly include traffic information, toll service, internet access, games, entertainment etc.

V. VANET ARCHITECTURE

A VANET system architecture consists of different domains and many individual components as depicted in Figure1 [10].

A. In-vehicle domain

This consists of an on-board unit (OBU) & one or extra application units (AU) inside a vehicle. AU executes a set of applications utilizing the communication capability of the OBU. An OBU is at least equipped by a (short range) wireless communication expedient dedicated for road safety, and potentially with other optional communication devices (for safety and non-safety communications). The distinction between AU & OBU is logical; they can also exist in a single physical unit [11].

B. Ad hoc domain

An ad hoc domain is composed of vehicles equipped with OBUs & road-side units (RSUs), forming the VANET. OBUs form a mobile ad hoc system which allows communications among nodes without the need for a centralized coordination instance. OBUs openly communicate if wireless connectivity exists among them; other multi-hop communications are used to forward data.

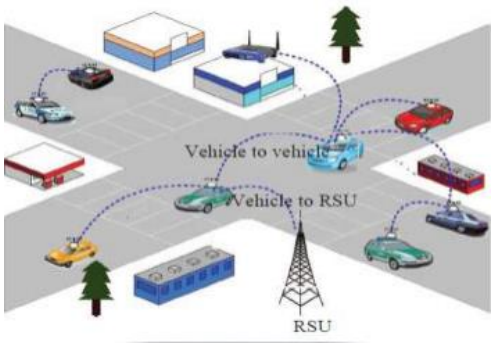

Figure 1 VANET system architecture

C. Vehicle to broadbandcloud Communication

It means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G. As the broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

VI. TOPOLOGY BASED ROUTING

Several VANET routing protocols have used topology based routing method. Topology based routing protocols use link's information inside the network to send the data packets from source to destination [12]. Topology based routing approach can be further categorized into three groups:

1. Proactive routing
2. Reactive routing
3. Hybrid routing

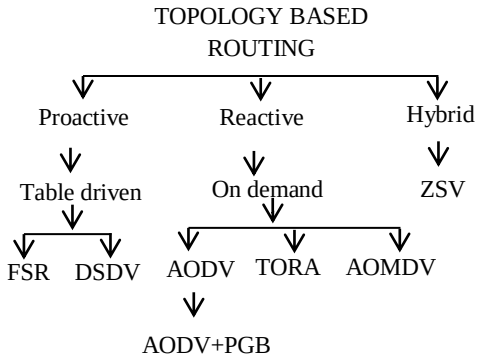

Figure 2 Topology based Routing

1. Proactive Routing:

Proactive routing protocols are mostly based on shortest path procedures. They keep information of all associated nodes in form of tables because these protocols are tabling based [13]. Furthermore, these tables are also shared with their neighbors. When any change occurs in network topology, each node updates its routing table. Strategies implemented in proactive algorithms are Link-state routing (e.g. OLSR) and distance-vector routing (e.g. DSDV). The working particulars for

proactive routing protocols are as follow: Destination Sequence Distance Vector Routing (DSDV) use Distance Vector shortest path routing algorithm, it provides loop open single path to the destination. DSDV sends 2 types of packets - full dump and incremental. In full dump packets, all the routing information is send while in incremental simply updates are send. It reduces bandwidth utilization by sending only updates instead of complete routing information.

Optimized link state routing (OLSR) maintains routing information by sending link state information. After every change in the topology every node sends updates to choosy nodes. By doing so, every node in the network receive updates only formerly. Unselected packets cannot re-transmit updates; they can only read updated information.

2. Reactive Routing:

On demand or reactive routing protocols were designed in such a manner to overcome the overhead that was generated by proactive routing protocols. This is over-come by maintaining only those routes that are currently active [14]. Routes are discovered and maintained for only those nodes that are presently being used to drive data packets from source to destination. Route discovery in reactive routing can be done by sending RREQ (Route Request) from a node when it requires a route to send the data to a specific destination. After sending RREQ, node then delays for the RREP (Route Reply) and if it does not receive any RREP within a specified time period, source node assumes that either route is not obtainable or route expired. When RREQ reaches the particular destination and if source node receives RREP then by using unicasting, information is furthered to the source node in order to ensure that route is obtainable for communication. Reactive routing can be classified either as source routing or hop-by-hop routing. In source routing complete route information from source to destination is involved in data packets. When these data packets are forwarded to other intermediate nodes in the network, every node takes route information from the data packet & stores it in the header of data packet.

3. Hybrid routing:

Hybrid routing protocol combine the advantages of both proactive and reactive approaches. In hybrid protocols, the network is divided into two levels. The inner layer is proactive, which maintains and updates information on routing between all nodes of a givennetwork at all times. Route updates are periodically performed regardless of network load, bandwidth constraints, and network size. Inner layer comprises easy to-maintain routes, where a routing table is maintained, whereas the outer layer is reactive, the route is determined on need basis. Thus, if a node wishes to initiate communication with another host to which it has no route, a global-search procedure is employed [15].

VII. CONCLUSION

In this paper, we have investigated the pros and cons of different routing protocols for inter-vehicle communication in VANET. By studying different routing protocol in VANET we have seen that further performance evaluation is required to verify performance of a routing protocol with other routing protocols based on various traffic scenarios. Comparison can be done among the routing protocols in the Overlay and so on. Proactive approaches for routing have the overhead of maintaining the routing table containing the information of all the nodes in the network and sharing it among the nodes, which reduces the usable bandwidth. On the contrary, reactive approaches discover the routes between the nodes that are communicating on-demand and hence less overhead of route maintenance is there in such approaches.

VIII. REFERENCES

[1]. Toor, Y., Muhlethaler, P., Laouiti, A and Fortelle, A., "Vehicular ad hoc networks: Applications and related technical issues," IEEE Commun. Surveys Tutorials, vol. 10, no. 3, pp. 74-88, 3rd Quarter, 2008.

[2]. Karp and Kung, H., "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. MpbiCom, pp.243-254, 2000.

[3]. Hussain, Rifaqat, et al., "Rethinking vehicular communications: Merging VANET with cloud computing." Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on.IEEE, 2012.

[4]. Baldini, Gianmarco, et al., "Identity-based security systems for vehicular ad-hoc networks." Connected Vehicles and Expo (ICCVE), 2013 International Conference on.IEEE, 2013.

[5]. Li, Wenjia and Houbing Song. "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks."IEEE Transaction, 2015.

[6]. Wei, Wei, et al., "SybilDefender: a defense mechanism for Sybil attacks in large social networks." Parallel and Distributed Systems, IEEE Transactions on 24.12 (2013): 2492-2502.

[7]. Xu, Q., Mark, T., Ko, J and Sengupta, R., "Vehicle-to-vehicle Safety Messing in DSRC," in proceedings of VANET, October 2004.

[8]. Yang, X., Lie, J., Zhao, J and Vaidya, N., "A Vehicle –to-Vehicle Communication Protocols for Cooperative Collision Warning,''Int'lConf. On Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004), Aug. 2004.

[9]. Yin, J., Eibatt, T., Yeung, G., Ryu, S. B., Habermas, Krishnan, H., and Talty, T., "Performance Evaluation of Safety Applications over DSRC Vehicular Ad hoc Networks," in Proceedings of VANET, October 2004.

[10]. Daniel Jiang ―IEEE 802.11p: towards an international standard for wireless access in vehicular environments‖, Vehicular Technology Conference, May 2008, pp.2036-2040

[11]. Festag, A., Noecker, G., Strassberger, M.,Lübke, A., Bochow, B., Torrent-Moreno, M.,Schnaufer, S.,Eigner, R., Catrinescu, C., and Kunisch, J., Now - Network on Wheels: Project Objectives, Technology and Achievements. In Proceedings of 6th International Workshop on Intelligent Transportation (WIT 2008), Hamburg, Germany, Mar 2008.

[12]. Abolhasan, M., Wysocki, t and Dutkiewicz, E., ―A review of routing protocols for mobile ad hoc networks‖, Ad Hoc Networks 2 , 2004 , pp. 1–22.

[13]. Mauve, M., Widmer, A., and Hartenstein, H., ―A survey on positionbased routing in mobile ad hoc networks,‖ Network, IEEE, vol. 15, no. 6, pp. 30 - 39, Nov/Dec 2001.
[14]. N. H; Tony Larsson, ―Routing Protocols in Wireless Ad Hoc Networks- A Simulation Study‖ Department Of Computer Science and Electrical Engineering, Luleå University of Technology, Stockholm, 1998.
[15]. Haas, Z. J and Pearlman, M. R., ―The performance of query control schemes for the zone routing protocol‖, IEEE/ACM Trans. Netw. 9, 4 (Aug. 2001), pp. 427-438.