QoS Realization for Routing Protocols in VANETs and Issues in Deployment

Venuprea[#1], Vansh Kaushal[#2], Surjeet[#3]

[1,2,3] Bharati Vidyapeeth's College of Engineering
New Delhi, India

Abstract* — Vehicular Ad Hoc Networks (VANETs), a subclass of Mobile Ad Hoc Networks (MANETs), are a promising approach in the development of Intelligent Transportation System (ITS). They are distinguished from other ad hoc networks by their hybrid network architectures, node movement characteristics and new applications. Due to the dynamic characteristics in vehicular environment, efficient routing remains a significant challenge in these networks. The objective of this paper is to present an overview of the important layers used in routing and desirable network parameters for VANETs. Comparative discussion of standard single-layer routing protocols is done in context of gaining superior performance. The respective taxonomy of major issues and challenges to routing for all vehicular applications is described.

Keywords — *QoS, routing protocols, VANETs, V2I, V2V.*

I. Introduction

Wireless networks [1] are computer networks that establish wireless data connections using electromagnetic radio waves between network nodes for communication. Wireless networking is a method by which homes, telecommunications networks and business installations avoid the cost of introducing cables in a building, or as a connection between different equipment locations. These are of two types as shown in Fig. 1: Infrastructure-based networks that use special nodes called Access Points (APs) which are wired to a backbone network and communicate wirelessly with other connected mobile nodes like WiFi and cellular networks. Ad hoc or infrastructure-less networks [2] where each node communicates wirelessly with each other temporarily without the aid of a fixed access point. They are usually used in cases where deployment of infrastructure is costly or not feasible. Such types of networks include Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs) and Static Ad Hoc Networks (SANETs).

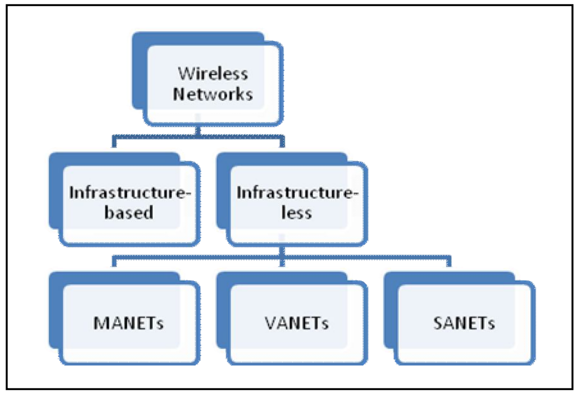


Fig. 1 Types of Wireless networks

MANETs [3] are an autonomous collection of wireless mobile nodes such as smart phones, laptops, PDAs etc. organized in a mesh topology. They employ wireless communication wherein each node participates as a source, destination or as an intermediate node to forward messages from its previous node. Since each node has a limited range, transmission takes place using multiple hops through intermediate nodes acting as routers as shown in Fig. 2. Major characteristics of MANETs include: autonomous mobile terminals, distributed operation, dynamic network topology due to arbitrary node movement and fluctuating link capacity.

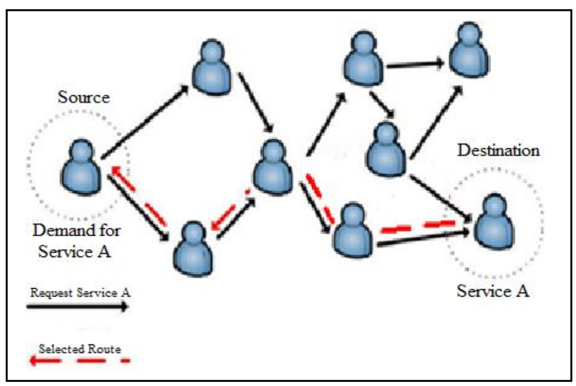


Fig. 2 Selection of route in MANETs

VANETs [4] are specialized form of MANETs under which vehicles are equipped with wireless transceivers to enable communication. They turn participating cars into wireless routers or nodes creating a wide range dynamic network. As cars fall out of the signal range and drop out of the network, other cars can join in maintaining a continuous network. A major application of VANETs is in the Intelligent Transportation System (ITS) [5] for cooperative traffic management, traffic monitoring, controlling traffic flows, blind crossing, prevention of collision etc. They provide abundant on-board infotainment services such as 3G access ensuring real time storage capacity and high processing power. Vehicles can communicate detour, traffic accident and congestion information with nearby vehicles early to reduce traffic jams near the affected areas. Other applications include [6] support in work of public services such as police, ambulance and other emergency units, road safety provisions like traffic services, alarm and warning messages and obtaining real time news, traffic updates and weather reports. Applications such as safety messaging are near-space applications, where vehicles in close proximity exchange status information to increase safety awareness. In contrast, applications such as traffic and congestion monitoring require collecting information from vehicles that span multiple kilometers.

VANETs use hybrid architecture [5] of WLAN/Cellular networks combined with ad hoc networks. They have fixed infrastructure gateways or access points called Road Side Units (RSUs) at traffic intersections connected to the Internet to gather routing information. Each vehicle has communication devices and Global Positioning System (GPS) receiver on the On-Board Units (OBUs) [7]. They support three type of communication as shown in Fig. 3: Vehicle to Vehicle (V2V), RSU to Vehicle (I2V) and RSU to RSU (I2I). The network nodes are limited to road topology while moving. If the road information like congestion, traffic, accident, detour etc. is available, one will be able to predict the future position of a node. Nodes support significant computing, communication and sensing capabilities as well as maintain a continuous transmission power to sustain these functions.

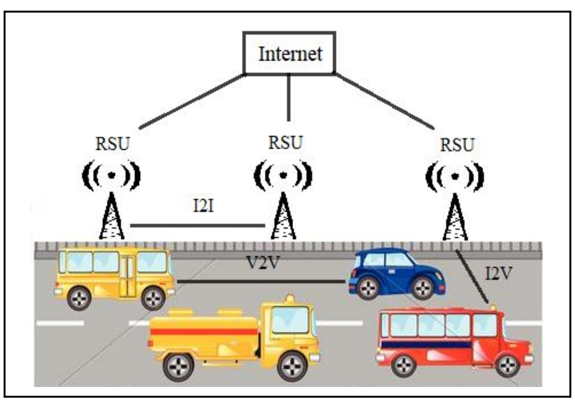


Fig. 3 System architecture of VANETs

In spite of varied applications, routing in VANETs [6] remains a significant challenge. Due to a highly dynamic topology, the underlying connectivity capabilities change rapidly, collected routing information becomes stale (route failure) and established communication routes become invalid in a short time. The resulting disruption of information flow causes considerable delays and route reconstruction depleting a significant amount of network resources.

VANETs support wireless communication for more customized and complete information exchange between vehicles. They have the ability to make roads safer especially in conditions considered hazardous and unavoidable like fog, black ice, accidents etc. Most of the infotainment applications have rigid requirements in terms of delivery delay and throughput. Vehicular networks are fast moving and highly dynamic due to which received information is short lived and requires quick action to ascertain reliability. Due to difference in architecture and characteristics, routing protocols of MANETs, when applied to VANETs result in poor route convergence, low communication throughput and frequent route disruptions. In spite of having huge potential to address safety and efficiency issues, these networks have not been able to attract commercial interest. In this context, this paper highlights basics of wireless networking and examines all single-layer routing protocols. The issues and challenges ahead in routing like mobility, scalability, distributed operation etc. are discussed.

The remaining paper is structured as follows: Section 2 talks about motivation for efficient deployment, Section 3 presents all the layers used in routing and discusses the important ones like the Data Link Layer and Network Layer in detail. Section 4 focuses on prevalent issues and challenges to efficient routing. This paper is concluded in Section 5.

II. MOTIVATION

Efficient deployment of VANETs helps develop a safer transportation system. This is guaranteed by quality of links that depends on network parameters such as:

Throughput: It is the maximum data rate that a network allows to be passed successfully through it in a specified period of time typically measured in bits per second (bps) [8].
End to end delay: It refers to the time taken for a packet to be transmitted across a network from the source to the destination [9].
Jitter: It is defined as the variation in the delay of received packets due to network congestion, improper queuing or configuration errors. [9].
Packet delivery ratio: It is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been initially transmitted by the sender [1].

Quality of Service (QoS) refers to the capability of a network to provide better service performance for selected network traffic in varied applications. Although a significant amount of work has been done on VANETs, most of the initially designed protocols involved in actual communication like Dynamic Source Routing (DSR), Ad Hoc On Demand Distance Vector (AODV) etc. consider only factors like minimum cost or minimum hop count [10] for route establishment ignoring all other QoS parameters. Therefore much scope of research still lies in areas of reliable routing.

III. LAYERS USED FOR ROUTING

Routing protocols are decomposed into layers [11] in order to reduce their complexity. Each layer has a particular abstract behaviour for use by the next layer in the model developed on the basis of the behaviour of its previous layer. The three lower layers of the OSI model namely Physical layer, Data link layer and Network layer are used for routing in Ad hoc networks.

Physical layer deals with the bit-level transmission between different devices and supports electrical and mechanical interfaces connecting to the medium for synchronized communication [12]. It provides the hardware means for sending and receiving data on a carrier, including cards, connectors, broadcast frequencies, modulation schemes and other low-level parameters dealing with the physical aspects of routing only. It is usually considered while developing cross-layer designs for stable route determination and hence has not been considered as a separate unit in this paper.

A. Data link layer

Data Link Layer [1] is one of the most important layers of the network model with complex functionalities and liabilities. It hides the details of the underlying hardware and represents itself to the upper layer as a medium for reliable data transfer as shown in Fig. 4. It performs several important functions such as error control, flow control, addressing, framing and medium access control. It consists of two sub layers namely: Logical Link Control (LLC) and Medium Access Control (MAC).

1) Logical link control

LLC provides physical medium independent data link layer services to the network layer [12]. It adds the Destination Service Access Point (DSAP) and the Source Service Access Point (SSAP) labels to each packet it receives from the network layer. The SAP's identify the application/users involved in the data transfer. It provides three types of services namely: unacknowledged connectionless service (LLC type 1 or LLC1 service), connection-oriented service (LLC type 2 or LLC2 service) and acknowledged connectionless service (LLC type 3 or LLC3 service).

2) Medium access control

MAC directly interfaces with the physical layer [13]. It provides services such as addressing, framing and medium access control. In many networking situations, several nodes must share the same physical transmission media. The link layer protocol has the responsibility to ensure that all the competing users of a shared resource successfully complete their transmissions. Multiple access link control is considered to be the most important service of the MAC layer. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The protocol may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit-switched or channelization-based channel access method is used. Various protocols like ALOHA, Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) and Carrier Sense Multiple Access/Collision Detection (CSMA/CD) have been developed for the purpose.

ALOHA – It was born out of the need for interconnecting terminals [14]. The original was referred to as pure ALOHA while the extended version which doubled the throughput of the system is known as slotted ALOHA. In the former, a user transmits whenever data is ready for transmission. If more than one user transmits simultaneously, the transmitted packets end up getting collided and are lost. The latter reduces the probability of collisions by having the nodes transmit in a synchronized fashion. It requires the channel to be divided in

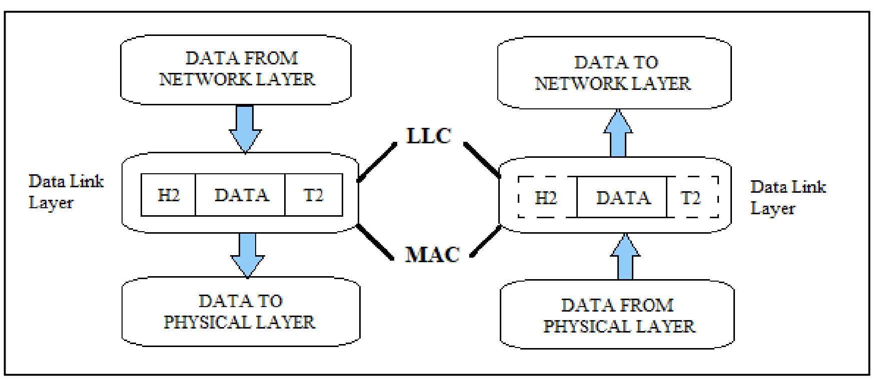


Fig. 4 Data link layer interfacing

time into discrete interval/slots and the node doesn't transmit as soon as a packet becomes ready for transmission.

CSMA/CD – In CSMA/CD, [15] the nodes, apart from sensing the channel, are also capable of detecting collisions in the channel. The moment a node detects a collision, it aborts its current transmission thereby saving time and bandwidth. It then transmits a brief jamming signal heard by all other nodes to stop any simultaneous transmission. The node waits for a random period of time and then restarts the process. A collision can be detected by comparing the power or pulse width of the received signal with that of the received signal.

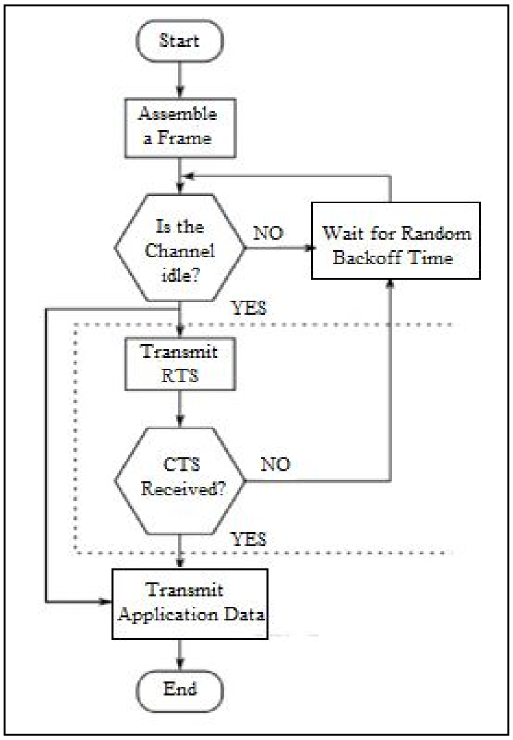


Fig. 5 Flow chart for CSMA/CA

CSMA/CA – It is a network multiple access method [16] in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle" as shown in Fig. 5.

Collision Avoidance: If another node was heard, the transmitting node waits for a random period of time for a free communication channel. When they do transmit, nodes send packet data in its entirety. It is particularly important for wireless networks, where the collision detection is unreliable due to the hidden node problem. Under ideal propagation conditions, Direct-Sequence Spread Spectrum (DSSS) provides the highest throughput for all nodes on a network when used with CSMA/CA.

Transmission: If the medium was identified as being clear, the node sends a Request To Send (RTS) signal. Upon receiving a Clear To Send (CTS) signal, it sends the frame in its entirety. The node awaits receipt of an acknowledgement packet from the access point to indicate the packet was received and check-summed correctly. If such an acknowledgement does not arrive in a timely manner, it is assumed that the packet collided with some other transmission, causing the node to enter a period of binary exponential back off prior to attempting to re-transmit.

B. Network layer

Network layer provides the means of transferring variable length network packets from a source to destination host via one or more networks using identifiable unique IP addresses [17]. It responds to service requests from the transport layer and issues service requests to the data link layer as shown in Fig. 6. It determines the best path according to network metrics like minimum hop count to a particular destination and then routes data accordingly. Special protocols [18] are used at the network layer to allow devices that are logically connected, or are trying to route traffic, to exchange information about the status of hosts.

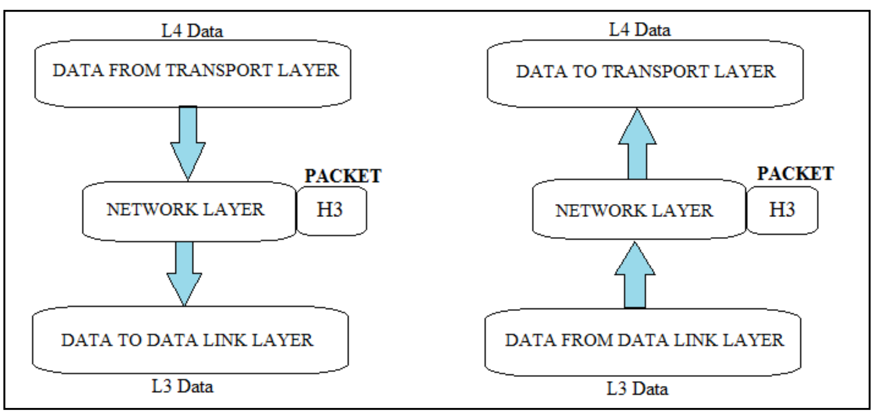


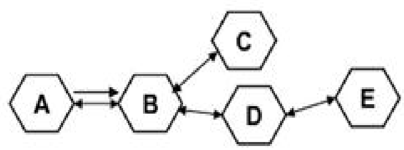
Fig. 6 Network layer interfacing

Based on the routing information update mechanism the network protocols can be divided as follows: Table-Driven (Proactive) or On-Demand (Reactive) [19].

1) Table-driven routing protocols

These protocols [20] are extensions of the wired network routing protocols. They maintain the global topology information in the form of tables at every node which are updated frequently in order to maintain consistent and accurate state information. Some of the standard proactive protocols are: Destination Sequence Distance Vector (DSDV) and Optimized Link State Routing (OLSR).

DSDV protocol [21] has nodes that maintain a table that contains the shortest distance and the first node on the shortest path to every other node in the network. Routes to all nodes are readily available at every node at all times that are updated at regular intervals. It incorporates table updates that are propagated throughout the network with an increasing sequence number tag to prevent loops, to counter the count-to-infinity problem and for faster convergence. For example as shown in Fig. 7, for a source node A communicating with destination E, the routing table holds destination as E, next hop as B and cost i.e. minimum hop count as 3.



Dest.	Next Hop	Cost	Seq. No.
E	B	3	60

Routing table for node A

Fig. 7 Route establishment in DSDV

OLSR is a proactive routing protocol [22] that employs an efficient link state packet forwarding mechanism. It optimizes the pure link state by reducing the size of control packets by declaring only a subset of the links during updates and by reducing the number of links that are used for forwarding. All the nodes elect group of nodes as Multipoint Relays (MPRs) which only broadcast the routing table as shown in Fig. 8. It does not generate any other control packet when a link is added or broken.

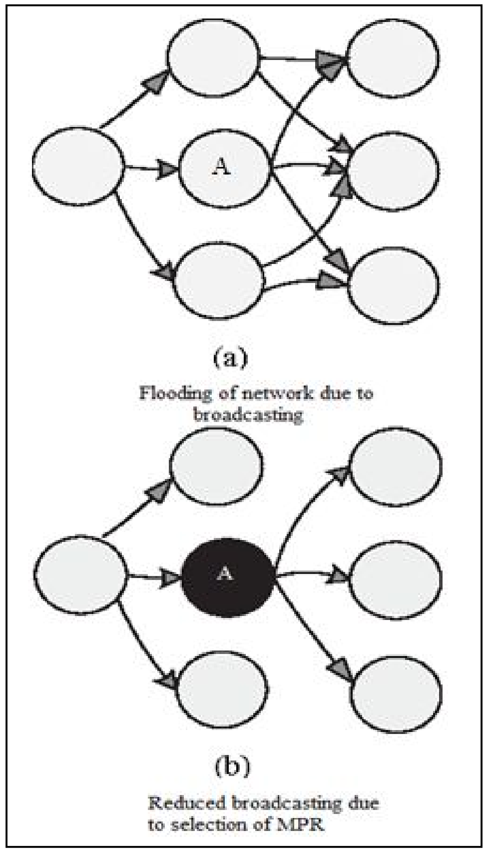


Fig. 8 Reduction in broadcasts using OLSR

Proactive protocols [23] are restricted to small network sizes due to availability of information of only neighbouring nodes and lack of knowledge for all other distant ones. With an increase in network size, the complexity and the processing overheads for the routing table increase decreasing system performance. Waiting for table update messages lead to excessive delay and stale information in the vehicular system.

2) On-demand routing protocols

On-demand routing protocols [19] execute the path-finding process and exchange information only when a path is required by a node to communicate with a destination. Ad Hoc On demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) are examples of some standard reactive protocols.

AODV [24] establishes routes when required by the system. It employs the concept of DSDV of using destination sequence numbers to identify the most recent path. The source node and the intermediate nodes store the next hop information corresponding to each flow for data packet transmissions. The source node floods the network with Route Request (RREQ) packets and may receive more than one route in the Route Reply (RREP). It then uses the destination sequence number to determine the up-to- date path for the destination as shown in Fig. 9. A HELLO message is used to maintain link

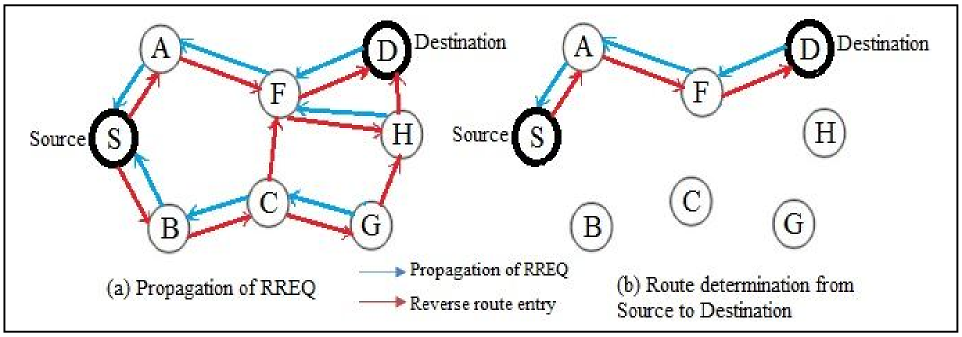


Fig. 9 AODV routing protocol

connectivity of the active route. The system broadcasts a Request Error (RERR) packet for broken links and repair actions. These maybe generated by a node or forwarded when received from any node.

DSR [25] is designed to restrict the bandwidth consumed by the control packets by eliminating periodic table update messages. It is beacon-less and does not require periodic hello packets to inform neighbouring nodes of each other's presence. The basic approach to establish a route is by flooding of Route Request (RREQ) packets by the source which is responded by the Route Reply (RREP) packets by the destination. The RREP carries the route between the source and destination to be used for communication as shown in Fig. 10. The control overhead is directly proportional to this path length making it inefficient for use in large networks.

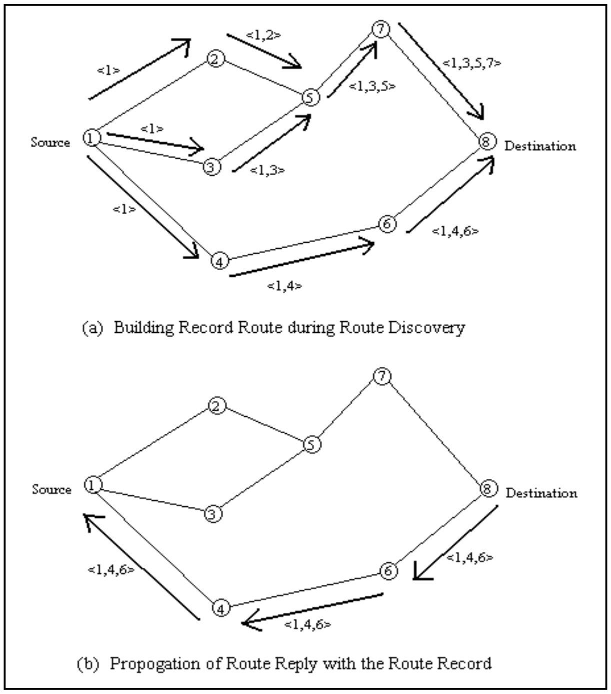


Fig. 10 Route determination using DSR

Reactive protocols [23] extend to large networks with reduced bandwidth wastage because of on-demand route establishment and faster operation making them a better alternative for effective routing in VANETs. However, they suffer high route determining latency and lack the ability to provide QoS parameters like delay, jitter, packet delivery ratio and throughput as demanded by the nodes or category of calls. This makes them inefficient for supporting differentiated classes of service.

IV. ISSUES AND CHALLENGES

VANETs are fundamentally different to MANETs in terms of special mobility patterns and rapidly changing topology in a large network [6]. Routing protocols of MANETs when applied to VANETs, lead to frequent route failures, poor throughput and less stable route formation due to this difference in architecture. The need for a robust protocol is strongly dependent on the dynamic characteristics. Efficient routing therefore continues to be a significant problem in this regard faced by the following challenges:

Mobility: The network topology is highly dynamic due to continuous movement of nodes [26]; hence an on-going session suffers frequent path breaks, packet collisions, transient loops, stale routing-information and difficulty in resource reservation. Disruption occurs due to the movement of intermediate or end nodes. Since such situations do not arise in reliable wired links, wired network routing protocols cannot be used in ad hoc networks with changing topologies. Effective and efficient mobility management is difficult to achieve.

Distributed operation: Ad hoc networks do not have centralized coordinators [2]. VANETs operate in environments where no centralized coordination is possible due to continuous movement and need large bandwidth. Therefore, nodes need to be scheduled in a distributed fashion for gaining access via exchange of control information with minimum overhead.

Bandwidth constraint: In a wireless network, the radio band is limited [27] and offers less data rates than wired network. This requires the routing protocol to use the bandwidth optimally by keeping the overhead as low as possible and maintaining the topology information. Since the channel is shared by all nodes in the broadcast region the bandwidth available per wireless link depends on the number of nodes and the traffic they handle. Thus only a fraction of the total bandwidth is available for each node.

Location-dependent contention: Load on wireless channel varies with the number of nodes present in a geographical region [28]. This makes the contention for a channel high when the number of nodes increases resulting in a number of collisions and subsequent wastage of bandwidth. Developing a routing protocol with mechanisms for uniform distribution of network load is needed.

Scalability: It is the ability of the routing protocol to perform efficiently in a network with a large number of nodes [4]. This requires minimization of control overheads and adaptation of the routing protocol to the network size.

Self-Organization: Wireless network activities like neighbour discovery, topology maintenance etc. [2] require the network to be able to organize and maintain itself. During network discovery, every node gathers and maintains information of its neighbours by periodic exchange of update information in the form of small packets called beacons. Topology maintenance requires the network to update topology information with respect to changes like node failure, depletion of power sources etc.

Security and Privacy: Lack of central coordination and shared wireless medium [29] makes VANETs more vulnerable to attacks than wired networks. These may include denial of service, consumption of scarce resources, host impersonation, information disclosure etc. This is mainly because of malicious nodes gaining access to data due to shared broadcast radio channel, insecure operating environment, lack of central points like routers and base stations, limited availability of resources and physical vulnerability of nodes to damage and theft.

Route reconstruction: Mobility of nodes causes frequent link failures [30], leading to dropping of source data packets. This reduces the packet delivery ratio. Potential mobility-induced link breaks generate a need to recover and reconfigure system nodes quickly for use in highly dynamic environments.

V. CONCLUSION

VANETs have promising applications in the Intelligent Transportation System (ITS). The design of efficient routing protocols in this regard is necessary and important. Due to difference in network architecture and dynamicity, the protocols for MANETs fail to satisfy the requirements of VANETs. In this investigation, various single-layer routing protocols are considered with focus on effective data transmission. The key challenges to establish a routing protocol with low communication delay, low overhead and minimum time complexity are discussed.

REFERENCES

[1] B. Forouzan and S. Fegan, *Data Communication and Networking*, 4th Edition, 2006.

[2] C. S. R. Murthy and B. S. Manoj, *Ad hoc Wireless Networks,* 1st Edition, 2007.

[3] N. Raza, M. Aftab, M. Akbar, O. Ashraf and M. Irfan, "Mobile Ad-Hoc Networks Applications and Its Challenges", *Scientific Research Publishing Communications and Network*, vol. 8, no. 6, pp. 131-136, Aug. 2016.

[4] A. Saha and D. Johnson, "Modelling Mobility for Vehicular Ad hoc Networks", *ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, pp.91-92, Oct. 2004.

[5] F. Li and Y. Wang, "Routing in Vehicular Ad Hoc Networks: A Survey", *IEEE Vehicular Technology Magazine*, vol. 7, no. 2, pp. 1556-6072, June 2007.

[6] K. Hussain, A. Awang, N. Kamel and S. Aissa, "Routing in Vehicular Ad-Hoc Networks: A Survey on Single and Cross-layer Design Techniques and Perspectives", *IEEE Access,* vol. 5, no. 3, pp: 9497-9517, Apr. 2017.

[7] S. Glass, I. Mahgoub and M. Rathod, "Leveraging MANET based Cooperative Cache Discovery Techniques in VANETs: A Survey and Analysis", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2640-2661, May 2017.

[8] S. Ullah, M. Chen, K. S. Kwak, "Throughput and Delay Analysis of IEEE 802.15.6-based CSMA/CA Protocol", *Journal of Medical Systems*, vol. 36, no. 6, pp. 3875-91, Dec. 2012.

[9] J. He, L. Cai, J. Pan and P. Cheng, "Delay Analysis and Routing for Two-Dimensional VANETs Using Carry-and-Forward Mechanism", *IEEE Transactions on Mobile Computing,* vol. 16, no. 7, pp. 1830 – 1841, July 2017.

[10] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in sparse vehicular ad hoc wireless networks", *IEEE Journal on Selected Areas in Communications,* vol. 25, no. 8, pp. 1538–1556, Nov. 2007.

[11] F. Behrouz and M. Firouz, *Computer Networks: A Top Down Approach*, 1st Edition, 2012.

[12] J. Zhu, Y. Zou and B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks", *IEEE Access*, vol. 5, pp. 5313-5320, Apr. 2017.

[13] L. L. Peterson and B. S. Davie, *Computer Networks: A Systems Approach*, 3rd Edition, 2007.

[14] *R. Ma, V. Mishra and D. Rubenstein,* "An Analysis of Generalized Slotted-Aloha Protocols", *IEEE/ACM Transactions on Networking*, vol. 17, no. 3, pp. 936-949, June 2009.

[15] [15] S. Xuejan and Z. Naitong, "Performance analysis of the dynamic CSMA/CD protocol in a wireless channel", *Journal of Systems Engineering and Electronics*, vol. 14, no. 3, pp. 28-32. Sept. 2003.

[16] R. laufer and L. Kleinrock, "The Capacity of Wireless CSMA/CA Networks", *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1518-1532, June 2016.

[17] [17] J. Jeong, S. Guo, Y. Gu, T. He and D. Du, "Trajectory-based data forwarding for light-traffic vehicular ad hoc networks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 743–757, Mar. 2011.

[18] A. Abdrabou and W. Zhuang, "Probabilistic delay control and road side unit placement for vehicular ad hoc networks with disrupted connectivity", *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 129–139, Jan. 2011.

[19] [19] P. Syal and T. Kaur, "A Study of Routing Protocols for Vehicular Ad-Hoc Networks", *International Journal of Engineering Trends and Technology (IJETT),* vol. 15, no. 1, Sep. 2014.

[20] S. Panichpapiboon and W. Pattara-Atikom, "A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks", *IEEE Communication Surveys Tutorials*, vol. 14, no. 3, pp. 784–798, Oct. 2012.

[21] A. Kaur, "Mobility model based performance analysis of DSDV mobile ad hoc routing protocol", *Recent Advances and Innovations in Engineering* (ICRAIE), May 2014.

[22] J. Toutouh, J. Nieto and E. Alba, "Intelligent OLSR Routing Protocol Optimization for VANETs", *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1884-1894, May 2012.

[23] M. Faezipour, M.Nourani, A. Saeed and S.Addepalli, "Progress and challenges in intelligent vehicle area networks", *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, Feb. 2012.

[24] R. Shorey, A. Ananda, M. Chan and W. Ooi, *Routing Algorithms for EnergyEfficient Reliable Packet Delivery in Multihop Wireless Network*, 1st Edition, 2007.

[25] V. Frias, G. Delgado, A. Ayala and M. Igartua, "MM-DSR: Multipath QoS routing for multiple multimedia sources over Ad Hoc mobile networks", *IEEE Latin America Transactions*, vol. 5, no. 6, pp. 448-456, Oct. 2007.

[26] J. Harri, F. Filali and C. Bonnet, "Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy", *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 19-41, Dec. 2009.

[27] C. Wu, X. Chen, Y. Ji, T. Kato and S. Ohzahata, "Efficient Broadcasting in VANETs Using Dynamic Backbone and Network Coding", *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp: 634-651, Nov. 2016.

[28] N. Taherkhani and S. Pierre, "Centralized and Localized Data Congestion Control Strategy for Vehicular Ad Hoc Networks Using a Machine Learning Clustering Algorithm", *IEEE Transactions on Intelligent Transportation System*, vol. 17, no. 11, pp. 3275-3285, Nov. 2016.

[29] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks", *Communication Systems and Networks*, July 2011.

[30] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato and Y. Nemoto, "A Stable Routing Protocol to Support ITS Services in VANET Networks", *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp: 3337-3347, Nov. 2007.