QOS IN GEOCAST ROUTING FOR VANETS

***Indradeep Verma, ** Dr. Prashant Singh**

**Research Scholar, Dr. K N Modi University, Rajasthan, INDIA*
&
Asstt. Prof, Deptt. of Computer Science & Engineering, GNCT, Greater Noida, INDIA
***Prof. & Head, Deptt. of Information Technology, Northern India Engineering College, New Delhi, INDIA*

ABSTRACT

In this article we are to be able understand Quality of Services of Vehicle Ad-Hoc Network with various factors like Congestion, jitter, etc.

KEYWORDS: *VANET, QoS (Quality of Services), Network, Geocast Routing*

1. INTRODUCTION

Network over computer (voice or data network) is a telecommunications network which allows computers to transfer information. In computer networks, networked enabled devices transmit information with each other along network nodes (data connections). The connections between network enabled device nodes are established using either wired media or wireless media. The best-known computer network is the Internet.

Network enabled computer devices that originate, route and terminate the data packets are called network nodes can include nodes such as personal telephones, computers, client & servers as well as networking hardware. Two such devices can be said to be networked together when any device is able to exchange data and information with the other device, whether or not they have a direct or routed connection to each other.

Computer networks provides the knowledge of transmission media used to carry their signals, the communications protocols to optimize network traffic, the network's area area based on size, topology and organizational intent. In most cases, communications protocols are layered (OSI Model) on other more specific or more general transmissions protocols, except for the physical layer that directly deals with the communication media.

Computer networks support an anonym's number of applications such as access to the WWW, video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as others.

1.1 Network Types

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Storage Area Network (SAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)

2. GEOGRAPHIC ROUTING

Geographic Routing (also called geo-routing or position-based routing): is a steering principle that relies on geographic location information. It is mostly proposed for wireless networks and based on the design that the source sends a message to the geographic place of the destination in its place of using the network address. The idea of using spot information for routing was primarily proposed in the 1980's in the vicinity of packet radio networks and interconnection networks. Geographic routing requires that every one node can determine its own location and that the resource is aware of the spot of the destination. With this kind of information a message can be routed to the destination point without the knowledge of network topology or the prior route detection.

There are a mixture of approaches, such as single-path, multi-path and flooding-based approaches. The majority of single-path strategies rely on two techniques: Greedy forwarding and Face routing technique. Greedy forwarding attempt to bring the message get closer to the destination in every step using only restricted information. Thus, each node forwards the significant message to the neighbor that is most appropriate from a local point of observation. The most suitable neighbor can be the single, who minimizes the distance to the destination in apiece step (Greedy). On the other hand, one can consider another concept of progress, that is the projected remoteness on the source-destination-line (MFR, NFP), or the minimum angle among neighbor and destination (Compass Routing). Not all of these strategies are loop-free, i.e. a message can travel among nodes in a assured constellation. It is known that the essential greedy strategy and MFR are loop free, while NFP and Compass Routing are not of this kind [3,5].

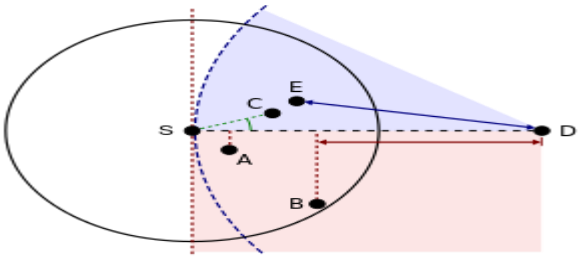

Figure 1.3: Greedy Forwarding.

Greedy forwarding alternatives are the source node (S) has different choices to discover a relay node for auxiliary forwarding a message to the destination (D). A = adjacent with Forwarding Progress (NFP), B = Most Forwarding evolution within Radius (MFR), C = Compass Routing, E = Greedy

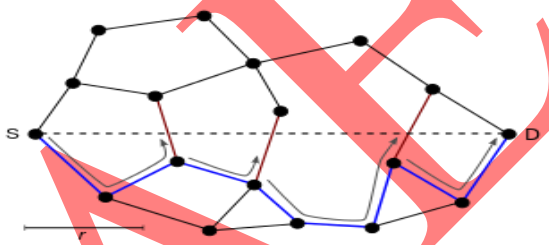

Figure 1.4: Greedy Face Routing

Face Routing: A message is routed along the core of the steps of the communication chart, with the steps changes at the edges crossing the S-D-line (red). The concluding routing path is exposed in blue.

Greedy forwarding can escort into a dead end, where there is rejection neighbor closer to the destination. Then, face routing assists us to recover from this situation and discover a path to another node, where Greedy forwarding can be recommenced. A revival strategy such as face routing is necessary to guarantee that a message can be delivered to the destination. The amalgamation of greedy forwarding and face routing was first proposed in 1999 under the middle name GFG (Greedy-Face-Greedy). It assures the delivery in the so-called unit disk graph network model. Various alternatives, which were proposed later, in addition for non-unit disk graphs, are based on the ideology of GFG [2, 4].

Even though originally developed as a routing design that uses the substantial positions of each node, geographic routing algorithms have as well been applied to networks in which everyone node is associated with a spot in a virtual space, unconnected to its physical position.

The process of decision a set of virtual positions designed for the nodes of a network such that geographic routing using these locations is guaranteed to succeed is called Greedy Embedding.

3. QUALITY OF SERVICES (QoS)

Quality of service (QoS) measures the overall performance of a computer network, predominantly the performance seen by the clients of the network.

To quantitatively measure the quality of service, several connected aspects of the network service are frequently considered, such as error rates, bit rate, throughput, transmission delay, availability, jitter, etc.

Quality of service (QoS) is mostly significant for the transport of network traffic with unusual requirements. Many technologies has been developed to permit the computer networks to become as functional as telephone networks for audio conversations, over and above supporting new applications with even stricter service demands.

In the telephony field, Quality of service (QoS) was defined by the ITU in 1994. Quality of Service includes requirements on every one aspect of a connection, like service response time, loss of packets, signal-to-noise ratio, crosstalk, echo, interrupts, frequency rejoinder, loudness levels, and so on. A division of telephony QoS is the Grade of Service (GoS) requirements, which include aspects of a link relating to the capacity and coverage of a network, for example certain maximum blocking probability and outage prospect.

In the ground of computer networking and additional packet-switched telecommunication networks, the traffic engineering expression refers to resource reservation control mechanisms moderately than the accomplish service quality. Quality of service is the capability to provide different precedence to different applications, users, or data flows, or to guarantee a assured level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be certain. Quality of service agreement are important if the network capacity is inadequate, particularly for real-time streaming multimedia applications for instance voice over IP, online games and IP-TV, since these frequently require fixed bit rate and are holdup sensitive, and in networks where the capability is a limited resource, for example in cellular data communication.

Protocols that support QoS may agree on a network traffic contract with the application software and reserve competence in the network nodes, for example throughout a session establishment phase. Throughout the session it may monitor the accomplish level of performance, for example the data transfer rate and delay, dynamically control scheduling

priorities in the network nodes. It may discharge the reserved capacity during a slash down phase.

A best-effort service provider does not support quality of service. Any substitute to complex QoS control mechanisms is to offer high quality communication over a best-effort network by over provisioning the capacity; as a result it is sufficient for the predictable peak network traffic load. The resulting nonappearance of network congestion reduces the need for QoS mechanisms.

QoS is sometimes have alternative definitions, rather than referring to the ability to reserve resources. Quality of service sometimes refers to the intensity of quality of service, i.e. the assured service quality. High QoS is frequently confused with a high rank of performance or achieved service quality, for example elevated bit rate, near to the ground latency and low bit error probability.

An unusual and disputable characterization of QoS is the service used especially in application layer for telephony and streaming video is the requirement on a metric that replicate or predicts the subjectively experienced quality. In this situation, QoS is the tolerable cumulative effect on subscriber fulfillment of all imperfections distressing the service. Other terms with comparable meaning are the quality of experience (QoE) subjective business concept, the necessary "user perceived performance", the necessary "degree of satisfaction of the user" or the targeted "number of happy customers". Examples of procedures and measurement methods are mean opinion score (MOS), perceptual speech quality measure(PSQM) and perceptual evaluation of video quality (PEVQ).

3.1 History

Usually internet routers and LAN switches operate on a greatest effort root. These equipments are less costly, less complex and much faster, thus more acceptable than competing more compound technologies that provided QoS mechanisms. There are four "Type of service" bits and three "Precedence" bits provided in each IP packet header, but they were not usually appreciated. These bits were afterward re-defined as Differentiated services code points (DSCP).

A number of efforts for layer 2 technologies that insert QoS tags to the data have expanded popularity in the past. Examples are frame relay, Asynchronous Transfer Mode (ATM) and Multiprotocol Label Switching (MPLS). In spite of these network technologies remaining in use today, this kind of network vanished attention after the arrival of Ethernet networks. Today Ethernet is the most popular in layer 2 technology. Ethernet uses 802.1p to signal the precedence of a frame.

3.2 Qualities of Traffic

In packet-switched networks technology, quality of service is influenced by a variety of factors, which can be separated into "human" and "technical" factors. Human factors include: constancy of service, availability of service, delays, client information. Technical factors include: reliability, effectiveness, scalability, grade of service, maintainability etc.

Many things can turn out with the packets as they travel from source to destination, ensuing in the following problems as seen from the point of view of the correspondent and receiver:

3.3 Low Throughput

Due to unstable load from different users sharing the same network resources, the bit rate (the maximum throughput) that can be supplied to an assured data stream may be excessively low for real time multimedia services if all data streams acquire the same scheduling priority.

3.4 Dropped Packets

The routers may fail to deliver some packets if their data loads are tainted, or the packets reach your destination when the router buffers are already full. The accepting application may inquire for this information to be retransmitted, probably causing severe delays in the general transmission.

3.5 Errors

Occasionally packets are corrupted due to bit errors source by noise and interference, particularly in wireless communications and extensive copper wires. The receiver has to sense this and, just as if the packet was dropped, may inquire for this information to be retransmitted.

3.6 Latency

It may take a long time for every packet to arrive at its destination, because it gets held up in stretched queues, or it obtain a less direct route to keep away from congestion. This is unusual from throughput, as the delay can put up over time, even if the throughput is approximately normal. In some cases, too much latency can leave an application such as VoIP or online gaming unusable.

3.7 Jitter

Packets from the source will arrive at the destination with dissimilar delays. A packet's delay differs with its position in the line of the routers all along the path between source and destination and this position can differ unpredictably. This discrepancy in delay is known as jitter and can dangerously affect the quality of streaming audio or video.

3.8 Out of Order Delivery

When a compilation of connected packets is routed through a network, unlike packets may take different routes, each received in a different delay. Resultant is that the packets reach your destination in a different order as they were sent. This setback requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state, once they reach their destination. This is primarily important for video and VoIP streams where quality is dramatically affected by both latency and lack of sequence.

4. QOS IN VANETs

VANETs are dispersed, self organizing link webs skilled up from traveling around vehicles, and are consequently demarcated by tremendously eminent speed and controlled degrees of liberty in nodes movement prototype. Such particular features frequently times create average networking protocols incompetent or unusable in VANETs, and this, joined besides the giant encounter that the contract of VANET technologies could have on the automotive marketplace, it clarify the generated manipulation in the development of link protocols that are explicit to vehicular networks. The honest believed of VANET is straight forward: seize the broadly adopted and inexpensive wireless natural span web (WLAN) knowledge that connects notebook computers to every single complementary and the Internet, and, beside an insufficient squeeze, installed on the vehicles. Of sequence, if it were honestly that unambiguous, the vigilant. VANET scrutiny area should credibly not ever have formed. Vehicular environment produced exceptional opportunities, trials, and requirements. If vehicles can undeviatingly contrary alongside every single supplementary and next to groundwork, a mutually new prototype for vehicle protection requests can be generted. Even supplementary non-safety requests can elevate road and vehicle efficiency. Second, new trials are vessel by elevated vehicle speeds and exceedingly pulsating working environments. Third, new necessities, essential by new shelter of life proposition, have a new outlook for eminent packet transfer rates and low packet latency. Further, client contract and governmental lapses hold extremely elevated potential of privacy and security. Even now a day’s, vehicles fabricate and examine colossal numbers of data, even however usually this data is self-collected inside an introverted vehicle. With a VANET, the ‘horizon of awareness’ for the vehicle or driver radically grows. The VANET contact can be completed undeviatingly among

vehicles as 'one-hop' contact, or vehicles can retransmit memos, thereby enabling 'multi-hop' communication. To raise coverage or toughness of contact, communicate at the roadside can be deployed. Roadside foundation can additionally be utilized as an entrance to the Internet and, therefore, data and context data can be collectively, stored and processed somewhere e.g., in Cloud infrastructures. The earth of vehicular appeal and inter-networking technologies is well-known on an interdisciplinary authority in the cross serving of contact and networking, automotive electronics, road process and involvement, data and capability provisioning. VANET can consequently be supposed as a very important portion of intelligent transportation arrangements (ITS). Vehicular Ad-Hoc Web (VANET) contact has presently come to be gradually more accepted scrutiny case in the extent of wireless networking as well as the automotive manufacturing industries. The goal of VANET scrutiny is to expand a vehicular contact agreement to enable quick and cost-efficient allotment of data for the benefit of passengers, protection and console. VANETs need particular networking methods alongside practicability and performance

5. DOUBTS ABOUT QUALITY OF SERVICE OVER IP

The internet-2 mission establishes, in 2001, that the QoS protocols were almost certainly not deployable within its Abilene Network with the equipment available at that time. Equipment accessible at that time relied on software to execute QoS. The crowd also predicted that "logistical, financial, and organizational blockade will block the way toward every bandwidth guarantees" by protocol modifications intended at QoS. They believed that the financial side would support network providers to deliberately eat away at the quality of best effort traffic as a way to thrust customers to higher cost QoS services. Instead they projected over-provisioning of capacity as much cost-effective at that time.

Abilene network study was the base for the testimony of Gary Bachula to the US Senate Commerce Committee's investigation on Network Neutrality in near the beginning of 2006. He uttered the opinion that adding additional bandwidth was more effective than any of the other various schemes for completing QoS they examined.

Bachula's testimony has been mentioned by proponents of a regulation banning quality of service as proof that no rightful purpose is dish up by such an offering. This argument is reliant on the hypothesis that over-provisioning is not a form of QoS and that it is constantly possible. Cost and other factors influence the ability of carriers to construct and maintain lastingly on over-provisioned networks.

6. REFERENCES

1. Ali, S., & Bilal, S. (2009). An intelligent routing protocol for VANETs in city environments. In Proceedings of 2nd international conference on computer, control and communication, IC4 2009 (pp. 1–5), February 2009.

2. Balon, N. (2006). Introduction to vehicular ad hoc networks and the broadcast storm problem. http://www.csie.ntpu. edu.tw/~yschen/course/96-2/Wireless/papers/broadcast-5.pdf (accessed: May 29, 2010).

3. Basagni, S., Chlamtac, I., Syrotiuk, V., & Woodward, B. (1998). A distance routing effect algorithm for mobility (DREAM). In Proceedings of ACM international conference on mobile computing and networking (pp. 76–84), Dallas, TX, October 1998.

4. Bickel, G. (2008). Inter/intra-vehicle wireless communication. http://userfs.cec.wustl.edu/~gsb1/index.html#toc (accessed: May 29, 2010).

5. Biswas, S., Tatchikou, R., & Dion, F. (2006). Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. IEEE Communication Magazine, 44(1), 74–82.

6. Blum, J., & Eskandarian, A. (2006). Fast, robust message forwarding for inter-vehicle communication networks. In Proceedings of IEEE intelligent transportation systems conference (ITSC'06) (pp. 1418–1423).

7. Festag, A. (2009). Global standardization of network and transport protocols for ITS with 5 GHz radio technologies. In Proceedings of the ETSI TC ITS workshop, Sophia Antipolis, France, February 2009.

8. Füßler, H., Mauve, M., Hartenstein, H., Käsemann, M., & Vollmer, D. (2002). A comparison of routing strategies for vehicular ad hoc networks (Technical report, TR-02-003). Department of Computer Science, University of Mannheim, July 2002.

9. Gerlach, M. (2006). Full paper: assessing and improving privacy in VANETs. www.network-on-wheels.de/downloads/ escar2006gerlach.pdf (accessed: May 29, 2010).

10. Harsch, C., Festag, A., & Papadimitratos, P. (2007). Secure position-based routing for VANETs. In Proceedings of IEEE 66th vehicular technology conference (VTC-2007), Fall 2007

11. Harsch, C., Festag, A., & Papadimitratos, P. (2007). Secure position-based routing for VANETs. In Proceedings of IEEE 66th vehicular technology conference, VTC-2007, Fall 2007 (pp. 26–30), Baltimore, September 2007.

12. Hartenstein, H. (2001). Position-aware ad hoc wireless networks for inter-vehicle communications: the fleetnet project. In Proceedings of the 2nd ACM international symposium on mobile ad hoc networking & computing, Long Beach, CA.

13. IEEE Standard 1455-1999 (1999). IEEE standard for message sets for vehicle/roadside communications (pp. 1–130).

14. IEEE Standard 1609.1-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments (WAVE)—resource manager (pp. 1–63).

15. IEEE Standard 1609.2-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments—security services for applications and management messages (pp. 1–105).

16. IEEE Standard 1609.3-2007 (2007). IEEE trial-use standard for wireless access in vehicular environments (WAVE)—networking services (pp. 1–87).

17. IEEE Standard 1609.4-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments (WAVE)—multichannel operation (pp. 1–74).

18. IEEE Standard 802.11 (2007). IEEE Std. 802.11-2007, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications.

19. IEEE Standard 802.16-2004 (2004). IEEE standard for local and metropolitan area networks, part 16: air interface for fixed broadband wireless access systems. Vehicular ad hoc networks (VANETS): status, results, and challenges

20. Jiang, D., & Delgrossi, L. (2008). IEEE 802.11p: towards an international standard for wireless access in vehicular environments. In Proceedings of 67th IEEE vehicular technology conference on vehicular technology (pp. 2036–2040), May 2008.

21. Jinyuan, S., Chi, Z., & Yuguang, F. (2007). An ID-based framework achieving privacy and non-repudiation. In Proceedings of IEEE vehicular ad hoc networks, military communications conference (MILCOM 2007) (pp. 1–7), October 2007.

22. Karp, B., & Kung, H. (2000). Greedy perimeter stateless routing for wireless networks. In Proceedings of ACM international conference on mobile computing and networking (MobiCom 2000) (pp. 243–254), Boston, MA, August 2000.

23. Kudoh, Y. (2004). DSRC standards for multiple applications. In Proceedings of 11th world congress on ITS, Nagoya, Japan.

24. Leontiadis, I., & Mascolo, C. (2007). GeOpps: geographical opportunistic routing for vehicular networks. In Proceedings of IEEE international symposium on world of wireless, mobile and multimedia networks (WoWMoM 2007), Helsinki, Finland, 2007.

25. Mohandas, B., & Liscano, R. (2008). IP address configuration in VANET using centralized DHCP. In Proceedings of 33rd IEEE conference on local computer networks, Montreal, Canada, October 2008.

26. Naumov, V., & Gross, T. (2007). Connectivity-aware routing (CAR) in vehicular ad-hoc networks. In Proceedings of 26th IEEE international conference on computer communications, Infocom 2007, Anchorage, Alaska, 2007.

27. Notice of proposed rulemaking and order FCC 02-302. Federal Communications Commission, November 2002.

28. Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

29. Stampoulis, A., & Chai, Z. (2007). A survey of security in vehicular networks. http://zoo.cs.yale.edu/~ams257/projects/ wireless-survey.pdf (accessed: May 29, 2010).

30. Standard specification for telecommunications and information exchange between roadside and vehicle systems—5 GHz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications. ASTM E2213-03, September 2003.

31. Sun, S., Kim, J., Jung, Y., & Kim, K. (2009). Zone-based greedy perimeter stateless routing for VANET. In Proceedings of international conference on information networking, ICOIN 2009

32. Yang, K., Ou, S., Chen, H., & He, J. (2007). A multihop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular networks. IEEE Transactions on Vehicular Technology, 56(6), 3358–3370.

33. Yin, J., Elbatt, T., & Habermas, S. (2004). Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In Proceedings of VANET'04, Philadelphia, PA, USA, October 2004.

34. Yu, D., & Ko, Y.-B. (2009). FFRDV: fastest-ferry routing in DTN-enabled vehicular ad hoc networks. In Proceedings of 11th international conference on advanced communication technology (Vol. 2, pp. 1410–1414), February 2009.