International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Review on Various Approaches for Designing of VANET Scenario

Namit Aggarwal[1], Manasvi Mannan[2]

[1]Punjab College of Engineering Technology, Lalru (Punjab), Electronics & Communication Engineering

[2]Assistant Professor, Punjab College of Engineering and Technology, Lalru (Punjab)

Abstract: ***In this paper various techniques studied and how to use for VANET. VANET is extension of MANET that deals with vehicles for communication of auto driven system. In this approach the nodes have been approved as vehicles that connected to read side units available in the communication area. RSU available are concerned for transmission of information about traffic density, collision, position & speed of the nodes. The RSU transmit the safety message over the communication range for reliable communication by avoiding collision b/w he nodes. Various protocols had been utilized for reliable communication & transmission of safety message.***

Keywords: VANET, Delay, Bandwidth, Intermediates nodes & hopes, AODV, DSR for communication bandwidth nodes

1. Introduction

1.1 Ad-Hoc networks are the autonomous systems consist of mobiles nodes that communicate with each other using wireless communication. Here a node can be a PDA, a laptop, a mobile phone or another communication device with some characteristics that are limited storage capacity, bandwidth and battery power. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. [1] [3]

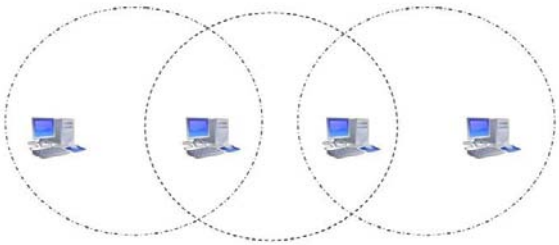


Figure 1.1: Ad hoc networks with four nodes

Ad hoc network do not have any pre-existing infrastructure. They are self-organized, self-configured, and self-controlled networks. This type of network can be set up or deployed anywhere and anytime because it poses very simple setup and no or minimal central administration. The network is characterized by the absence of central administration devices such as base stations or access points.

Furthermore, nodes are free to move independently in any direction, and therefore will change its links to other devices frequently. The primary challenge in building a wireless ad hoc network is to equipping each device to continuously maintain the information required to properly route traffic. This means if link breakages occur the network has to stay operational by building new routes.

Security: It is imperative that information cannot be inserted or modified by a malicious person. Someone classify attackers as having three dimensions: "insider versus outsider", "malicious versus rational", and "active versus passive". The types of attacks against messages, can be described as follows: "Bogus Information", "Cheating with Positioning Information", "ID disclosure", "Denial of Service", and "Masquerade". The reliability of a system where information is gathered and shared among entities in a VANET raises concerns about data authenticity. For example, a sender coul misrepresent observations to gain advantage (e.g., a vehicle falsely reports that its desired road is jammed with traffic, thereby encouraging others to avoid this route by changing route and providing a less congested trip).

There are various threats in VANET like threats to availability, threats to authenticity, threats to confidentiality. These threats include denial of service attack, malware attack, spamming, black hole attack, masquerading, reply-back attack, GPS spoofing, tunneling, position faking attack.

1.2 VANET

VEHICULAR ad hoc networks (VANETs) are expected to support a large spectrum of mobile distributed applications that range from traffic alert dissemination and dynamic route planning to context-aware advertisement and file sharing. Considering the large number of nodes that participate in these networks and their high mobility, debates still exist about the feasibility of applications that use end-to-end multichip communication. Wireless ad hoc networks have the characteristic to be infrastructure-less and do not depend on fixed infrastructure for communication and dissemination of information. The architecture of VANET consists of three categories: Pure cellular/WLAN, Pure Ad hoc and hybrid. VANET may use fixed cellular gateways and WLAN/WiMax access points at traffic intersections to connect to the internet, gather traffic information or for routing purposes. This network architecture is called pure cellular or WLAN. VANET

can comprise of both cellular network and WLAN to form a network. Stationery or fixed gateways around the road sides also provides connectivity to vehicles. In such a scenario all vehicles and road side devices form pure mobile ad hoc networks. Hybrid architecture consists of both infrastructure networks and ad hoc networks together. No centralized authority is required in VANET as nodes can self organize and self manage the information in a distributed fashion. Since the nodes are mobile so data transmission is less reliable and sub optimal.

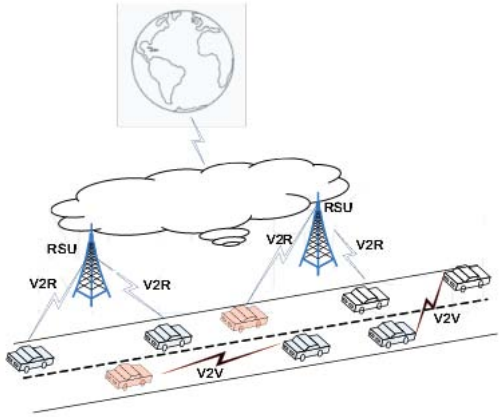


Figure 1.2: VPN architecture

2. Approaches Used in Face Recognition

2.1 DSRC

The primary motivation for deploying DSRC is to enable collision prevention applications. These applications depend on frequent data exchanges among vehicles, and between vehicles and roadside infrastructure DSRC, which is a candidate for use in a VANET, is a short to medium range communication service that supports both public safety and private communication. The communication environment of DSRC is both vehicle-to-vehicle and vehicle-to/from-roadside. The VANET aims to provide a high data rate and at the same time minimize latency within a relatively small communication zone Dedicated Short-Range Communication (DSRC) is a standard that aims to bring vehicular networks to North America. Traffic fatalities have been a long standing problem in the United States, as in the rest of the world. As an indication of the severity of the problem, in 1999 there were 6,279,000 motor vehicle accidents that accounted for 41,611 deaths in the United States [12]. In 1991, the US Congress passed the Intermodal Surface Transportation Efficiency Act of 1991 that resulted in the creation the first generation of Intelligent Transportation System (ITS). The goal of the ITS program is to incorporate technology into the transportation infrastructure to improve safety. The first generation of the Dedicated [7]

2.2 MAC

Media Access Control protocols such as TDMA, FDMA, or CDMA are difficult to implement for VANET. For any of these protocols to be used either time-slot, channels, or codes need to be dynamically allocated, which requires synchronization that is difficult to achieve in a network where the nodes have a high degree of mobility. The objective of the media access control layer is to arbitrate the access to the shared medium, which in this case is the wireless channel. If no method is used to coordinate the transmission of data, then a large number of collisions would occur and the data that is transmitted would be lost. The ideal scenario is a MAC that prevents nodes within transmission range of each other from transmitting at the same time, thus preventing collisions from occurring. Equally important, the media access control must be fair, efficient, and provide the ability to prioritize traffic. Another obstacle restricting the wide-spread adoption of vehicular ad hoc networks is that is based on the wireless protocol IEEE 802.11, that was designed for networks with different characteristics than a VANET. A large focus of the 802.11 standards has been on wireless LANs. The majority of the 802.11 protocols are designed around the fact that a centralized controller is present in the network, the access point (AP). In vehicular ad hoc networks the use of an AP is limited to situation where a RSU is present. In a WLAN communication tends to be point-to-point. On the other hand, a large portion of the communication in a VANET is broadcast in nature. For these reasons, some modifications to the 802.11 protocols are necessary. The purpose of the MAC sublayer is to establish rules for accessing the common medium so that it can be shared efficiently and fairly among a set of STAs. The IEEE 802.11 rules fall into two categories: the session-based rules that define steps a STA must take before it is allowed to communicate information on behalf of Layer 3, and the frame by frame rules governing an individual transmission. The IEEE 802.11p amendment makes significant changes to the session-based rules, while using the frame-by-frame rules as defined in the baseline IEEE 802.11 standard. [4]

2.3 CSMA

The term “Carrier Sense” signifies the capability of the terminal to listen to the channel and find out whether it is busy or not. At first sight it seems that with CSMA one can succeed in avoiding collisions altogether. Indeed, if all terminals transmit their packets only when the channel is not busy and pick a random retransmission time if they find the channel busy, then it seems that a collision will occur only when two or more terminals begin transmission simultaneously, an event that is quite unlikely. However, the situation is not as rosy as it seems, due to the finite time it takes for a signal to propagate from one terminal to another. The modified CSMA system, whose principles of operation were described above, comes by the name CSMA/CA, where CA stands for Collision Avoidance. The acronym signifies that collisions are soughtto be avoided and not that they are avoided altogether. Due to the retransmission policy of the CSMA system, collisions that may occur are not detrimental: in case of collision, the ACK message or RTS CTS messages will not be received and the transmitting terminal will defer its transmission for a later time. However, if the propagation delays are relatively large and the system is heavily loaded, collisions may degrade the performance of the system.[1]

2.4 MACA

MACA does not make use of carrier-sensing for channel access. It uses two additional signaling packets: the Request-To-Send (RTS) packet and the Clear-To-Send (CTS) packet. When a node wants to transmit data packet, it first transmits an RTS packet. The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet. Once the sender receives the CTS packet without any error, it starts transmitting the data packet. If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back-off for a random interval of time before retrying. In the BEB mechanism each time a collision is detected, the node doubles its maximum back-off window. Neighbor nodes near the sender that hear the RTS packet do not transmit for a long enough period of time so that the sender could receive the CTS packet. Both the RTS and the CTS packets carry the expected duration of the data packet transmission. A node the receiver, upon hearing the CTS packet, defers its transmission till the receiver receives the data packet. Thus, MACA overcomes the hidden terminal problem. Similarly, a node receiving an RTS defers only for a short period of time till the sender could receive the CTS. If the node hears NO CTS during its waiting period, it is free to transmit packets once the waiting interval is over. Thus a node that hears only the RTS packet is free to transmit simultaneously when the sender of the RTS is transmitting data packets. Hence the exposed terminal problem is also overcome in MACA.[1]

3. Literature Survey

Katrin (2011) et al. in the paper "How Severe is the Hidden Terminal Problem in VANETs when Using CSMA and STDMA?" propose a definition of the hidden terminal problem suitable for broadcast transmissions and proceed with a case study to find how the packet reception probability is affected by the presence of hidden terminals. Two different medium access control methods; carrier sense multiple access (CSMA) from IEEE 802.11p and self-organizing time division multiple access (STDMA), are subject of investigation through computer simulations of a highway scenario with a Nakagami fading channel model. The results reveal that the presence of hidden terminals does not significantly affect the performance of the two MAC protocols. STDMA shows a higher packet reception probability for all settings due to the synchronized packet transmissions.[6]

John (2011) in the paper "Dedicated Short-Range Communications (DSRC) Standards in the United States" explains the content and status of the DSRC standards being developed for deployment in the United States. Included in the discussion is the IEEE 802.11p amendment for wireless access in vehicular environments (WAVE), the IEEE 1609.2, 1609.3, and 1609.4 standards for Security, Network Services and Multi-Channel Operation, the SAE J2735 Message Set Dictionary, and the emerging SAE J2945.1 Communication Minimum Performance Requirements standard. The paper shows how these standards fit together to provide a comprehensive solution for DSRC. Most of the key standards are either recently published or expected to be completed in the coming year. A reader will gain a thorough understanding of DSRC technology for vehicular communication, including insights into why specific technical solutions are being adopted, and key challenges remaining for successful DSRC deployment. The U.S. Department of Transportation is planning to decide in 2013 whether to require DSRC equipment in new vehicles.[7]

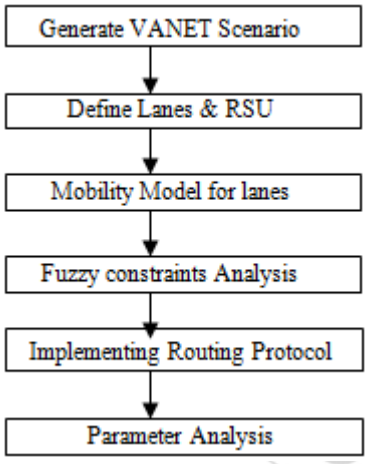
Mohammad (2008) et al. in the paper "Reliable Inter-Vehicle Communications for Vehicular Ad Hoc Networks" propose an alternative solution, based on retransmissions, to ensure the reliable delivery of safety messages. They argue that the specific characteristics inherent in VANETs, such as the limited density of vehicles, anticipated bandwidth and the tolerable delay, allow us to deploy a retransmission strategy. Furthermore, they prove that their proposed scheme establishes fair channel access for the consecutive retransmission opportunities of contending neighbors. Simulation results confirm that our heuristic method dramatically improves the probability of reception of safety messages regarding conventional methods. Safety message exchange is the most prevalent part of inter vehicular communications which is crucial for enhancing safety and efficiency in transportation networks. Moreover, since the dissemination of safety messages directly influences our lives, their reliable delivery is of great importance. Most packet collisions in VANETs occur due to hidden nodes. In unicast communications a two-way handshaking is performed prior to the actual transmission in order to alleviate the hidden node problem. However, this procedure congests the network with a lot of overhead in case of broadcast, which is the dominant mode of communication in VANETs.[9]

Yousefi (2007) et al. in the paper "Performance of beacon safety message dissemination in Vehicular Ad hoc Networks (VANETs)" investigate the feasibility of deploying safety applications based on beacon message dissemination through extensive simulation study and pay special attention to the safety requirements. Vehicles are supposed to issue these messages periodically to announce to other vehicles their current situation and use received messages for preventing possible unsafe situations. They evaluate the performance of a single-hop dissemination protocol while taking into account the quality of service (QoS) metrics like delivery rate and delay. They realize that reliability is the main concern in beacon message dissemination. Thus, a new metric named effective range is defined which gives us more accurate facility for evaluating QoS in safety applications specifically. Then, in order to improve the performance, the effects of three parameters including vehicle's transmission range, message transmission's interval time and message payload size are studied. Due to special characteristics of the safety applications, they model the relationship between communication-level QoS and application-level QoS and evaluate them for different classes of safety applications. As a conclusion, the current technology of IEEE 802.11 MAC layer has still some challenges for automatic safety applications but

it can provide acceptable QoS to driver assistance safety applications.[8]

Prabhakar et al. in the paper "Comparative Study of VANET and MANET Routing Protocols" presents the various protocols optimized for both the MANET and VANET. A protocol is analyzed from the existing reactive protocols which will be efficient for both the MANET and VANET. Mobile Ad-hoc Network (MANET) that is used to provide communications between nearby vehicles, and between vehicles and fixed infrastructure on the roadside. Though VANET is a type of MANET but the routing protocols of MANET are not feasible with VANET and if they are even feasible then they are not able to provide the optimum throughput required for a fast changing vehicular ad-hoc network. The difference between VANET and MANET is that in VANET, the nodes are moving on predefined roads, and their trails aren't too complicated and this is where the routing protocols have to be modified or changed. The differences in the architecture and characteristics have been studied in this paper to suggest the best out of the existing routing protocols.[10]

4. Proposed Work



Phase 1:
In this phase VANET scenario has been designed by defining numbers of vehicles, number of Lanes, Speed in a particular lanes & RSU position of the nodes. Various properties also have been described like Internet, MAC Types.

Phase 2:
In this phase fuzzy membership constrain has been evaluate for reliable communication. These constrains utilize different parameters like number of intermediate node, Number of hopes, Delay, Bandwidth, Probability of collision. After analysis of these parameters fuzzy rules have been evaluated that define which rules must follow.

Phase 3:
In this phase after using fuzzy rules various routing protocol have been used that work on the principle of fuzzy rules for reliable communication. At last various parameters like packet delivery ratio, packet loss, packet delay and throughput has been measured for performance evaluation.

5. Conclusion

In VANET on-demand/ Proactive protocol had been used for communication that computes the routing path dynamically at the time of transmission. Reactive protocol choose shortest path for communication but the shortest path does not guarantee of delivery of safety message. In the base paper other factor like Delay, probability of collision; Bandwidth had been considered to develop surgery construct rules for communication. This causes problem for communication due to selection of rules. To overcome this fuzzy constant must include number of intermediates nodes & number of hopes used for transmission of safety message. At last we got various types of parameters like Delay, Bandwidth, Intermediates nodes & hopes. On the basis of these parameters we conclude that our system gives us better results.

References

[1] Sharanappa P. H. and Mahabaleshwar S. K., "Performance Analysis of CSMA, MACA and MACAW Protocols for VANETs" International Journal of Future Computer and Communication, Vol. 3, No. 2, April 2014.
[2] Khalid Abdel Hafeez, Lian Zhao, Bobby Ma, Jon W. Mark, "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications" IEEE Transactions On Vehicular Technology, Vol. 62, No. 7, September 2013.
[3] Mahalle N.S., Deshmukh G.D., Raut A.S. and Totawar A.L. "A Dsrc Based Smartvanet Architecture", International Journal of Wireless Communication, Volume 2, Issue 2, 2012, pp.-35-37.
[4] Chan-Ki Park1, Min-Woo Ryu2, and Kuk-Hyun Cho, "Survey of MAC Protocols for Vehicular Ad Hoc Networks" Smart Computing Review, vol. 2, no. 4, August 2012.
[5] Saurabh D. Patil, D.V. Thombare, Vaishali D. Khairnar, "DEMO: Simulation of Realistic Mobility Model and Implementation of 802.11p (DSRC) for Vehicular Networks (VANET)" International Journal of Computer Applications, Volume 43–No.21, April 2012.
[6] Katrin Sjöberg, Elisabeth Uhlemann, and Erik G. Ström, "How Severe is the Hidden Terminal Problem in VANETs when Using CSMA and STDMA?" IEEE Vehicular Technology Conference (VTC Fall), pp. 1-5, 5-8 Sept. 2011.
[7] John B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States", Proceedings of the IEEE (Volume:99 , Issue: 7), pp. 1162 – 1182, July 2011.
[8] Yousefi Saleh, Fathy Mahmood, Benslimane Abderrahim, "Performance of beacon safety message dissemination in Vehicular Ad hoc Networks (VANETs)*" Journal of Zhejiang University SCIENCE A, 2007.

[9] Mohammad Nekoui and Hossein Pishro-Nik, "Reliable Inter-Vehicle Communications for Vehicular Ad Hoc Networks" *www.ecs.umass.edu/~nekoui/VINT-Nekoui-final.pdf*
[10] Prabhakar Ranjan, Kamal Kant Ahirwar, "Comparative Study of VANET and MANET Routing Protocols" *rgconferences.com/proceed/acct11/pdf/053.pdf*.
[11] Der-Jiunn Deng, Hsin-Chin Chen, Han-Chieh Chao, Yueh-Min Huang, "A Collision Alleviation Scheme for IEEE 802.11p VANETs" Wireless Pers Commun.
[12] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security 15 (2007) 39–68 39, IOS Press
[13] IEEE Draft Standard for Information Technology Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments, IEEE Std. 802.11, 2012.
[14] IEEE Standard for Information Technology—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Std. 802.11e-2005, Amendment to IEEE Std. 802.11.
[15] IEEE Standard for Wireless Access in Vehicular Environments(WAVE)—Multi-Channel Operation, IEEE Std. 1609.4, Feb. 2011.
[16] Draft Amendments for Wireless Access in Vehicular Environments(WAVE), IEEE P802.11p/D5.0, 2009.
[17] K. A. Hafeez, L. Zhao, L. Zaiyi, and B. N.-W. Ma, "The optimal radio propagation model in VANET," in Proc. 4th ICSNC, 2009, pp. 6–11.
[18] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks," in Proc. 1st ACM Int. Workshop Vehicular Ad Hoc Netw., 2004, pp. 10–18.
[19] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicleto- vehicle communication: Fair transmit power control for safety-critical information," IEEE Trans. Veh. Technol., vol. 58, no. 7, pp. 3684–3703,Sep. 2009.
[20] E. M. Vaneenennaam, W. Kleinwolterink, G. Karagiannis, and G. J.Heijenk, "Exploring the solution space of beaconing in VANETs," in Proc. 1st IEEE VNC, Tokyo, Japan, 2009, pp. 1–8.
[21] K. Bilstrup, E. Uhlemann, E. G. Strom, and U. Bilstrup, "Evaluation of the IEEE 802.11p MAC method for vehicle-to-vehicle communication," in Proc. IEEE 68th Veh. Technol. Conf., 2008, pp. 1–5.
[22] Z.Wang and M. Hassan, "How much of DSRC is available for non-safety use?" in Proc. 5th ACM Int. Workshop Veh. Inter-NETw., 2008, pp. 23–29.
[23] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535–547, Mar. 2000.
[24] D. X. Xu, T. Sakurai, and H. L. Vu, "An access delay model for IEEE 802.11e EDCA," IEEE Trans. Mobile Comput., vol. 8, no. 2, pp. 261– 275, Feb. 2009.
[25] J. Y. Lee and H. S. Lee, "A performance analysis model for IEEE 802.11e EDCA under saturation condition," IEEE Trans. Commun., vol. 57, no. 1, pp. 56–63, Jan. 2009.
[26] X. Ma and X. B. Chen, "Delay and broadcast reception rates of highway safety applications in vehicular ad hoc networks," in Proc. Mobile Netw. Veh. Environ., May 2007, pp. 85–90.
[27] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in Proc. IEEE Veh. Technol. Conf., 2007, pp. 2199–2203.
[28] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, "Modeling prioritized broadcasting in multichannel vehicular networks," IEEE Trans. VehTechnol., vol. 61, no. 2, pp. 687–701, Feb. 2012.