INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 6 June 2016.

A REVIEW ON THE VANET TRAFFIC CONGESTION METHODS

Gurjot Kaur[1], Upinderpal Singh[2],

CSE department, Chandigarh Engineering College, Landran, Mohali

kgurjot75@yahoo.in[1], cecm.cse.upinder@gmail.com[2]

Abstract: The vehicular ad-hoc networks (VANET) congestion control methods are utilized to minimize the traffic congestion across the busy squares or the roads. The vehicular clusters usually consist of the vehicular nodes and the road side units (RSU). The existing models based upon the traffic congestion control for VANETs have been critically studied for their drawbacks and shortcomings. Mainly, the existing models found working on the improvement of the shortcomings of the earlier congestion control schemes and worked towards removing them effectively. The effective queuing methods have been utilized for the traffic congestion control. The service queue (SQ) and control queue mechanisms have been utilized to curb the congestion problem in the VANETs. This has been observed primarily that the methods associated with the periodic updates (beacons) based method has been utilized to send the traffic on the expiry of time-interval to minimize the traffic congestion control. The multi-factor message similarity scanning has been utilized to avoid the flow of duplicate messages across the VANETs to minimize the traffic congestion. Also the Messages with hop-count 0 are also discarded to avoid the data loops to avoid congestion. For the improvement in the performance the dynamic priority tagging after determining the importance of the traffic inflows with message classification and path planning can be incorporated over the VANETs to decongest the networks in the proposed schemes. Also, the multilink traffic flow shaping based methods can be utilized to control the traffic congestion in the proposed solution.

Keywords: VANETs, traffic shaping, dynamic inflow shaping, traffic peak analysis, heavy load determination.

INTRODUCTION

The most beneficial advantage are improving the knowledge based real time traffic signaling system, reduced the vehicular emissions and improve the safety of the vehicles. The ambition of VANET is to establish a vehicular communication system to produce fast and cost effective delivery of the data for the passenger defense and relief. The vehicular ad hoc network becomes the important part for the future intelligent road

traffic management system. It provides the as many advantages as compared to the current traffic management systems.

The vehicular system builds up of huge number of nodes. This vehicular node will require an authority to conduct it. Each vehicular node can communicate with one another by using a short radio signal called DSRC (dedicated short range communication). This communication is the ad hoc communication in which the no wires required, the node can move freely. Road side unit (RSU) connects the vehicles with one another and other network devices as shown in the Figure1.1. Each vehicular node has an OBU (on board unit) which is responsible for connecting the node with the RSU through the DSRC signals and the device named TPD (Tamper Proof Device) which contains the info. Such as vehicle secrets, driver's identity, trip details, speed, route, information about the vehicle keys. VANET can be view as a self- governing system which can assign the traffic and emergency information to the nodes at a regular interval.

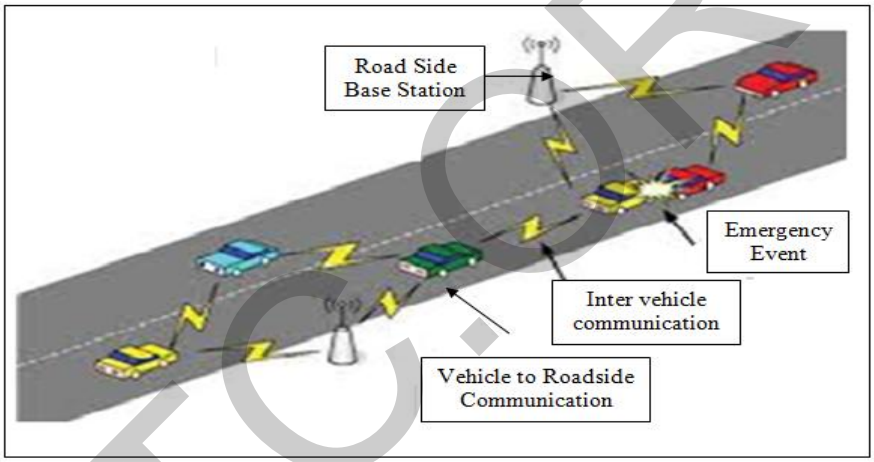

Figure 1.1: Vehicular Ad hoc network

The vehicular networks have a lot of advantages over the ordinary traditional wireless system like LTE, UMTS and Wi-MAX networks. The major advantages are less cost of maintenance and implementation, self-determining and self-organization. In future, the VANET becomes the practical application of MANET. The vehicles which have the wireless interface are interconnected with the vehicular network. The vehicles are able to produce the required power for the wireless communication. The VANET delay tolerant networks depend on the opportunistic contacts among the vehicular nodes to transmit the data in a store carry and forward DTN paradigm. It works as follows: the source node introduces a data bundle and stores in a form of constant storage until a communication event occur. The bundle may be onwards when the source node in contact with intermediary node which is responsible for bundle delivery.

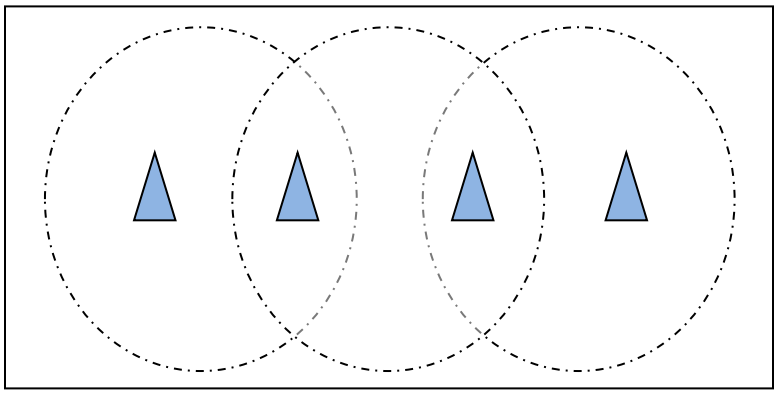

Figure 1.2: Ad hoc Network

The vehicular network is the self-configuring similar to the MANET. It is framework less network in which the mobile devices connected by wireless. Every device can move freely in any direction but within the range. It is assuming that it is the only system that will combine the technology are fire and police vehicles used to exchange the information with one another for the safety reasons. They do-not have the already existing infrastructure. They are self-organizing, self-configured, self-governing, self-controlled networks. The ad hoc network can be extend or dispose anytime and anywhere. They have no or less central authorization or simple set up. The central administration devices may be the base stations or the access points.

Ad hoc networks are the self-governing systems which is build up of the mobile nodes. The nodes can communicate with one another by using the wireless communication as shown in the Figure 1.2. The node may be a laptop, mobile phone, PDA and some other communication device which has the limited storage capacity, bandwidth and battery power. An ad hoc network indicates the set of networks where all the devices have the identical status and within the range they are able to connect with the other ad hoc network devices.

LITERATURE REVIEW

Specht, S. M. et al. [1] describes the DDoS attack models and proposes genetics to characterize the characteristics of the software attack tools used the scope of DDoS attacks and the countermeasures available. These genetics highlights patterns in various DDoS attacks, tools and similarities, to help in the development of more generalized solutions to responding DDoS attacks, containing new derivative attacks. Chen, R. et al. [2] combined the pushback concepts and packet marking to represent a new technique named Attack Diagnosis. Under this technique, an Intrusion Detection System is installed at the victim which is used to determine the attack. The victim pass through this information to the upstream routers to mark the packets which have the trace back information. And after that upstream routers escape the attack packets. Chen, R. et al. [3] proposed

Throttling or rate limit to lighten these attacks. The work which had been already done was in the direction of prevention, detection and trace-back of DDOS attacks. Few research efforts have been put towards the mitigation of DDOS attacks. Srinath, R. et al. [4] proposed Cluster Based Secure Routing Protocol (CBSRP). It is a MANET routing protocol that ensures secure communication among the mobile nodes and secure key management. One Way Hashing technique and digital signature are uses for secure communication. According to cluster based secure routing protocol, it makes a group of small clusters which is made up of 4-5 nodes. The communications among the mobile nodes take place after forming the cluster. Inside the cluster, there is forever a cluster head or cluster node. The cluster head is not always permanent like another nodes lying in the queue. Based on the priority, the new cluster head is chooses from the remaining nodes. One way hashing technique is used to authenticated the mobile nodes inside a cluster. Digital Signature is not urgent inside cluster communication. We proposed to use Digital Signature for the cluster-cluster communication. Whenever we divide the whole network into the small set of clusters, the CBSRP guarantees the secure communication. Hung, C. C. et al. [5] presented traditional ad hoc routing protocols are not fine adapted for these high dynamic networks. In this paper they suggest (HVN) Heterogeneous Vehicular Network architecture and the mobility pattern aware routing for the heterogeneous vehicular network. In this paper, the HVN architecture combines the VANET technology with the Wireless Metropolitan Area Network (WMAN) and stocks the advantages of better coverage in WMAN. Vehicles in HVN can exchange the information with each other and access Internet everywhere. The routing protocol for HVN is unique from those used in MANET or VANET, that's why their focal point is the routing issue in the HVN. For HVN they propose the Mobility Pattern Aware Routing Protocol (MPARP) to supply more reliable or decent V2V service. According to this protocol the 802.16 is used as the base station which hold information table. The table contains every vehicle's id, its current speed and current position. It will change whenever there is a position modify for any one of the members in the table. This protocol uses some format for transmit messages. Qian, Y. et al. [6] proposed an analysis for the vehicular networks on a priority based secure MAC Protocol and consider that the MAC Protocol can obtain both QOS and security in the vehicular ad-hoc networks. In this paper he suggested that the MAC Protocol is having messages with several priorities for various applications to access dedicated short range communication (DSRC) channel. The secure MAC Protocol will use a part of IEEE 1609.2 .Security infrastructure containing PKI and ECC, the secure communication message format of vehicular networks. The priority based channel access according to the QOS necessity of the applications. Tamana, E. et al. [7] proposed Pushback to diminish or lighten the distributed denial of service attacks. It is relied upon the improved Aggregate based congestion control (IACC) algorithm. This algorithm is implemented on the routers to security against bandwidth consumption attacks. Here, firstly we compare the packet's attack signature. If it is matched then the packet is

transfer to the rate limiter. The rate limiter helps to examine whether to discard the packet or not. After that Pushback daemon drop the packets with the help of upstream routers. Wu, M. et al. [8] analyzes the performance of Multicast Ad hoc on demand Distance Vector (MAODV) protocol which is the reactive multicast routing protocol under the impact of wormhole nodes under various scenarios. In the route discovery process, they form a Worm Hole Secure MAODV by providing a certificate based authentication mechanism. This technique can greatly increase network performance even when the malicious nodes are present. WHS-MAODV is as effective as MAODV in finding and managing routes in addition to producing the required security. The proposed protocol shorten the packet loss because of the malicious nodes to a considerable range thereby enhance the performance. Sharma, E. G. et al. [9] proposed several type of challenges and security problems of VANET been analyzed and discussed. In this paper, the set of solution to resolve or clarify these challenges and problems are discussed. According to this, every vehicle has OBU (On Board Unit). The OBU unit link vehicles with RSU via DSRC. The TPD (Tamper Proof Device) is the device that holds the vehicle secrets such as keys, route, speed driver's identity, trip detail etc. Different attacks considered are DOS, Alteration Attack, and Replay Attack Fabrication Attack. The several attackers are Selfish Driver, Pranksters and Malicious Attackers etc. According to this paper, the different vehicular network challenges are Mobility, Volatility, Privacy VS Authentication, Privacy VS Liability, Network Scalability and various security requirements are Authentication, Availability, Non repudiation, Privacy, Integrity , privacy, Confidentiality.

FINDINGS OF LITERATURE REVIEW

The existing model is entirely based upon the cooperative VANETs and facilitates to exchange the positioning and status information between VANET neighbors. The exchange of messages up to 1-hop is considered as the control channels in periodic fashion. The ability of the network to dynamically adapt the congestion behavior in the different segments in the vehicular networks around the intersection points plays the important role in the de-congestion models. The efficient and effective model for the vehicular network congestion control is realized by developing the congestion aware model with utilizes the channel load and its associative principles for the purpose of efficient metric calculation and evaluation. To date, congestion and awareness management protocols are ordinarily designed and evaluated severally, though each are needed for the reliable and economical operation of conveyance networks. During this context, this paper proposes the devaluated INTERN solution, a replacement management protocol that integrates two congestion and awareness management processes. The simulation results obtained for 3 completely different eventualities demonstrate that INTERN is in a position to satisfy the applications' needs of all vehicles, whereas effectively dominant the channel load. The results obtained highlight the challenges ahead with rising machine-controlled vehicles.

METHODOLOGY

This research project will start with a detailed literature review on the various VANET mobility and collision avoidance and coverage schemes. Then, a detailed coverage and connectivity mechanism would be designed to prevent the issue of non-connected nodes and to provide the maximum message reach in VANETs. The results obtained from the simulation would be deeply analyzed and compared to the existing models of the congestion control for the vehicular networks.

CONCLUSION

The problem of the congestion usually arise in the vehicular networks and causes the various performance issues such as higher transmission delay, data loss, overloaded network equipment etc. The congestion control becomes the necessity in order to keep the vitality of the network for the efficient data transfer mechanisms and efficient path formation among the urban VANET clusters to efficiently provide the associated services such as traffic density updates, collision updates, hurdles detector and information broadcasting, etc. In this paper, we are proposing the traffic flow control mechanism among the vehicular networks, which utilizes the traffic awareness reporting and flow isolation methods for the decongestion of the vehicular data and updates. The proposed model will utilize the direction based guided protocol to select and control the paths selected for the data delivery among the vehicular content delivery network (VCDN) for the quick and efficient updates. The proposed model is expected to solve the problem more efficiently and effectively for the decongestion than the existing models.

REFERENCES

[1]. Specht, S. M., & Lee, R. B. (2004, September). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In *ISCA PDCS* (pp. 543-550).

[2]. Chen, R., Park, J. M., & Marchany, R. (2006). TRACK: A novel approach for defending against distributed denial-of-service attacks. *Technical P~ eport TR ECE—O6-02. Dept. of Electrical and Computer Engineering, Virginia Tech.*

[3]. Chen, R., Park, J. M., & Marchany, R. (2007). A divide-and-conquer strategy for thwarting distributed denial-of-service attacks. *Parallel and Distributed Systems, IEEE Transactions on, 18*(5), 577-588.

[4]. Srinath, R., & Srinivasan, D. R. (2007, June). Ac: Cluster based secure routing protocol for wsn. In *Networking and Services, 2007. ICNS. Third International Conference on* (pp. 45-45). IEEE.

[5]. Hung, C. C., Chan, H., & Wu, E. H. K. (2008, March). Mobility pattern aware routing for heterogeneous vehicular networks. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE* (pp. 2200-2205). IEEE.

[6]. Qian, Y., Lu, K., & Moayeri, N. (2008, November). A secure VANET MAC protocol for DSRC applications. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* (pp. 1-5). IEEE.

[7]. Tamana, E., & Bhandari, A. Router Based Mechanism for Mitigation of DDoS Attack-A Survey. *International Journal of Computer Applications Technology and Research*, *3*(7), 420-426.

[8]. Wu, M., & Kim, C. (2010). A cost matrix agent for shortest path routing in ad hoc networks. *Journal of Network and Computer Applications*, *33*(6), 646-652.

[9]. Sharma, E. G., & Narula, E. T. Security Challenges and Attacks in Vehicular Ad hoc Network.

[10]. Sepulcre, Miguel, Javier Gozalvez, Onur Altintas, and Haris Kremo. "Integration of congestion and awareness control in vehicular networks." *Ad Hoc Networks* 37 (2016): 29-43.

[11]. Ghaleb, Fuad A., M. A. Razzaque, and Ismail Fauzi Isnin. "Security and privacy enhancement in vanets using mobility pattern." In *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*, pp. 184-189. IEEE, 2013.

[12]. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." In *New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on*, pp. 393-398. IEEE, 2010.

[13]. Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)." In *Road Transport Information and Control (RTIC 2012), IET and ITS Conference on*, pp. 1-6. IET, 2012.

[14]. Javed, Muhammad A., and Jamil Y. Khan. "A geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." In*Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pp. 1-6. IEEE, 2011.

[15]. Hung, Chia-Chen, Hope Chan, and EH-K. Wu. "Mobility pattern aware routing for heterogeneous vehicular networks." In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pp. 2200-2205. IEEE, 2008.

[16]. Dias, João A., João N. Isento, Vasco NGJ Soares, Farid Farahmand, and Joel JPC Rodrigues. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks." In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 51-55. IEEE, 2011.

[17]. Moser, Steffen, Simon Eckert, and Frank Slomka. "An approach for the integration of smart antennas in the design and simulation of vehicular ad-hoc networks." In *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 36-41. IEEE, 2012.

[18]. Sumra, Irshad Ahmed, Halabi Hasbullah, J. A. Manan, Mohsan Iftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network." In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pp. 708-714. IEEE, 2011.

[19]. Sumra, Irshad Ahmed, Halabi Hasbullah, and J-L. A. Manan. "VANET security research and development ecosystem." In *National Postgraduate Conference (NPC), 2011*, pp. 1-4. IEEE, 2011.

[20]. Chen, Lu, Hongbo Tang, and Junfei Wang. "Analysis of VANET security based on routing protocol information." In *Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on*, pp. 134-138. IEEE, 2013.

[21]. Khabazian, Mehdi, and M. K. Mehmet Ali. "A performance modeling of vehicular ad hoc networks (VANETs)." In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 4177-4182. IEEE, 2007.

[22]. Qian, Yi, Kejie Lu, and Nader Moayeri. "Performance evaluation of a secure MAC protocol for vehicular networks." In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1-6. IEEE, 2008.