Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.116 – 121

RESEARCH ARTICLE

INTELLIGENT HAZARD ROUTING FOR VANETs WITH POINT OF INTEREST EVALUATION TECHNIQUE

Needhi Lathar[1], Shashi Bhushan[2], Munish Mahajan[3]

[1]Department of Information Technology, CEC Landran (Mohali), India

[2]Department of Information Technology, CEC Landran (Mohali), India

[3]Department of CGC-COE[2], CEC Landran (Mohali), India

[1] nidhilather999@gmail.com, [2] shashibhushan6@gmail.com, [3] cec.manish@gmail.com

Abstract — The automatically driven vehicle based networks (VANETs) are prone to various routing hazards. The collisions on the roads, other hurdles such as tree falling, road damages to external stimulate block the roads and do not leave any place for vehicles to pass through. In such cases, it becomes essential to route the vehicles through the backup paths in order to avoid the hazardous hurdles produced on the roads due to any reason. In this paper, we have proposed the new paradigm in the hazardous routing protocol for the automatically driven vehicle based VANETs. The proposed model would be evaluated on the basis of accuracy, route persistence, probability of detection, probability of false alarm, etc.

Keywords: hazard routing, VANETs, Mobilization, collision avoidance.

I. INTRODUCTION

The inter connectivity of vehicles and road side units are required to complete a network in vehicular network. The node-to-node to RSU architecture is an idea which is used to connect the not-in-range nodes with the in-range nodes so that they can be provided with the hazardous messages earlier and hence, in other words, we are increasing the coverage area. Thus, if the not-in-range nodes are receiving the information about the hazardous earlier they can change their route on time and hence, performance of VANET is improved by enhanced connectivity schemes.

To create a mobile network, a Vehicular Ad hoc Network, or VANET uses moving cars or vehicles as nodes in a network. A VANET allows cars approximately 100 to 300 meters from each other to connect by turning each participating car into a wireless node or router and hence, creates a network with a wide range. Whenever any car falls out of the signal range and leaves the network, other cars can join in and create a mobile network. The estimations say that the first system that will

integrate with this technology are police and fire vehicles that will communicate with each other for safety purposes. Vehicular networks are developed to improve the safety measures for the transportation and providing them with new mobile applications and services so that they can move with greater efficiency to avoid the traffic. Vehicular networks are becoming a crucial component for the future intelligent road traffic management systems where future intelligent road traffic management systems are expected to offer several features as compared to the current traffic management system.

The features or advantages provided by the future intelligent road traffic management systems are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. Researchers are working for more than a decade to develop a suitable Vehicular Ad hoc Networks (VANETs) for traffic safety systems. VANETs are considered as the intelligent systems which can distribute traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UTMS, Wi-MAX networks and these advantages are self-organization, low cost of implementation and maintenance and lower local information dissemination time. VANETs can be said as the practical implementation of MANETs in future. This vehicular network is made up of the vehicles which have wireless interface and are interconnected to transfer information. The vehicles can easily provide power for connection for wireless communication and if other communication hardware like antennas are required, they can also be used without causing any major problems. The focus of VANET is to provide cost-effective and timely information to the vehicles or passengers so that they can commute without any disturbances on the way because of hazardous.

Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry – and - forward DTN paradigm that works as follows. A source node originates a data bundle and stores it using some form of persistent storage, until a communication opportunity (i.e., a contact) arises. This bundle may be forwarded when the source node is in contact with an intermediate node that can help bundle delivery. Afterwards, the intermediate node stores the bundle and carries it until a suitable contact opportunity occurs. This process is repeated and the bundle will be relayed hop by hop until reaching its destination (eventually and over time).

The main difference between VANET and MANET are its mobility model. When a vehicle is moving on a road, its mobility pattern must include with the topology of the road. This constraint is called as mobility. In addition, the behaviour of different drivers are different as in a normal condition, their speeds can vary from 60 km/hr to 130 km/hr. So, we can't apply any random mobility model on all of the drivers. The mobility model will always be dynamic, not static. And, the relative speeds of the vehicles will always be higher especially when moving in different directions.

II. PROBLEMS FOUND IN EXISTING MODELS

Ghaleb F. et al. proposed the paper which presents a mobility pattern based misbehaviour or hazardous situation detection in VANETs. This paper differentiates the attacker into 2 categories- insiders and outsiders where insiders is a legitimate node which might intentionally or unintentionally make misbehaviour or unauthorized actions, such as modify, fabricate or drop the message in order to impersonate other node identities. And, outsider is a kind of intruder aim to interfere the communication among VANET nodes. Misbehaviour can be viewed as following two perspectives in VANETs- (i) physical movement and (ii) information security perspectives. This paper includes algorithm to detect the misbehaviour which is Location-Aided Routing for MANET (ALARM) and relies on location information and routing time[2].

Sharma G. et al. proposed the paper which includes analysis and discussion for various types of security problems and challenges in VANETs and also the solutions for these problems and challenges. According to this paper, each vehicle has 2 devices OBU (On Board Unit) and TPD (Tamper Proof Device) where OBU connects vehicles with RSU via DSRC and TPD hold the vehicles secrets like keys, driver identity, trip details, route, speed etc. Various attacks discussed in this paper are DOS, Fabrication Attack, Alteration Attack, Replay attack and various attackers are Selfish Drivers, Malicious Attackers and Pranksters. According to this paper various 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 and Confidentiality.

Seuwou P. et al. proposed VANET as a technology that uses moving cars as nodes in a network to create a mobile network. VANET enables two types of communication- vehicle to vehicle (V2V) and vehicle to road-side infrastructure (V2I). This converts every participating car into a wireless router or node which allows connection between other cars in a radius approximately 100 to 300 meters, thus creating a network of wide range. In this paper author proposed various issues of effective security in VANETs. Also, he discussed various attacks in VANETs. He classified attacks into two broad categories- (i) physical attach which occurs because of two problems- tamper proof device and event data recorder, and (ii) logical attack which occurs because of virus, Trojan horse and protocol weak spot[4].

Qian.yi et al. proposed an overview on a priority based secure MAC protocol for vehicular networks and he assumes that the MAC protocol can achieve both QOS and security in vehicular networks. According to this paper the MAC protocol is having messages with different priority for different applications to access DSRC (Dedicated Short Range Communication) channel. And, the proposed secure MAC protocol will use a part of IEEE 1609.2, security infrastructure including PKI and ECC, the secure communication message format of vehicular networks, and the priority based channel access according to the QOS requirement of the applications[13].

Javed.M.A. et al. proposed a technique namely geocasting packet transmission to transfer safety message in vehicular network. To analyse the performance of the proposed model, he used OPNET based simulation model. VANET is considered as self organizing autonomous system which can distribute traffic and any kind of emergency information to vehicles in a timely manner. The proposed protocol selects the furthest vehicle for rebroadcasting the message with the help of backoff window design and hence reduces the number of packet transmission which ultimately lowers the contention levels. The proposed protocol generates lower broadcast overhead and packet loss ratio as compared to the other protocols. Also, it offers very low convergence and warning notification time compared to the other protocols[5].

M. A. Berlin and Sheila Anand et al. proposed a protocol namely Direction based Hazard Routing Protocol which helps timely delivery of the hazardous information to the vehicular traffic. This timely delivery helps to prevent collisions and hence increases the safety. The focus of the proposed work is road hazard information dissemination on highways where the traffic is sparse. As the traffic is assumed to be sparse, V2V communication would not be a feasible solution. The protocol proposes the deployment of RSUs relatively close to each other with capability of communicating with its neighboring RSUs and with the vehicles travelling on the highway. The communication range (CR) of RSUs would extend to single and multi-lane highways so that all the lanes are within its communication zone[1].

The model is designed to solve the problem of information dissemination or broadcast in the cluster about the obstacles produced due to fall of trees, landslide, maintenance work, etc. Such information is very importantly to be delivered to all of the nodes travelling towards the hurdle in order to change their route of travel effectively. The proposed model is used to avoid the traffic jams and accidents due to latter described obstacles. The vehicle route optimization or route change is quite important to keep the uninterrupted vehicular movement on the roads. In the existing solution, the major objective is to broadcast the information about the hurdle (so called hazard in the existing work) in the VANET cluster, which can be used by the vehicles to take safety action to avoid the hazardous locations.

The existing protocol, DHRP (direction based hazard routing protocol), takes an account on the geographic location of the nodes and the hazard to keep the nodes updates, which will be travelling towards the hazardous location. The existing model contains various problems. At first, it does not take the not-in-range nodes into account. It means the nodes which are not in range would not be delivered (or guaranteed delivered) the broadcast message about the hazard after they will join an RSU. Such problem must be taken into account to avoid the danger on the life of the people travelling in any such vehicle which is out of reach during the message broadcast.

The node failure in the existing scheme can also cause hazardous situations. The node failure can cause collision, traffic chaos or other movement related hazards. The node failures can be covered up using the unicast query messages.

III. SUMMARY OF THE TECHNIQUES SURVEYED

Authors and Year	**Problem Addressed**	**Techniques Proposed**	**Experimental Results**	**Expected Outcome**
Ghaleb F. et. al. (2013)	Security and Privacy in VANETs using Mobility Pattern	Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network	The proposed algorithm by which the misbehavior can be detected.	Physical movement, Information security.
Sharma G. et.al (2010)	Security Analysis Of Vehicular Ad Hoc Network	Analysis of Prankster, Selfish Driver, Fabrication	OBU (On Board Unit) based vehicles with RSU via DSRC and	Authentication, Availability, Non repudiation, Privacy,

		Attack, Replay Attack, etc. for VANETs.	TPD(Tamper Proof Device) hold the vehicle secrets like keys, drivers identity, trip detail, route, speed etc.	Integrity , privacy, Confidentiality
Seuwou. P et. al. (2012)	Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)	Discussed various attacks in VANET, according to him the attacks are classified into two broad categories first one is physical attack	Attack classification has been done in this performance analysis	Logical attacks has been surveyed which occur due to the virus, Trojan horse and protocol weak spot.
Qian.yi et.al.	Performance evaluation of a secure MAC Protocol for vehicular network	Priority based secure MAC Protocol for smooth mobility in vehicular networks	MAC Protocol is having massages with different priority for different application to access DSRC channel for better performance.	Level of Security, Probability of Exposure.
Javed.M.A. et.al.	A Geocasting technique in an IEEE802.11p based vehicular Ad hoc network for road traffic management	Geocasting packet transmission technique to transfer safety message in a vehicular network	The proposed protocol offer very low convergence and warning notification time compared to the other protocols.	Low Broadcast, Low convergence.
Hung C.C. et.al.	Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks	Heterogeneous Vehicular Network (HVN) architecture and a mobility pattern aware routing	HVN integrates Wireless Metropolitan Area Network (WMAN) with VANET technology and reserves advantages of better coverage in WMAN and high data rate in VANET	Vehicle id, current position, and current speed

FUTURE SCOPE

In the future, the VANETs can lead towards higher order or data optimization or movement protocols for the higher level of mobility with lowest or no probability of collision or mis-movement. The VANETs must be made capable of controlling their mobility with the optimized transmission model for the maximum coverage.

REFERENCES

[1] Berlin, M. A., and Sheila Anand. "Direction based Hazard Routing Protocol (DHRP) for disseminating road hazard information using road side infrastructures in VANETs." *SpringerPlus* 3 (2014): e173-e173.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Abdalla, Ghassan MT, Mosa Ali Abu-Rgheff, and Sidi Mohammed Senouci. "Current trends in vehicular ad hoc networks." *Proceedings of UBIROADS workshop*. 2007.

[15] Bibhu, Vimal, et al. "Performance Analysis of black hole attack in VANET." *International Journal of Computer Network and Information Security (IJCNIS)* 4.11 (2012): 47.

[16] Chim, Tat Wing, et al. "SPECS: Secure and privacy enhancing communications schemes for VANETs." *Ad Hoc Networks* 9.2 (2011): 189-203.

[17] Chim, Tat Wing, et al. "Security and privacy issues for inter-vehicle communications in VANETs." *Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops' 09. 6th Annual IEEE Communications Society Conference on*. IEEE, 2009. Dias, João A., et al. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks."*GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011.

[18] Douceur, John R. "The sybil attack." *Peer-to-peer Systems*. Springer Berlin Heidelberg, 2002. 251-260.

[19] Guette, Gilles, and Ciarán Bryce. "Using TPMs to secure vehicular ad-hoc networks (VANETs)." *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*. Springer Berlin Heidelberg, 2008. 106-116

[20] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. Vol. 3. IEEE, 2003.

[21] Khabazian, Mehdi, and M. K. Mehmet Ali. "Generalized performance modeling of vehicular Ad Hoc networks (VANETs)." *Computers and Communications, 2007. ISCC 2007. 12th IEEE Symposium on*. IEEE, 2007.

[22] Leinmüller, Tim, et al. "Improved security in geographic ad hoc routing through autonomous position verification." *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. ACM, 2006.

[23] Lo, Nai-Wei, and Hsiao-Chien Tsai. "Illusion attack on VANET applications-A message plausibility problem." *Globecom Workshops, 2007 IEEE*. IEEE, 2007.

[24] Mahmood, Raja, and A. I. Khan. "A survey on detecting black hole attack in AODV-based mobile ad hoc networks." *High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on*. IEEE, 2007.

[25] Malla, Adil Mudasir, and Ravi Kant Sahu. "Security Attacks with an Effective Solution for S Attacks in VANET."*International Journal of Computer Applications* 66.22 (2013).

[26] Manvi, S. S., M. S. Kakkasageri, and D. G. Adiga. "Message authentication in vehicular ad hoc networks: Ecdsa based approach." *Future Computer and Communication, 2009. ICFCC 2009. International Conference on*. IEEE, 2009.
[27] Park, Soyoung, et al. "Defense against sybil attack in vehicular ad hoc network based on roadside unit support."*Military Communications Conference, 2009. MILCOM 2009. IEEE*. IEEE, 2009.
[28] Parno, Bryan, and Adrian Perrig. "Challenges in securing vehicular networks." *Workshop on hot topics in networks (HotNets-IV)*. 2005.
[29] Paxson, Vern. "Bro: a system for detecting network intruders in real-time." *Computer networks* 31.23 (1999): 2435-2463.
[30] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks." *Journal of Computer Security* 15.1 (2007): 39-68.
[31] Zhou, Liang, and Han-Chieh Chao. "Multimedia traffic security architecture for the internet of things." *Network, IEEE* 25.3 (2011):35-40.

