ISSN PRINT 2319-1775 Online 2320-7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

Proposed Study & Experiments to Improve the Quality of Service and Security for VANETs

Dr.Gurjeet Singh
Associate Professor
Department of Computer Science & Engineering
Sant Baba Bhag Singh University
Jalandhar

Abstract
Vehicular Ad-hoc Networks (VANETs), which are a new emerging network technology derived from ad-hoc networks. In the field of Intelligent Transportation Systems (ITS), communications without a wire between vehicles (V2V) appear as an accident prevention solution offering a wider vision than conventional sensors. By linking vehicles to telecommunications network (V2I), new perspectives are offered both passengers and driver with conventional communication applications such as access Internet, e-learning, games or chat. This means that future mobile networks like VANETs will have to integrate communications, mobility, Quality of Service (QoS) and security. In this paper, we propose to contribute on how to improve security without degrading the quality of service QoS in a highly mobile environment as VANETs network.

Keywords: VANETs, QOS, Security, Mobility, ITS

1. Introduction
VANETs refers to a network created in an ad-hoc manner where different moving vehicles and other connecting devices come in contact over a wireless medium and exchange useful information to one another. A small network is created at the same moment with the vehicles and other devices behaving as nodes in the network. Vehicular Ad-hoc Networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of Wi-Fi. Other Wireless Technologies are Cellular, Satellite and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS). Vehicular ad-hoc networks are responsible for the communication between moving vehicles in a certain environment. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V)

VANET can be characterized by the following factors:

- **Network topology:** Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.
- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units.
- **Unlimited power and storage:** It is assumed that the nodes in VANET are capable of possessing an unlimited amount of power as well as storage capacity. Therefore the nodes are free to exchange the data without the foundations of power consumption or storage wastage.
- **On board sensors:** VANET assumes that the nodes are seldom equipped with on board

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

sensors which are capable of transmission of information to other devices or nodes.

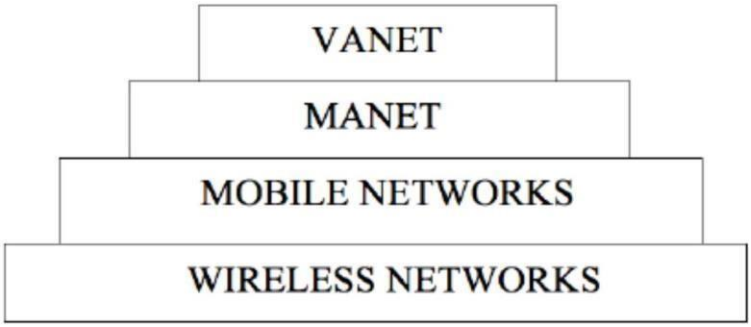


Figure 1 Wireless network hierarchy

A VANET network is a feature of MANET networks where mobile nodes are vehicles equipped with computers, network cards and sensors. Like any other ad hoc network, vehicles can communicate with each other or with base stations placed along the roads. The figure 1 shows the hierarchy of wireless networks where it diagrams the inclusion of VANET in MANET, MANET networks in the Mobile and mobile networks in wireless networks.

2. Communication in Vanets

Vehicular networks are the basis of exchanges for intelligent transport systems. From an architectural point of view, communication in a VANET can be either:

1) Vehicle-to-Vehicle (V2V)
2) Vehicle to Infrastructure (V2I)
3) Hybrid Communication.

A) Vehicle-to-Vehicle (V2V)

A vehicle network is seen as a special case of MANET where energy constraints and memory capacity are relaxed and where the mobility model is not random but predictable with great mobility. No infrastructure is used, no installation is needed on the roads and all vehicles are equipped to communicate directly with each other anywhere, whether on highways, mountain roads or urban roads, which can provide a less expensive and more flexible communication.

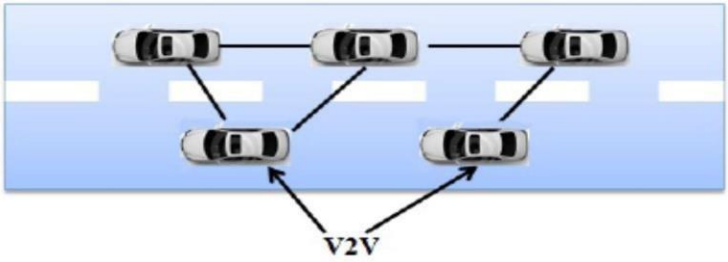


Figure 2 Vehicle-to-Vehicle Communication

B)Vehicle to Infrastructure (V2I)

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

V2I approach is based on the client/server model where vehicles are clients and stations installed along the road are the servers. These servers are connected to each other via a wired or wireless interface. All communication must go through them. They can also offer users more services on trafficking, internet, exchange car-to-home communication data and even car to the garage for the remote diagnosis.

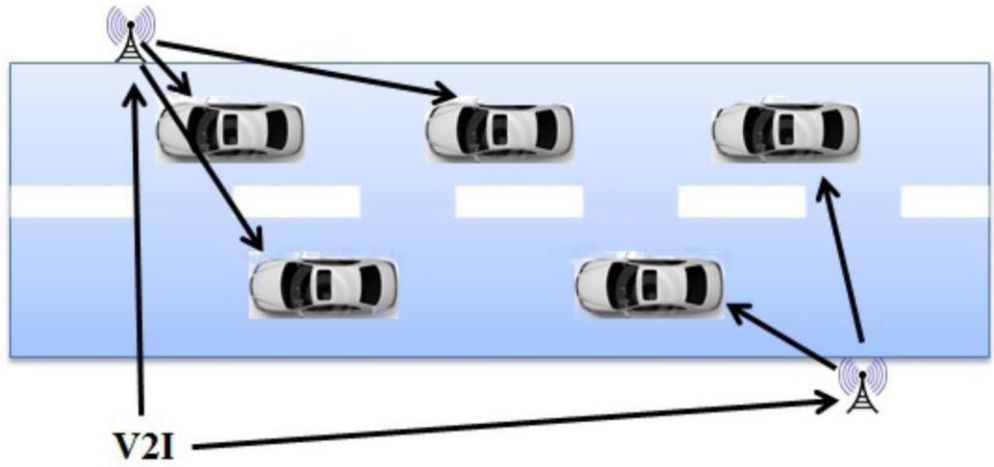


Figure 3 Vehicle-to-Infrastructure Communication

C) Hybrid Communication

The combination of these two types of communication architecture provides interesting hybrid architecture. Indeed, the increase of infrastructure is limited, the use of vehicles as relays can extend this distance. Nevertheless, the inter-vehicular communications suffer from routing problems on long distance transmission. In such situations, access to infrastructure can improve network performance.

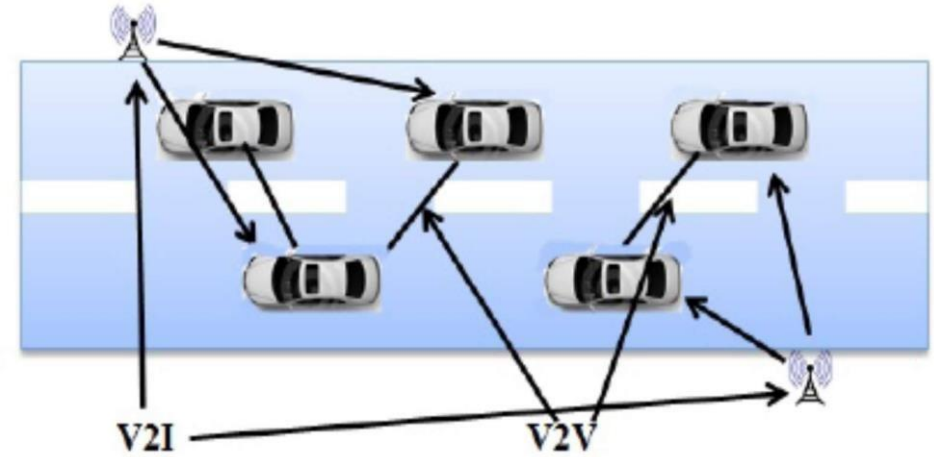


Figure 4 Hybrid Communication

3. Quality of Service in Vanets

QoS is defined as a set of service requirements that needs to be met by the network while transporting a

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

packet stream from a source to its destination. In wired networks, the QoS parameters are generally described in terms of delay and throughput. The QoS parameter in vehicular ad hoc networks is difficult to meet because of the network topology changes, scalability, the delay-constrained routing and the impact of density and driving environments on the offered QoS services. We have two kinds of traffic over VANETs:

- **Real-Time, RT**: such as safety messages and video/ audio signals
- **Non-Real-Time, NRT:** such as e-maps and road/vehicle traffic/ weather information.

The difference between RT and NRT imposes diverse quality of service (QoS) requirements for VANET designs. QoS is a big challenge when the VANET is under contention based (e.g. IEEE 802.11 protocol) environments, where the packet delay and data congestion level increase dramatically as the total number of vehicles contending for the common wireless media. Sending and receiving correct data in a fixed duration of time is critical in this type of networks. Safety warning applications require minimum End- To-End delay because if a warning message is received with high delay, that message could be useless for preventing an accident. Due to the instability of the paths in VANETs, proactive routing protocols such DSDV and OLSR may fail. These protocols are based on the exchange of routing tables between neighbor nodes. This becomes worse in case of large scale networks. Reactive protocols do not use routing tables but use a flooding method for route discovery that initiates more routing overhead and also suffer from the initial route discovery process. Thus, they become unsuitable for security applications in VANET. AODV is an example of a reactive protocol. AODV floods the network with route request packets which leads to high overhead. The frequent topology changes in VANETs cause an important traffic which consists on control messages. In addition, the main drawback is that AODV needs end-to- end paths for data forwarding, which is difficult to handle because in VANETs end-to-end paths break often due to high speeds of vehicles. The non-contention-based method Time Division Multiple Access (TDMA) was proposed as an efficient solution in the physical layer for mobile and sensor networks. This method consists in allocating a time slot for each node to send its packets. It is efficient because it provides high reliable communications, and resolves the problem of hidden nodes.

4. Security in Vanets

Security is not a separate issue but linked to the control and management of QoS network and services. Security is an important issue in any communication system. Due to the fact that VANETs are composed of number of communicating autonomous entities moving at high speed, the randomness of the connectivity between the vehicles and their relative geographic positions raises concerns about users and data security. Most desired security attributes as criteria to measure security for all VANET applications are authenticity, privacy, availability confidentiality, and non-repudiation. Attacks in VANETs hinder vehicles communications by deteriorating or interrupting their functions. There are several techniques proposed to encounter Sybil attack in VANETs such as statistical and probabilities approaches, signal strength and session keys. Another category of attacks on the data integrity is spoofing which consists on node impersonation. Spoofing is an attempt by a node to send modified version of the message and claims that the message comes from the originator for the unknown purpose.

Messages should reach the destination within the relevant time period. As VANETs consist on vehicles moving at high speed, the development of secure routing protocols is necessary.

A Symmetric-Masquerade Security Scheme (SMSS) was proposed to achieves security requirements of V2V communications while keeping a low system overhead. In a first step, a vehicle entering the

Coverage of a certain BS, it broadcasts a message containing a public key to apply for a pseudonym and another one as a pre-shared key which is updated periodically. The message includes a time stamp to avoid replay attacks. After that, the BS assigns a local pseudonym to the vehicle. To protect the privacy of each vehicle, only the base station knows their real names and their corresponding pre-shared key. So when vehicles within the coverage of a BS want to communicate, the BS assists the symmetric key exchange between them to verify the integrity of the nodes. After the symmetric keys are exchanged between the communicating vehicles, a link is established for a short time to allow secure end-to-end communications without the assistance of the BS. When a vehicle leaves the range of a base station, it returns the pseudonym that will be assigned to a future entering vehicle. BSs maintain a table which records the uni- mapping between the pseudonyms and the real identifications of current users. This mechanism allows the BS to identify imposture immediately. This security scheme does not create overhead in the network such as asymmetric schemes where private and public keys are exchanged between communicating entities.

5. Simulation Model

In this paper we are going to study the different scenario's i.e high speed highway environment, variable speed vehicle environment and city environment. In each network base station is mounted in the centre. In these different environments we are going to communicate vehicles with base station, base station with vehicles and vehicle to vehicle.

A) High speed highway environment

A high speed highway movement with dual lane opposite directions across some kilometer distance can be consider within the simulations. Each vehicle will get different high speed just like road vehicles.

Parameters	Quantity
No of vehicles	25
Speed (Kmph)	10, 25, 50, 75, 100, 120
Transmission range	10 km
Packet size	1000 bytes
Traffic Type	UDP/CBR
Mac	802.16e

Table 1 High speed highway environment

Variable speed vehicles environment In Variable speed vehicles environment all vehicles slows down at certain point of the road due to presence of external factor along the road such as road constructions, accident, etc. Such condition reduces distance between vehicles and increases vehicle network density.

B) Variable speed vehicle environment

In this all vehicles slow down at certain point of the road due to presence of external factor along the road such as road constructions, accident etc. Such condition reduces distance between vehicles and increases vehicle network density.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

Parameters	Quantity
No of vehicles	25
Speed (Kmph)	15, 30, 60, 70, 80, 100
Transmission range	10 km
Packet size	1000 ytes
Traffic Type	UDP/CBR
Mac	802.16e

Table 2 Variable speed vehicle environment

C) City Environment

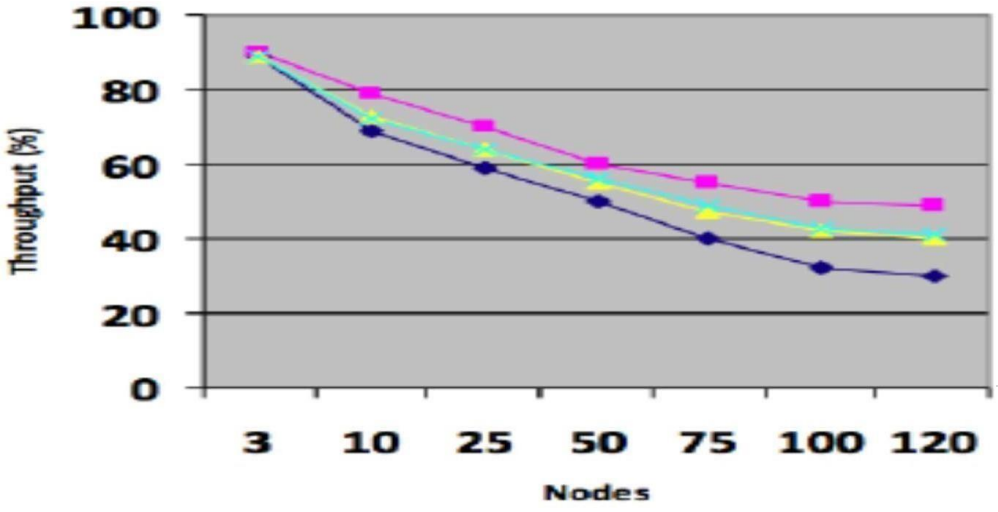
In this environment we are going to create the scenarios of some roads of the city having vehicles from which some of the vehicles will vary their speed time to time and some of them will stop just like real road environment.

Parameters	**Quantity**
No of vehicles	25
Speed (Kmph)	20, 35, 55, 70, 90, 110
Transmission range	10 km
Packet size	1000 ytes
Traffic Type	UDP/CBR
Mac	802.16e

Table 3 City environment

6. Results

This system will be more efficient, fast than existing system by using AMC techniques in Wimax. Our throughput should be more than the existing network, jitter should be as low as possible, delay is less than 2.5 msec, more than 95% packet delivery ratio and minimum packet loss ratio. The throughput, end to end delay results are shown below for weak and strong mobility. Here we can see that for SNR values the throughput is maximum. This throughput f the network is going to improve by increasing the packet size and reducing the packet interval time.



ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

Figure 5 Throughput for weak mobility

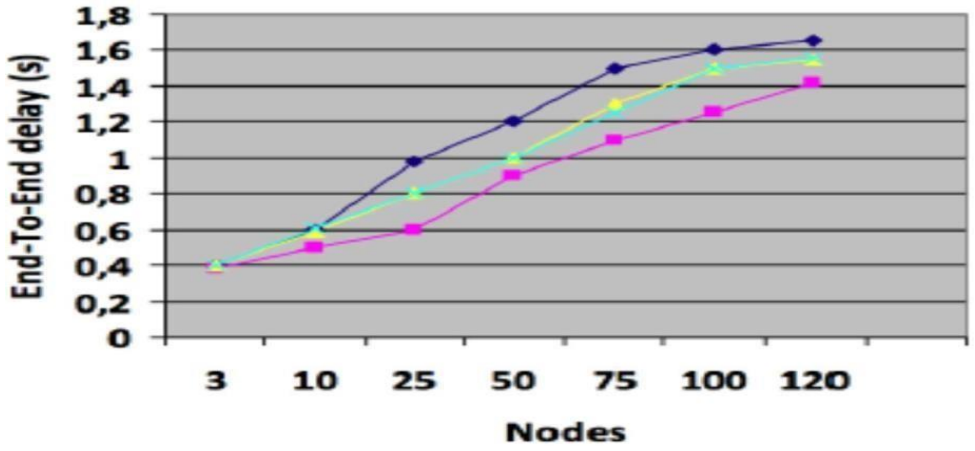


Figure 6 End to End Delay for weak mobility

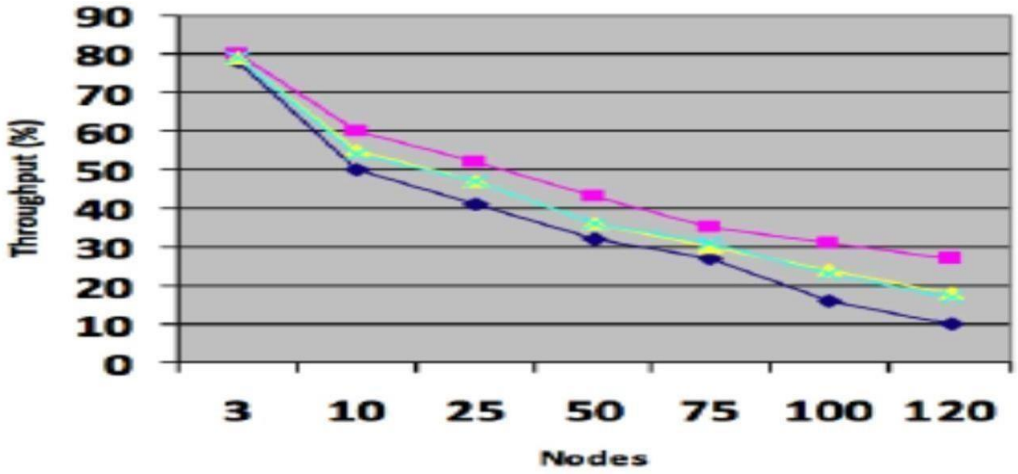


Figure 7 Throughput for strong mobility

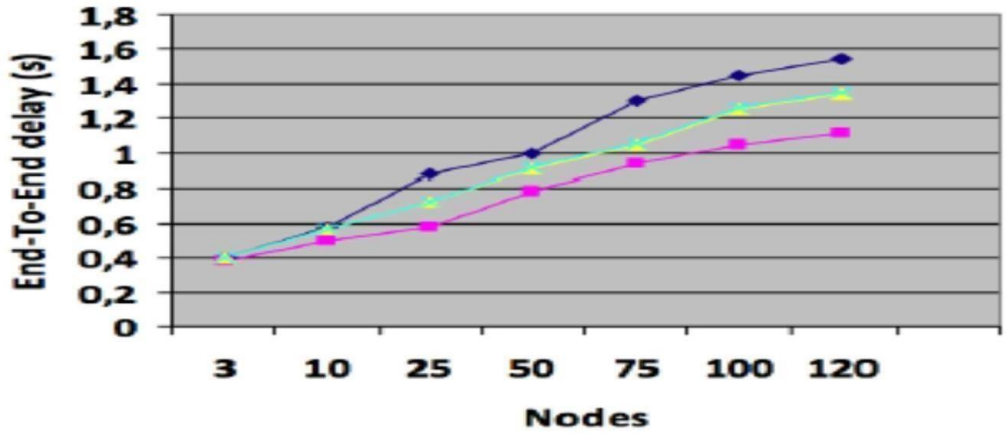


Figure 8 End to End Delay for strong mobility

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 1, Jan 2023

7. Conclusion

To prepare the future, we considered VANETs as a good example for future technologies and we proposed several study and experiments to improve the quality of service and security for VANETs. Unlike other wireless environments that are mostly stationary or with low mobility, data transmission in VANETs poses more challenges that must be addressed. Since the topology is constantly changing, vehicles could move away from their home network and cause connectivity breakage. In order to cope with this problem, a vehicle connected to the wireless network should be able to move using different access points available along the road. These access points could belong to different networks or wireless technologies like Wi-Fi, WiMAX.

References

[1] C. Fouque, P. Bonnifait, and D. Betaille, “Enhancement of global vehicle localization using navigable road maps and dead-reckoning,” in 2008 IEEE/ION Position, Location Navigation Symp.

[2] K. Golestan, S. Seifzadeh, M. Kamel, F. Karray, and F. Sattar, “Vehicle localization in VANETs usingdata fusion and v2v communication,” in 2012 ACM DIVANet.

[3] P. Oliver, F. Moosmann, and A. Bachmann, “Visual features for vehicle localization and ego-motion estimation,” in 2009 IEEE Intelligent Veh.

[4] Diyar Khairi M S DEEI, FCT Amine Berqia DEEI, et al. Design and implementation of a secure nemo. International Journal of Computer Science and Information Security, 10(11):1,ISSN 1947-5500, 2012.

[5] Diyar Khairi M S, Amine Berqia, ”Li-Fi the future of Vehicular Ad hoc Networks”, Journal ”Transactions on Networks and Communications”, UK ISSN: 2054-7420.

[6] Diyar Khairi M S, Amine Berqia, ”Survey on QoS and Security in Vehicular Ad hoc Networks”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 42-52, 2015.

[7] Diyar Khairi M S, Amine Berqia, ”Improving TCP Performance on WAVE Networks”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, 2015.

[8] Gurjeet Singh & Dr.Vijay Dhir, “Comparison Analysis of Secure Multicasting Routing Protocols in Mobile Adhoc Networks” International Journal of Modern Engineering & Research Technology, Volume 6, Issue 1, 2019.

[9] Gurjeet Singh & Dr.Vijay Dhir, “A Novel Tree Based Multicasting Routing Protocol for Mobile Adhoc Networks” International Journal of Innovative Technology and Exploring Engineering, Volume- 8 Issue-5,2019.

[10] Gurjeet Singh & Dr.Vijay Dhir, “A Novel Protocol for Infrastructure Based and Infrastructure Less Multicasting Routing Protocol in Mobile Adhoc Networks” International Journal of Engineering and Advanced Technologies, Volume-8 Issue- 5, 2019.

[11] Z. Hasan, H. Boostanemehr and V. K. Bhargava (2011). "Green Cellular Networks: A Survey, SomeResearch Issues and Challenges," Communications Surveys & Tutorials, IEEE, Vol. 13, No.4, pp. 524-540, Fourth Quarter.

[12] C. E. Perkins and E. M. Royer (1999). Adhoc on-demand distance vector routing. In Proc. Second IEEE Workshop Mobile Computing Systems and Applications WMCSA '99, pages 90-100.

[13] Puneet Manchanda and Parvinder Bangar (2014). Modified AODV-R Routing Protocol‖, International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 16, Issue 01, pp. 96-101.

[14] W. A. Moreira, R. Lopes Gomes, and A. J. Gomes Ableem (2009). A multiple metric approach for routing in wireless mesh networks. In Proc. IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks & Workshops WoWMoM, pages 1-6.
[15] Samir R. Das, Charles E. Perkins, and Elizabeth M. Royer (2000). "Performance Comparison of Two On demand Routing Protocols for Ad Hoc Networks." Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Tel Aviv, Israel, p. 3–12.
[16] S. B. Chaabene, T. Yeferny, and S. B. Yahia (2019) “A roadside unit placement scheme for vehicular ad-hoc networks,” in International Conference on Advanced Information Networking and Applications. Springer, pp. 619–630.
[17] S. Allani, T. Yeferny, R. Chbeir, and S. B. Yahia (2016) “A novel vanet data dissemination approach based on geospatial data,” Procedia Computer Science, vol. 98, pp. 572–577.
[18] L. Liu, C. Chen, T. Qiu, M. Zhang, S. Li, and B. Zhou (2018) “A data dissemination scheme based on clustering and probabilistic broadcasting in vanets,” Vehicular Communications, vol. 13, pp. 78–88.