Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

PERFORMANCE ENHANCEMENT AND SECURITY ASSISTANCE FOR VANET USING CLOUD COMPUTING

R. Neelaveni,
Assistant Professor,
Department of ECE,
MNMJEC.
Email id: veniganesh5@gmail.com

Abstract: The vehicular-adhocnetwork (adhocNet) termed to be prominent way of information transfer using vehicles plays a significant role in the development of the intelligent and safe transportation, to avoid the unwanted causalities. They provide a more comfortable way of driving and travelling; by providing the complete details entailed for the travel, utilizing the nearby vehicles and the roadside unit. But due to certain security issues arising in the information transmission by the conventional methods of the vehicular- adhocNet, the conventional method of vehicular- adhocNet seems to be inefficient. So the paper proposes a modified vehicular- adhocNet that replaces the cloud computing in the place of the road side unit to provide a enhance security in the information transmission, thus improving the performance of the vehicular- adhocNet as a whole. The performance evaluation of the proposed method using the NS-2 on terms of the improve security, delay and the throughput proves its significance.

Keywords: Vehicular-adhocnetwork, adhoc network, roadside unit, cloud computing, security assistance and performance enhancement.

1. INTRODUCTION

The adhoc network designed for a particular purpose of communication framing, its own network without any infrastructure, with the capability of conveying the information can be subdivided as mobile adhoc networks, wireless adhoc networks, wireless sensor networks, vehicular adhoc networks and the flying adhoc networks. The vehicular adhoc networks are prominent strategy that plays a significant role for the development of the intelligent transportation [1]. The vehicular –Adhoc remains popular as it is mainly concerned on the road safety and the traffic management. They pave way for a peaceful driving that is comfortable and helpful for the person driving as well as the person travelling along [2].

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

The communication through the vehicular-adhocNet is usually done between two vehicles or vehicles to the infrastructure, usually a road side unit; this provides clear information of the real time scenario that are taking place on road and helps to avoid the situations that create fatalities. Usually the vehicular-adhoc network usually updates information to the next vehicle using the road side units that are available or the intermediate vehicle that is connected.

The share information's regarding the causalities on road, the natural disasters caused on the road, the intensity of the traffic, the routes maps, parking lots etc. The information transferred over utilizing the wireless local area network via the road side unit is, on certain times are not properly directed or hacked or modified resulting in , inefficient message delivery causing losses. The fig.1 shows the conventional vehicular adhoc network.

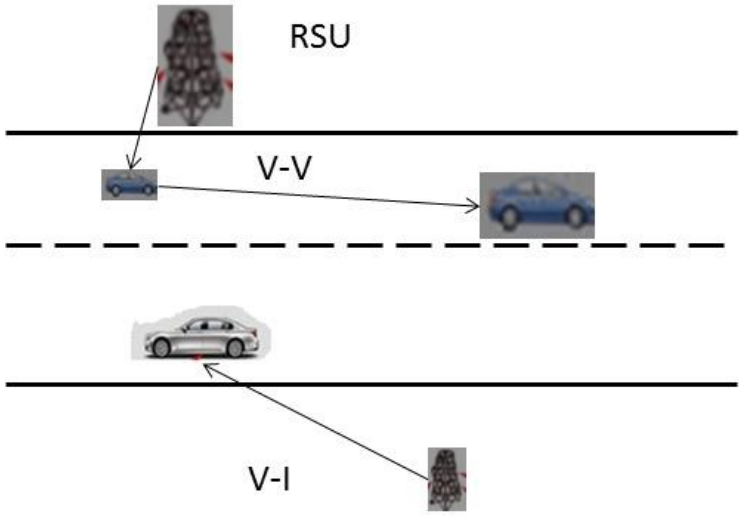

Fig .1 Conventional VANET

So the paper aims to propose a modification in the conventional vehicular-adhoc network, by replacing the road side units with the cloud computing, in order to have an improved security and performance.

The remaining of the paper is organized with the 2. The related works, 3. The proposed work that enables a cloud computing in the process of routing information to the respective vehicles that are connected based on the demand by the vehicle. 4 .the Results and discussion and 5. Conclusion

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

2. RELATED WORKS

Yousefi, et al [1] presents the survey on the challenges and the problems in the current networks and provides a brief explanation on the significance of the vehicular adhoc network. Zeadally et al [2] the survey details some of the recent research benefits of the vehicular-adhoc network Hartenstein,et al [3] details the tutorial based of the vehicular –adhoc network. Li et al [4] presents the detailed survey on the routing algorithms for the vehicular-adhocNet integrating the cellular network and the wireless local area network Al-Sultan et al [5] the paper details the concepts vehicular-adhocNet by providing a comparative study of the same Martinez, et al [6] the paper describes simulators used for the vanet for by providing a survey and the comparative study. Eze et al [7] the author details the significance and the essential details regarding the potentials of theVANET. ,Bitamet al [8], the VANET employing cloud computing in realizing the alternative routes with the improvement in the performance of the VANET is explored in the paper. He et al [9], the author employs the conditional privacy preserving authentication to elude the problems in the privacy preserving of the VANETS Abdelgadir et al[10], the paper explores the suitable routing for the VANET in the of a particular city Contreras et al [11] the solutions of the big data that are significant in the handling the problem emerging in the VANET are presented in the paper. Hasrouny et al [12] and the Samara et al [13] address the security issues related to the vehicular –AdhocNet. Hahn et l[14] gives the details of the security issues in the development of the intelligent transportation systems.

3. PROPOSED WORK

The proposed work paving way for secured vehicular-adhocNet by modifying the frame work of the conventional vehicular-adhocNet by alternating the rod side unit with the cloud computing services is handled by engaging the edge devices instead of the road side unit, the edge device, play perfect alternative role by providing a secured way of information transmission that enhances the timely delivery of the information packets. The proposed work before proceeding with the steps involved in the process explores the detailed characteristics of the conventional vehicular-AdhocNet and security issues faced by it.

3.1. THE SIGNIFICANT CHARACTERISTICS OF THE VANET

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

The vehicular-AdhocNet characterized with the ability of interacting with the vehicles that are connected and it is also capable of performing sufficient interaction with the infrastructure which is RSU in case of a conventional method, some of its characteristics that makes its necessary for the security for the system.

(i).The communication taking place utilizing the wireless medium entails a transmission that is secure to avoid the unwanted access

(ii).The vehicular-AdhocNet that poses a mobile nature makes it difficult to envision its position the vehicle and the topology of the network. So this characteristic of the vehicular-AdhocNet makes it necessary for the security, by providing authentication, handshaking and other measures paving way for a secured action.

The security provision in the conventional method of the vehicular-AdhocNet causes unnecessary delay degrading the performance of the system causing an unnecessary delay in the message transmission leading to the loss of the path or the data. So it becomes necessary to secure the transmission as well as deliver them within time. This has paved way for the proposed method that alternates the edge devices instead of the road side unit and seeks the cloud services, to improve the security and the performance of the vehicular-AdhocNet.

3.2. THE MODIFIED VEHICULAR –ADHOCNET

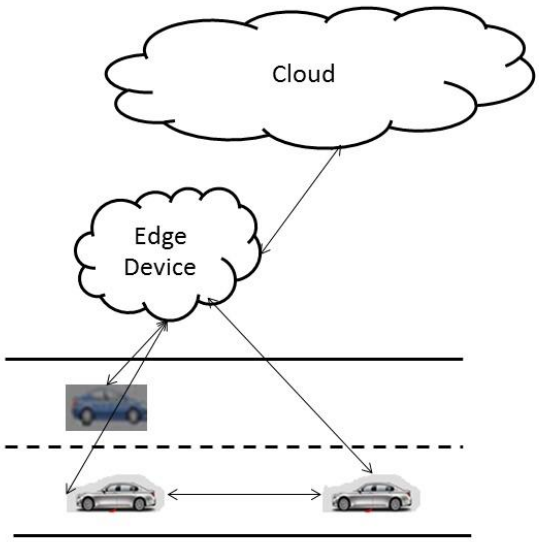

Fig .2 The Proposed Modified VANET

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

The proposed method replaces the road side unit with the edge device, so the edge device on receiving any requisition of service from any of the vehicles responds immediately without any delay and sends the summary of the process done alone to the cloud service. The step below explains the stages in the security assistance and the performance enhancement provided by the edge and the cloud computing to the vehicular network.

Step1: For a network (N) holding a considerable count of vehicles (V) where$V = \{V_1, V_2, \ldots \ldots V_i\}$ the communication is proceeded over the wireless LAN utilizing the edge device instead of RSU to overcome the delay in the information transmission and have a speedy process.

Step 2: The approximate member query filter (AMQF) is engaged for the security purpose in both the edge and the vehicles to elude the unnecessary hackings and the attacks. Every vehicle in the network retains a AMQF of all the vehicles prevailing in the network and enrolls itself to nearby edge device each time it enters the arena of the edge node and the edge nodes updates the information the vehicle list table that is maintained , the enrollment includes an identification for the vehicle (V_{id}) . The edge node in response provides a public key that is common for all the vehicles in the arena of the edge.

Step3: The vehicle requesting for a interaction to a vehicle or an edge is subjected to the AMQF to identify whether it is an attacker or the member. Once it is found to be member then proceeds with the acknowledgement paving way for the transmission and the reception of the information's. Otherwise terminates the communication after verifying whether it is a member or not with the update table in edge case of a vehicle to vehicle communication. In case of vehicle to Edge communication this is not necessitated as the edge refers with the update table before interacting with any communicator who request for a service. The flow chart in the fig .3 below explains the steps of the security enhancement achieved in the vehicle to vehicle communication along with the edge

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

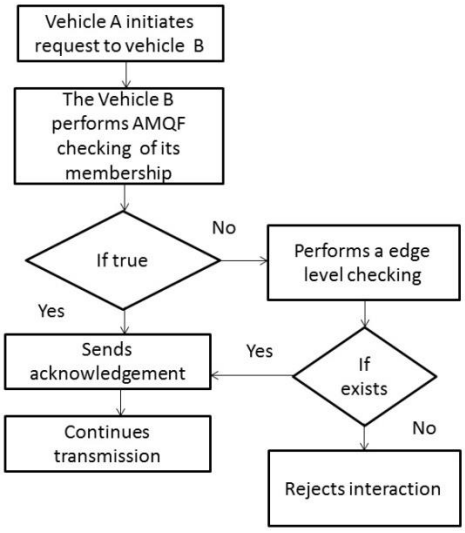

Fig .3 Proposed Vehicle to Vehicle Communication

The fig .4 shows the security enhancement achieved in the vehicle to the edge interaction to improve the performance of the vehicular-AdhocNet and stop the unwanted access to elude the loss of the data and the delay data.

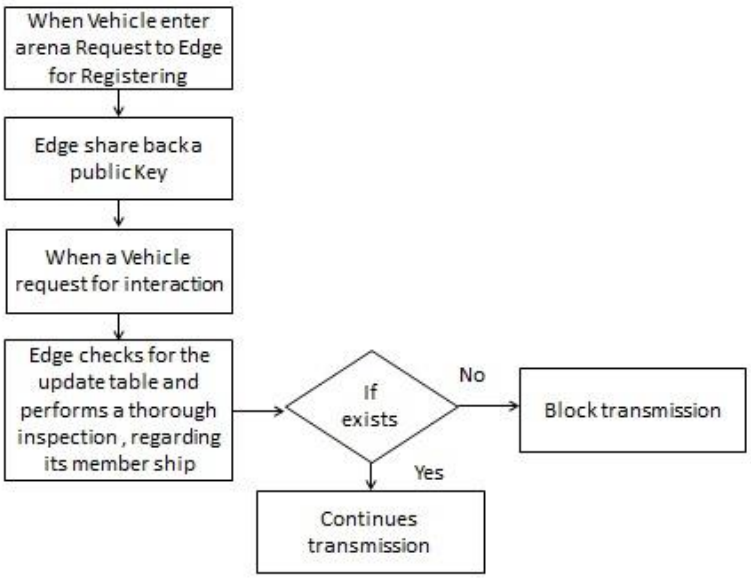

Fig .4 Proposed Vehicles to Edge Communication

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

Thus the above steps enable the vehicles to have a secured access. Further as the edge device are closely situated to the vehicles the request that are time exigent are handled by the edge device itself avoiding the delay that could be incurred by the using of the RSU.

4. RESULTS

The evaluation of the proposed model using the network simulator 2 for a number of vehicle in network ranging from the 100 to 500 , over a simulation area of 1000sq.m , with the packet size of 1000bytes , initial energy of 100 joules and a simulation time of 100 milliseconds. The proposed method is validated with the conventional method to evince the performance enhancement of the modified vehicular-AdhocNet.

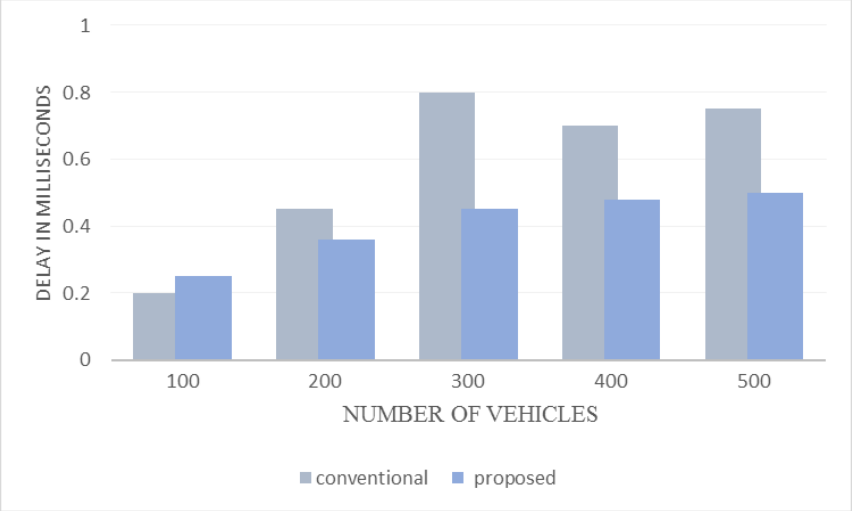

Fig .5 Delay incurred

The fig .5 shows the delay incurred in the transmission and the reception of the information of the proposed method and the prevailing method, the results acquired shows that the security provisioning engaged through the AMQF, avoids the losses of the information and the retransmission of the information thus improving the delay of the modified VANET compared to the Conventional VANET.

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

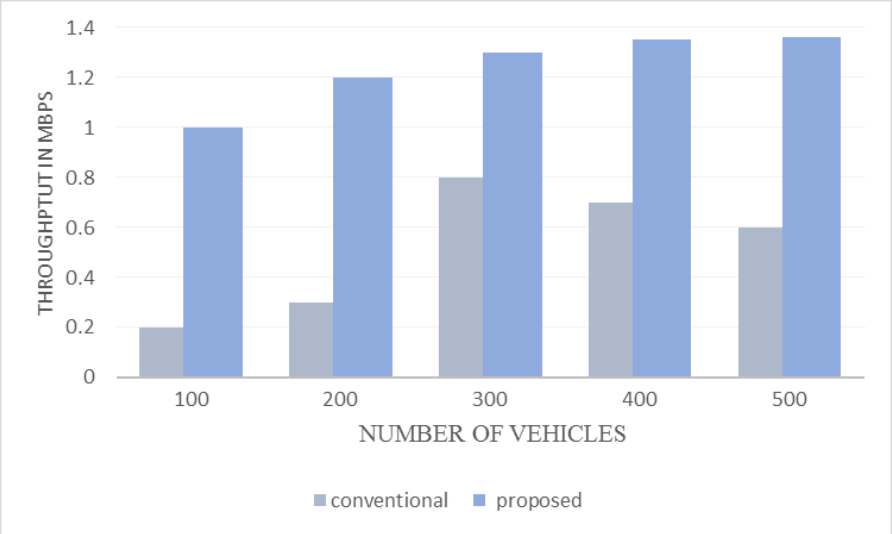

Fig .6 Throughput

The Fig 6 Shows the throughput enhancement of the modified vehicular-AdhocNet in comparison with the conventional vehicular-AdhocNet and shows the throughput achieved by the proposed method is 37.4% improved compared to the prevailing methodology.

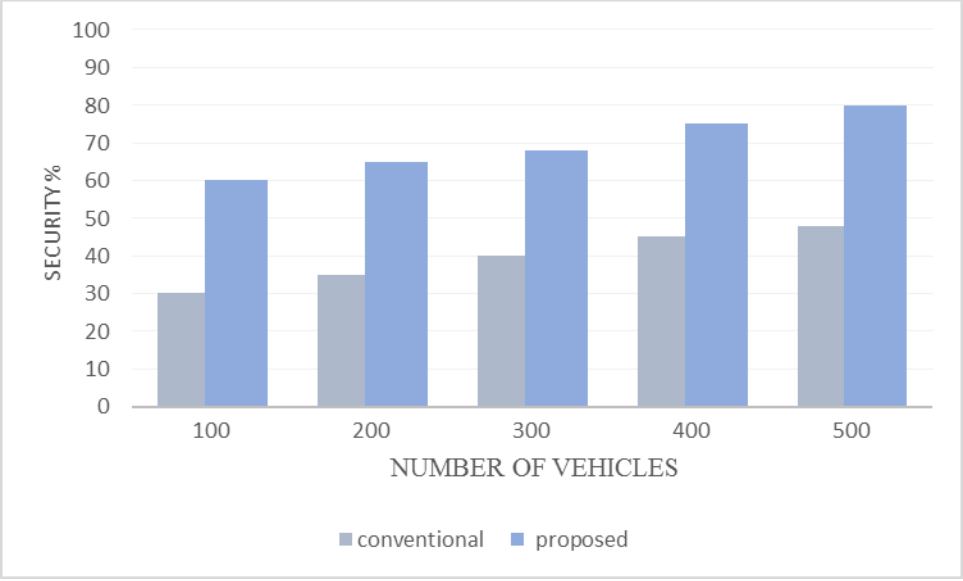

Fig.6 Security Percentage of the Proposed

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

The fig.7 showing the percentage of the security enhancement achieved by the proposed method, ensure the secure transmission and the reception of the information employing the AMOF for the edge and the vehicles, this secure transmission also cause improvements in the number of the successful transmission and minimization of the losses of information.

5. CONCLUSION

The paper proposes a modified vehicular-AdhocNet, for ensuring a secured transmission and the performance enhancements. For this purpose the road side unit of the conventional vehicular adhoc network is replace with the edge device of the cloud computing to have improved performance and further the AMQF is utilized in both the edge and the vehicle device to avoid the interactions of the attackers who indulge in hacking and altering of the information leading to the information loss. The validation of the same with the prevailing vehicular adhoc network using the network simulator 2 shows the heightened performance achieved by the modified vehicular-AdhocNet in comparison to conventional vehicular adhoc network

References

1. Yousefi, Saleh, Mahmoud Siadat Mousavi, and Mahmood Fathy. "Vehicular ad hoc networks (VANETs): challenges and perspectives." In *2006 6th International Conference on ITS Telecommunications*, pp. 761-766. IEEE, 2006.
2. Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular ad hoc networks (VANETS): status, results, and challenges." *Telecommunication Systems* 50, no. 4 (2012): 217-241.
3. Hartenstein, Hannes, and L. P. Laberteaux. "A tutorial survey on vehicular ad hoc networks." *IEEE Communications magazine* 46, no. 6 (2008): 164-171.
4. Li, Fan, and Yu Wang. "Routing in vehicular ad hoc networks: A survey." *IEEE Vehicular technology magazine* 2, no. 2 (2007): 12-22.
5. Al-Sultan, Saif, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. "A comprehensive survey on vehicular ad hoc network." *Journal of network and computer applications* 37 (2014): 380-392.
6. Martinez, Francisco J., Chai Keong Toh, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni. "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)." *Wireless Communications and Mobile Computing* 11, no. 7 (2011): 813-828.

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/No.01
Pages: 36-45
https://irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.004

7. Eze, Elias C., Si-Jing Zhang, En-Jie Liu, and Joy C. Eze. "Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development." *International Journal of Automation and Computing* 13, no. 1 (2016): 1-18.
8. Bitam, Salim, Abdelhamid Mellouk, and Sherali Zeadally. "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks." *IEEE Wireless Communications* 22, no. 1 (2015): 96-102.
9. He, Debiao, Sherali Zeadally, Baowen Xu, and Xinyi Huang. "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks." *IEEE Transactions on Information Forensics and Security* 10, no. 12 (2015): 2681-2691.
10. Abdelgadir, Mayada, Rashid A. Saeed, and Abuagla Babiker. "Mobility routing model for vehicular Ad-Hoc networks (VANETS), smart city scenarios." *Vehicular Communications* 9 (2017): 154-161.
11. Contreras-Castillo, Juan, Sherali Zeadally, and Juan Antonio Guerrero Ibañez. "Solving vehicular ad hoc network challenges with big data solutions." *IET Networks* 5, no. 4 (2016): 81-84.
12. Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. "VANet security challenges and solutions: A survey." *Vehicular Communications* 7 (2017): 7-20.
13. Samara, Ghassan, and Yousef Al-Raba'nah. "Security Issues in Vehicular Ad Hoc Networks (VANET): a survey." *arXiv preprint arXiv:1712.04263* (2017).
14. Hahn, Dalton A., Arslan Munir, and Vahid Behzadan. "Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges." *IEEE Intelligent Transportation Systems Magazine* (2019).

ISSN: 2582-4104 (online)