IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 10, Issue 03, March 2023 https://www.ijirae.com/archives

A Security Protocol for V2V Communication using NS2 Network Simulator

Sanjay S Tippannavar*
Department of Electronics and Communication Engineering,
JSS Science and Technology University, Mysuru, India
Sanjayu2345@gmail.com
Meghana N
Department of Electronics and Communication Engineering,
JSS Science and Technology University, Mysuru, India
meghana.n02@gmail.com
Yashwanth S D
Assistant Professor, Department of ECE,
JSS Science and Technology University, Mysuru, India
yashwanth@sjce.ac.in

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.10/Issue03/MRAE10081
Research Article | Open Access | Double-blind Peer-reviewed | Article ID: IJIRAE/RS/Vol.10/Issue03/MRAE10081
Received: 04, March 2023 | Revised: 14, March 2023 | Accepted: 19, March 2023 Published Online: 31, March 2023
Volume 2023 | Article ID MRAE10081 https://www.ijirae.com/volumes/Vol10/iss-03/02.MRAE10081.pdf
Article Citation: Sanjay,Meghana,Yashwanth (2023). A Security Protocol for V2V communication using NS2 Network Simulator. IJIRAE:: International Journal of Innovative Research in Advanced Engineering, Volume 10, Issue 03 of 2023 pages 49-57 https://doi.org/10.26562/ijirae.2023.v1003.02
BibTeX sanjay2023security
Academic Editor-Chief: Dr.A.Arul Lawrence Selvakumar, AM Publications, India

Abstract: The principles of MANETs, or mobile ad hoc networks, form the foundation of vehicular ad hoc networks (VANETs). Vanet was first introduced as "Car to Vehicle ad hoc mobile communication and networking" in 2001. In order to build a communication network and transfer data among vehicles, Vanet were invented. Vanet uses a variety of means to establish communication, including vehicle-to-vehicle communication. In this project, both roadside-to-roadside and vehicle-to-roadside communications are employed, and vehicle-to-roadside communication is taken into consideration. A different term for VANETs is Intelligent Transportation Networks. The "Internet of Vehicles" (Vanet) has expanded into a larger system and will ultimately become the internet. There will be a "Internet of autonomous vehicles" in the not too distant future. Wireless networking is used by Vanets for networking and communication; even LTE and 5G may be used by vanets. In this project, a protocol is being developed to provide security for the established connection in Vanet, i.e., to recognise and stop any network intrusions. The NS2 network simulator is used to implement this protocol for testing purposes.

Keywords: Vehicular ad hoc networks (VANETs), mobile ad hoc networks (MANETs), ad-hoc,NS2, V2V, Communication, Security protocols, Wireless Networking.

I. INTRODUCTION

VANET stands for Vehicle ad hoc network VANET and MANET are the current two forms of mobile wireless network architecture (mobile ad hoc network). Infrastructure networks are sometimes referred to as cellular networks. A wireless network connects each base station in a vanet, which has a fixed base station. The base station's broadcast range identifies a cell. In this context, vehicles are referred to as nodes, and all nodes within this base station transmission range communicate with the base station as well as with each other. The three types of communication in the VANET are vehicle-to-vehicle, vehicle-to-roadside unit, and roadside unit-to-roadside unit communication. VANET communication takes occur through wireless networks like WLANs; no fixed routers are needed. Each node may move around and connect other nodes dynamically as needed. Nodes work together on projects like organising and managing networks. Nodes may move around at whim, and the network can be moved as a whole. If they are unable to interact directly with the target nodes, nodes in a communication network establish a connecting network with neighbouring nodes and link to the destination node. These nodes also serve as routers. The Ad hoc Network is seen in Fig. 1. The main difference between the two kinds of networks is that an ad hoc network lacks a centralised entry point. In the vehicle ad hoc network, there are no mobile switching nodes or base stations. VANET has gotten a lot of interest in the research on this topic because of its advantages and applications. Since that no infrastructure has been developed, a wireless network may be put up very rapidly. While utilising VANET, there are a few factors that must be considered, such as safety concerns, cost, and security measures. A significant industry using ad hoc networks is the military.

In addition to emergency search and rescue operations, sensor deployment, conferences, exhibitions, virtual classroom operations, and operations in locations where constructing infrastructure is difficult and expensive, the growing user base has given rise to more applications for the VANET network and communication. Ad hoc may be deployed quickly since it lacks infrastructure.

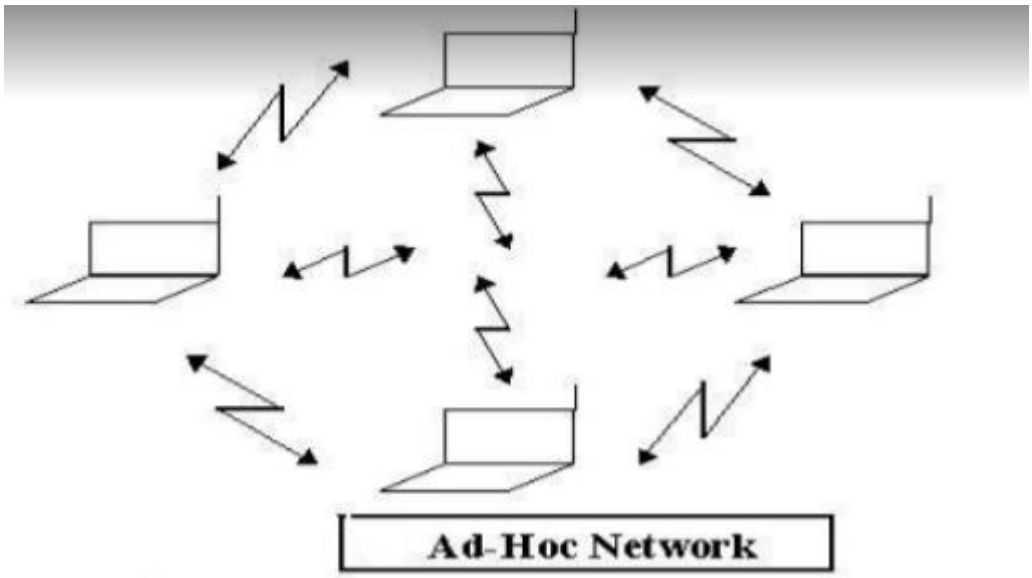

Fig.1. Ad Hoc Network

The VANET communication technology integrates WLANS, cellular, and ad hoc networks to provide connection. The ad hoc network is being developed with the new objectives of providing services for comfort and safety to automobiles. The VANET's primary safety functions include collision warning, lane change alarm, traffic jam alarm, and road block alarm. Users of vehicles may access the internet and other multimedia via the numerous comfort-related service categories. Among the most difficult VANET research topics include the design of routing protocols, data interchange, data security, and data privacy. VANETS provide value-added services like vehicle safety, automated toll payment, traffic management, navigation, location-based services like identifying the nearest gas station, hotel, or lodge, and entertainment apps like giving access to the internet. In order to meet these problems, we want a secure protocol that provides high bandwidth, greater connection, low latency, real-time application, as well as protection from security intrusions.

II. RECENT WORKS

Mobile cellular networks may provide significant coverage for users in automobiles, but they often fall short of the requirements of services that need stringent real-time safety. In order to meet the ITS's communication demands, the Heterogeneous Vehicular Network (HetVNET), which integrates DSRC and cellular networks, is a potential choice. Despite the large number of articles that have been published on each of these subjects, DSRC and cellular network research are still in their infancy. In-depth examination of existing wireless network applications for HetVNETs is provided in this paper. I'll start by comparing and summarising the requirements for safety-related and non-safety services. After introducing a HetVNET framework that utilises a variety of wireless networking strategies, numerous applications for various typical situations are detailed. In order to construct such HetVNETs, one must have a good understanding of heterogeneity and the challenges it poses. As a consequence, HetVNETs 28 carefully examines and investigates the main problems and possible solutions for the network and Medium Access Control (MAC) layer **[1]**.

The three primary pillars of smart cities may be considered as the Internet of Things, mobile wireless networks, and data mining technologies. Our cities are becoming more intelligent than ever thanks to massive volumes of IoT data. Data-driven management has the potential to greatly increase the operational efficiency of transportation networks by providing a clear and useful picture of passengers' travel behaviour. In this study, we focus on the data loss and internal time discrepancy aspects of the data validity problem in a cellular network-based transportation data collection system **[5]**. The creation of an effective platform for vehicular communication is made challenging by the fact that new ITS and vehicular applications (such as trip planning) necessitate intensive big data processing and real-time pervasive information collection efforts in order to support quick decision-making and feedback to moving vehicles. In this article, we suggest TrasoNET, a combined network architecture that integrates networking and data analysis to provide connected cars real-time intelligent transportation services **[6]**.

The GPSR protocol offered by this study features less end-to-end latency and is based on a neutral network. the time difference between the current node's neighbours while sending greetings. This method considers how far apart the current node and the target node **[7]**. Using a method for updating route information, this research examines several routing protocols. The NS-2 environment with dynamic node mobility is used to evaluate and analyse performance metrics like as throughput, average end-to-end latency, and packet delivery ratio **[8]**.

A smart city's smart traffic is its main pillar. The vehicle ad hoc network's (VANET) routing algorithm is a key element of smart traffic. References that just discuss simulation, choosing the wrong simulation platform, a challenging method, and other issues are drawbacks. They developed a novel approach to handle the aforementioned problem after analysing algorithms like AODV, DSDV, GPSR, and DSR [9]. While the VANET field of study is still in its infancy, it has already started to focus on a variety of services offered to network users as well as strategies for allowing nodes on lanes next to them to connect with one another. After contrasting different existing protocols like ARAN, SMT, SEAD, NDM, etc. with different solutions discovered and discussed by researchers to address security issues and other VANET Challenges, we can say that some existing protocols are incredibly complicated, time-consuming, computational, and awkward.

III. METHODOLOGY

In Fig. 2 below, the VANET Block Diagram is shown. The blocks in the block diagram represent the generation of vehicles, modelling of their movement, routing of the vehicles, and environment databases. For the purpose of simulating the movement of the vehicles, vehicle generation offers information about the starting place, the final destination, and the vehicle itself. The position and speed of the vehicle are outputted and communicated to the environment database as a consequence of the vehicle information supplied to the modelling of the movement of the vehicle. The network information is exchanged for the environment database. The information modelling gets routing information.

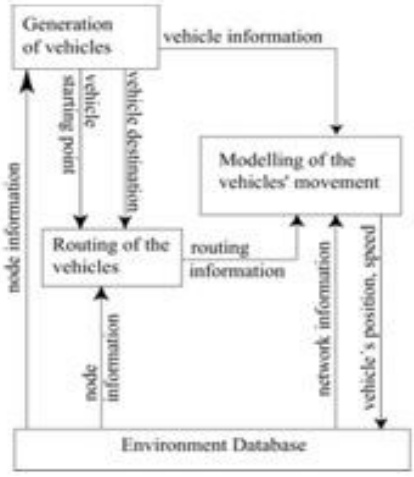

Fig.2. Block Diagram of VANET.

The environment database gives node details for both vehicle creation and routing. Mobile, infrastructure, and general are the three categories of vanet components. Mobility covers all mobile technology, such as laptops, cellphones, and smart watches, whereas infrastructure refers to things like roads and bridges. Although the core infrastructure domain contains items like cameras, traffic lights, and other such items, the infrastructure domain includes facilities for managing traffic and controlling vehicles. The last category, the generic domain, includes both public and private infrastructure. In addition to having three domains—the infrastructure domain, the ad hoc domain, and the in-vehicle domain—the European VANET architectural specifications are somewhat different from those in the United States. Network Simulator, or NS2 (Version 2) It is commonly used by researchers to evaluate the efficacy of cutting-edge techniques. By using nodes/routers, connections, and the capability to mimic both wired and wireless network services and protocols, NS2 enables you to build up a computer network (such as routing algorithms, TCP, and UDP). Next, to move data (packets) over the network, you may utilise a range of different protocols at various points. Network Simulator 2 is a popular open-source discrete event simulator for computer networks. The basic architecture of NS2 is depicted in Fig. 3.

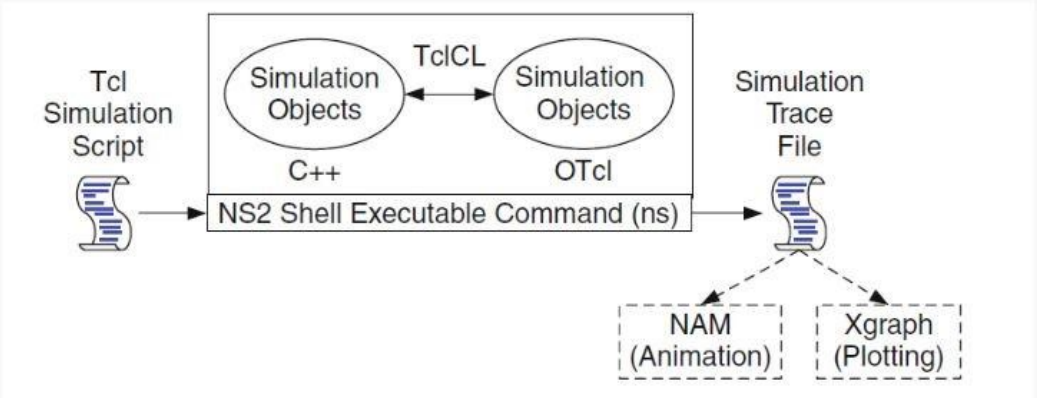

Fig.3. Architecture of NS2

Fig. 3 above depicts the NS2 architecture. The executable command ns is available to users of NS2, and it takes the name of a Tcl simulation scripting file as an input argument. The name of a Tcl script that generates a simulation is provided by users as an input parameter to the ns command of the NS2 executable.

In order to display graphs and/or create animation, a simulation trace file is often generated. The ns2 simulator is used to create a network topology. The below Fig 4 shows the working of the NS2.

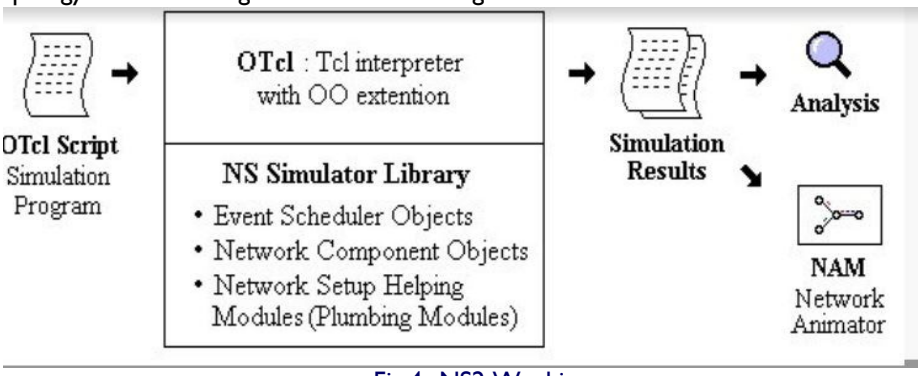

Fig.4. NS2 Working.

Fig. 5 below shows the data flow diagram, sometimes referred to as a bubble chart. It is a simple graphical formalism that may be used to represent a system in terms of the input data, the various operations that are carried out on it, and the output data that the system generates.

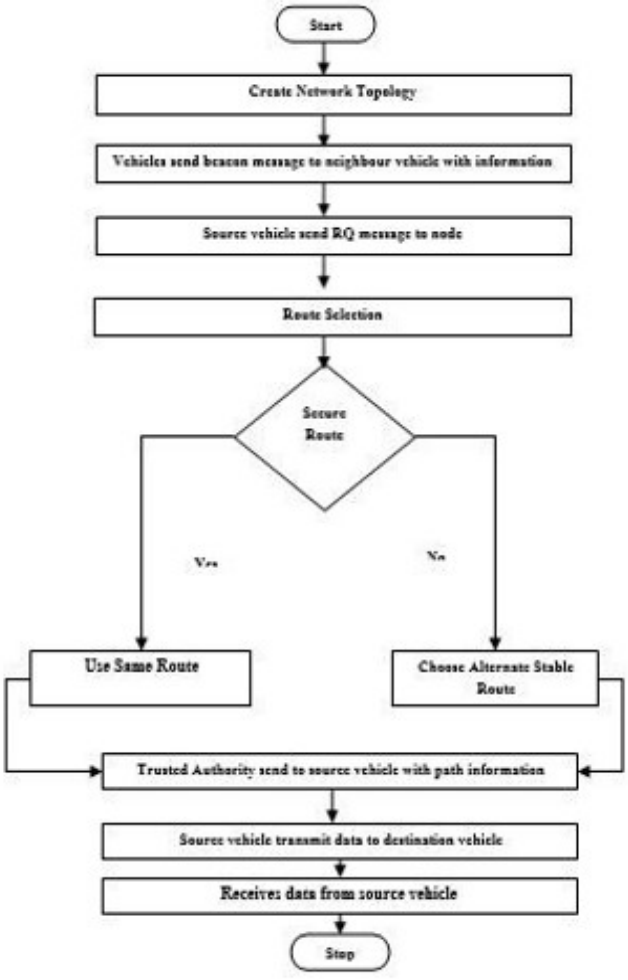

Fig.5. Data Flow diagram of the proposed model.

Both a flow chart and a data flow diagram are used to depict the movement of the newly developed protocol. In this network setup for the experiment, NS2 is used to establish the source nodes, destination nodes, roadside units, and the trust authority. I have considered 50 nodes in the network, of which 33 to 48 are considered for communication either as source nodes or destination nodes, and the remaining nodes are considered to be the roadside unit and trustworthy authority. The source vehicle sends each of the neighbouring nodes a beacon message to initiate communication. The key must be verified as legitimate by both the sender and recipient nodes in order for the connection to be initiated. A distinct key is sent to the sender and recipient nodes using the hash key method. A similar attempt will be made by the sender node to establish connections with neighbouring nodes in order to create a route to the destination node and transfer the message.

The node is malicious and is trying to establish a connection by posing as someone else if the unique key shared by the sender and recipient nodes does not match. The message is securely sent to the destination node using this route, avoiding any hostile nodes in the process. After certification, trustworthy authorities vouch for this route, which was produced using routing-based protocols.

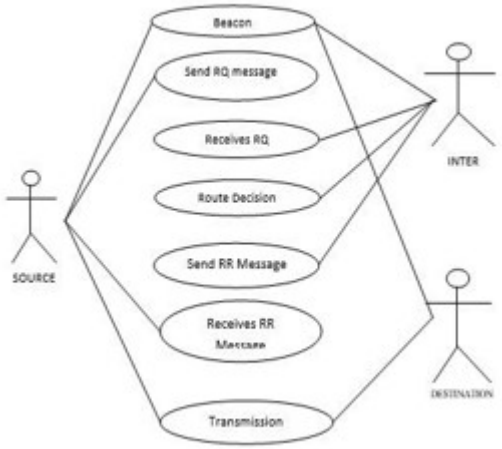

Fig.6. Use Case Diagram.

Fig. 7 depicts the Class diagram, which describes which nodes have type information and their roles. The source, who is in possession of the beacon message, gathers the route information and transmits the data in accordance with it. The intermediate node chooses the paths for data transmission between the sender and receiver nodes, as well as determining the positions of the source and destination nodes. After processing the data after receiving the beacon message, the destination node emits an acknowledgement of its actions.

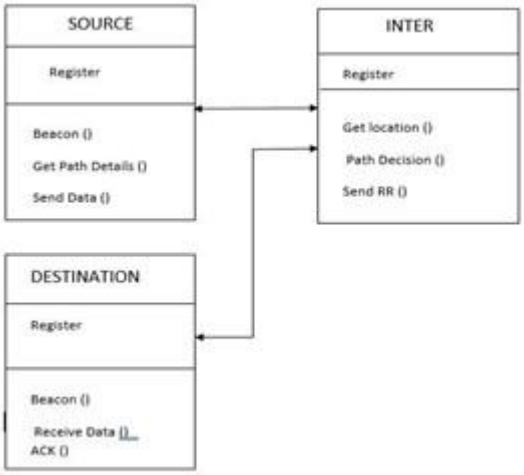

Fig.7. Class diagram

Fig. 8 below depicts a sequence diagram, a form of interaction diagram, that shows how processes relate to one another and in what order. This concept is based on a message sequence chart.

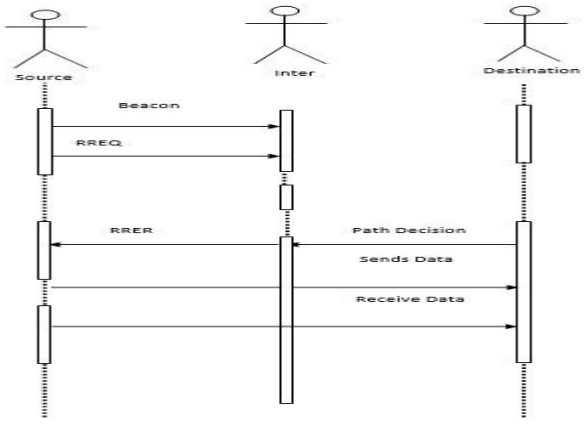

Fig.8. Sequence Diagram

ISSN: 2349-2163
https://www.ijirae.com/archives

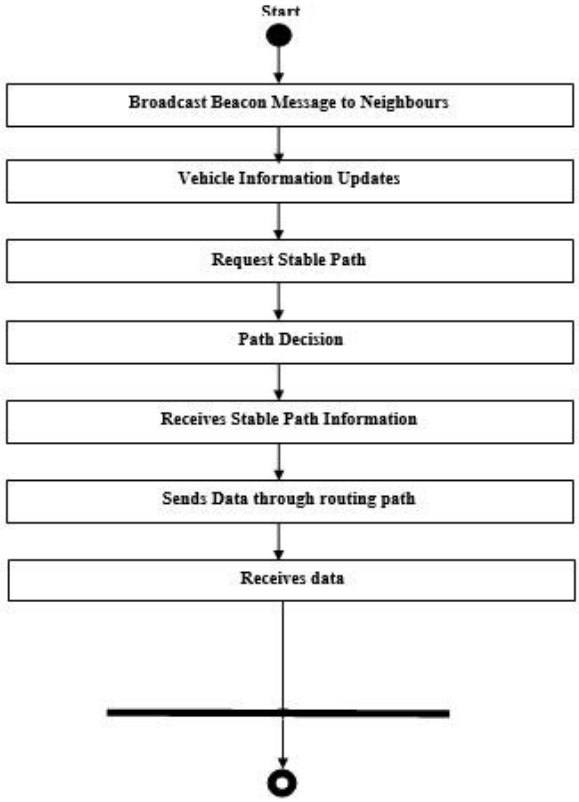

Fig.9. Activity Diagram

Fig. 9 shows the activity diagram, which represents the process of sequential activities. Activity diagrams may be used to illustrate the operational and business processes that occur in sequential order inside system components. An activity's flow diagram shows the whole control process. Fig. 10 depicts the System design of the proposed model.

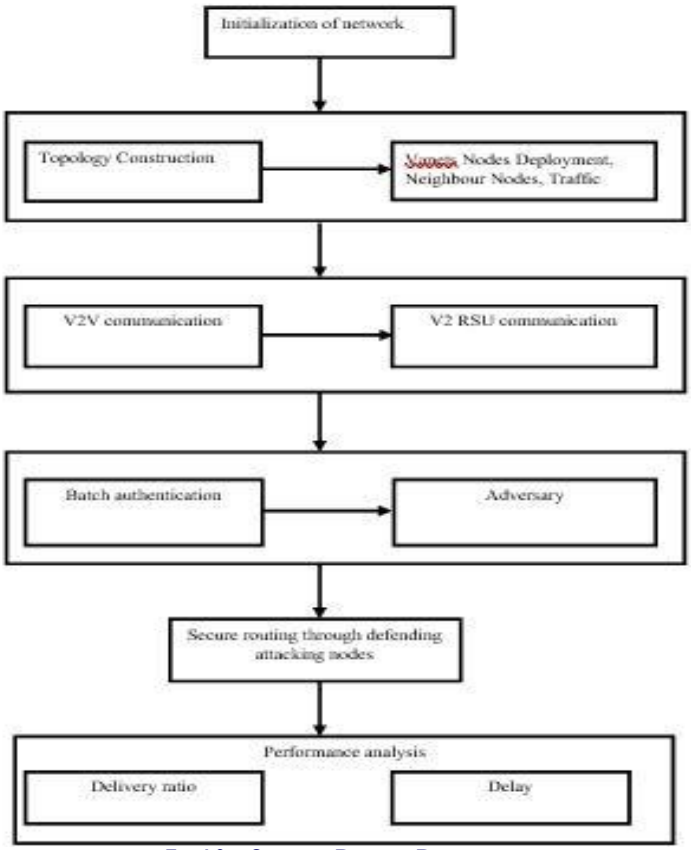

Fig.10. System Design Diagram

IV. RESULTS AND DISCUSSIONS

Here are a few screenshots that show the simulation's many stages. The snapshot of the first stage in Fig. 11 depicts the source vehicle, which is the sender node that communicates with the receiver node and delivers the information from the beacons. Any node between vehicle IDs 33 and 48 is suitable for use as a source node, however node 35 has been selected.

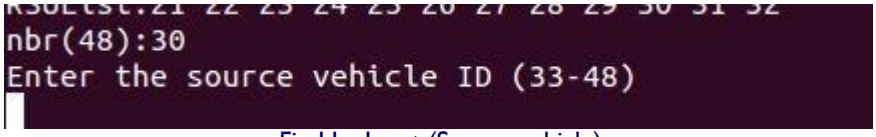

Fig.11. Input (Source vehicle).

Fig. 12 displays a snapshot of the second phase. The destination node must be given the destination vehicle ID since it is the receiver node that receives the information from the sender node. Any node between Vehicles 33 and 48 may be considered the destination node, with the exception of the originating vehicle ID, and has selected Node 48 as the destination node.

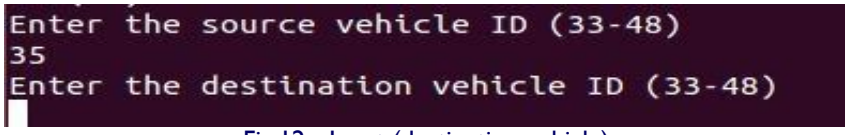

Fig.12. Input (destination vehicle).

Here, the green circle represents a trustworthy source of information, the square box at the border of the road represents the unit by the side of the road, and the circle points represent the road's nodes (vehicles). Every node, roadside unit, and trusted authority is shown in Fig. 13 together with the NS2 simulator. The request is sent from the source node to the destination node to begin a discussion. Using position-based routing techniques, the locations of the source node and destination node in the network are identified. The routing-based protocol is used to find the best path to send the information to the target node after the locations of the source and destination nodes have been established. A request will be made to the nodes that enter this route by the connection's sender node. The hash key technique is used to create a private, unique key between the communication entities. Before the key is created, the user's identification is verified with a reliable authority; the key is only created when the authority has authenticated the user's identity. The communication units trade these unique keys. The output of the NS2 simulation is depicted in Fig. 13.

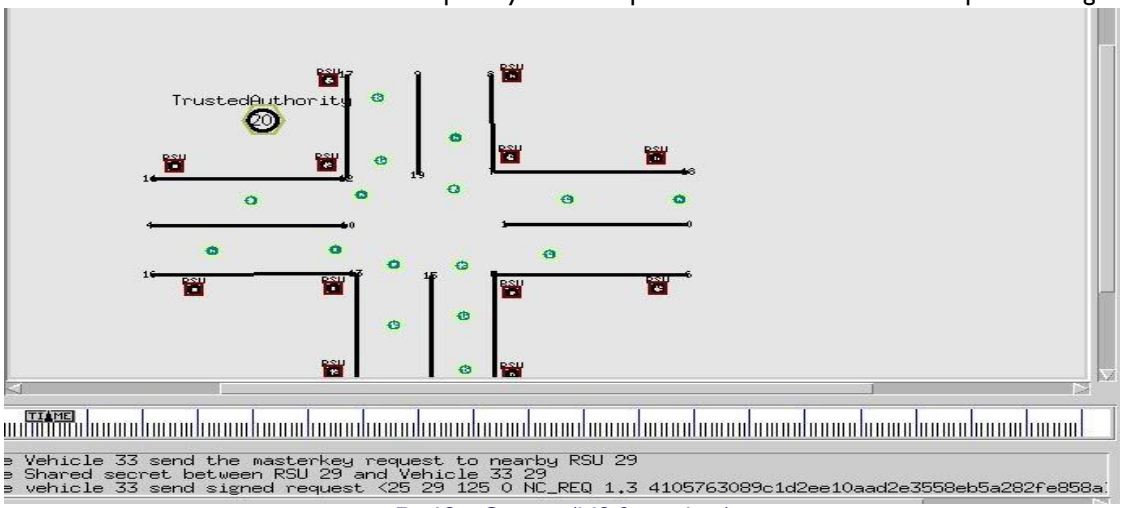

Fig.13. Output (NS-2 window).

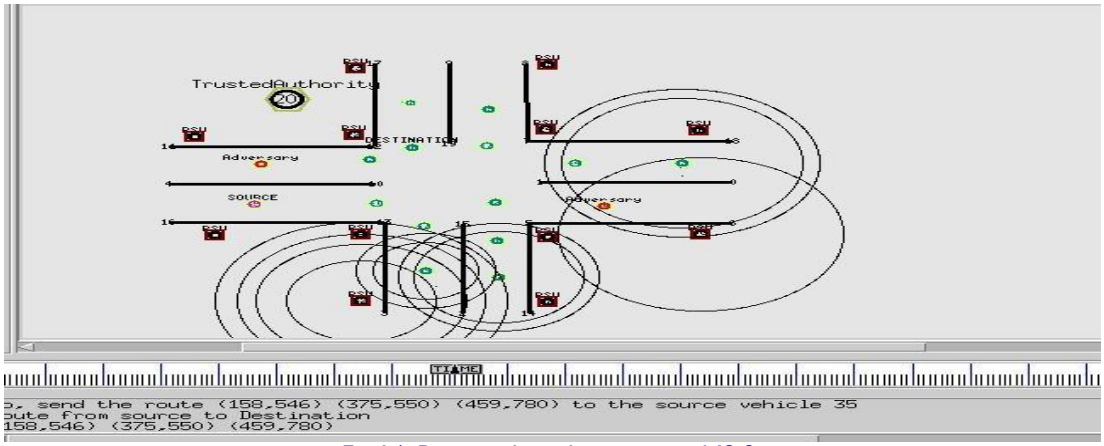

Fig.14. Position based routing on NS-2.

The malicious nodes will get a different key that does not match the key that the source node will have, and this is how the malicious node is identified and the source node learns about the adversary node in the information chain. Fig. 14's red highlights indicate the attacker node in the network.

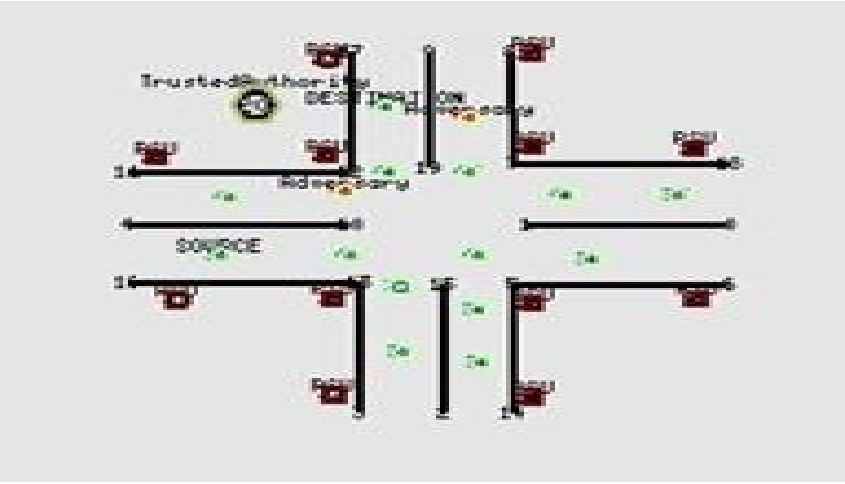

Fig.15. Segmentation of authorized nodes and malicious nodes on NS2 window.

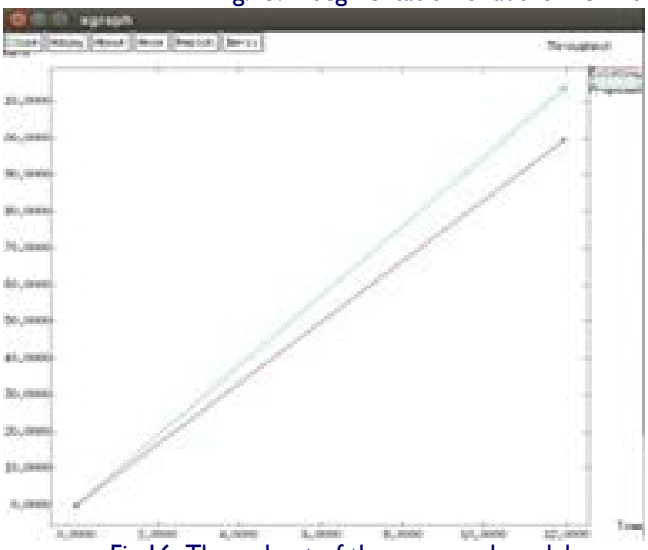

Fig.16. Throughput of the proposed model.

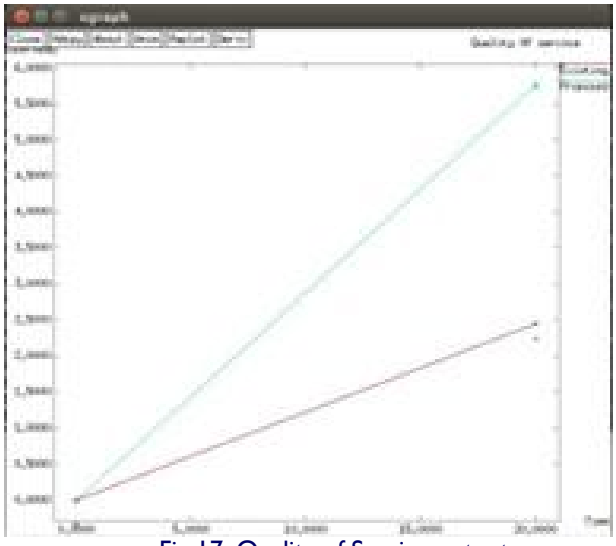

Fig 17. Quality of Service output.

Fig. 18 displays the output table where the output from the current and proposed models is compared with the study in [1].

	Existing Model	Proposed Model
Throughput	99.96	113.35
Packet delivery ratio	0.2160	0.3107
End-to-End Delay	498.76	378.68
Quality of service	2.45	5.76

Fig.18. Comparison table of the existing work and proposed work.

V. CONCLUSIONS

Following are the findings of the experiment: The Vanet, its communication security, and other protocols are the subject of extensive study in order to provide the driver with security. Vanet communication is a crucial research hypothesis. In this project, secure communication has been established between the sender, intermediate, and receiver nodes. Additionally, we have developed a protocol that satisfies the following criteria: data integrity, data origin authentication, and non-repudiation, which provides conditional privacy and security against attacks.

We have developed a vanet protocol that connects to the nodes in the range area via communication from both vehicle-to-vehicle and vehicle-to-roadside unit. We've shown how the protocol we built may be used to find and prohibit hostile nodes or other undesired nodes by alerting the server and utilising a different communication route. By using graph representation and contrasting the existing paradigm with the suggested model, we have attempted to highlight the percentage of security, bandwidth, end-to-end latency, overhead, and throughput. With the NS2 tool, one may see the whole network. The vast variety of applications for VANET protocols, including enhanced traffic efficiency, entertainment, and passenger safety, has led to a thorough examination of these protocols. Due to management problems brought on by a lack of adaptability, scalability, inadequate connectivity, and insufficient intelligence, vanet communication is having trouble keeping up with the advent of smart automobiles. The main goals of this work were to develop a security protocol that provides adequate security above the level of the existing protocol; however, more work needs to be done to raise the security percentage, specifically by enhancing data authentication, conditional privacy, and security against attacks.

REFERENCES

1. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495-1505. https://doi.org/10.1109/jiot.2018.2836144
2. Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE, 99(7), 1162-1182. https://doi.org/10.1109/jproc.2011.2132790
3. Fadilah, S. I., Abd Wahab, M. H., Mohd Shariff, A. R., Mohd Zaini, K., Shibghatullah, A. S. (2016). Improving vehicular ad hoc networks (VANET) communication performance by using time gap following distance (TGFD) model. https://doi.org/10.1109/isms.2014.123
4. Qian, Y., Moayeri, N. (2008, May). Design of secure and application-oriented VANETs. In VTC Spring 2008-IEEE Vehicular Technology Conference (pp. 2794-2799). IEEE. https://doi.org/10.1109/vetecs.2008.610
5. Eze, E. C., Zhang, S. J., Liu, E. J., Eze, J. C. (2016). Advances in vehicular ad-hoc networks (VANETs): https://doi.org/10.23919/iconac.2017.8082036
6. Challenges and road-map for future development. International Journal of Automation and Computing, 13(1), 1-18.
7. Zuo, J., Wang, Y., Liu, Y., Zhang, Y. (2010, September). Performance evaluation of routing protocol in VANET with vehicle-node density. In 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM) (pp. 1-4). IEEE. https://doi.org/10.1109/wicom.2010.5600844
8. Chen, J., Rajib, P., Choi, Y. J. (2021, January). An efficient neural network-based next-hop selection strategy for multi-hop VANETs. In 2021 International Conference on Information Networking (ICOIN) (pp. 699-702). IEEE. https://doi.org/10.1109/icoin50884.2021.9333974
9. Rajhi, M., Madkhali, H., Daghriri, I. (2021, January). Comparison and analysis performance in topology-based routing protocols in vehicular adhoc network (VANET). In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1139-1146). IEEE. 9) Liu, Y. (2021, May). VANET Routing Protocol Simulation Research Based on NS-3 and SUMO. In 2021 IEEE 4th International Conference on Electronics Technology (ICET) (pp. 1073-1076). IEEE. https://doi.org/10.1109/ccwc51732.2021.9375830
10. S. S. Tippannavar, E. A. Madappa and R. S. B, "Automatic Accident Alert System – Early Accident Prediction and Warning for the consumers," 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 2022, pp. 1-6, doi: 10.1109/MysuruCon55714.2022.9972367. https://doi.org/10.1109/mysurucon55714.2022.9972367
11. S. S. Tippannavar, S. B. Rudraswamy, S. Gayathri, S. P. Kulkarni, A. Thyagaraja Murthy and S. D. Yashwanth, "Smart Car - One stop for all Automobile needs," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 54-59, https://doi.org/10.1109/icccis56430.2022.10037715
12. Sanjay,Yashwanth,Megha,Shachee (2023). LC2BS – Low cost secondary Braking System implemented using Arduino and Motor Speed Control Mechanism, International Journal of Innovative Research in Advanced Engineering, Volume 10, Issue 02 of 2023 pages 18-23 https://doi.org/10.26562/ijirae.2023.v1002.02
13. S. S. Tippannavar, S. D. Yashwanth, M. P. Madhu Sudan, K. M. Puneeth, B. N. Chandrashekar Murthy and M. S. Vinay Prasad, "Analysis Of Performance of different Control Techniques on Anti-Lock Braking System," 2022 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), Bengaluru, India, 2022, pp. 35-40, https://doi.org/10.1109/centcon56610.2022.10051207