International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 153-159 www.ijaem.net ISSN: 2395-5252

Advanced Clustering Technique Using Securing Vehicular Ad-hoc Network against Malicious Vehicles

E. Nithya, M.C.A., [1] , P. Hemalatha, M.Sc(CS)., M.Phil.,[2]

[1,2]*Assistant Professor, Department of Computer Science, Kaamadhenu Arts and Science College, Sathyamangalam,Tamilnadu*

Date of Submission: 01-10-2022 Date of Acceptance: 10-10-2022

ABSTRACT: Vehicular Ad-hoc NETworks (VANETs) are a contemporary technology that assists a vehicle and its driver in a variety of ways. VANETs' key features are nodes, which are vehicles with reasonably high mobility and a continually changing topology. When it comes to data transmission in VANETs, a source node must rely on intermediary nodes to transfer data packets to the destination node through multi- hop paths. VANETs may provide improved performance if all of its nodes communicate effectively and cooperatively,safety. A good clustering method is necessary for network stability and network productivity. This clustering Algorithm known as Monitoring Malicious vehicle which is used to isolate the malicious vehicle from the network. This Clustering algorithm will not allow the malicious vehicle to participate in the network by blocking communication with other vehicles. The HMAC protocol is tested in Network Simulator (NS2) for speed and accuracy, and it is also compared to the AODV routing system. It has been discovered that when VANET is in a high mobility and adaptable architecture, ACT performs much better. The proposed protocol's performance is assessed using the following performance metrics: average end-to-end latency, throughput, routing load, and packet delivery ratio. The proposed protocol's performance is assessed in the presence of malevolent (route modifiers and packet droppers) vehicles, and the findings reveal that the suggested protocol achieves higher accuracy and outperforms the AODV routing protocol.

Keywords: ACT, VANET, RSU, CH, Malicious Vehicle, HMAC, AODV, Routing

I. INTRODUCTION

Capability and the extremely changeable topology of Vehicular Ad Hoc Networks (VANETs) are the most significant barriers to the widespread use of this promising technology.

Adopting an effective VANET technology with well-developed architecture is no longer an essay, which is why VANET architecture is a prominent issue among research scholars. There are several network types accessible, including ad-hoc networks, sensor networks, computer networks, and IoT device networks. One of the most significant issues in a sensor network is organising network nodes to ensure connection and optimal efficiency in terms of taken parameters. Energy is a significant component in sensor networks since battery capacity is restricted and energy limits are crucial in sensor network longevity. As a result, it is critical to create a network with a strong architecture and appropriate operation in a dedicated network, and several designs and protocols have been established to organise the sensor network. Sensor nodes are organised into distinct clusters, and one sensor node from each cluster is chosen as the cluster head (CH), who subsequently serves a unique role as a vital routing element as an alternative to the malicious node. Furthermore, each CH develops a transmission schedule for the cluster's sensor nodes. Schedule allows for automated topology change inside a cluster based only on the shortest distance with CH. The clustering notion is being used in the VANET structure. Several clustering strategies have been discovered to be used in VANET.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 153-159 www.ijaem.net ISSN: 2395-5252

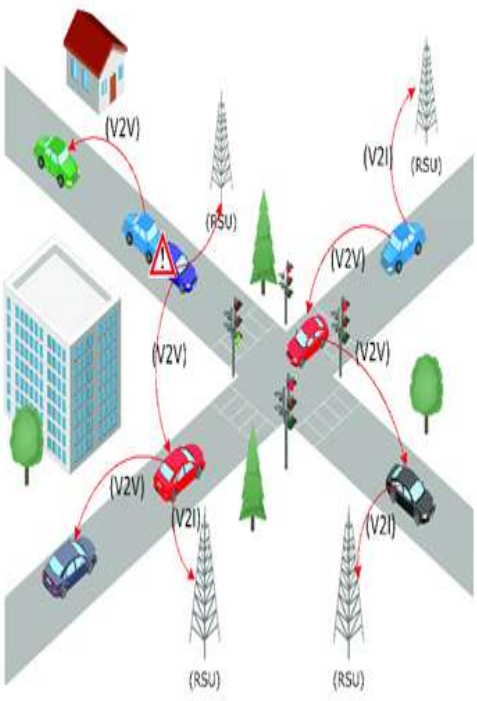

Figure 1: VANET Architecture

In VANET, a multi-expert-based stable bunching approach is used. This strategy involves RSU experts and vehicle operators. The size of the group is varied and chosen by RSU specialists based on relative versatility, which is recorded by the average speed of the significant number of cars in extends. Following the formation of the group, the RSU operator selects and selects the appropriate bunch head based on weight factor, with the vehicle with the highest weight factor selected as CH. The movement of control messages between vehicles during the bunch and group head selection arrangement introduces directing overhead into the system. We employ RSU for bunch organisation and group head selection, which helps to reduce system steering overhead. The selection of different group sizes based on all factors considered and the typical speed of vehicles will aid in the formation of long-living bunches. When reproduction is performed in NS2, the presented method outperforms in terms of bunch life time, CH choice time, and group construction time.

The primary goal for the proposed work is to construct a stable bunch based on vehicle speed and neighbour list. To complete the specified work, we use adaptable and static programming techniques. RSU operators form the group and choose the group leader, after which the group is left to function on its own. Bunch the board is completed by the group leader, and it also interacts with the group to move all other part cars.

II. BACKGROUND STUDY

In [7], a new architecture was proposed to mitigate many VANET attacks while maintaining data privacy and security. The suggested architecture uses timestamps and hashing techniques to keep the messages transmitted fresh. The trustworthiness of any node that injects false data into the VANET will be reduced significantly

Zhexin Xu suggested an innovative adaptive multichannel MAC protocol to improve the utilisation and equity of the intended time-slot allocation method for VANETs. The suggested protocol is essentially based on the concept of SD-TDMA. The goal is for collision clients to be able to participate in the time slot allocation mechanism as soon as possible following the commencement of SCHI. [8]

Laisen Nie et al offered anspatio-temporal aspects of visitors matrix are taken into account in anomaly identification, as well as a CNN-primarily based fully anomaly detection method. The hierarchical convolution and sub-sampling layers extract multi-fractal and coffee- rank characteristics thoroughly for estimating community web site visits. In addition, a threshold-based fully entirely method is alluded to in this strategy for the identification of anomalies. The simulated results claim that their suggested methodology may detect abnormalities in ordinary website online site visitors flows exactly for VANETs utilising the resource of way of reading the provided method employing the real community dataset [10].

Zhihao Ding suggested a stepped forward routing protocol in VANETs as a way of improving on the previous approach of the current GPSR routing protocol. The highlight of our suggested routing protocol is that it reduces route elimination and manual route dependability.They used mobility and MAC cast off estimates to enhance the GPSR routing protocol's following hop preference approach. Our routing protocol's strategy is entirely dependent on vehicular digital devices, which may provide a massive quantity of vehicular data. They provided mobility information (velocity and route) as well as MAC remove estimate in the succeeding hop choice approach to improve the direction's reliability and decrease waste. [11]

Mohit Virendra. aim of [12] was to achieve trust on the basis of keys in mobile ad hoc networks. The trust based physical logical domains

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 153-159 www.ijaem.net ISSN: 2395-5252

was introduced for grouping nodes and getting distributed control over the network..

N. B. Gayathri et al. have developed a green certificates-a lot less authentication system for batch verification in VANETs. The suggested approach does not make use of bilinear pairings over elliptic curves. In terms of authentication, integrity, privacy, non-repudiation, traceability, anonymity, and revocation, the suggested approach is friendly. Our methodology employs a batch verification method to validate a pair of signatures in a single example, significantly reducing the computational effort on RSUs [13].

Mumin Ozpolat et al. suggested a tractable insurance model for city mmWave ad hoc vehicular networks for two specific cases. It is well known that line methods may be used to version vehicular networks, which facilitates assessment. The mathematical model, which was built with the help of Monte Carlo simulations, revealed that city mmWave ad hoc vehicle networks have a likely usable resource entirely connected visitors, which, in comparison to VANET, is more sensitive to a rise in transmitter density [14].

Xinxin He et al. presented a tighter TC with higher high quality in a large-scale fading environment. Within the Rayleigh fading environment, a basic expression of TC applied to a sparse site visitors scenario and a TC improved application to a dense net web page website online site visitors scenario are derived. As a consequence, in a dense visitor scenario, the TC of a linear VANET under Rayleigh fading channels is determined using the basic formula [16].

Zhiwei Yanget et al. provided a totally new clustering set of rules for VANETs with the helpful resource of considering automobile navigation routes. Based entirely on the overlapping insane portions of routes from unique motors,they created a feature to predict the duration that motors may likewise additionally additionally moreover continue to be buddies in future voyage. Cluster heads are chosen based entirely on the total period that a vehicle may keep its network in the future. Their recommended approach type of parameter has progressed universal normal performance metrics, along with the presence of clusters, and a broad range of reputation changes [19].

III. SYSTEM MODEL

The attacker affects and modifies the nodes such that they do not relay information. These occupy the information that is produced by nodes and is sent. The reprogrammed nodes are known as black hole nodes, and the area in which they are located is known as the black hole region. During the communication process, the Sybil attacker connects with the other node using a one-hop mechanism. In such case, each node has access to any other regular node, and it is the simplest approach to get data from nodes such as node location and id. Every node has sensible agents that are localised to preserve the accept as true with and neighbour node records. The dynamic consider updating mechanism is maintained by making use of some of the following matrices. They are the amount of power spent, the community's latency, the number of lost packets, node capabilities, and neighbour node collaboration.

Message Authentication and Integrity: A hub vehicle should be able to authenticate that a message was delivered, passed, and tagged by an outside hub or vehicle (or a legal gathering portion) without being altered, modified, or changed by anybody.

Identity protection Isolation security: A vehicle's actual and distinct personality should not be linked or related to any message so that other cars or even RSUs can't expose a vehicle's true character by breaking down numerous messages delivered by it.

Traceability: As far as I am aware, a vehicle's true nature should be concealed if and when necessary. The TA should be able and in a position to recognise and understand a vehicle's true nature and link the message to the sender.

Vehicle Deployment and Network Construction: VANET is a network of nodes that are moving VANET's goal is to offer communication amongst exceptional nearbyvehicles.

Mobile Domain: This domain is divided into two parts. Vehicle domain, which includes all moving vehicles such as buses, trucks, and so on. The second component consists of mobile devices, which include all portable devices such as PDAs, laptops, and smart phones.

Infrastructure Domain: It has two folds as well. Road- side infrastructure comprises of stationary road-side entities such as traffic signal poles and so on, while centralised infrastructure domain consists of a central management centre, traffic management centre, and so on.

Generic Domain: It includes both network infrastructure and personal infrastructure, such as all internet mobile and data servers that support

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 153-159 www.ijaem.net ISSN: 2395-5252

VANET architecture.

The communication between all VANET devices is accomplished via the use of a wireless channel known as wave. This kind of connectivity and message transmission provides us with a wealth of information to drivers and passengers, as well as allowing security apps to improve security and provide a more comfortable driving experience. The most important gadget components are the utility (AU), (OBU), and (RSU).

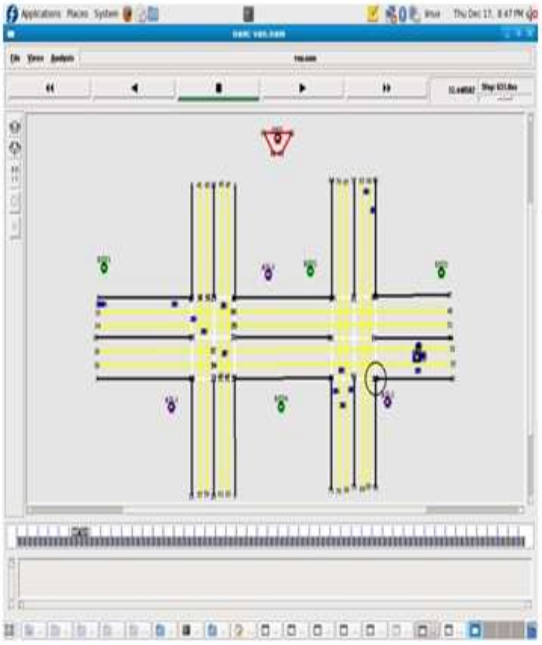

Figure 2: Roadmap generation using Ns2 simulation tool.

On board unit (OBU): An OBU is a wave gadget generally mounted over vehicle the fundamental primary work of the OBU are

1. Positive message move.
2. Wireless Radio access
3. Specially appointed and Geographical directing
4. System clog control
5. Information security and IP versatility.

B. Application unit (AU): The AU is a circuit device built within the vehicle mode that employs the applications programming provided by the provider while employing the OBU's communication capabilities. The AU is used to operate the Internet [8]. The AU can be a devoted circuit gadget for security applications or a standard gadget, for example, a single computerised associate to run the Internet. The AU can be interconnected to the OBU through a wired or remote association and may live with the OBU in a solitary physical gadget unit the distinction between the AU and the OBU is coherent.

Roadside Unit (RSU): The RSU is a remote device that is often located along the street side or in designated places, such as junctions, squares, streets, or near parking spaces. The RSU is outfitted with one system gadget gear for a dedicated brief small - extension correspondence based on IEEE802.11p radio-based innovation, and it may also be equipped with additional system gadgets to be used for correspondence within the infrastructural arrange.

1. Extending the correspondence scope of the specifically designated system by re-circulating data to various OBUs and transmitting data to various RSUs in
2. Executing security applications, for example, a low scaffold mishap cautioning or work zone using framework infrastructure to vehicle (I2V) and acting as a data source.
3. Making Internet access available to OBUs.

Attack Construction:

An attack launched by an external source against a portion of a network's nodes. The attacker affects and modifies the nodes such that they do not relay information. These occupy the information that is produced by nodes and is sent. The reprogrammed nodes are known as black hole nodes, and the area in which they are located is known as the black hole region.

The sensor nodes in the network are represented by the little green circles. The black hole area is the name given to the holding zone. The attacked intruded route traffic is always automatically discarded. The black hole area serves as the entry point for a huge variety of assaults. Because of the attacker's activity, the network's quality of service is greatly impacted, resulting in packet loss, increased latency, and lower throughput.

A Sybil attack produces a large number of identities from the same faulty node. This form of attack is the most hazardous to the VANET since it serves as a gateway for other types of assaults such as wormholes and sinkholes. The Sybil attacker is created when one node talks with another using a one-hop mechanism during the communication process. In such case, each node has access to any other regular node, and it is the simplest method to get data from nodes such as node location and id, among other things. Using this information, the attacker node will generate similar ids in order to launch assaults on the regular nodes.

Clustering Technique:

The trust-white value of the nodes, the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 153-159 www.ijaem.net ISSN: 2395-5252

trust value of the route, and the coverage area of the nodes that are directed to the child nodes by a fuzzy based cluster This technique focuses on cluster routing via the use of a fuzzy (fcm-fuzzy cluster mechanism) approach in which the cluster head is chosen at random and all nodes have the same amount of strength. The nodes with the most spiritual force are chosen as CH.

Because the method is one of the centralised CH choice algorithms, the CH is responsible for consumption of energy calculation and direction routing considerations decision here, the major advantage is to decrease the node distance. On the introductory condition accept as true with price is suggested the use of the immediately talk with the neighbour communicate nodes. There are sensible agents in each node who are localised to manner and accept as true with, and neighbour node records are also kept. The dynamic consider updating mechanism is maintained by making use of some of the following matrices. They are the amount of power spent, the community's latency, the number of lost packets, node capabilities, and neighbour node collaboration.

NSO Optimization:

Node Swarm Optimization (NSO) is a technique of development in which regular species social fundamental practises are taken into account with the ultimate goal of computation. It is a swarm intelligence system that relies on the populace to execute an improvement procedure
with the goal of improving a wellness work. This technology employs a swarm with the purpose of searching on each node and recording the health assessment of each molecule. The particles are then linked with their coordinating speed. It will help the node make the shift to a legal region by taking into account the enhanced wellness capacity's cost. From every piece of information nearby, best position increases the worldwide best situation to identify the group head position in order to limit the overall vitality consumption. When compared to other scientific and heuristic techniques, PSO calculationhas higher productivity and throughput.

HMAC- cross layer Approach

- Initially, the node begins by determining the best intermediate node from the location. This is made feasible via the periodic dissemination of greeting messages. In this example, the greeting message is exchanged every 30 seconds. And the hello memory is then transmitted between nodes, enabling the nodes to discover the next neighbour and the information is saved in the neighbourslist.
- The node begins sensing important characteristicsand sends data to the destination using CSMA technology. This technique is repeated until two requirements are met. They are as follows: (a) there should be no rise in traffic load; and (b) there should be no emergency packettransmission.
- The transmission of high-priority region-based data has started. If any node is detected as being in the high precedence area, those surrounding nodes store the data and switch to TDMA, providing the current slot to the node that is in thehigh precedence zone.
- If two nodes occupy the high priority zone in the current slot, they will be allocated to transmit data one after the other. Finally, CSMA mode will be enabled.
- The packet contains all of the node identifying information, and those data are transferred together with the packets, increasing the speed of data flow from one node to another. The buffer level of the node furthest from the sink is extremely low, causing the node to migrate closer to the sink node in order to boost the buffer level. The network's threshold value is specified here to compute total memory availability.

IV. RESULTS AND DISCUSSION

The Proposed ACT method to implemented by using Ns2 simulation tool. In existing AODV protocol has compared with the proposed protocol. The comparison charts like delay, PDR, Energy, Routing overhead, packet loss, throught parameters are given.

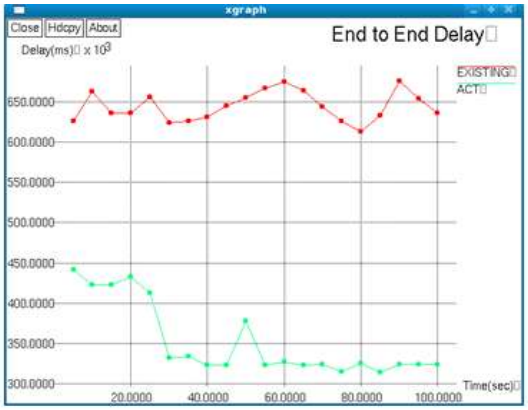

Figure 3: End to End delay comparison chart

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 153-159 www.ijaem.net ISSN: 2395-5252

Figure 4: Packet delivery ratio

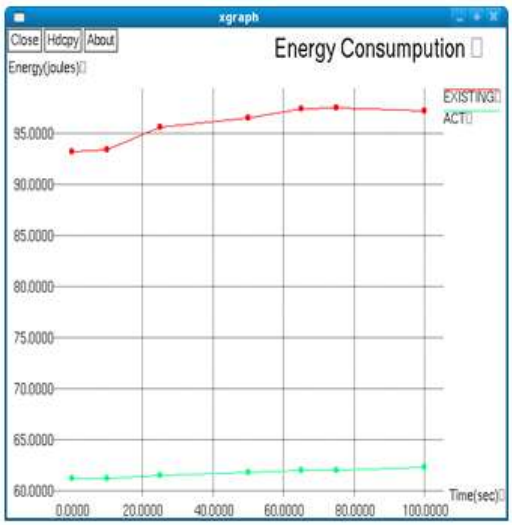

Figure 5: Comparison chart for Energy consumption

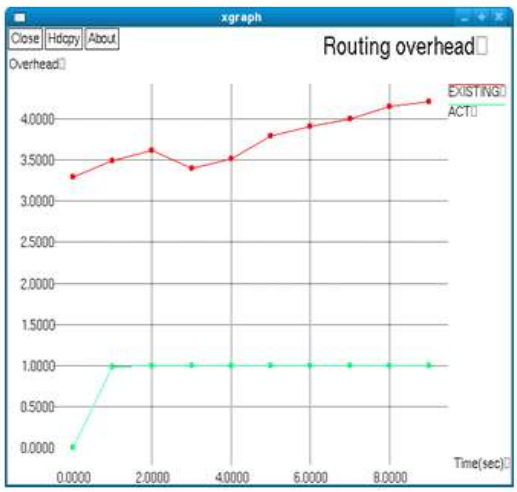

Figure 6: Comparison chart for routing overhead

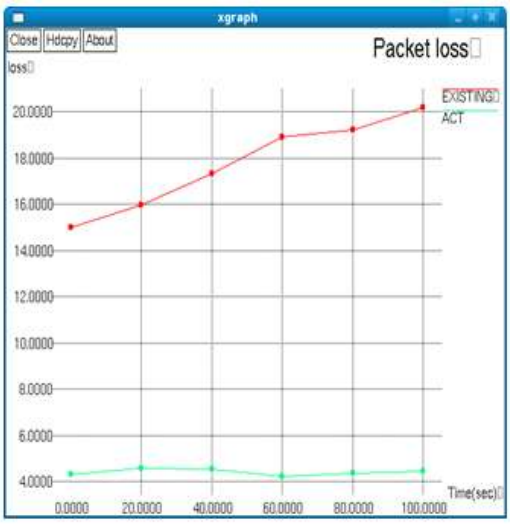

Figure 7: Packet loss comparison

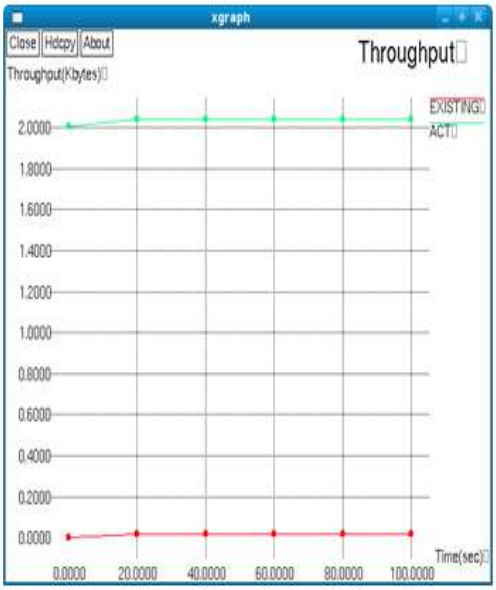

Figure 8: Throughput comparison chart

In figure 3 to 8 are represented the comparison chart for the delay, PDR, Energy, Routing overhead, packet loss, throught parameters. When comparing the Existing method AODV protocol, the proposed method achives the better performance.

V. CONCLUSION

The network connection is an essential requirement in the case of VANET, and the security of the vehicular ad hoc network is greatly rising day by day due to the adoption of transportation systems. The issues of VANET security must yet be addressed for fully protected VANET environments. The Advanced Clustering Technique (ACT) method that we devised is a

scalable mechanism that makes effective use of the number of equipped cars travelling in a road section to estimate overall traffic density optimally. An ACT technique has been presented for creating a stable cluster in VANET and removing rogue nodes from the network. The advanced clustering approach is used to offer a stable cluster head and to remove malicious nodes, the PSO optimization is used to generate node records and to estimate their health, and lastly the HMAC protocol is used for energy efficiency. We will continue to enhance the PDR and communication overhead.

Furthermore, evicting any selfish node encourages selfish nodes to collaborate. Through simulations, we demonstrated that our scheme could detect and evict all malicious nodes from the VANET while simultaneously increasing throughput and minimizing delay. Our solution encourages all nodes to participate in providing accurate information without being self-serving. We want to use a verification tool in the future to ensure that our scheme is robust to various attacks and that it only selects the most trustworthy nodes in the VANET. Furthermore, we would like to conduct a similar analysis on a real-world system

REFERENCES

[1]. ZhexinXu et al," Adaptive multichannel MAC protocolbased totally on SD-TDMA mechanism for the vehicular advert hoc network", IET conversation, Vol. 12 Iss. 12, pp. 1509- 1516, 2018.

[2]. Milind R. Penurkar et al," Opportunistic Routing set of rules for routing messages in Emergency situations the use of Vehicular put off Tolerant network",IEEE,2018

[3]. Van O et al," Combining Spatial and Social recognition in D2D Opportunistic Routing", IEEE Communications magazine,2018.

[4]. Ms. Varsha T. Lokare et al." Markov Chain based totally absolutely Opportunistic Routing Protocol to beautify the overall overall performance of the MANET", IEEE XploreCompliant, 2018.

[5]. Li et al," glide-layer and reliable Opportunistic Routing algorithm for cell advert Hoc Networks", IEEE, 2018.

[6]. Hajer Ben Fradj et al," Comparative have a have a have a have a look at of Opportunistic Routing in wireless Sensor Networks",IEEE,2018

[7]. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors 2019, 19, 4954. [CrossRef].

[8]. ZhexinXu et al," Adaptive multichannel MAC protocol based on SD-TDMA mechanism for the vehicular ad hoc community", IET Commun., 2018, Vol. 12 Iss. 12, 2018.

[9]. Xiaoping Yang et al," development of GPSR protocol in Vehicular ad hoc community", IEEE, 2018.

[10]. Laisen Nie et al," Spatio-Temporal network website internet web page traffic Estimation and Anomaly Detection based totally mostly on Convolutional Neural

[11]. community in Vehicular ad-Hoc Networks",IEEE,quantity4,2018.

[12]. Zhihao Ding et al," Mobility based Routing Protocol with MAC Collision development in Vehicular advert Hoc Networks", IEEE, 2018.

[13]. Mohit Virendra, Murtuza Jadliwala, Madhusudhanan Chandrasekaran and Shambhu Upadhyaya: Quantifying Trust in Mobile Ad-Hoc Networks, Integration of Knowledge Intensive Multi-Agent Systems, 2018.

[14]. N. B. Gayathri et al," inexperienced Pairing-loose Certificateless Authentication Scheme with Batch Verification for Vehicular advert-hoc Networks", IEEE, 2018.

[15]. MuminOzpolat et al," A Grid-primarily based completely insurance assessment of city mmWave Vehicular advert Hoc Networks", IEEE, 2018.

[16]. Leandro N. Balico et al," Localization Prediction in Vehicular advert Hoc Networks", IEEE, 2018.

[17]. Xinxin He et al," Transmission potential assessment for Vehicular advert Hoc Networks", IEEE, 2018.

[18]. Abdel-Mehsen Ahmad et al," Chain-primarily based absolutely records Dissemination in Vehicular advert-hoc Networks", IEEE, 2018.

[19]. Abdul Rahim Ansari et al," correct 3-D Localization method for Public safety packages in Vehicular advert-Hoc Networks", IEEE, 2018.

[20]. Zhiwei Yang et al," Navigation direction based genuinely robust Clustering for Vehicular advert Hoc community", IEEE, 2018