Vehicular Ad-Hoc Networks (VANET)

Danda Nandhini[1] , Dr. K Suresh Babu[2]
Master of Technology[1], Associate Professor[2]
Department of Computer Science,
JNTUH School of Information Technology,
Hyderabad, Telangana, INDIA,500085

Abstract:- Wir simulate VANET connection using NS2 and several protocols such as ADV, DSDV and DSR and then compare their performance using PDR (PDR). High PDR protocols are regarded as efficient and dependable. We're utilising packet encryption and decryption in our project to keep communications between cars safe. Both vehicles will send and receive encrypted signals about the distance and other traffic conditions while they are in close proximity, and these messages will be decoded when they are received. The VANET sensor cannot be hacked by anyone who is able to decipher the messages that are exchanged in the network.

Our SUMO simulator is used to produce traffic mobility traces, which are then used to calculate protocol performance in NS2. The NS2 protocol will send alerts when a car arrives within a certain distance of another vehicle in this trail.

When two vehicles get within a certain distance of one another, they exchange encrypted and decrypted distance messages, and one of the vehicles will halt and resume motion when the road is clear. I'll present the implementation in video so you can see the results for yourself.

I'll plot the PDR performance of the DSDV, AODV, and DSR protocols after they've all been run.

Keywords:- *VANET; NS2 Protocol; SUMO Simulator; AODV; DSDV; DSR.*

I. INTRODUCTION

Since the beginning of wireless communication, VANET has been one of the most important fields of research. Taking a look at VANET's history before getting into its specifics is a good place to start. It is safe to say that all ad hoc networks descend from WANET, which is represented in Figure 1. There's no need for a third-party infrastructure when it comes to VANET, the sibling of MANET. Due to its simplicity and essential nature, MANET is widely employed in the military. similar to that of data exchange among multiple computers. VANET has several similarities to MANET but also some differences. Mobile nodes (MN) and roadside units (RSU) make up the VANET (Yong et al. 2016). Sensors that are embedded in the vehicle and used for signal processing (data sharing) between RSUs and RSUs' RSUs are known as on board units (OBU). MN and the internet are connected via RSUs, which are located in fixed sites. An internet-based service that promises to prevent traffic accidents is one of the VANET's offers.

The development and deployment of vehicle ad hoc (VANET) networks is critical to the development and deployment of self-driving and partially self-driving vehicles (SDRVs).which is why VANETs are of tremendous interest. The VANETs are vulnerable to a wide range of attacks. In automobile ad hoc networks, security is a major concern [1]. In this study, we explore DoS (denial of service), black hole/grey hole, wormhole, and rushing attacks on the network layer. As part of our research, we've developed an IDS to protect the network layer of VANETs against potential attacks. Since routing protocols are used at the network layer, it is necessary to have a security system for them. Proactive, reactive, or hybrid routing is used in ad hoc networks. Use of a reactive routing system such as on demand vector is common in autonomous cars (AODV). The AODV protocol was chosen because of its high throughput, minimum delay, and sequence numbering [3]. When AODV is compared to other routing protocols, the sequence numbers help it perform better. Communication with the outside world is critical for autonomous and semi-autonomous vehicles, which rely significantly on external communication. This can be done by thwarting collaboration by attacking RSUs and vehicles with attacks like the grey hole and rushed attacks [2]. An important feature of VANETs is that they allow traffic from mobile devices and roadside infrastructures to exchange packets, but rogue nodes generate chaos or drop packets instead of forwarding them to their intended destinations. A "grey hole" attack could target the network layer of an autonomous vehicle's communication system. For security reasons, packets that are intercepted and not intended for their designated receiver are rejected. Increased overhead and lower packet delivery rate (PDR) [2] are also possible consequences of attacks. It is difficult to distinguish between normal and malicious behaviour in AODV assaults because of this. It is possible to direct a network to send all packets to a new node, but it can then be instructed to gradually drop some or all of the packets it receives from the new node. DoS attacks against on-demand ad hoc network routing protocols like AODV can be extremely damaging to routing technologies like AODV and DSR. During the road discovery phase, the source vehicle uses VANETs to transmit RREQs (road requests) to the destination vehicle. As a result of this phenomena, running cars will receive and transfer packets without any delay (zero latency) [5]. A node that was pushed into receiving the packet will discard it as a duplicate because it had received it from the attacker. [5] If these attacks are near the source or destination vehicles, they are more effective. In self-driving or semi-semi-semi self-driving cars, external and internal communication systems are critical. A multitude of problems can arise for vehicles in these networks, including the inability to access essential information. Figure 1 shows a VANET.

An IDS for autonomous and semi-autonomous vehicles is presented in this research to protect external communication against grayhole and hurried attacks. Suggested real-time detection of anomalous behaviour prevents anti-malicious vehicle communication.

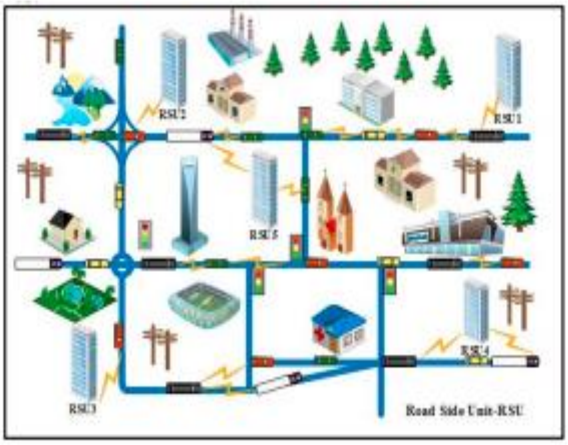


Fig. 1: An illustration of how emergency situations are handled on the road

For example, the IDS uses the simulator's trace files to identify both normal and abnormal VANET behaviour. There is a direct correlation between the quantity and kind of features in the proposed security system and its detection rate and false alarm rate. Based on our prior research [6,7], From the trace file, we were able to identify an important feature. SVM and feed forward neural networks are the foundations of our suggested IDS (FFNN). The usefulness of these artificial intelligence networks, particularly in self-driving automobiles, has been extensively studied.

II. LITERATURE SURVEY

A. *SelfDriving Vehicle Networks: Detection of Grey Holes and Rushing Attacks:*

Cargo ad hoc networks are critical to the development of self-driving and semi-autonomous vehicle networks. These networks assist passengers, drivers, and vehicles alike. In order to anticipate the surrounding environment, these vehicles exchange cooperative awareness messages (CAMs) and control data. VANETs must contend with a slew of dangers, including black hole, grey hole, and hurried attacks. IDS that employs anomaly detection to protect external communications from grey hole and hurried assaults is presented in this paper. According to numerous studies, grey hole assaults in VANETs provide a big challenge since they have two distinct forms of behaviour: normal and abnormal. These attacks, which try to block transmission, have a direct and negative impact on the mainstream acceptance of this new class of autos. Using a network simulator's trace file, a suggested IDS uses features collected from the trace. A support vector machine and a feed-forward neural network were used to create the intelligent IDS in our article. The suggested approach uses the trace file's most critical properties. If you want to reduce false alarms and detection rates, it's best to remove unnecessary features.

B. *The results of a comprehensive survey on security services in mobile ad hoc networks*

Drivers and passengers alike will benefit from using Vehicular Ad hoc Networks (VANs) to access safety and other information apps (VANETs). On board units (OBUs) and wireless communication devices form a network in a VANET, which is self-contained and independent. As a result, VANETs are critical to the development of smart transportation in the future. Despite the widespread use of VANETs, various security vulnerabilities and challenges must be addressed before they can be implemented in practise. Security measures in VANETs have been extensively explored, however they have not been proven to be useful. VANET characteristics and security issues are discussed here. Other frequent threats, such as availability and confidentiality and authentication and integrity and non-repudiation are also described.

C. *Vehicular Ad Hoc Network Security Threats:*

Car-to-car and car-to-roadside communication are two ways in which the Vehicle Ad Hoc Network (VANET) improves road security and alleviates traffic bottlenecks in smart transportation systems. Although VANET security is a worry, experts are becoming more concerned. VANET stands out from other ad hoc networks because of its dynamic topology and hybrid structural design. Due to their importance in VANETs, the development of security measures to verify and delete harmful transmissions must take place. Initially, we'll review the security threats that VANET confronts and possible solutions to those threats. Next, we'll divide the defence systems into important categories and undertake critical evaluations of their performance. As a result, we've put up a list of open VANET security research questions that we hope will stimulate the interest of academics.

D. *Issues of Routing in VANET:*

In addition to VANETs, there are other subclasses of mobile networks. Wireless connection between autos and roadside infrastructure devices is made possible via VANET. Vehicle-to-vehicle communication enhances safety, convenience, and pleasure. The quality of communication is directly influenced by network routing. routing protocols dictate how data travels via the network. VANET routing protocols were analysed in this study. It was our major goal to find the optimum way for ad hoc routing in VANETs, and we wanted to know which one worked best. VANET routing protocols were tested on a highway and in a city. The finest routing protocols were selected after a thorough literature review. The protocols were evaluated based on their throughput and packet drop metrics. We used MATLAB to generate a graph to compare the results of several routing algorithms. It was also calculated to highlight the disparities in the outcomes of each scenario. We may conclude that A-STAR performs best in city contexts, while GPSR performs best in highway environments. Using VANET's position-based routing solution, we discovered that it outperformed traditional topology-based routing in a wide range of cases. A universal routing protocol for VANET, however, does not exist. Since vehicle speed, driving environment, and other factors influence the selection of one routing protocol, it is difficult for a VANET to select a single protocol that is appropriate. Distinct types of networks may have a different effect.

Thousands of people around the world have been killed in traffic accidents [8]. VANETs for intelligent transportation systems will make future transportation safer for people and cars (ITS). Their purpose is to improve traffic systems and reduce human error-related accidents in order to assure the safety of road users. In real-time applications, warning messages and cooperative awareness messages (CAMs) between self-driving vehicles and remote sensing units (RSUs) are crucial. Consequently, VANET security is a major priority. Some research aims to improve VANETs' defence systems against malicious attacks. VANETs are vulnerable to hacking, and this study proposes a novel approach to securing VANETs against this threat. An important element of this new approach is a system for verifying messages to ensure that all participants are informed of the current status. Using this method, researchers can reduce the number of attacks and manage the dangers. The security technique given by Banerjee can detect and neutralise grey hole and black hole attacks on MANETs. In instead of transmitting all of the data in one direction, the data is broken up into equal blocks and sent to the target node via a different path. The system can identify a malicious route if the received data is different in size from the transmitted data because the destination node validates the sent data's size. [9] There is a path and a group of hostile nodes that must be avoided, and this is where resending data is necessary [9]. In order to safeguard Wireless Mesh Networks (WMNs) from rushed attacks, Reddy et al. developed cross-layer intrusion detection (CLID). The CLID was implemented at the network and MAC layers to reduce false alarms. A network simulator was used to test the security system that had been proposed by the cooperative intrusion system. Al Shahrani has tackled the issue of SDSR overhead and time in two different ways [10]. An intrusion detection system developed by Pavani et al. made it possible to identify both black hole and grey hole assaults on MANETs. Decision Tree (C–4.5), Multilayer Perceptron (MLP), K-Nearest Neighbor (KNN), and Support Vector Machine (SVM) algorithms were all used in the research (SVM). The proposed method was tested on the network simulator version 2 (NS2). There were less false positives and a higher degree of precision when using MLP to detect intrusions in the studies. In order to create an intrusion detection system, Kaur et al. utilised a backpropagation neural network [12]. This security solution was created in the first place to guard against black hole attacks on MANETs. The researchers were able to demonstrate the effectiveness of ANNs by using a range of performance measures to evaluate IDS efficacy in MANETs. Detection techniques employed by IDSs fall into two categories. Anomaly detection [13] and misuse detection are two examples of these methods. In our research, we talk about a security system that looks for anomalies. Signature-based or other attack detection systems are incredibly accurate and produce very few false alarms, but they are unable to detect newly found threats. Anomaly or behaviour detection relies on nodes' typical behaviour. An attack is any behaviour that deviates dramatically from the norm. These anomaly detection systems are computationally expensive and difficult to manage tiny changes in behaviour in addition to their high rate of false alarms.

E. Existing system:

VANET security is vital for the safety of passengers and drivers. Algorithms must be developed to ensure the safety of the system Security services include access, confidentiality, authentication, data integrity, and nonrepudiation.

III. PROPOSED WORK

VANET Security Detection and Prevention

A. Research methodology:

a) VANET characteristics:

As in VANETs, ad-hoc wireless communication is commonplace. The properties of a VANET are a blend of those of a wireless medium and those of an ad hoc network. Here are several VANET-specific traits that are discussed.

VANETs are more mobile than MANETs, on average. It's common for the nodes in VANET to travel at rapid speeds. As a result, the network's nodes are more mobile, which minimises the amount of time they spend exchanging information.

Due to the rapid mobility of vehicles, the topology of VANETs is constantly changing, making it a highly dynamic network. To attack the entire VANET network, attackers need only exploit a vulnerability in the network's topology, making it difficult to identify rogue vehicles.

It is imperative that VANET nodes get information in a timely manner so that they can make decisions and take appropriate actions in response to the information.

VANETs don't have the same power limits as MANETs because the OBUs have long-lasting batteries that provide constant power.

A VANET's network density varies depending on vehicle traffic density, which can be low in rural and suburban regions and high during traffic jams.

There are frequent disconnections between the vehicles and the VANET network due to wireless connectivity. Vehicle nodes may periodically disconnect from the network due to the dynamic topology, extreme weather, and the high density of vehicles.

Data transmission in VANETs should be anonymous because of the usage of the wireless media as the transmission medium. It is possible for anyone to malfunction on the same frequency if the wireless communication medium is not adequately safeguarded.

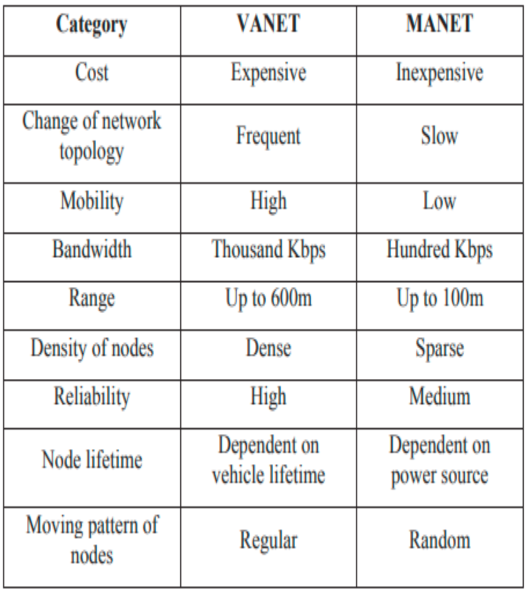
From 0.01 dBm up to 28.8 dBm, the highest transmission power of WAVE design is possible, and the related coverage distance spans from 10 metres to 1 kilometres. Since the transmission power is so low, the coverage area is limited.

Reflection, diffraction, refraction, and scattering in urban areas limit the performance of DSRC wireless communication.

There are no issues with VANETs' computing power or energy storage capacity. In large-scale contexts, processing massive amounts of data is a need, and it is unquestionably a difficult problem to solve.

Vehicle-to-vehicle networks (VANETs) are a subset of MANETs in which all of the nodes are vehicles. VANET, on the other hand, There are several differences between the two, notably the higher expense. Compared to MANET, VANET's network topology changes more frequently due to the greater speed of vehicles over mobile nodes. If you're using a VANET or a MANET, the nodes follow a preset path. Compared to MANET, VANET's mobility signalling is more sophisticated, requiring a larger bandwidth. On the basis of this table, it's easy to discern the distinctions between VANET and MANET.

Table I: Differences between VANET and MANET.



Category	VANET	MANET
Cost	Expensive	Inexpensive
Change of network topology	Frequent	Slow
Mobility	High	Low
Bandwidth	Thousand Kbps	Hundred Kbps
Range	Up to 600m	Up to 100m
Density of nodes	Dense	Sparse
Reliability	High	Medium
Node lifetime	Dependent on vehicle lifetime	Dependent on power source
Moving pattern of nodes	Regular	Random

Table 1

Nodes in VANETs are highly mobile. VANET has a variety of ways to communicate. Vehicle-to-Vehicle (V2V) communication, as depicted in Fig. 1, is possible between two vehicles. Vehicle to Infrastructure (V2I) communication is also necessary for cars to exchange information with roadside infrastructures. In addition, roadside units and infrastructures connect with each other on the roadside. Due to the great mobility of VANET, communication is quite difficult.

One sort of application on VANET is primarily concerned with safety, while the other is concerned with providing additional convenience.

Examples of safety applications include: The ultimate purpose of these VANET apps is to save human lives on the street. These safety apps have as a feature the delivery of safety-related data to the actual recipient in real time. Listed here are some safety-related uses:

It is in this category that lane-changing messages, CCA, and navigation are all included. It is the fundamental goal of CCA to avoid collisions. These programmes will promptly notify the driver if a collision is imminent, so they can turn the vehicle or lower the speed and avoid a collision (s). If one of your vehicles detects an accident, you may be notified to take a different route.

Information Messages (IMs) include toll booths, construction zones, and speed limitations.

Post-crash, obstacle, stop light (ahead), toll point, and road condition warnings (WMs) are all instances of WMs. On detection, vehicles may begin delivering warning messages (WMs) to other vehicles in the area, helping them avoid collisions.

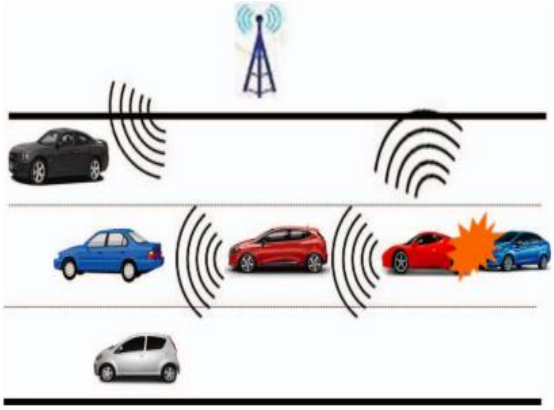


Fig. 2: This is a safety application: a warning that an accident may occur.

B. Comfort Applications

Comfort applications are aimed towards improving passenger comfort and enhancing the efficiency of transportation. VASs (Value Added Services) that can be used by VANET can include these applications. There are a number of applications that could be useful to long-distance car passengers.

The following are a few examples:

- Automated toll collection: Payment is made electronically using this service. As a result, there is no need for a vehicle to stop to pay fines.
- The location of restaurants, gas stations, retail malls and ATMs can be sent to the vehicles for use in location-based applications. Using a vehicular network, these data can be sent between vehicles in order to make travel easier.

- In Fig. 3, passengers can connect to the Internet while riding in a vehicle. They have access to the internet and can use it to receive and send email. The expense of installing infrastructure along the roadside can be reduced by distributing these information via automotive networks.

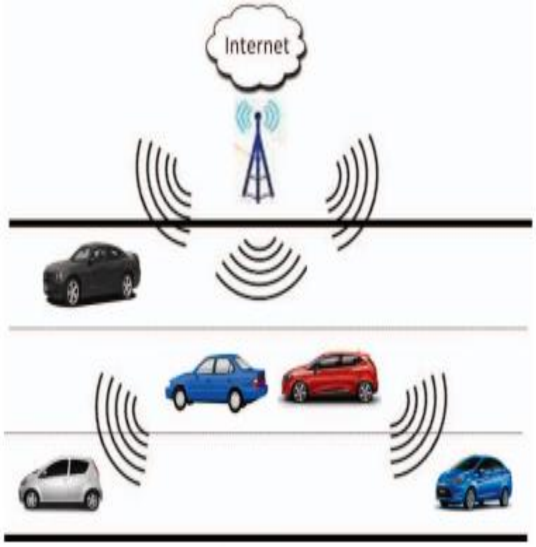


Fig. 3: Internet access is one of the most popular convenience features these days.

- VANET can be used to share entertainment applications, including as songs, movies, games, and more, between cars.
- routing in mobile ad hoc networks

It is possible to choose from a large number of routing protocols for mobile networks. MANET does not use a predetermined network topology. They may therefore adapt to any running topology because of their dynamic nature. To top it all off, there's no one way for routing in MANET, since the network is formed on the fly. Such wireless communication is provided by MANET, which is characterised by the mobility of its nodes. In addition, MANET provides the mobile nodes with an environment in which they can connect at any time and communicate with one other. The ability to connect and communicate with other devices, as well as exchange data among them, has been incorporated in a number of modern handheld devices. Routing protocols are essential for the successful transfer of data between network nodes. Due to its dynamic and ad hoc nature, routing protocols for MANETs are one of the most complex domains. In order to keep up with the ever-changing nature of networks, many routing protocols have been devised so far. Routing protocols in MANET have considerable challenges in discovering routes, maintaining routes, and adapting to changes in the network architecture. The dynamic nature of ad hoc networks necessitates the development of a variety of routing protocols. Topology-based routing refers to a group of these many protocols. We also discuss topology-based routing protocols in this chapter. VANET protocols and protocols of various types were thoroughly analysed to determine their appropriateness.

IV. VANET ROUTING PROTOCOLS

A. *Vehicular Ad Hoc Network Routing:*

In the previous sections, we discussed the similarities and differences between VANET and MANET. Because of the network's high mobility, frequent topological changes, and short life lifetime, routing decisions are more complicated. Additional features, such as road layout and different settings, such as city and highway, make routing in VANET more challenging. Unlike MANET's topology-based routing, VANET makes routing decisions based on the location of the network's nodes. Further, we'll show how VANET uses location-based routing to accomplish this task.

Virtual Area Network (VANET) requires a routing system that can keep pace with the network's ever-changing environment, which calls for position-based routing. Researchers must rely on node placements to enable successful communication between the source and the destination. Route data from source to destination based on nodes' geographic position. Assumed that each node has a GPS or other location-determining service. As a result, each node has access to information about its neighbours, as well as information about its origin and destination. Unlike topology-based routing, position-based routing requires additional information from each node participating in VANET, and that additional information is obtained using GPS. Cargo networks can communicate hop-by-hop using position-based routing. In a position-based routing system, beaconing, location service and servers, as well as recovery and forwarding algorithms, are all important components. Nodes broadcast their position and unique identifier to other nodes via beaconing (IP ADDRESS). When a node receives a beacon from a neighbouring node, its location database is updated. Beacons can be used to communicate this information to a node's one-hop or next-hop neighbours. Location services and servers: Any time a node's location table is missing or the node wants to know where a certain node is located, the location service is there to assist. [25] Location queries are sent with the requested node's unique ID, as well as the number of sequence and hops, to track the requested node's current physical location. Neighbors will respond with their current location, and if the desired node is identified among the requesting node's nearby neighbours, it will respond with that message. Updates to the location table are made by a node that originates from the target node. 28 a strategy for progress and recovery Recovering techniques are used to transfer data between nodes. VANET used three types of forwarding methods to transfer data packets between locations: Intense flooding that travels in a single direction "Hierarchical forwarding" is a technical term. The term "greedy forwarding" comes to mind next. [26]. Restricted directional flooding targeted both nodes and the "forwarding zone." This method does not necessitate the presence of neighbouring nodes. A forwarding zone is used to route packets from a source node to a destination node. which is established between these two points. If the source node sends a large number of packets to the forwarding zone, this may cause the forwarding zone to expand. By implementing "Distance-aware-timer based Suppression technique," we may overcome these concerns. "Mobility-centric data dissemination algorithm for vehicular networks"

(MDDV) [7] is an example of a restricted directed flooding protocol. Hierarchical forwarding is another forwarding approach for position-based routing algorithms. packets are routed through a hierarchical structure. Neighboring nodes, as well as those further away, benefit from hierarchical forwarding. The terminodes project's "geodesic packet forwarding" (GPF) and "anchored GPF" were the forwarding strategies employed for hierarchical routing [26]. For position-based routing, greedy forwarding is a useful method of sending packets to the nearest neighbours.. The sender node forwarded packets over the smallest number of hops available. If there is no adjacent node to recover from a failure, then this tool is used. Greedy perimeter stateless routing is an example of a greedy forwarding scheme. Position-based routing does not necessitate regular updates, but topology-based routing must. When a packet needs to be forwarded, the path is determined. Additionally, position-based routing comprises information about the source, destination, and their surrounding nodes [28]. As a result of these features, position-based routing is a good fit for VANET. Node location information is used in a number of routing techniques presented by researchers. In spite of their suitability for vehicle communication, these routing systems nonetheless face a number of difficulties. We'll take a look at some recently proposed routing protocols and the difficulties they face. In addition, we'll look into what recent developments have been made to address these challenges.

Our study's simulation results were assessed and analysed in this chapter. Throughput and packet drop measures were used to evaluate routing protocols. Router protocols in VANET were tested in two separate networks: one on the highway and another in a city. At low and high node speeds, we used GPSR and AODV to test for the highway. A large metropolitan area with radio obstacles was used to test the performance of the AODV, GPSR, and A-STAR routing protocols. The following table provides information on the throughput and packet drop rates of several VANET routing protocols.

Routing Protocol	Throughput (KB/ sec)	Packet Drop
AODV	7370	16090
GPSR	12449	15073

Table 2: Using a node's speed of 20 m/s, the highway scenario results

Routing Protocol	Throughput (KB/ sec)	Packet Drop
AODV	5043	16712
GPSR	12209	13877

Table 3: With a node's speed of 30 m/s, the highway scenario results

- This reveals that GPSR outperforms AODV in both highway conditions when it comes to throughput. Increasing the speed of the nodes has no noticeable impact on GPSR's throughput rate. On the other side, AODV's throughput performance is influenced by the fast speeds of the nodes.

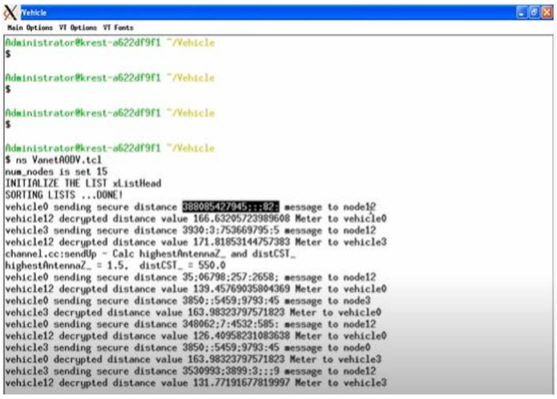
- The performance of both protocols changed minimally in terms of dropped packets while nodes were moving at 20 m/s. The GPSR's drop packet rate decreased in direct proportion to the node's increased speed. A slight increase in packet loss can be expected even with the high-speed nodes of AODV. The speedy movement of nodes did not affect GPSR's overall performance, which means it surpasses AODV in terms of throughput. The slower the nodes move, the lower the throughput of AODV is, and this is something we found out the hard way. Increasing the GPSR's speed also helps to lower the drop rate of packets in GPSR.

Routing Protocol	Throughput (KB/ sec)	Packet Drop
AODV	9921	7573
GPSR	13859	6495
A-STAR	19008	2457

Table 4: City scenario Results

- In city settings, the node's speed was much lower than on highways. The three methods are equally effective in this case, which is why they all work.
- AODV and GPSR were beaten by A-STAR in terms of throughput and dropped packets in Table 5. Even with AODV, GPSR outperformed it in terms of throughput. We found that A-STAR had a greater throughput rate than AODV or GPSR. Although AODV and GPSR are slightly different in terms of drop packet performance.
- It is clear from the above results that A-STAR is scalable in VANET city setups. We also discovered that the performance of GPSR and AODV differed slightly in terms of dropped packets. In the presence of a radio impediment, GPSR has a higher throughput than AODV.

V. RESULTS



```
Administrator@krest-a622df9f1 ~/Vehicle
$

Administrator@krest-a622df9f1 ~/Vehicle
$

Administrator@krest-a622df9f1 ~/Vehicle
$

Administrator@krest-a622df9f1 ~/Vehicle
$ ns VanetAODV.tcl
num_nodes is set 15
INITIALIZE THE LIST xListHead
SORTING LISTS ...DONE!
vehicle0 sending secure distance 388085427945;::82: message to node12
vehicle12 decrypted distance value 166.63205723989608 Meter to vehicle0
vehicle3 sending secure distance 3930:3:753669795:5 message to node12
vehicle12 decrypted distance value 171.81853144757383 Meter to vehicle3
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
vehicle0 sending secure distance 35;06798;257:2658; message to node12
vehicle12 decrypted distance value 139.45769035804369 Meter to vehicle0
vehicle0 sending secure distance 3850::5459;9793:45 message to node3
vehicle3 decrypted distance value 163.98323797571823 Meter to vehicle0
vehicle0 sending secure distance 348062;7:4532:585: message to node12
vehicle12 decrypted distance value 126.40958231083638 Meter to vehicle0
vehicle3 sending secure distance 3850;:5459;9793:45 message to node0
vehicle0 decrypted distance value 163.98323797571823 Meter to vehicle3
vehicle3 sending secure distance 3530993;3899:3:;:9 message to node12
vehicle12 decrypted distance value 131.77191677819997 Meter to vehicle3
```

Fig. 4: Execution of AODV.

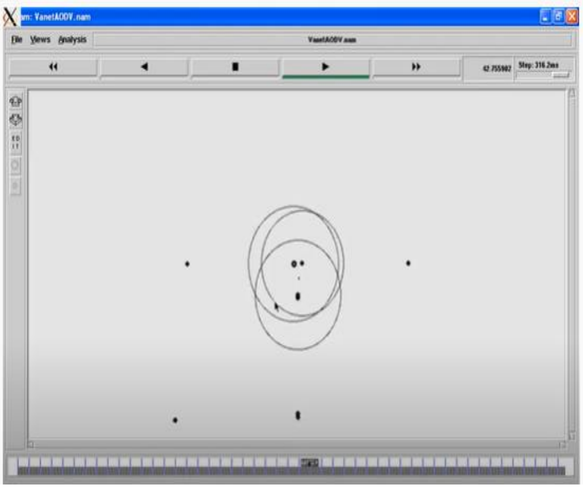
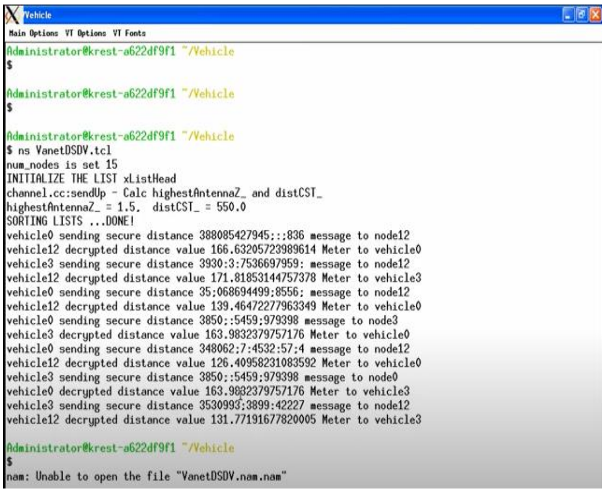


Fig. 5: Result of AODV.



```
Administrator@krest-a622df9f1 ~/Vehicle
$

Administrator@krest-a622df9f1 ~/Vehicle
$

Administrator@krest-a622df9f1 ~/Vehicle
$ ns VanetDSDV.tcl
num_nodes is set 15
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
vehicle0 sending secure distance 388085427945:::836 message to node12
vehicle12 decrypted distance value 166.63205723989614 Meter to vehicle0
vehicle3 sending secure distance 3930:3:7536697959: message to node12
vehicle12 decrypted distance value 171.81853144757378 Meter to vehicle3
vehicle0 sending secure distance 35;068694499;8556; message to node12
vehicle12 decrypted distance value 139.46472277963349 Meter to vehicle0
vehicle0 sending secure distance 3850::5459;979398 message to node3
vehicle3 decrypted distance value 163.9832379757176 Meter to vehicle0
vehicle0 sending secure distance 348062;7:4532:57;4 message to node12
vehicle12 decrypted distance value 126.40958231083592 Meter to vehicle0
vehicle3 sending secure distance 3850::5459;979398 message to node0
vehicle0 decrypted distance value 163.9832379757176 Meter to vehicle3
vehicle3 sending secure distance 3530993;3899:42227 message to node12
vehicle12 decrypted distance value 131.77191677820005 Meter to vehicle3

Administrator@krest-a622df9f1 ~/Vehicle
$
nam: Unable to open the file "VanetDSDV.nam.nam"
```

Fig. 6: Execution of DSDV.

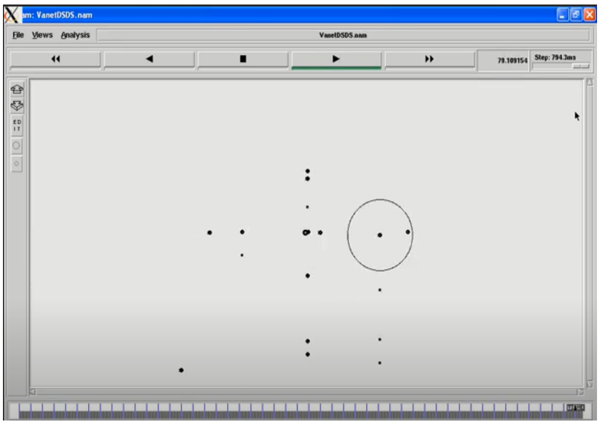


Fig. 7: Result of DSDV.

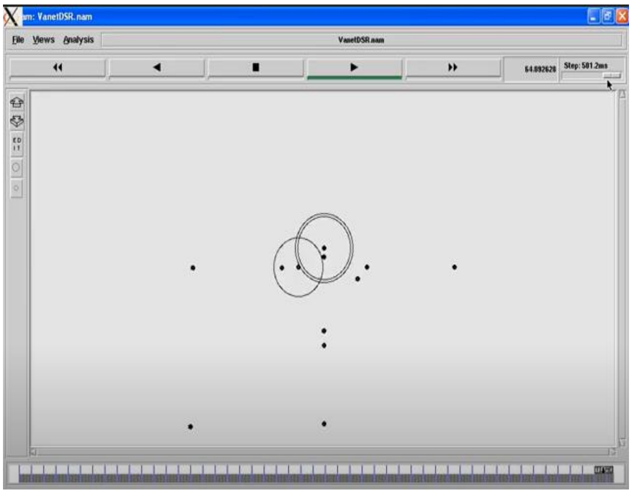


Fig. 8: Result of DSR

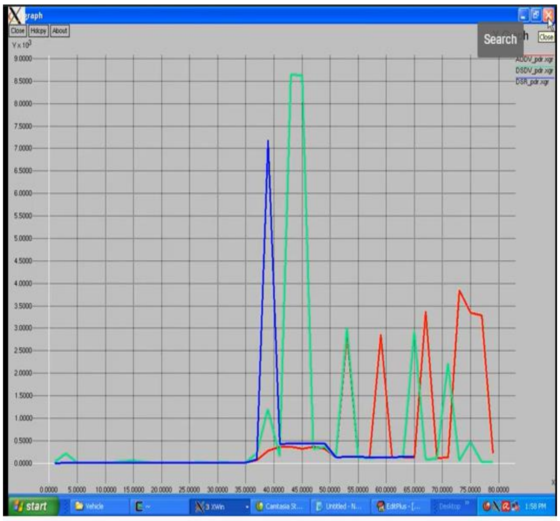


Fig. 9: Resutling Graph 1.

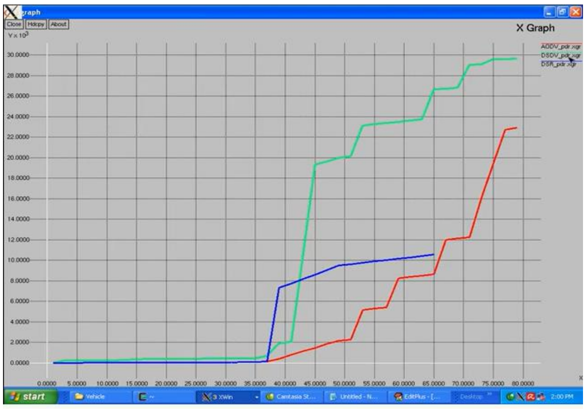


Fig. 10: Resulting Graph 2.

VI. CONCLUSION

Several articles on VANET applications, security, and routing protocols have been evaluated in this study. In terms of security, VANET is behind the curve. Many 978-1-5386-5696-9/18/$31.00 20181EEE researchers were involved in the development of the VANET authentication protocol. However, there is little effort put into ensuring the confidentiality and availability of the information. There is a need for additional work on VANET security because it has become the most important demand for users. Many academics have investigated this topic thoroughly and found that AODV is the best protocol for VANETs in terms of routing protocols.

REFERENCES

[1.] Alheeti et aI. (2015), On the detection of grey hole and rushing attacks in self-driving vehicular networks, in Proc. of 7th Computer Science and Electronic Engineering Conference (CEEC), pp. 231-236.

[2.] Azees, M., Vijayakumar, P. and Deborah, J. (2016), Comprehensive survey on security services in vehicular ad-hoc networks, in Proc. of International Journal of lET Intelligent Transport Systems, vol. 10, pp. 379-388.

[3.] Gupta, P. and Chaba, Y, (2014), Performance Analysis of RoutingProtocols in Vehicular Ad Hoc Networks for Cbr Applications Over Udp Connections, in Proc. of International Journal Of Engineering And Computer Science, vol. 3, pp. 6418-6421.

[4.] Hassan, A.S.A., Hossain, M.S and Atiquzzaman, M. (2016). Security Threats in Vehicular Ad Hoc Networks, in Proc. of International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 404-411.

[5.] Jain, J. and Jeyakumar, A. (2016), An RSU Based Approach: A solution to overcome major issues ofRouting in VANET, in Proc. of International Conference on Communication and Signal Processing (ICCSP), pp. 1265-1269.

[6.] Jiang, S., Zhu, X. and Wang, L. (2016), An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs, in Proc. of EEE Transactions on Intelligent Transportation Systems, vol. 17, pp. 2193-2204.

[7.] Karimireddy, T. and Bakshi, A. (2016), A Hybrid Security Framework for the Vehicular Communications in VANET, in Proc. of International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1929-1934.

[8.] Kaur, A. and Malhotra, J. (2015), On The Selection of Qos Provisioned Routing Protocol Through Realistic Channel for VANET, in Proc. of International Journal of Scientific and Technology Research, vol. 4, issue. 07.

[9.] Lo, N.W. and Tsai, J.L. (2016), An Efficient Conditional PrivacyPreserving Authentication Scheme for Vehicular Sensor NetworksWithout Pairings, in Proc. of IEEE Transactions on Vehicular Technology, vol. 17, pp. 1319-1328.

[10.] Lu, R., Lin, X., Liang, X. and Sheen, X. (2012), A Dynamic PrivacyPreserving Key Management Scheme for Location-Based Services in VANETs, in Proc. of IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp. 127-139.