International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

Improved Performance and Cooperative Safety in VANETs using Enhanced AODV Protocol-VRP

Riya Rajan
PG Student,Dept.of Electronics&Communication Engineering
Mount Zion College of Engineering, Kadammanitta

Hari S
Asst.Professor in Electronics and Communication Engineering
Mount Zion College of Engineering, Kadammanitta

Abstract- **Vehicular Ad-hoc Network (VANET) is an emerging new technology, which brings a lot of research interests in wireless network domain. It is a collection of vehicles in a wireless network that are dynamic in nature and communicate with each other and also with nearby Road Side Units (RSUs). These networks are used in real time scenarios. VANETs can provide improved safety applications like enhancing the driving conditions and reducing the chances of accidents, intelligent transport applications like traffic monitoring, traffic management, platooning, vehicle tracking etc…., comfort applications, efficiency and weather information. But the VANET is time critical, where safety messages should be delivered as fast as possible without much of delay which is a challenge. Security is another major challenge in VANET because the wireless medium used here can render the network vulnerable to security attacks such as interference, jamming and eavesdropping. Thereby, in this paper we propose a modification on Ad-hoc On-Demand Distance Vector (AODV) routing protocol in order to increase the speed and to decrease the delay. Routing using this enhanced AODV protocol which is named as VRP, also increases the throughput and overall performance of the network. To protect the network from security attacks, RSA cryptographic technique is employed here. Finally, extensive simulations are conducted using network simulator NS3 to evaluate the performance of VRP, compared with AODV. Results show that VRP performs better than AODV in the area of VANETs.**

Keywords— VANET, AODV routing protocol, security, attacks, RSA cryptosystem

I INTRODUCTION

Road accidents has a dreadful increase now a days even though several advanced in-vehicle safety-oriented devices exists. The main instigation of these accidents are faults, made by human. Several studies showed that most of the accidents that occurred could be avoided if the drivers are leaded with proper warning messages at the right time [1]. Intelligent transportation system (ITS) plays an important role in achieving traffic efficiency by reducing traffic related problems. It enhances users by providing prior information regarding traffic and real-time running information, thus improving safety and comfort. Vehicular Ad-Hoc Network (VANET) is a growing and most challenging research area to provide intelligent transportation system services to the users. They are certain types of Mobile ad- hoc Networks (MANETs), where moving vehicles are considered as nodes and connected to each other and thus forming a network. It is a self governing and self-coordinating wireless communication network [2]. The main objective of this system is to send data and information between vehicles and thereby increasing safety.

VANET changes each and every engaging vehicle in to a wireless router and helps vehicle drivers to communicate among themselves to avoid any critical situations like road accidents, speed control, traffic jams, unseen obstacles, free passage of emergency vehicles etc... It facilitates communication among nearby vehicles, between vehicle to vehicle (V2V) and nearby fixed equipment called road side unit (RSU) , which is vehicle to infrastructure (V2I) [3]. Besides improved safety applications, VANET also provides intelligent transport applications, comfort applications, efficiency and weather information. Some of the unique properties of VANET includes dynamic topology changes due to high mobility, infinite energy supply, road pattern restriction, scalable network size, predefined directions etc… The communication in VANETs are supported by the dedicated short range communication (DSRC) where the US FCC has allocated 75 MHz of spectrum in the 5.9 GHz band to enhance the safety and capacity of the transportation system. It also provides short range communication with a lower latency. Some of the popular architectures of VANETs are wireless access in vehicular environment (WAVE) by IEEE, CALM by ISO and Car to car net by C2C communication consortium. WAVE assigns two modes of communication which are safety related applications (non IP) and non safety related applications based on IPV6. To ensure a modular handling of the diverse issues at different layers, the standard is divided in to different sub standards. A Continuous Air Interface for Long to Medium Range (CALM) was designed to address the issues of continuous communication among vehicles and between vehicles and road side infrastructure. The concept of CALM is based on heterogeneous cooperative communication framework to provide continuous communication to user transport. C2CNet architecture has been proposed for safety applications. C2C-CC deals with safety as well as non-safety applications. C2C-CC is designing C2CNet protocol that differs from IP. It provides fast data transmission for vehicle to vehicle and vehicle to infrastructure communication [4].

Due to high mobility of nodes and fast topology changes in VANET, it faces more challenges than other networks. One of the main challenge in VANETs is the time critical issue where, safety messages should be delivered as fast as possible without much of delay. Then only the nodes can take

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

decision and perform actions accordingly. Also security and privacy requirements in VANETs should be assured as VANET provides the road safety applications which are life critical therefore, security of these messages must be satisfied. The secure routing problem becomes more challenging due to the characteristics of VANETs. Thus security is another major challenge in VANETs [5]. The goal of this study is to makeover those challenges in VANETs. Routing protocol also plays an important role in VANETs. Because, the aim of the routing protocol is to compute the optimal path between any source and destination pair with minimal control traffic overhead.

This paper presents an enhanced version of AODV routing protocol named as VRP routing protocol for routing in VANETs, with the aim of increasing the speed and decreasing the delay in the network. Here hop selection is done based on certain criteria's where, hop selection is minimized by considering factors such as by calculating the speed of vehicles. In a car parking area, speed of the vehicles lying in that area will be zero thus it can be avoided. Also in a four-way scenario, calculation of speed, direction and position of vehicles travelling in opposite direction can be neglected. Thus minimizing the total no: of hops taken into account and thereby decreasing the delay and increasing the speed and throughput. Security is also achieved using RSA cryptographic technique to protect the network from security attacks.

II RELATED WORK

Researchers have done many efforts for finding the best routing protocols in VANET system. Also different routing protocols has been evaluated with different VANETs simulator in terms of network parameters. The related works of this paper can be grouped in to three categories. First one is the topology based routing protocol in VANETs, the second one is the position based routing protocol and the last one is the MAC protocols in VANETs.

Routing protocol plays a vital role in the performance of VANETs. Also the routing protocols applied on MANET cannot be used directly on VANET. Temporally Ordered Routing Algorithm (TORA) which is one of the topology based routing protocol is unsuitable in VANETs, because of its need for geographical location information [6]. As highly changing topology is one of the characteristics of VANET networks, routing protocols must be applied effectively. In [7] two routing protocols, reactive protocol RBVT-R and proactive routing protocol RBVT-P were proposed. These protocols were compared with protocols like AODV, OLSR and GPSR that are applied on MANET and also with GSR protocol that are applied on VANETs. Results showed that the two protocols RBVT-R and RBVT-P outperform the existing protocols in terms of delivery ratio and delay. Reduction of bandwidth consumption and control overhead makes AODV suitable for VANETs. In [8] a PAODV routing protocol is proposed by doing certain modifications to the existing AODV protocol. Here route discovery phase is eliminated by restricting neighbor's distance and number of restricted routes which inturn helps in reducing the control overheads.

In [9] two routing protocols, Ad-hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) were simulated and analyzed. They came to the following finding that AODV protocol is more suitable for VANET than the DSR protocol. Also it is more flexible with VANETs for high speed and complex transportation system than DSR. In [10] for reducing the packet delay, an improvement to AODV routing protocol is done and a new protocol called AODV-BD is proposed. When local repairing is continuing AODV-BD establishes a routing to the destination node by broadcasting data packets. As a result, both data packets and request packets will be broadcasted.

Medium access control (MAC) protocol schedules the cooperative sharing of physical resources as a result the performance of cooperative safety mainly depends on it. In [11] carrier sense multiple access with collision avoidance (CSMA/CA) has been applied as standardized MAC protocol in dedicated short range communications (DSRC). But there exists certain drawbacks which are, the performance degrades with increase of loads. Also, it cannot provide delay bounded access for VANETs and a strict quality of service (QOS) for cooperative safety.

In [12] two outstanding TDMA MAC protocols, STDMA and VeMAC in VANETs has been proposed. TDMA MAC protocol provides better performance as load increases and also enables delay bounded access. But it cannot handle varying vehicle density perfectly, particularly the constant change in vehicle density. Nodes in both protocols reserve slots based on what they sense. The difference between both protocols is in its perception range. For STDMA, it is one-hop and and for VeMAC it is two-hop. But the challenging vehicular environment leads in high packet error rate which in turn leads to inaccurate perception and causes more collisions.

In [13] a software defined network (SDN) based MAC protocol is proposed to handle the challenges in VANETs such as high mobility and dynamic network densities. Here decoupling of control plane and data plane is done which provides greater rapidness and liveliness. Thus it can handle rapid mobility and varying vehicle density. SDN provides flexibility and programmability to networks along with new services and features to VANETs. SdnMAC also eliminates merging collisions with a lowest packet loss rate.

III PROPOSED SYSTEM

A. AODV ROUTING PROTOCOL FOR VANET

Ad-hoc On-demand distance vector (AODV) is one of the most popular reactive routing protocol which is simple, efficient and on-demand routing protocol. It provides route purely on-demand which makes it very useful for VANET applications. Thus it reduces large amount of overhead. One of the major achievements of the AODV routing protocol is the maximum utilization of the bandwidth and also it operates on hop by hop pattern. The algorithm enables self-starting, dynamic and multi hop routing between engaging nodes that wish to establish routes and maintain an ad-hoc network. It allows nodes to find routes quickly to new destinations and does not require to maintain routes to those destinations where communication is not active[14]. One advantage of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

AODV over DSR protocol is that, there is no need to include the source route with each packet. Thus reduction in routing protocol overhead is achieved. Other advantages of AODV routing protocols are, the connection setup delay is lower and also destination sequence number are used to find the latest route to the destination. As it only maintains one route that is actively used, AODV can adapt to these changes quickly[15]. In VANETs, there occurs a sudden change in topology frequently and also the number of nodes used are large. Therefore, AODV is more suitable than any other protocol in this network.

Routing using AODV consists of two phases which are, route discovery process and route maintenance process. When a node requires route to the destination, it initiates a route discovery process within the network. Once a route found the process is completed and all possible route permutations are calculated [16]. Route maintenance is the process which is done by means of the route error packets (RERR) when there occurs a link breakage. The message types defined by AODV are, Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs). As well as the sequence number, routing information also has a timeout associated with it. For connectivity information and signal link breaks on active routes with error messages, AODV can use hello messages.

A. Route Discovery

When a node wants to transmit data and there has no route to destination and no information about them in its routing table, route discovery phase begins. Here the source node broadcasts a route request packet (RREQ) to its neighbor. The broadcasted RREQ contains addresses of source and destination, their sequence numbers, broadcast ID and a counter, that counts how many times RREQ has been generated from a specific node. This RREQ contains the latest sequence number for this route, which assures loop-free networks. Upon reception of broadcast query (RREQ) nodes record the address of those nodes that send the query in their routing table. This process of recording its previous hops are called backward learning. Through the complete path that has been obtained from backward learning from the source to destination, a reply packet (RREP) is sent through it. A forward path from the source is also established as the nodes record its previous hop at each stop of the path. As long as the source uses it, the path will be maintained. Here route table management is done with the help of destination sequence numbers.

B. Route Maintenance

When nodes in the network detects that a route is no more valid for communication, all related entries for those invalid routes are deleted from the routing table. An RREP is also send to current active neighboring nodes to make aware them about the invalid routes. AODV always maintains only loop free routes. Hello messages and link-layer acknowledgements (LLACKS) were used to ensure from bidirectional paths and to detect failed links. When link breakage occurs, generated route Error (RERR) packet with a fresh sequence number (known sequence number plus one) is send towards the source node. When a source node receives RERR, it will reinitiate route discovery process if a route is still needed.

B. ENHANCED AODV PROTOCOL – VRP

A new routing protocol named as VRP is proposed for vehicular ad-hoc networks which is the modification of Ad-hoc On-demand distance vector (AODV) routing protocol. Here hop selection is reduced by considering factors such as speed and direction of the vehicles. At first an ideal node is found which has certain speed and direction. Thereafter the remaining nodes are compared with the speed and direction of ideal node. In the AODV routing protocol's route discovery process, broadcasting is done through flooding which means that all nodes within the transmission range of source node receives control packet. The control packets are used to discover routes to the destination. These discovered routes are subsequently used to send data packets. Only those nodes that are unreachable from source node does not receive packet. Thus flooding delivers packet to too many nodes which in turn creates more link breakages and always route maintenance required. This flooding, thus affects the performance of overall wireless network. Node exceptions can be done to reduce this flooding issue. While in AODV all neighbor nodes are selected during broadcasting. In the proposed VRP protocol, two criteria's are applied to the existing AODV protocol to improve its performance. The criteria's those applied are speed and direction. We can distinguish between the nodes whether it may be wanted or not based on these criteria. These criteria's are evaluated while selecting neighbor nodes for broadcasting and thus unwanted nodes are avoided. This results in increased life time and throughput, reduced link breakages and delay. Thus increasing overall performance of the network.

A wireless network can be created by using the components of a mobile node and its configurations in every layer. Data communication between nodes can be initialized with transport and application layer agents that are required to be attached to both sender and receiver nodes. The physical layer facilitates the configuration of channel, interfaces, antenna type, signal propagation model, energy model, error model etc…In the simulation parameters setup of VANET, wireless channel is the channel type and wireless physical is the network interface type used. The antenna model configured is the Omni directional antenna as they provides good all round coverage and also commonly used in cellular telephone sets and wireless routers. The radio propagation model implemented is the two-ray ground reflection model as it considers both the direct path and a ground reflected path which gives more accurate result. In successive layers, different type of interface queues , MAC layer protocols , Network layer protocols, Transport layer protocols and Application layer protocols can be applied. The interface queue type used is the Drop Tail queue model and IEEE 802.11 is the MAC type. VRP is used as the network layer protocol as it has many advantages over other protocols in the case of VANETs and therefore used for routing. TCP and FTP are configured as the transport layer and application layer

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

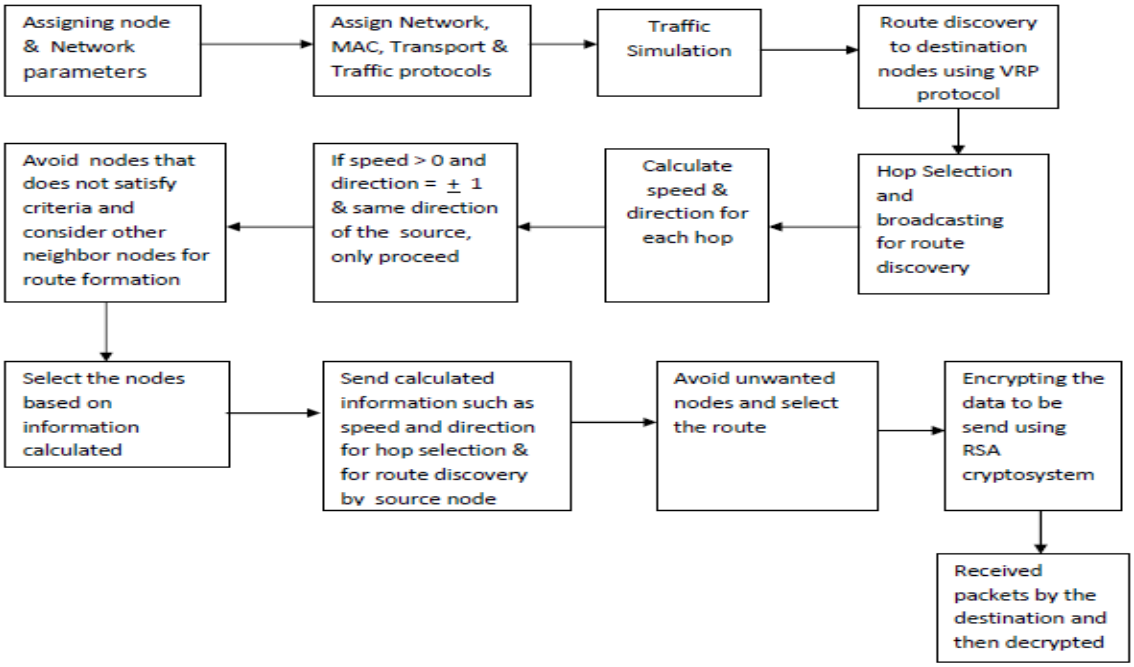

Fig.1. Block diagram of the proposed system

protocols respectively. Application layer agents have the choices for packet size, data rate, data transmission interval, start and stop time of data transmission. Thereafter sufficient wireless nodes are created and they are configured with the initial mobile node parameter setup. The connectivity of these wireless nodes are determined by their distance from one another. As wireless nodes can move, their distances from one another change over time. The topology used here is flat grid. To keep track of each node's position in the topology grid, we need to create a General Operations Director (GOD) object. The God object stores, the total number of mobile nodes and a table of shortest number of hops required to reach from one node to another. Also the next hop information is normally loaded into god object from movement pattern files, before simulation begins. The node mobility model can be created with specification of target location and speed and nodes with different communication range can be configured.

After the simulation parameter setup, route discovery using VRP routing protocol is done here. Before selecting the hops for broadcasting, speed and direction of each hop is calculated and compared with the ideal node. If speed of the node is greater than zero and direction of the source node which is equal to positive one or negative one, whether same with that of the neighboring hop the hop will be selected. Positive value of direction indicates that the vehicle is moving in forward direction and negative value indicates that the vehicle is moving in opposite direction with that of source. And if the condition is not satisfied consider next node and so on. Thus selecting the nodes that satisfied the condition based on the information calculated. Also sending this calculated speed and direction information to other nodes for hop selection and for route discovery by source node. Thus unwanted nodes are avoided and route is selected. Here special packets are used which contains position, speed and direction information. The criteria that speed should be greater than zero has been set in order to ensure that the vehicle is moving. Thus hop selection can be minimized by eliminating
those hops that does not satisfy the criteria. Also when considering a four way scenario, those nodes whose direction opposite to ideal node should not be considered. RSA cryptography technique is used to encrypt the data to protect it from intruders before sending it through the network.

Security is an important issue for routing in VANETs and the characteristics of VANETs make the secure routing problem more challenging. Various security requirements that are essential for VANETs are, authentication, message integrity, message non-repudiation, access control, message confidentiality, privacy and real-time guarentees [17]. RSA, has been commonly used for secure transmission of data. Here the encryption key is used as public and the decryption key is kept private. This asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers which is the factoring problem. The operation of RSA algorithm involves four steps which are, key generation, key distribution, encryption and decryption [18]. At the receiver side the packets are received and then decrypted. Nodes that are assigned with this application can only perform encryption and decryption. Here we assigned all nodes with this application thus all nodes can perform this operation.

IV SIMULATION ENVIRONMENT

Network simulator, ns-2 simulator is used here for the experiments. It is a discrete event simulator developed by the University of California at Berkeley. We are using NS2 for simulations of protocols. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks [19]. A typical wireless NS-2

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

simulation produces an event trace file and an animation trace file which is used by the included utility NAM to provide animation of the simulation. Transmission of packets between the wireless nodes can be viewed during animation. At the end of simulation, an event trace file is generated which follows a specific format for wireless networks that include event type, time, nodes involved in it, and data specifications. It can be analyzed using the specific AWK scripts for performance analysis.

1.1 Simulation parameters

The parameters which are used for performance evaluation are,

1. *Throughput*

It defines the amount of data that is delivered from one node to another via a communication link. The throughput is measured in Packets per unit TIL or bits per TIL. TIL is Time Interval Length. More is the throughput of sending and receiving packets better is the performance. Lesser is the throughput of dropping packets better is the performance.

2. *Average throughput*

It is the average of total throughput. It is also measured in Packets per unit TIL or bits per TIL.

3. *Packet Drop*

It defines the total number of data packets that could not arrive the destination successfully. Packet drop occurs due to congestion, faulty hardware and queue overflow etc. Lower packet drop rate shows higher protocol performance.

4. *Average simulation End to End delay (End2End delay)*

This parameter gives the overall delay, from packet transmission by the application agent at the source node upto packet reception by the application agent at the destination node. Lower delay shows higher protocol performance.

V RESULTS AND ANALYSIS

This section verifies the effectiveness of the VRP protocol over the conventional AODV protocol, by showing computer simulation results. Analysis of both protocols has been done using performance metrics such as average throughput, average drop and average end to end delay.

A. Output Trace File:

Output trace file for AODV routing protocol and VRP routing protocol are generated for fourteen nodes. Simulations are done for fourteen different node numbers at different vehicle speeds. Fig. 2 shows the output trace file of AODV and fig. 3 shows VRP routing protocol.

```
M 1.00000 0 (101.00, 500.00, 0.00), (1200.00, 500.00), 15.00
M 1.00000 1 (203.00, 499.00, 0.00), (1175.00, 500.00), 15.00
M 1.00000 2 (300.00, 501.00, 0.00), (1150.00, 500.00), 15.00
M 1.00000 3 (395.00, 500.00, 0.00), (1125.00, 500.00), 15.00
M 1.00000 4 (1102.00, 77.00, 0.00), (50.00, 75.00), 15.00
M 1.00000 5 (1004.00, 78.00, 0.00), (75.00, 75.00), 15.00
M 1.00000 6 (951.00, 77.00, 0.00), (100.00, 75.00), 15.00
M 1.00000 7 (876.00, 77.00, 0.00), (125,00, 75.00), 15.00
M 1.00000 8 (603.00, 129.00, 0.00), (1200.00, 129.00), 15.00
M 1.00000 9 (601.00, 466.00, 0.00), (1200.00, 466.00), 13.00
M 1.00000 10 (696.00, 265.00, 0.00), (50.00, 265.00), 12.00
M 1.00000 11 (491.00, 323.00, 0.00), (1200.00, 323.00), 13.00
M 1.00000 13 (541.00, 293.00, 0.00), (1250.00, 293.00), 20.00
s 4.000000000 _8_ AGT  --- 0 tcp 40 [0 0 0 0] ------- [8:0 9:0 32 0]
r 4.000000000 _8_ RTR  --- 0 tcp 40 [0 0 0 0] ------- [8:0 9:0 32 0]
s 4.000000000  8  RTR  --- 0 AODV 48 [0 0 0 0] ------- [8:255 -1:255
```

Fig.2 Output trace file of AODV

```
M 1.00000 0 (101.00, 500.00, 0.00), (1200.00, 500.00), 15.00
M 1.00000 1 (203.00, 499.00, 0.00), (1175.00, 500.00), 15.00
M 1.00000 2 (300.00, 501.00, 0.00), (1150.00, 500.00), 15.00
M 1.00000 3 (395.00, 500.00, 0.00), (1125.00, 500.00), 15.00
M 1.00000 4 (1102.00, 77.00, 0.00), (50.00, 75.00), 15.00
M 1.00000 5 (1004.00, 78.00, 0.00), (75.00, 75.00), 15.00
M 1.00000 6 (951.00, 77.00, 0.00), (100.00, 75.00), 15.00
M 1.00000 7 (876.00, 77.00, 0.00), (125.00, 75.00), 15.00
M 1.00000 8 (603.00, 129.00, 0.00), (1200.00, 129.00), 15.00
M 1.00000 9 (601.00, 466.00, 0.00), (1200.00, 466.00), 13.00
M 1.00000 10 (696.00, 265.00, 0.00), (50.00, 265.00), 12.00
M 1.00000 11 (491.00, 323.00, 0.00), (1200.00, 323.00), 13.00
M 1.00000 13 (541.00, 293.00, 0.00), (1250.00, 293.00), 20.00
s 3.100000000 _10_ AGT  --- 0 SP 512 [0 0 0 0] ------- [10:0 8:1 32 0]
r 3.100000000 _10_ RTR  --- 0 SP 512 [0 0 0 0] ------- [10:0 8:1 32 0]
s 3.100000000 _11_ AGT  --- 1 SP 512 [0 0 0 0] ------- [11:0 8:1 32 0]
r 3.100000000 _11_ RTR  --- 1 SP 512 [0 0 0 0] ------- [11:0 8:1 32 0]
s 3.100000000 _10_ AGT  --- 2 SP 512 [0 0 0 0] ------- [10:1 9:1 32 0]
```

Fig.3 Output trace file of VRP

B. Output NAM File:

NAM file visualizes the animation of mobile nodes within the network. The output NAM visualization of AODV and VRP routing protocol for a number of 14 nodes at different speed is shown in the following figure.

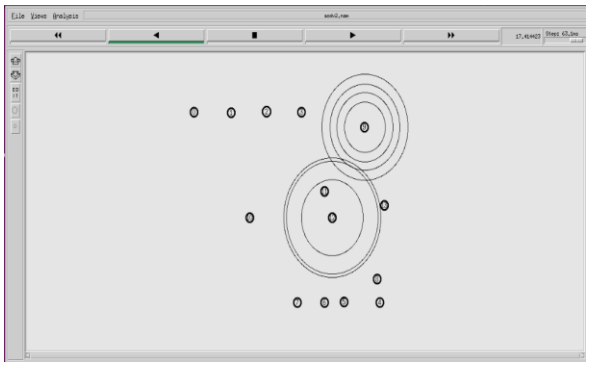

Fig.4. Output NAM file of VRP

C. Graphical results for performance analysis

Here the performance of AODV routing protocol is compared with that of the proposed VRP protocol in terms

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

of performance parameters such as average throughput, average drop and average end to end delay. Results obtained are mentioned in the following tabular column.

TABLE I
Comparison of AODV and VRP routing protocols based on the performance parameters

PARAMETERS	AODV Routing protocol	VRP Routing protocol
Average throughput	904	1018
Average packet drop	45	47
Average end to end delay	83.9552 ms	46.0039 ms

By analyzing the above results, we can understand that VRP routing protocol achieves a better throughput of 1018 when compared with that of AODV. As throughput increases drop also increases manually. But in the case of VRP protocol, for more than hundreds of increase in throughput only an amount of 2 increased in the packet drop. When considering the delay, VRP achieves lesser end to end delay when compared with AODV which is essential for VANETs. Thus it can be concluded that VRP offers better speed and performance than existing AODV protocol. The graphical analysis of the above mentioned parameters except delay are shown in the following figure.

A. Average throughput

It is one of the important parameter that can be used to measure the system performance. It can be defined as the packets per unit time interval length. Fig.3, represents the average throughput of AODV and fig.4, indicates the average throughput of VRP in two segments. One is VRPCM, which is normal and the other is VRPSEC, in which encryption and decryption is done. The graph shows that VRP achieves better throughput than AODV routing protocol.

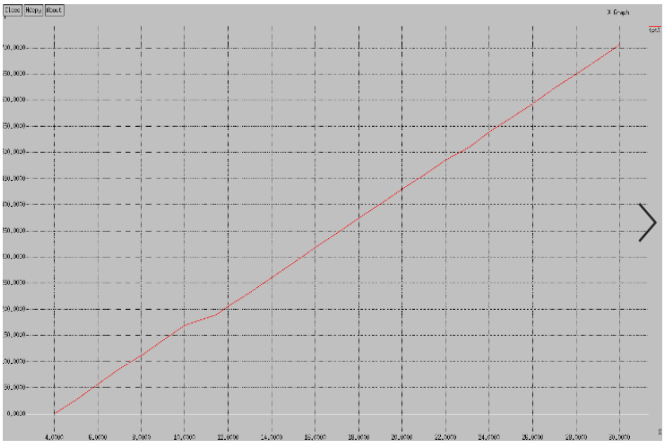

Fig.5. Average throughput versus time of AODV

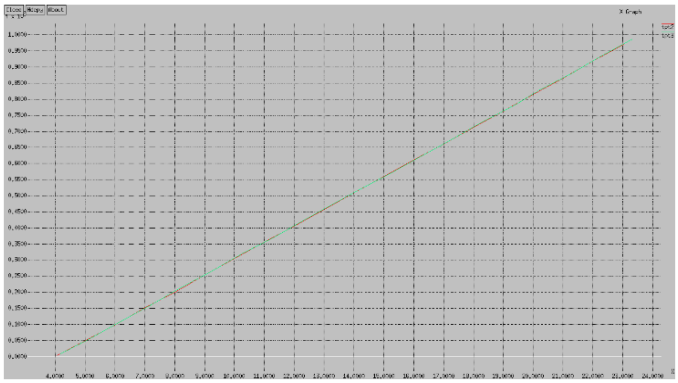

Fig.6. Average throughput versus time of VRP

B. Packet drop

It indicates the number of packets that have not reached the destination. The following figure, Fig.5, shows the packet drop for AODV and fig.6, VRP respectively. Since there occurs an increase in throughput, drop also will increase. But in the case of VRP for an increase of hundreds in throughput only packet drop of two has been occurred.

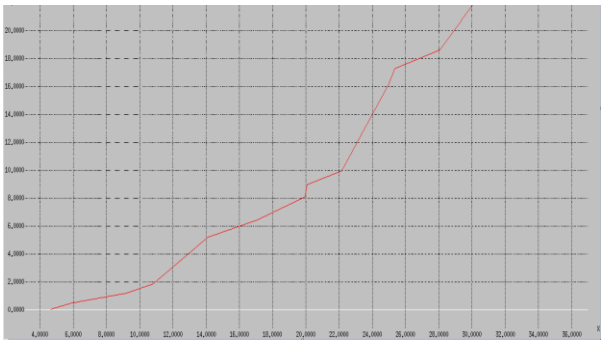

Fig.7, Packet drop versus time of AODV

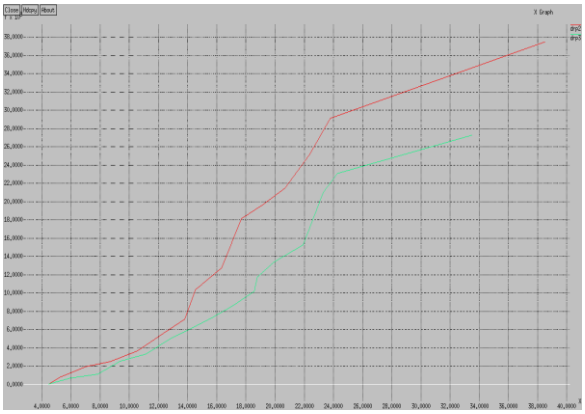

Fig.8, Packet drop versus time of VRP

From the simulation results for various cases, it can be summarized that the average throughput, average packet drop and average end to end delay obtained for AODV and VRP is analyzed and it can be concluded that VRP performs better than AODV in all the above cases and hence VRP is more suitable for VANETs.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

VI CONCLUSION

In this paper, we have proposed a new routing protocol, VRP which is the modification of existing AODV routing protocol. The main goal of this protocol is to handle some of the challenges in VANETs such as time critical issue and security issue. VRP uses two important parameters which are speed and direction as the criterion for hop selection. Thus instead of selecting all the neighboring hops, here hop selection is minimized based on this criteria during the route discovery phase. Thus speed and throughput of the network can be increased along with much lesser delay. RSA cryptosystem is also implemented to protect the network from security attacks and to ensure integrity of the messages transferred. Finally, our simulation results showed that VRP achieves better throughput, lesser delay and lesser packet drops when compared with that of AODV routing protocol. Thus we can say that VRP performs better than AODV in the area of VANETs.

REFERENCES

[1] Elias C. Eze, Sijing Zhang, Enjie Liu, Joy C. Eze, "Advances in Vehicular Ad-hoc Networks (VANETs) : Challenges and Road map for Future Development", International Journal of Automation and Computing, Volume 13, Issue 1, pp 1–18, February 2016.

[2] Valsangkar Farid , Prof Shirgan S.S , Kadganchi Harshad, " Design and Analysis of AODV Routing Protocol in VANET Using NS2", International Journal for Research in Applied Science and Engineering Technology, Vol. 2, Issue IX, September 2014.

[3] Rajvardhan Somraj Deshmukh, Tushar Singh Chouhan and P.Vetrivelan, " VANETS Model:Vehicle-to-Vehicle, Infrastructure-to-Infrastructure and Vehicle-to-Infrastructure Communication using NS-3", International Journal of Current Engineering and Technology, Vol.5, No.3 , June 2015.

[4] Elias C. Eze, Sijing Zhang and Enjie Liu, "Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 12-13 September 2014.

[5] Shubham Kapoor and Surjeet, "VANETs: Basics, Issues and Challenges in its Practical Deployment", International Journal of Engineering Trends and Technology (IJETT) – Volume 57, Number 2 - March 2018.

[6] Anuj K. Gupta, Dr. Harsh Sadawarti, Dr. Anil K. Verma, "Performance analysis of AODV, DSR & TORA Routing Protocols", International Journal of Engineering and Technology, Vol.2, No.2, April 2010.

[7] N. Josiane, R. Neeraj, and W. Guiling, "VANET routing on city roads using real-time vehicular traffic information", IEEE Transactions on Vehicular Technology, Volume: 58 , Issue: 7 , Sept. 2009.

[8] A. Omid, B. Reza and M. Abdollahi, "Improving route stability and overhead of the AODV routing protocol and makeing it usable for VANETs", 2009 29th IEEE International Conference on Distributed Computing Systems Workshops, DOI,10.1109/ICDCSW, 2009.

[9] J. Liu, F. Chen and J. Xu, " The study of routing strategies in vehicular ad-hoc networks", 978-1-4244-7555-1/10, IEEE, 2010.

[10] L. Baozhu, L. Yue and C. Guoxin, "Improved AODV routing protocol for vehicular ad hoc network", 3rd International Conference on Advanced Computer Theory and Engineering(ICAC), 2010.

[11] K. Sjoberg, E. Uhlemann, and E. G. Strom, "How severe is the hidden terminal problem in VANETs when using CSMA and STDMA?" in Proc. IEEE Veh. Technol. Conf. (VTC Fall), pp. 1–5, Sep. 2011.

[12] H. A. Omar, W. Zhuang, and L. Li, "VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs," IEEE Trans. Mobile Comput., vol. 12, no. 9, pp. 1724–1736, Sep. 2013.

[13] Guiyang Luo, Jinglin Li, Lin Zhang, Quan Yuan, Zhihan Liu, and Fangchun Yang, "sdnMAC: A Software-Defined Network Inspired MAC Protocol for Cooperative Safety in VANETs", IEEE Transactions On Intelligent Transportation Systems, Issue: 6, Volume: 19, Year: 2018.

[14] C.Perkins and E. Royer, "The ad hoc on-demand distance vector protocol", in Ad hoc Networking, Addison-Wesley, pp. 173–219, 2000.

[15] N. Surayati, M. Usop, and A. Abdullah, "Performance evaluation of AODV, DSDV & DSR routing protocol in grid environment", IJCSNS International Journal of Computer Science and Network Security, Vol.9 No.7, July 2009.

[16] Asma Ahmed, A. Hanan, Izzeldin Osman, "Aodv Routing Protocol Working Process", Journal of Convergence Information Technology (JCIT)Volume 10, Number 2, March 2015.

[17] Dr. Nirbhay Kumar Chaubey, "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study", International Journal of Security and Its Applications Vol. 10, No. 5, pp.261-274, 2016.

[18] M. Preetha1 , M. Nithya, "A Study And Performance Analysis Of RSA Algorithm", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 6, pg.126 – 139, June 2013.

[19] T. Issariyakul and E. Hossain, Introduction to Network Simulator NS2, Springer Science+Business Media, LLC, ISBN: 978-0-387-71759-3, 2009.