A robust self adaptive collision avoidance method for modern VANETs

Poonam[1], Pawan Luthra[2]

1 Department of computer Science Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur

2 Department of computer Science Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur

Email:[1]poonam942@gmail.com, 2pawanluthra81@gmail.com

Abstract—The VANETs growing at large scale. The automobile manufacturer across the world have started working on the VANETs after understanding the high significance of the inter-connectivity between the vehicles to share the information about weather, traffic, collisions, hurdles, etc. The proposed model has been designed to overcome the problem of active updates regarding the blank hurdles or collisions, which have marked the hurdle on the way. The proposed model has been designed to flood the updates within the VANET cluster in order to reduce the threat of collisions or traffic jams due to the occurring hurdles or collisions. The proposed model uses the distance based hurdle detection mechanism with auto-updation within the VANET cluster. The proposed model has been evaluated on the basis of various performance parameters for its performance in the given scenario. The experimental results have shown the effectiveness of the proposed model.

Keywords—VANET, Collision avoidance, collision detection, heuristic VANETs, RSU.

1. Introduction

The key advantages are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. Researchers in communications engineering and traffic management systems are engaged for more than a decade to develop suitable Vehicular Ad hoc Networks (VANET) for traffic safety systems [1, 2]. VANETs can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UMTS, LTE and Wi-MAX networks. Main advantages are low cost of implementation and maintenance, self- organization and lower local information dissemination time. VANET is evolving as one of the practical applications of MANETs in the future. This vehicular network is interconnected with vehicles which have wireless interface. The vehicle can easily provide the required power for wireless communication, and adding antennas or additional communication hardware does not cause major problems. The goal of VANET is to develop a vehicular communication system to provide quick and cost-efficient distribution of data for the benefit of passenger safety and comfort [3]. Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry and forward DTN paradigm that works as follows. A source node originates a data bundle and stores it using some form of persistent storage, until a communication opportunity (i.e. a contact) arises [4]. This bundle may be forwarded when the source node is in contact with an intermediate node that can help bundle delivery. Afterwards, the intermediate node stores the bundle and carries it until a suitable contact opportunity occurs. This process is repeated and the bundle will be relayed hop by hop until reaching its destination eventually and over time [5, 6].

The main differences between VANET and MANET are Mobility Model. When a vehicle travelling on the road of a city or a freeway, its mobility pattern must consists with the topology of the road. We call this constraint as Mobility In addition; the behaviours of drivers are different to each other, so we can't just use the Random Waypoint mobility model to simulate the movement pattern of vehicles in VANET, Dynamic Mobility and High Relative Speed – In general case, the moving speed of the vehicle is up to 60 – 130km/hr. And the relative speed of vehicles will be higher, especially when moving in the different direction.

Ghaleb F. et al. [7] proposed the Security and Privacy Enhancement in VANETs using Mobility Pattern. This paper is presenting a mobility pattern based misbehaviour detection approach in VANETs. According to this paper the attackers can be classified as insider and outsider. Insider is a legitimate node might intentionally or unintentionally make unauthorized or undesirable actions (Misbehaviour), such as modify, fabricate, drop the messages in addition to, and impersonate other node identities. Outsider, on the other hand, is a kind of intruder aim to intercept, misuse ordenial of the communications among VANET's nodes. Misbehaviour in VANETs can be viewed two perspectives: (i) physical movement and (ii) information security perspectives. Anonymous Location-Aided Routing for MANET (ALARM) is used for vehicular network which relies on the location information and corresponding time. This paper includes algorithms by which the misbehavior can be detected. **Sharma G.** et al. [8] proposed the Security Analysis of Vehicular Ad Hoc Network (VANET). In this paper various type of security problems and challenges of VANET been analyzed and discussed; author of this paper also discuss a set of solution to solve these challenges and problems. According to this paper each vehicle has OBU (On Board Unit). **Seuwou. P** et al. [9] has proposed the Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs). VANET is technology that uses moving cars as nodes in a network to create mobile networks. VANETs enable vehicles to communicate amongst themselves (V2V communications) and with road-side infrastructure (V2I communications). Every participating car is turned into a wireless router or node, allowing connection between other cars in a radius approximately of 100 to 300 meters, thus creating a network with a wide range. In this paper he proposed various issues of effective security in VANET. **Qian.yi** et al. [10] conducted the Performance evaluation of a secure MAC Protocol for vehicular network. In this paper, an overview on a priority based secure MAC Protocol for vehicular networks is proposed and MAC Protocol can achieve both QOS and security in vehicular networks. In this paper, the MAC Protocol having massages with different priority for different application to access DSRC (Dedicated short range communication channel) channel is proposed.

In this paper, we simulated on-demand routing protocols like Ad Hoc On-demand Distance Vector (AODV) and Enhanced Direction based Hazard Routing Protocol (EDHRP) using open source network simulator NS2. Network simulator is a package of tools that simulates behavior of networks such as creating network topologies, log events that happen under any load, analyze the events and understand the network. Performance of the VANET is measured using metrics like Delay, Energy, PDR and Throughput, Data Loss, Network Load, Energy Consumption.

2. System model

The proposed model uses two protocols for its working: Ad Hoc On-demand Distance Vector (AODV) and Enhanced Direction based Hazard Routing Protocol (EDHRP). AODV routing protocol is used for routing and it establishes a route to a destination only on demand. AODV routing protocol uses a broadcast route discovery mechanism and dynamically establishes the route from source to destination for sending HM. Selective Forwarding can happen only if the highway has enough vehicles to forward the HM and this procedure minimizes network overhead and improves reliability of the transmission. If there are no other vehicles on the highway, it would not be possible for the Hazard Observer to locate a forwarder node. Then one of the following two things can happen: in the first instance, Hazard Observer would take a U turn and proceed back in the direction from which it originally came. When it reaches the communication range of any RSU, it would receive the HM and reply with the hazard message. In the second instance, it could proceed further in the same direction in the opposite lane and send hazard message to the corresponding RSU.

EDHRP is enhanced protocol of DHRP for safely delivery of hazard messages. The biggest challenge for VANETs is when the traffic is sparse. In that case, EDHRP provides the hazard related information to all nodes via RSUs. Instead of flooding the entire data, only the valuable information is sent to the nodes and false information is rejected. RSUs broadcasts the hazards related message to all the nodes only once and if somehow any node disconnects and could not get the message; in that case, RSUs keeps an updated table which have entries for all the connected or disconnected nodes and thus if any node disconnects then RSU re-sends message to that particular node only after the connection is established again. Thus, network load is highly reduced and performance is greatly increased. It provides messages regarding collision, when a fix hazard is blocking the way, and Sybil attack, when fake hazard is created by some prankster. It intimates the node to change their route safely at an interspacing distance of 20 meters between the node and the hazard. It also helps to join the nodes which are out of any RSU's range by connecting them with the one of the nodes among the in-range nodes. Thus information is passed as RSU-to-node-to-node structure. RSU decides the edge node which is in its range and nearest to the out-of-range node. If somehow that edge node fails, RSU gives this connecting responsibility to another node which is nearest to the out-of-range node.

In the proposed model, focused upon the following parameters have been taken, which are used for the working of the movement control and backup path allocation. For the hurdle detection or the collision detection, the distance plays the major role in finding the correct location of the hurdle or collision. The distance formula is used tocompute the gap between the nodes and the hurdle that will be calculated by the following formula:

$$\sqrt{(X1 - X2)^2 + (Y1 - Y2)^2}$$

Where,$(X1, Y1)$are the coordinates of node 1 and $(X2, Y2)$are the coordinates of node 2.

The displacement can be used to get the movement or distance travelled by the VANET node in the given interval. It is the distance calculated of a particular node's location at two different time intervals and is calculated by the following formula:

$$\sqrt{(X - X')^2 + (Y - Y')^2}$$

Where,(X, Y) is the position of node at time interval t1 and $(X^{'}, Y^{'})$ is the position of node at time interval t2.
Direction of the movement is important in order to know whether the detect hurdles come in the way of the given VANET node or not.The movement of a node from initial location to final location confirms its direction.Point of Hurdle (Position) is also an important factor for the proposed model.It is the present location of a node which is defined as(X, Y). If the position of node is not moving then it can be termed as a point of hurdle.
The proposed model is entirely based upon the hazard or hurdle routing for the VANETs. The proposed model calculates the node positions and look for the hurdles continuously in the travelling path of the nodes in the cluster. The proposed model is aimed at finding and avoiding the hazard situations in the VANET clusters. The proposed model is designed to protect the VANETs from the occurring of the collisions due to the hurdles or hazards in the given VANET paths. The following is the hurdle or hazard detection algorithm for the VANET cluster:

Algorithm 1: Hurdle Detection Algorithm (HDA)

1. The nodes in the cluster scan their locality and objects in the range of their distance sensors deployed for obstacles.
2. The nodes are programmed to find the obstacle with the given distance or threshold.
3. The programmed nodes actively scan the distance from objects in their way.
4. If an object is found on the distance lower than the given threshold
5. The object is marked as the hurdle.
6. The node stops itself for the moment.
7. All of the following nodes are updated about the hurdle position and situation.
8. The node calculates the alternative path around the hurdle.
9. The node takes the backup path and crosses the hurdle with uninterrupted movement module.
10. End IF

The nodes in range are updated about the hurdle and take the backup paths according the given alternative path using the hurdle detection algorithm. The nodes update their information and follow the calculated instructions by the HDA module. In case, a node is left out of the reach during the transmission range of an RSU (road side unit), the node finds the way to the RSU through the other nodes in its range as well as in the range of the road side unit (RSU). The proposed model is equipped with the hurdle detection algorithm with the unicast updates for the newly joined member in the cluster to update them about the hurdles produced in the given interval.The one-hop distance is allowed using the existing model for the connectivity of the unassigned, non-connected and non-covered nodes in the RSU coverage. The extended coverage algorithm for the RSU coverage elongation is allowed till the nodes located on the one-hop distance from the member nodes of the given cluster. The RSU stores the updates about all of the hurdles produced in the cluster in the given interval length. The given interval length is the length of the period for which the RSU will store the information of the hurdles in the unicast table. The newly joined nodes are updated about the hurdles found in the given interval by the unicast update propagation model. This algorithm is as following:

B. Algorithm 2: RSU recursive updates and membership program(RSU-RUMP)

1. When a node found itself not in the reach of any RSU
2. Node sends the query to the nodes in range for their distance from any RSU.
3. The nodes reply with their membership with RSU.

4. The nodes on the one-hop distance are shortlisted.
5. The node with the minimum distance from target node is selected as the next-hop member.
6. The node joins the nearest RSU through the next-hop member node.
7. The RSU forwards the hurdles updates in the form of unicast update packets.
8. The newly joined member will update itself about the hurdle information and will follow the given movement protocol designed for the hurdle avoidance protocol.

A. *Algorithm 3: Hazard Routing Algorithm*

1. Start the Road side Unit.
2. Start the VANET nodes in the cluster.
3. Each node shares its coordinate (X, Y) information with all the nodes in cluster.
4. Note: The nodes not sending the coordinate information will not become the member of cluster.
5. Calculate the following:
6. Distance
7. Displacement
8. Direction
9. Position
10. Flexibility for connectivity:

$$N_s = \int_{n=1}^{N} (d) \leq 250$$

If $\mathrm{N_i} = (1,2,3 \ldots \ldots \mathrm{N})$ is RSU
Connect $\mathrm{N_i}$to $\mathrm{N_s}$.

3. RESULT ANALYSIS

Throughput: The amount of data transferred from one place to another or processed in a specified amount of time. It is usually measured in Kbps, Mbps, and Gbps. In simulation, the attacker nodes are programmed to flood the victim node with the various flooding formations or methods. The throughput has been obtained from the simulation in order to evaluate the performance of the proposed model. The throughput is calculated at an interval of every 0.5 seconds. The throughput in the simulation is the number of Megabits has been recorded at approximately 19 Mbps of highest throughput in the WSN cluster. The simulation statistics has been recorded for 12 seconds. Approximated average of the proposed model has been recorded at 10 Mbps overall throughput in the WSN cluster in the given configuration. The proposed model has been shown the improvement in the results from the existing model by 15-20%.

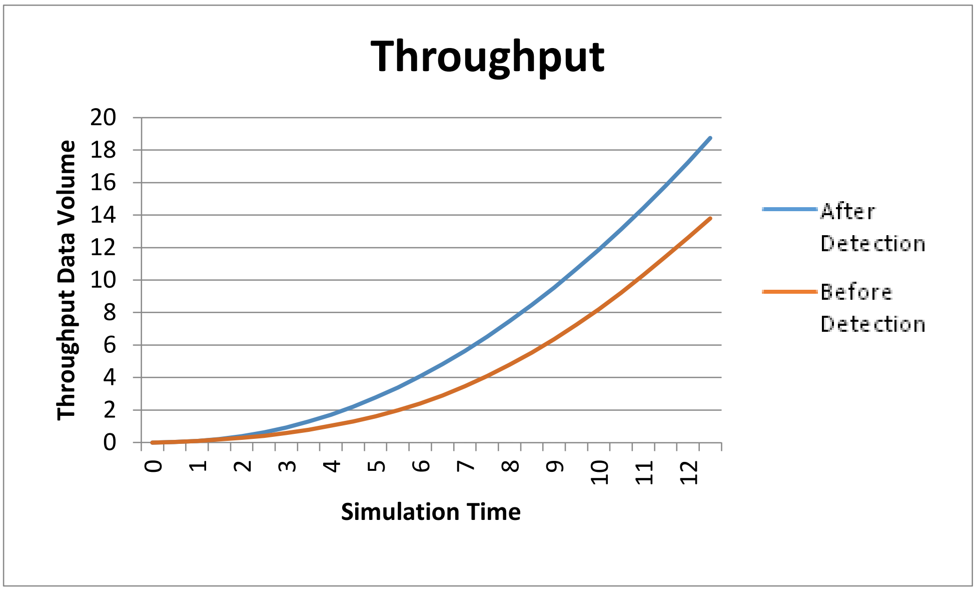

Figure 1: Network Throughput

Table: 1 Values of throughput before detection and after detection

Throughput	Before detection	After detection
5s	0	0
10s	1	2
15s	3	5
20s	7	10
25s	14	19

End to End Delay: It is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. When the nodes transmit the data in the inter-cluster formation, the congestion is caused over the communications links after the link overloading with the higher volumes of data. Such heavier volumes in result, increases the transmission delay from the given WSN scenario.

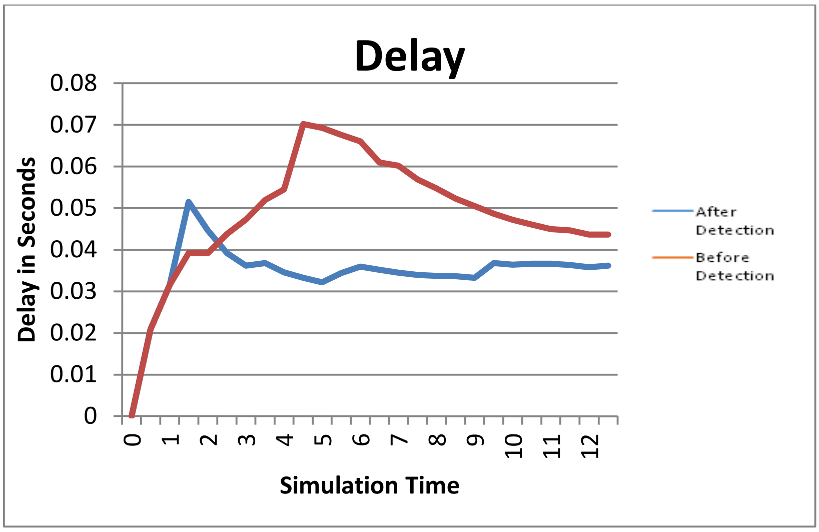

Figure 2: Network Delay

Table: 2 Values of Delay before detection and after detection

Delay	Before detection (sec)	After detection (sec)
5s	0.04	0.05
10s	0.05	0.03
15s	0.06	0.03
20s	0.05	0.03
25s	0.03	0.03

The delay has been recorded in the above figure. The proposed model has scored the maximum transmission delay at around 0.05 seconds at maximum, whereas less than 0.035 seconds in the overall simulation time. The proposed model has shown the improvement by approximately 0.02 seconds.

Packet Delivery Ratio: It is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. It is calculated by subtracting lost packets from total number of packets and divided by number of packets transmitted. In graph of packet delivery ratio, time (seconds) is taken as X-axis and PDR is taken as Y-axis. Figure 3 shows the PDR of a simulation when data is shared between the several nodes together during the given simulation length.

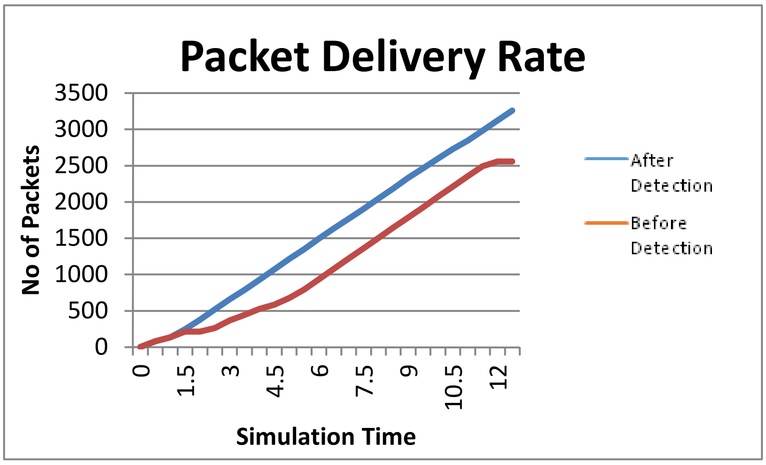

Figure 3: Packet Delivery Rate

Table: 3 Packet delivery rate before detection and after detection

Packet delivery Rate (packet)	Before detection	After detection
5s	400	450
10s	500	1000
15s	1000	1500
20s	1800	2000
25s	2500	3200

The maximum PDR has been recorded near 100 percent, whereas the lowest at zero during the no-traffic hours and minimum value has been recorded under 10 during the partial convergence phase of the network. The average packet delivery ratio has been recorded at more than 85 percent during the attack hours. The proposed model has been recorded with approx. 15% improvement.

Data Loss: The data loss or packet loss is the parameter indicates the data lost during the communication between the two given points within the given simulation. The data loss is increased heavily during the attack hours, which must be prevented by using the security scheme. Our security scheme against the denial of service and distributed denial of service attacks has been evaluated using the data loss parameters also. The total data loss has been nearly 9000 packets in the whole simulation, where hundreds of Mb/s of data has been transferred. The 9000 packets consist only 360,000 bytes of data, when a packet length is generally 40 bytes. The total data consists of only 360 Kb/s, which is nearly 0.01 % of the total data being transferred between the two points.

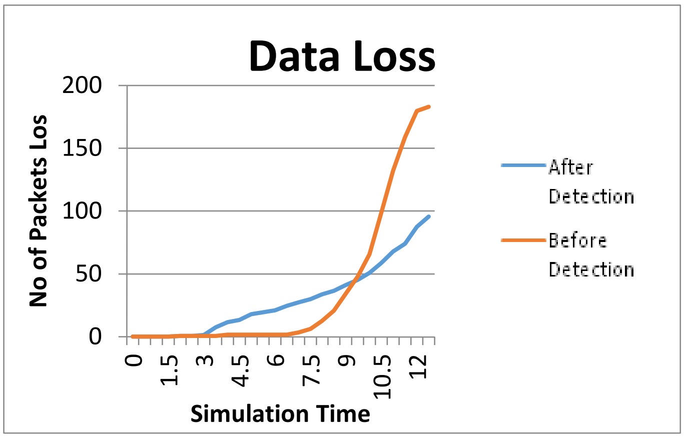

Figure 4: Data Loss

Table: 4 Values of Data Loss before detection and after detection

Data Loss (packets)	Before detection	After detection
5s	0	0
10s	0	20
15s	0	20
20s	60	40
25s	180	100

The data loss has been recorded at zero at some points, as the average data loss stays at almost 5 packets every 1000 packets being transferred between the network nodes in the given simulation during the attack hours with security implementation of the proposed model. The proposed model can be classified as the quite effective solution, which reduces the general data loss limit of 20% to merely less than 1%, which can be said to be the very effective security system.

Network Load: The network load is the parameter, which indicates the total data being transferred between the two nodes within the given cluster. The network load is the parameter which tells the volume of data being processed on a single node during the given time interval. The higher load increases the probability of data loss and higher delay, which comprises the weaker performance of the network. The given network load has been recorded at nearly 3.5 at maximum, which shows the significant reduction in the load during the attack hours using the proposed security model.

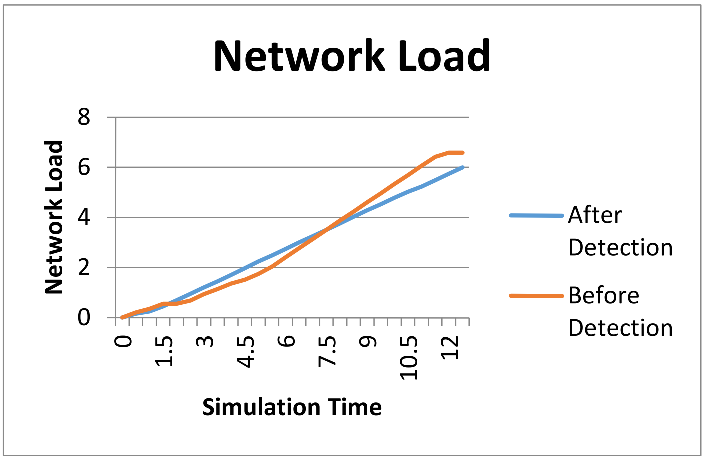

Figure 5: Network Load

Table: 5 Values of Data Loss before detection and after detection

Network Load (Mbps)	Before detection	After detection
5s	0.5	0.5
10s	1	1.5
15s	3	3
20s	4	4
25s	7	6

The minimum load has been recorded at zero during the no-traffic hours and very low (0.5 Mbps) during the attack hours with the security implementation over the network. The proposed model can be classified as the most effective from its performance obtained in the form of network load.

Energy Consumption: It is calculated by subtracting the present energy of a path from the Initial energy of path. When data is transferred between the network nodes, energy is consumed during the packet receive event, packet transmit event, during the idle or sleep state of the sensors. The energy is calculated after each interval of 0.5s in the given simulation scenario. Energy consumption is plotted across Y-axis and the simulation time on the X-axis. The energy consumption is the key parameter in the case of wireless sensor nodes. The lifetime of sensor nodes entirely depends upon the battery life which is directly proportional of the volume of data and amount of local processes on the node. The heavy data volumes are the key factor behind the energy consumption of the sensor nodes. The sensor node's energy consumption can be reduced by mitigating the heavy traffic volume by filtering the overflowing attack data from the ingress ports of the network nodes. The energy consumption reduction directly affects the network lifetime and elongates the network lifetime in the direct manner.

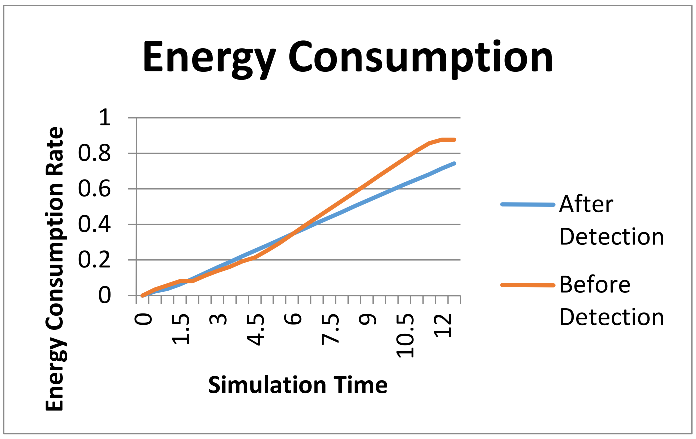

Figure 6: Energy Consumption

Table: 6 Values of Energy consumption before detection and after detection

Delay	Before detection	After detection
5s	0.1	0.1
10s	0.2	0.2
15s	0.4	0.4
20s	0.6	0.5
25s	0.9	0.7

The proposed model energy consumption has been recorded in the form of residual energy. The overall energy consumption has been drastically improved in the case of proposed model. The overall energy of the sensor nodes has been choked to 0.5 percent with 99.5 % residual energy remaining with the nodes to run for the hours. The simulation time of 10 seconds which includes the heavier traffic count during the attack simulation, the energy consumption has been reduced to the drastically low level, as per expected from the proposed defense model against the service unavailability attacks.

4. COMPARATIVE ANALYSIS

The final results have been also obtained from the simulation in the form of number of neighbor nodes and energy consumptions. The obtained parameters have been compared with the existing models.

Number of Neighbor Nodes: The number of neighbor nodes is the parameters which indicate the performance of particular nodes and their degree in context to their neighbor nodes. The higher number of neighbor nodes empower the node to make the multiple paths to keep the communication alive to the BTS or the sink node. The proposed model results have shown the effectiveness of the proposed model as the proposed model nodes have been staying connected to the higher number of nodes while compared to the existing number. In the proposed model, each node has minimum 5 numbers of nodes and maximum of 12 numbers of nodes as the neighbors to the nodes. The average value remains somewhere between the 9 numbers of the nodes has been recorded.

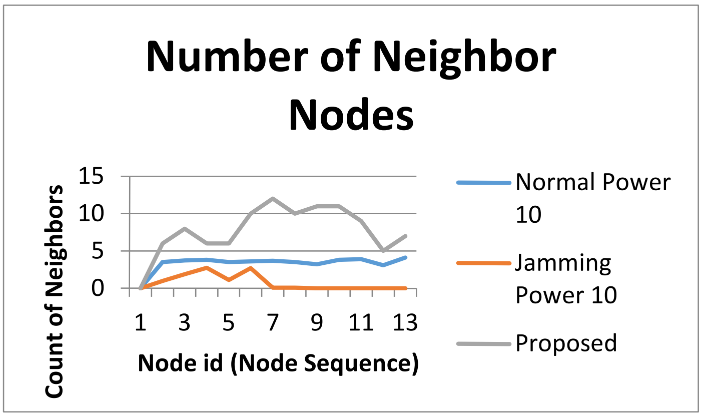

Figure 7: The count of neighbors in the existing vs. proposed models

Table 1: The comparison between the numbers of neighbours in the existing v/s proposed models

Node Sequence	Normal Power 10	Jamming Power 10	Proposed
0	0	0	0
1	3.51	1	6
2	3.75	1.9	8
3	3.8	2.75	6
4	3.51	1.1	6
5	3.6	2.7	10
6	3.7	0.1	12
7	3.5	0.07	10
8	3.2	0	11
9	3.8	0	11
10	3.9	0	9
11	3.1	0	5
12	4.1	0	7

Energy Consumption: The energy consumption is the parameter to estimate the power consumed by the sensor nodes in performing the operations on the sensor nodes to send, receive to route the data from one node or one path to another path. Also the nodes consume the energy while performing the sensing operations. The proposed model has been evaluated for the energy consumption against the energy consumption of the existing models in performing the similar operations over the similar amounts of data for the similar length of periods in the both of the simulations. The proposed model has been found more energy efficient than the existing model. The proposed model has been found consuming very low amount of energy in comparison with the existing models. The proposed results with the comparison to existing models haves been given as following:

Table 2: The comparison between the numbers of neighbors in the existing v/s proposed models

Number of Hops	Normal Power 10	Proposed	Jamming Power 10
0	0	0	0
2	240000	110	242000
4	250000	190	250000

6	250000	280	246000
8	257000	400	260000
10	246000	520	255000
12	300000	1000	320000

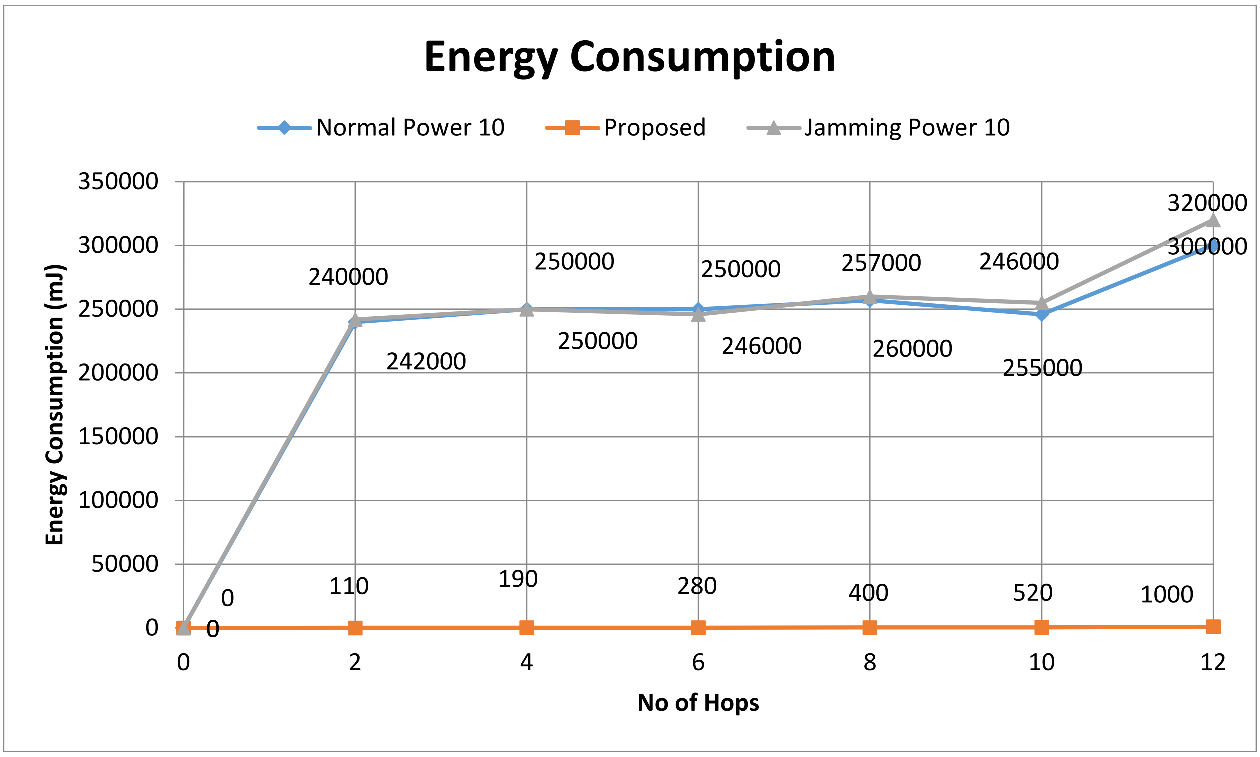

Figure 8: The count of neighbors in the existing v/s proposed model

5. Conclusion

The proposed model has been designed to mitigate the distributed denial of service attack from the vehicular network. The proposed model has been found efficient in detecting and mitigating the vehicular hurdles by using the active track hurdle detection algorithm. The proposed model bypasses the vehicular nodes to change their way from the path containing the hurdles. The proposed model has been also made capable of detecting the hurdles on the path created due to the vehicular collisions. The proposed model has been enabled with the ability to connect the nodes in the node-to-node and node-to-RSU in order to maximize the vehicular network reach. The proposed model performance has been evaluated on the basis of multiple parameters to judge the network performance. The performance parameters of transmission delay, network load, packet loss, energy consumption, etc has been evaluated for the performance of the proposed model in the wireless sensor network. The proposed model has been evaluated for the different levels of the attacks over the sensor network. All of the obtained results have indicated the effectiveness of the proposed model design in mitigating the attacks from the vehicular networks.

6. Future work

In the future, the proposed model can be enhanced using various other mechanisms of data pattern analysis and data filtering. The new pattern analysis method can be proposed to empower the security model design in mitigating the DDoS, DoS or other jamming attacks. The proposed model can be enhanced to work against the blackhole or sinkhole attacks to target the data transportation.It isa worm intelligence technique. Automatic decision for collsion can be take place. Auto traffic classification can be classified in order to target traffic or target update to the selective beneficial node.

References

1. Javed, Muhammad A., and Jamil Y. Khan. "A geocasting technique in an IEEE802. 11p based vehicular ad hoc network for road traffic management." Australasian Telecommunication Networks and Applications Conference (ATNAC), IEEE, pp. 1-6, 2011.
2. Hung, Chia-Chen, Hope Chan, and EH-K. Wu. "Mobility pattern aware routing for heterogeneous vehicular networks." Wireless Communications and Networking Conference, IEEE, pp. 2200-2205, 2008.
3. Dias, João A., João N. Isento, Vasco NGJ Soares, FaridFarahmand, and Joel JPC Rodrigues. "Testbed-based performance evaluation of routing protocols for vehicular delay-tolerant networks." GLOBECOM Workshops (GC Wkshps),IEEE, pp. 51-55, 2011.
4. Moser, Steffen, Simon Eckert, and Frank Slomka. "An approach for the integration of smart antennas in the design and simulation of vehicular ad-hoc networks." Future Generation Communication Technology (FGCT), IEEE, pp. 36-41, 2012.
5. Sumra, Irshad Ahmed, HalabiHasbullah, J. A. Manan, MohsanIftikhar, Iftikhar Ahmad, and Mohammed Y. Aalsalem. "Trust levels in peer-to-peer (P2P) vehicular network." 11th International Conference on ITS Telecommunications (ITST), IEEE, pp. 708-714, 2011.
6. Sumra, Irshad Ahmed, HalabiHasbullah, and J-L. A. Manan. "VANET security research and development ecosystem." National Postgraduate Conference (NPC), IEEE, pp. 1-4, 2011.
7. Ghaleb, Fuad A., M. A. Razzaque, and Ismail FauziIsnin. "Security and privacy enhancement in VANETs using mobility pattern." Fifth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, pp. 184-189, 2013.
8. Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security issues and challenges of vehicular ad hoc networks (VANET)." International Conference on New Trends in Information Science and Service Science (NISS), IEEE, pp. 393-398, 2010.
9. Seuwou, Patrice, Dilip Patel, Dave Protheroe, and George Ubakanma. "Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs)." Conference on Road Transport Information and Control, IET and ITS, pp. 1-6, 2012.
10. Qian, Yi, Kejie Lu, and Nader Moayeri. "Performance evaluation of a secure MAC protocol for vehicular networks." Military Communications Conference, IEEE, pp. 1-6, 2008.
11. Julio A. Sanguesa, Manuel Fogue, Piedad Garrido, Francisco J. Martinez, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni, "RTAD: A real-time adaptive dissemination system for VANETs", Vol. 60, pp.53–70, April 2015
12. Venkates , Indra, Murali, "Vehicular ad hoc networks (VANETS): issues and applications" Journal of Analysis and Computation, Vol. 8, No. 1, pp. 31-45, June 2012
13. K. Prem Kumar, S. Jemima Evangelin, V. Amudharani, P. Inbavalli, R. Suganya, U. Prabu, "Survey on Collision Avoidance in VANET" Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology, 2015
14. DivyaChadha, Reena, "Vehicular Ad hoc Network (VANETs): A Review", International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 3, Issue 3, pp.2339-2346, March 2015
15. Mohamed NidhalMejri, Jalel Ben-Othman, Mohamed Hamdi, "Survey on VANET security challenges and possible cryptographic solutions", Vol.1, Issue 2, April 2014, Pages 53–66
16. Ram Shringar Raw, Manish Kumar, Nanhay Singh "Security challenges, issues and their solutions for VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, pp. 95-105, September 2013
17. Dinesh V. Jamthe , S. S. Dorle, "Collision avoidance in ivan to maintain inter-vehicular distance on highways" International journal of engineering science & advanced technology, Vol. 2, Issue-3, 672 – 678, June 2012
18. Harjinderjeet Singh, Manuraj Moudgi, "Collision Avoidance Mechanism Using Multi-Layered Collision Detection Model for Vehicular Networks" International Journal of Computer Science Trends and Technology (IJCST), Vol. 3 Issue 4, Jul-Aug 2015
19. VanitaLonkar, Manoj Sharma, "Secure Technique for Collision Avoidance in Car-to-Car Communication" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 7, July 2013
20. P. Suresh, M. Ramya, "Collision Avoidance System for Safety Vehicular Transportation in VANET" Asian Journal of Technology & Management Research, Vol. 04, Issue: 02, pp. 30-34, Dec 2014