EasyChair Preprint

№ 6872

Gray Hole Attack Detection and Prevention System in Vehicular Ad-Hoc Network (VANET)

Gurtej Kaur, Meenu Khurana and Amandeep Kaur

October 19, 2021

Gray Hole Attack Detection and Prevention System in Vehicular Ad-Hoc Network (VANET)

Gurtej Kaur, Meenu Khurana, Amandeep Kaur
Chitkara Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab.

ABSTRACT

VANET plays a key role in the development of smart transportation. In the transportation system traffic goes too fast and scales in number, which raises numerous challenges, especially in communication security. When vehicles transfer safety information with each other malicious attacks can destroy or alter the information. These attacks are of various types faced by VANET. So, there is a need to detect and prevent these attacks. Every node in VANET performs as a router for corresponding nodes, so a malicious node can deliver fake routing messages to nodes, therefore affecting the network's performance. To solve these issues, the AODV routing protocol is used for detection and prevention of Gray Hole attacks. The network simulator NS2 is used for the simulation process. This work enhances the network performance by improving parameters such as PDR, throughput, packet loss, and delay.

Keywords: VANET, Ad-hoc, Gray Hole Attack, NS2, AODV, Performance metrics.

1 INTRODUCTION

1.1 VANET

To create a mobile network, Vehicle Ad-hoc Networks (VANET) use cars as mobile nodes. Through the implementation of VANET, any car can be used as a wireless node or router capable of establishing a wide-ranging wireless network between cars within 100 to 300 meters range. Once vehicles lose signal range and leave the network, new vehicles can join, making it possible for mobile networks to exist. Police and fire vehicles are known to be the first applications to use this technology for secure communications[1].

The VANET is not a new concept; it continually introduces unique challenges and issues for research. A VANET's primary function is to establish and maintain a communication network between collection of vehicles without using centralized control system [2]. Among the most significant applications of VANET are medical emergencies since there is no communication, yet critical to transmit information to save human lives. Unfortunately, in addition to these benefits of VANET, new problems and issues arise. The lack of infrastructure creates enormous responsibility for vehicles in VANET [3]. Every vehicle joins the network and maintains and governs the communication on the network as well as its communication requirements. VANET plays an important role in communication among dynamic vehicles in a limited range. When vehicles establish a connection with each other for transmission, is known as Vehicle-to-Vehicle (V-V) communication, and vehicles also can connect with infrastructures, for instance a Road Side Unit (RSU), that known as Vehicle-to-Infrastructure (V-I) communication [4]. Basic scenario of VANET is shown in fig 1.

The main objectives of the current work are as follows:

- To generate a VANET scenario by introducing RSU and vehicle properties.
- To introduce Gray Hole attack on the network.
- To detect the malicious node available in the network using neighboring information and PDR with PMOR.
- To evaluate various parameters PDR, Packet loss, Collision avoidance, and throughput for performance evaluation.

Optimal packet routing is a key component of the VANET design to effectively form a communication network. Various possible attacks are briefly introduced. The main concentration is on Gray Hole attack detection and prevention. Methodology and results are also addressed.

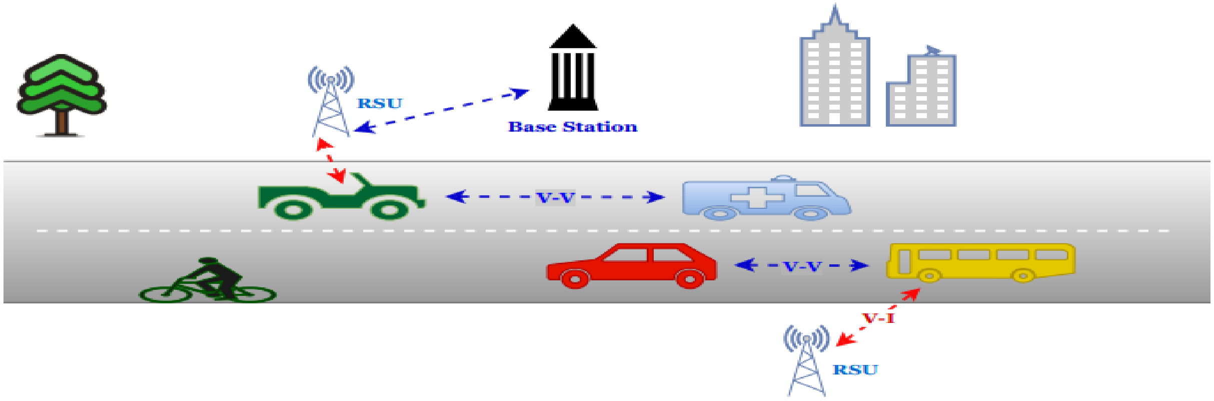


Fig 1. VANET

1.2 VANET ARCHITECTURE AND WORKING

There are many vehicles in the vehicular network, which are referred to as vehicular nodes. Each vehicular node requires some level of authority in order to control the system, and certification authority is used to govern it. Using 5.9GHz radio signals, the vehicular nodes must communicate over a distance of one kilometer. These signals have an adhoc connection that provides a wireless connection to move freely [1]. An onboard unit (OBU) is installed in every vehicle. It transmits radio signals between nodes and between routers, which facilitates communication between them. In a vehicular network, the road side unit serves as a router that is installed near the roads and is responsible for connecting vehicles and connecting those vehicles to other nodes, as shown in Fig 2. The vehicle also includes a Tamper Proof device (TPD), which stores vehicle-related information such as the driver's identity, vehicle speed, trip details, route information, and so on. Another device is the Electronic License Plate (ELP), which is a unique number for each vehicle that allows vehicles to be identified. For vehicular networks, GPS is used to determine the location of nodes. Each vehicle is equipped with GPS. The RSU device is designed to store all vehicle-related data.

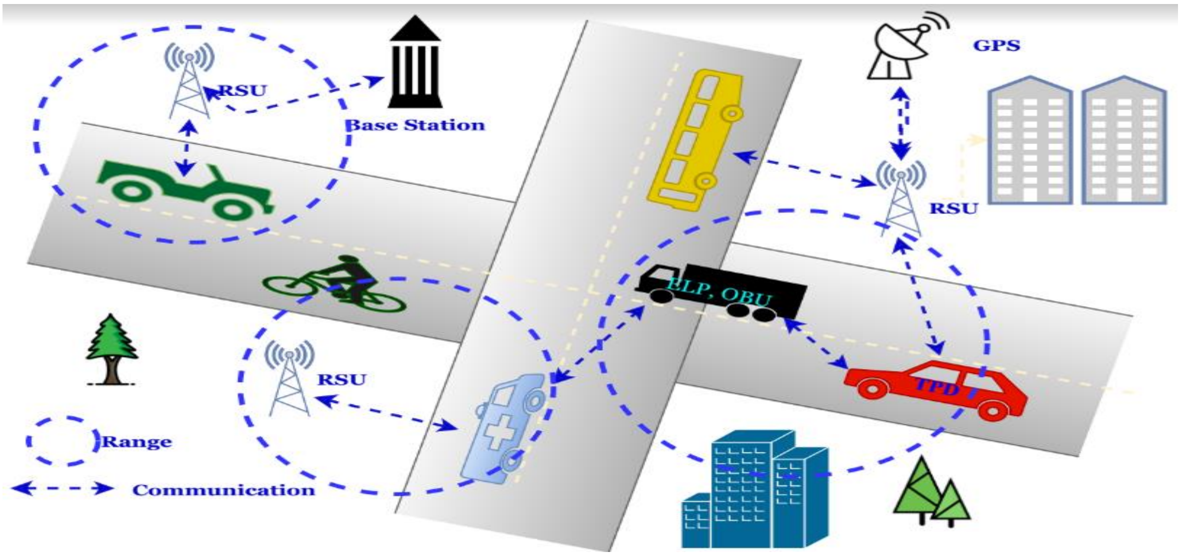


Fig 2. The working Architecture of VANET

VANET system architecture consists of different types of domains such as adhoc, in-vehicle and infrastructure domains and many individual components.

1.3 ATTACKS IN VANET

VANET is subject to several attacks, which are detailed in the sections that follow:

1.3.1 Denial of Service Attacks

The DoS attacker's primary goal is to restrict legal nodes from accessing network resources and consuming computational resources [5]. This floods the control channel with a large number of random messages and breaks the connection of transmission. This results in OBU and RSU being unable to effectively handle the load.

1.3.2 Broadcast Tampering

The attacker uses a broadcast tampering attack to insert erroneous messages into the network, causing disruption in routing. It is basically performed by internal attackers [6].

1.3.3 Sybil Attack

Sybil attack constructs different identities of numerous vehicles. It is possible to use those identities to cast any type of attack against a system. These fake identities hide the actual sender and make illusion to other vehicles about actual node [7].

1.3.4 Message Suppression Attacks

An attacker loses packets from the network intentionally, and these packets may include important information for the destination. It is possible that the attacker will ignore packets like these and use them again, if required. The objective of this attack is to restrict registration and insurance bodies from knowing about vehicle crashes and/or to prevent collision reports from being delivered to RSU [6].

1.3.5 Alteration Attack

The attack is launched by an attacker who modifies available data. Alteration attacks prevent the transmission of information from being sent, replay earlier transmissions, and modify the actual data entry by altering the transmission [7].

1.3.6 Black hole attack:

In VANET, Black hole attack randomly drops the entire packet so the network performance is degraded. A black hole node behaves like has shortest path information. So in this case, neighbors of the malicious node will always select it as best node. As a result, the malicious node is granted privileged access to the network, which it uses to launch the denial of service attack. [8]. In addition to one malicious node near the sender and destination nodes, the effect of this attack is much more vulnerable.

1.4 GRAY HOLE ATTACK

In the Gray Hole attack, a network node receives RREQ packets and discovers a route to the destination. It drops few data packets after discovering a route. Dropping against Gray Hole does not result in the loss of all data packets. Occasionally, the attacker will drop packets. It shows attacker act as a normal node sometimes and other times as a malicious node. The Gray Hole attack happens in two phases. Initially, a malicious node advertises itself as having a legitimate route to a destination node through the AODV protocol in order to intercept packets, despite the fact that the route is bogus. With a certain probability, the received packets are dropped by the node. It is more difficult to identify than the Black hole attack, where the malicious node drops incoming data packets on a regular basis. A Gray Hole's malicious behavior can manifest itself in a variety of ways. It simply drops packets coming from (or destined for) a specific node(s) in the network while forwarding all other packets. Another type of Gray Hole attack is a node that acts maliciously for a period of time by dropping packets but then returns to normal behavior. It also exhibit a combination of the above two behaviors, making detection more difficult [1].

In this case, attackers choose to use the selective data packet dropping method and represent themselves as authentic nodes for the purpose of gaining communication access [9]. Following that, the malicious node is always considered as a next-hop node and sends the packet to it. All incoming packets are collected by the malicious node, but they are dropped at random. The complete phenomenon makes it hard to detect and prevent damage because nodes can drop packets partially not only because they are malicious, but also because they are overloaded, congested, or selfish.

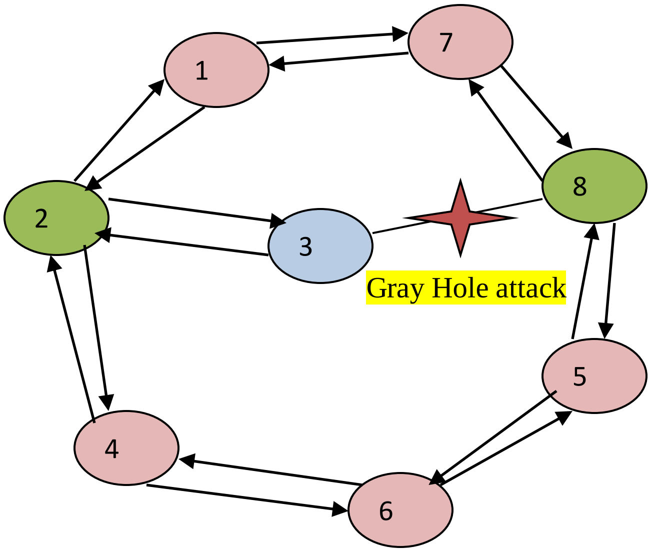


Fig 3. Gray Hole Attack

2. LITERATURE SURVEY

Swati Verma et al. [1] in VANET utilized the AODV routing protocol to ensure appropriate connection between nodes by transmitting the data. They have developed the Gray Hole attack on the AODV Routing algorithm and demonstrated its impact on VANET implementation. They evaluated variables such as packet delivery ratio (PDR), normalised routing load (NRL), latency, and throughput. As a result, NRL and PDR are on the increase and throughput values are declining.

Faisal Khan et al. [10] tackled the issue of filling transmission holes in VANET safety awareness messages. A new method for tracking safety messages at individual elements has been proposed to deliver the messages. A highly comprehensive simulation in ns-3 simulator of the propagation scenario is conducted, and the performance assessment of the NSN-H algorithm, along with three additional safety message dissemination methods, is given. Simulated results indicate that the NSN-H offers guaranteed reliability at the cost of just a negligible overhead delay of around five milliseconds even in scenarios with high traffic densities.

Ambuj Kumar et al. [11] a Group-based Exchange of SMS Messages Protocol is described. In suggested system, many techniques of Group creation are employed, which vary depending on the circumstance. In order to make our communication protocol trustworthy and efficient, we took into account different aspects such as message priority, context-based communication, and node velocity. It has been simulated to estimate the number of clusters formed and backoff counters used to check the efficiency of the group.

Congestion is found to rise with the Back-off counter and the performance of a network is measured by PDR.

Ankit Kumar et al. [12] proposed the AODV routing algorithm which successfully helps to detect and remove the black hole attack in VANET. In the results packet loss is much less in comparison with the previous AODV protocol. Work performance is analyses in terms of PDR. The proposed algorithm gives average throughput is 77.79 as compared to existing that was 29.74. Same as, the PDR is 75.28, in contrast, the existing has an average of 33.1. For future work, this approach can be applied for other attacks.

Andrew Fiade et al. [13] works on comparison of black hole and flooding attacks based on energy efficient AODV routing protocol. The testing scenario implemented on NS2, NAM, and MS Excel. Results shows throughput is 702,088 Kbps, packet loss is 32.444%, from end to end the delay is 287,625 ms, and energy consumed is 9,894 joules.

3. PROBLEM FORMULATION

In VANET varieties of attacks are susceptible. In the VANET environment safety message have to be transmitted in real-time so that collisions between different vehicles can be avoided. By performing attacks create an innumerable prudent identity for disturbing the network [7]. The disrupting of the network by malicious nodes may cause a problem in the transmission of valid information to the nodes available in the network. The information of a neighbor node has been recorded in order to locate malicious nodes in the network and avoid collisions.

We used the neighboring information of the nodes to overcome this problem of malicious nodes in VANET [14]. Malicious nodes create fake identities of other nodes, to disruption in networks, transmissions, and topologies. To eliminate this, information of neighboring nodes is collected and compared with the threshold values to find the malicious node.

4. METHODOLOGY

In the proposed work various steps have to be carried out for achieving the desired objective. In the completion of these objectives the phases have been described below:

Phase 1: In the first phase of the proposed work VANET scenario has been designed by initializing Lanes, vehicles, and RSU. These lanes have different speed structures and RSU since the coordinates of the vehicles available on the road [15].

Phase 2: In the second phase the malicious node has been introduced in the network that creates the duplicate ID of the other nodes available in the network and the position of the original node representing them on the other location that breaks the communication of the node.

Phase 3: In the third phase the detection of the malicious node has been done by using the neighboring information. The speed of each node is compared with other nodes available in the neighbor. If the speed of the node is compared with its threshold value that has been defined by RSU. Based on the comparison, legitimate and malicious nodes have been detected. After detection of malicious node, RSU broadcast message to all nodes available. Various parameters have been computed for the performance evaluation of the proposed work. These parameters are PDR, Packet loss, delay, and throughput.

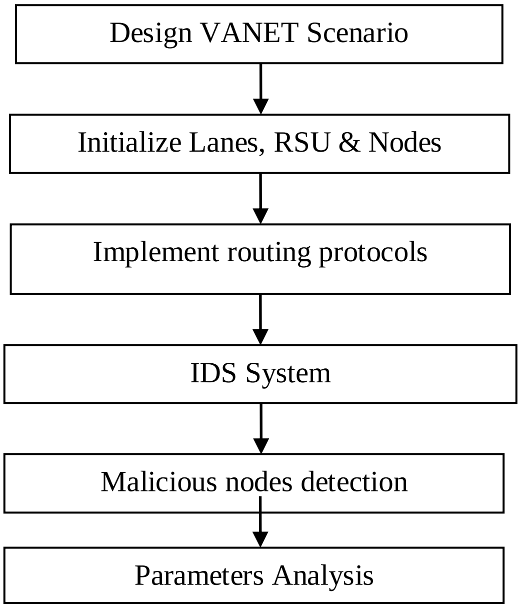

Design VANET Scenario
Initialize Lanes, RSU & Nodes
Implement routing protocols
IDS System
Malicious nodes detection
Parameters Analysis

Fig 4. The flow of Purposed Work

5. SIMULATION SETUP

We completed our work with the NS 2 simulator (Network Simulator 2). Specifically, to check how well the conventions are executed as the system's size grows, examinations were conducted on four different scales of full-fledged versatile hubs which are each 1,000m * 1000m in size. It was agreed that 50, 100, 150, and 200 hubs would communicate with the specifically designated system [16]. In the irregular position, hubs are produced haphazardly. Hubs were formed at random intervals, as though just a few hubs were entering the topology. A two-ray ground model was used for radio engineering. Omni Antenna was used as the radio wire model. For a reproduction, development was linear and hub pace was consistent.

Characteristics of Node:

1. Link-Layer: Logical Link (LL)
2. MAC: 802_11
3. Queue: Drop-Tail
4. Network Interface: wireless
5. Channel: wireless

We ran extensive simulations in NS2.34 to assess and compare the efficacy of various routing algorithms in a VANET. The simulations are all performed with constant mobility.

5.1 Performance metrics

a) **Packet Sent:** It refers to the number of packets sent by a source node [16].
b) **Packet received:** It refers to the number of packets received by a destination node.
c) **Throughput:** It is the average rate at which a data packet is successfully transmitted from one node to another during a certain time period. It is the number of packets sent by the source nodes over a communication network. Its measurement is in bits per second [1].

Throughput = (no of packets sent * actual size of packet) / Total delivery time

d) **Packet Delivery Ratio (PDR):** It is the number of data packets received at the destination divided by the total number of data packets provided by all sources. [12].

$$PDR = (Pk_r / Pk_s) * 100$$

Here, Pk_r is the total packets received and Pk_s is the total packets sent.

e) **End to End Delay:** This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay, and propagation delay [17]. It is calculated as

$$ED = (Tm_r - Tm_s)$$

Here, Tm_r receiving time and Tm_s is sent time of the packet.

6. EXPERIMENTAL RESULTS & DISCUSSION

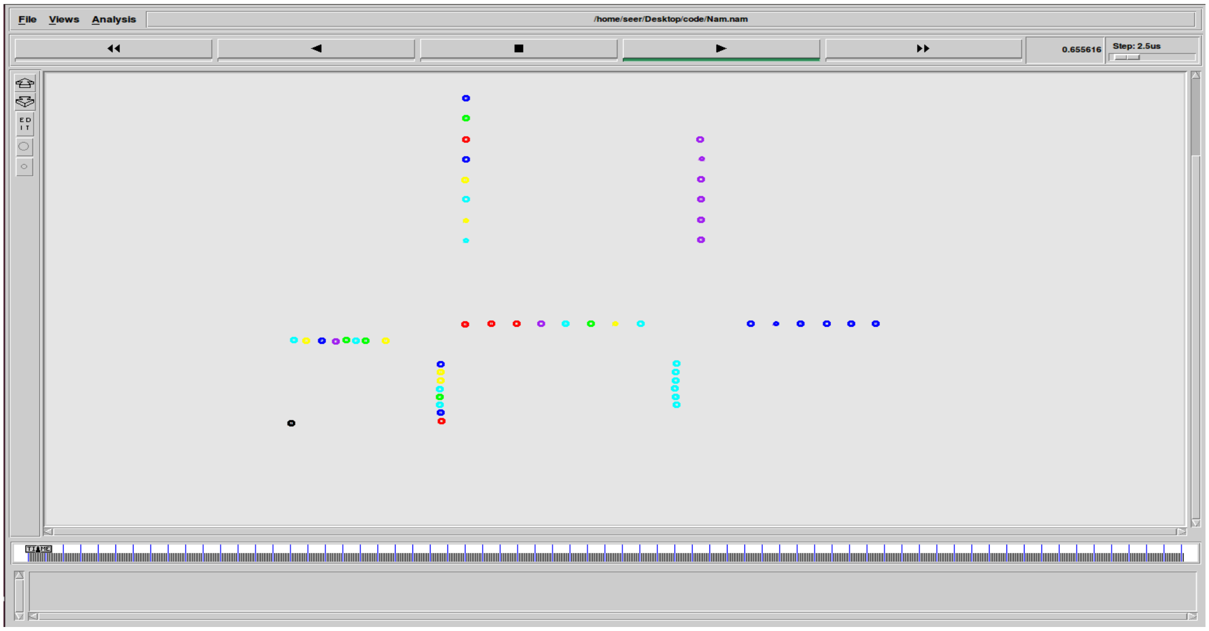


Fig 7. Node's Initialization

The fig 7 represents the number of nodes in the network. The number of nodes in this network is 52.

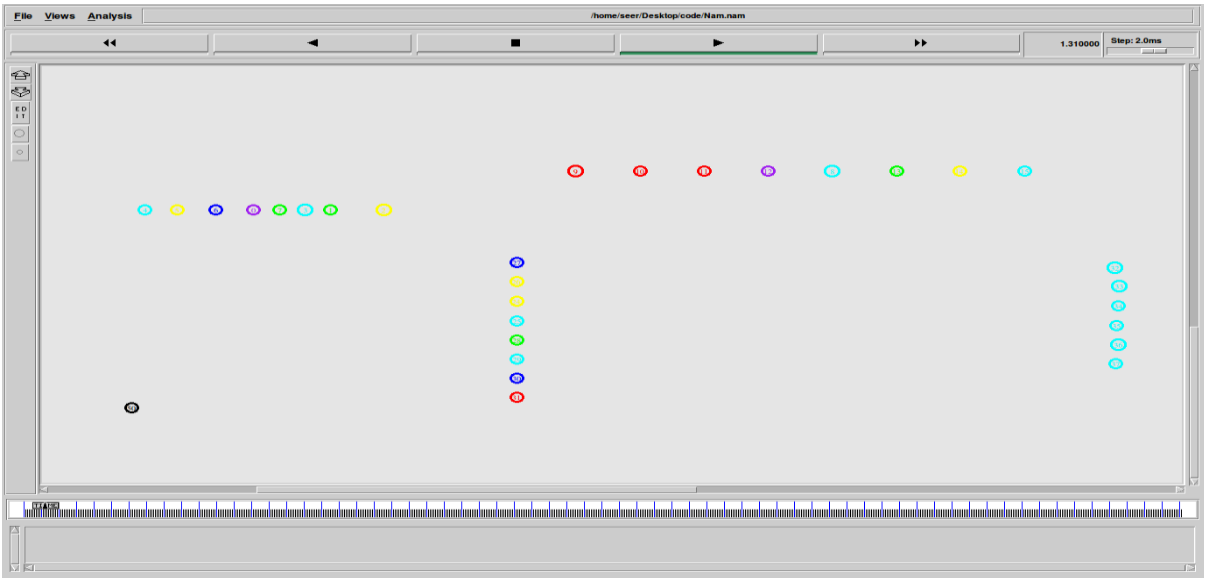
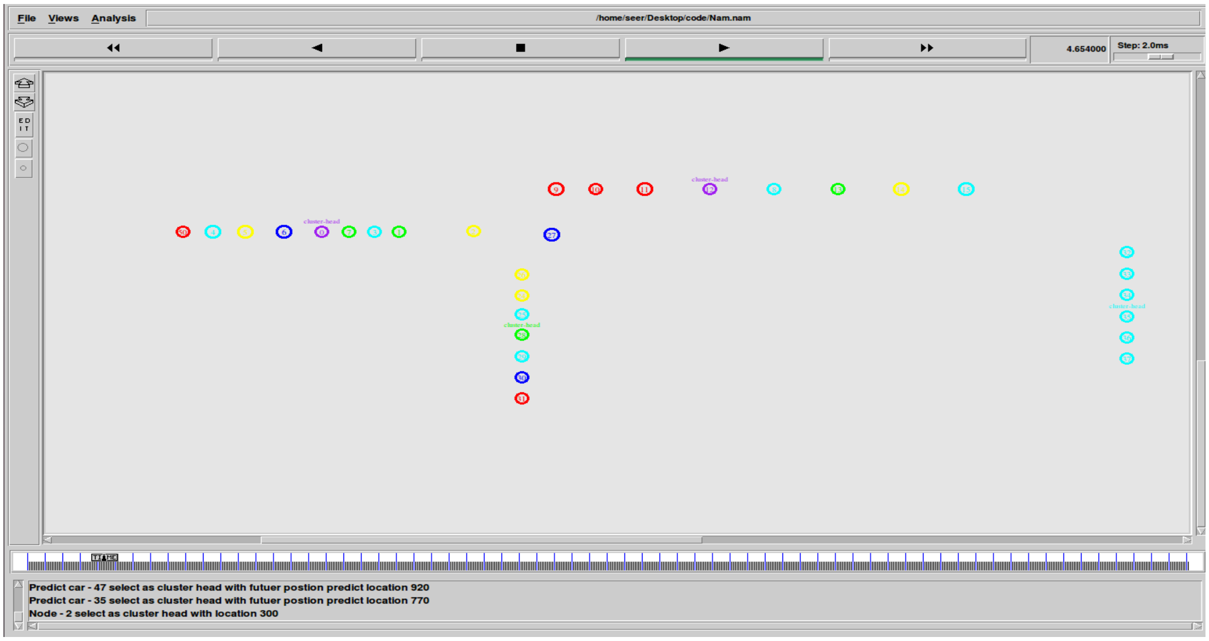


Fig 8. Mobility between vehicles

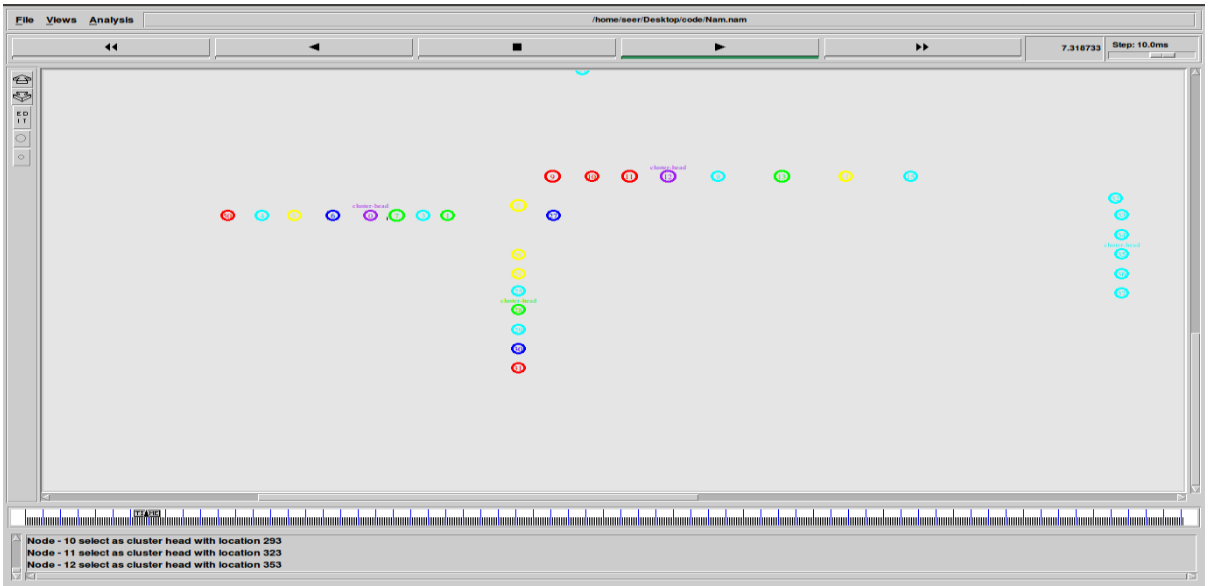
The fig 8 shows the mobility between the vehicles. The nodes start moving from one location to other location.



```
Predict car - 47 select as cluster head with futuer postion predict location 920
Predict car - 35 select as cluster head with futuer postion predict location 770
Node - 2 select as cluster head with location 300
```

Fig 9. Represent Clustering

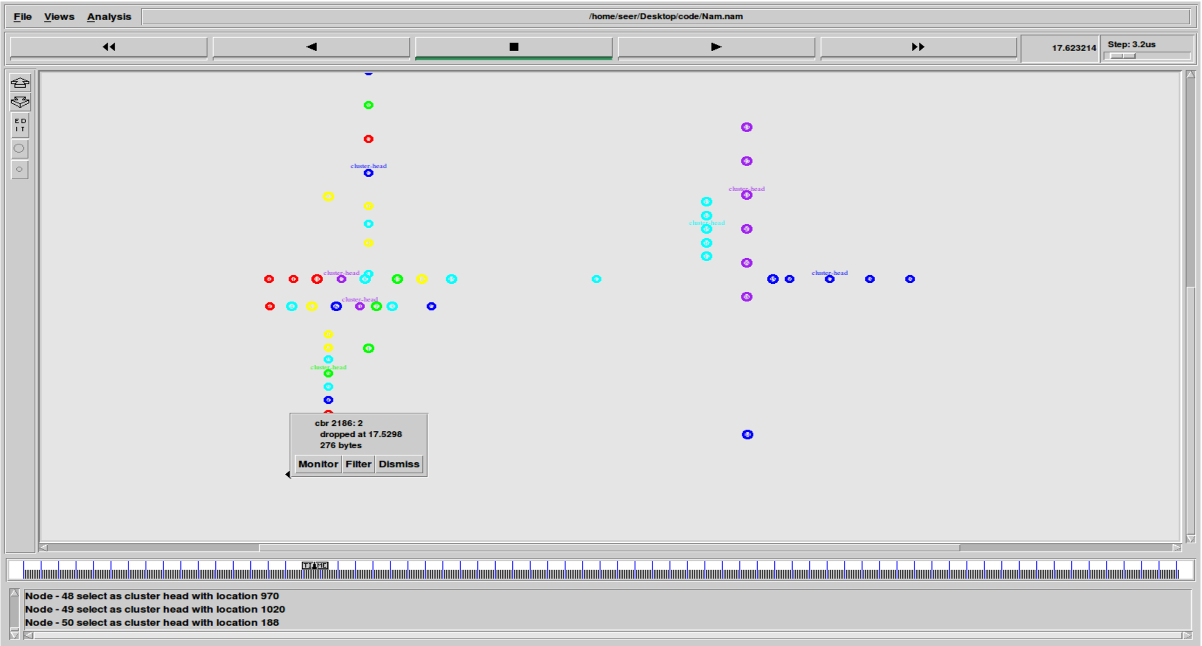
The fig 9 represents the clustering between the nodes. The nodes have been divided into different cluster on the basis of their properties. After clustering cluster head selection has been done.



```
Node - 10 select as cluster head with location 293
Node - 11 select as cluster head with location 323
Node - 12 select as cluster head with location 353
```

Fig 10. Cluster's Head Selection

The fig 10 represents the selection of cluster heads. The cluster head is selected on the basis of distance from other cluster nodes.

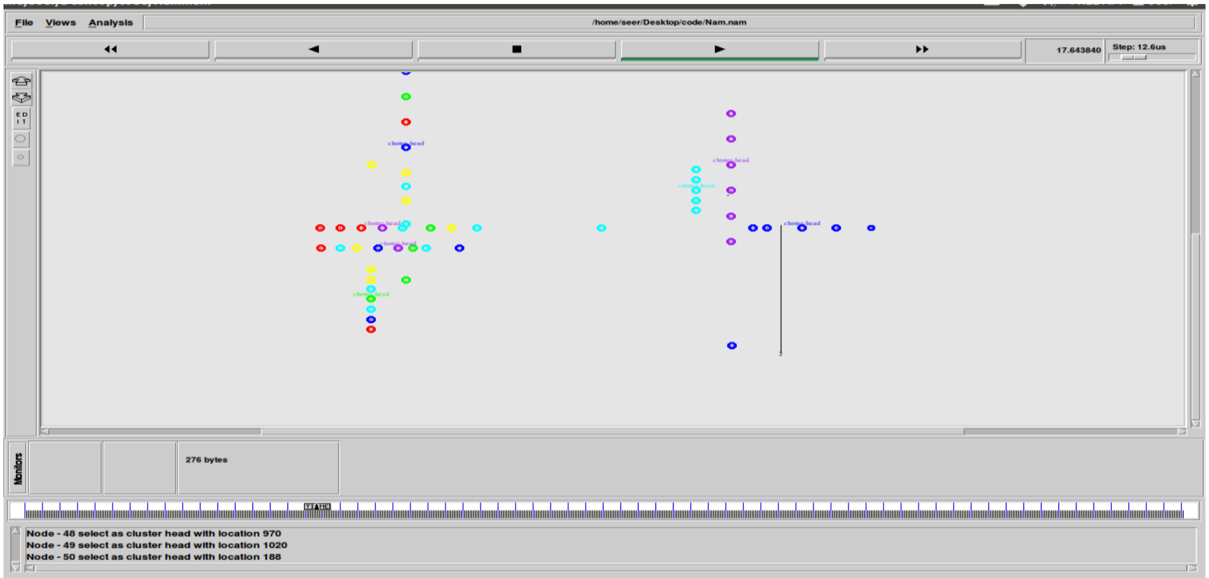


```
cbr 2186: 2
 dropped at 17.5298
 276 bytes
```

```
Node - 48 select as cluster head with location 970
Node - 49 select as cluster head with location 1020
Node - 50 select as cluster head with location 188
```

Fig 11. Data Monitoring during Transmission

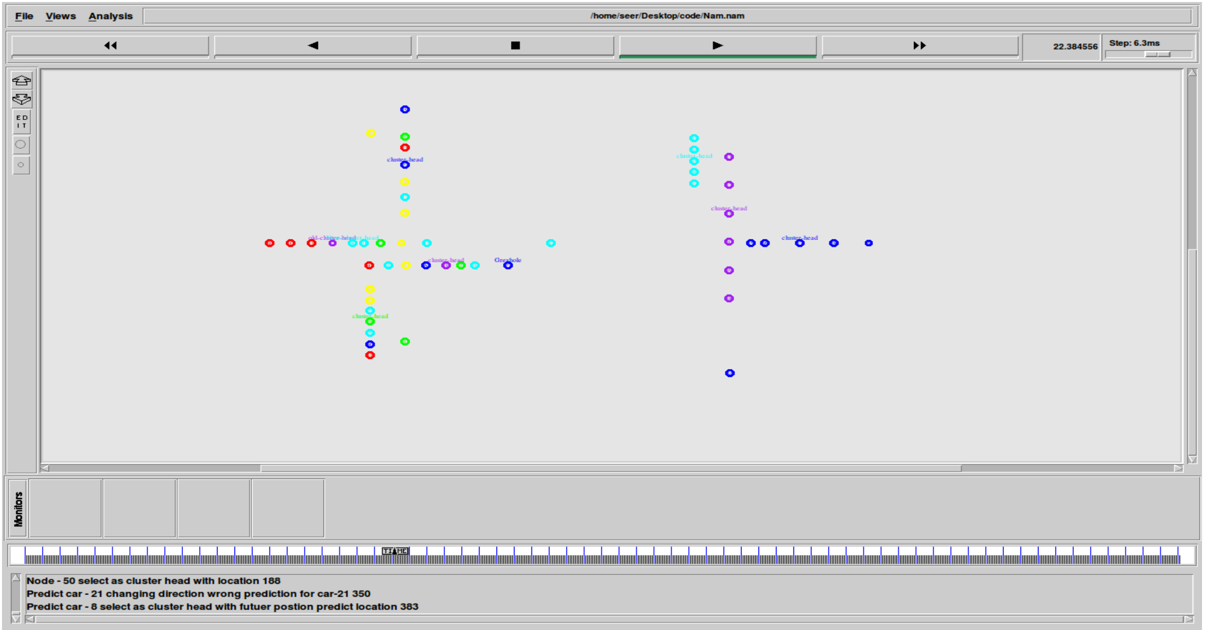
The fig 11 is use to represent the monitoring of data during the data transmission. During data monitoring message has been monitor that provides information about whole route occupied by the message header format in the message.



```
Node - 48 select as cluster head with location 970
Node - 49 select as cluster head with location 1020
Node - 50 select as cluster head with location 188
```

Fig 12. Data Monitoring during CBR

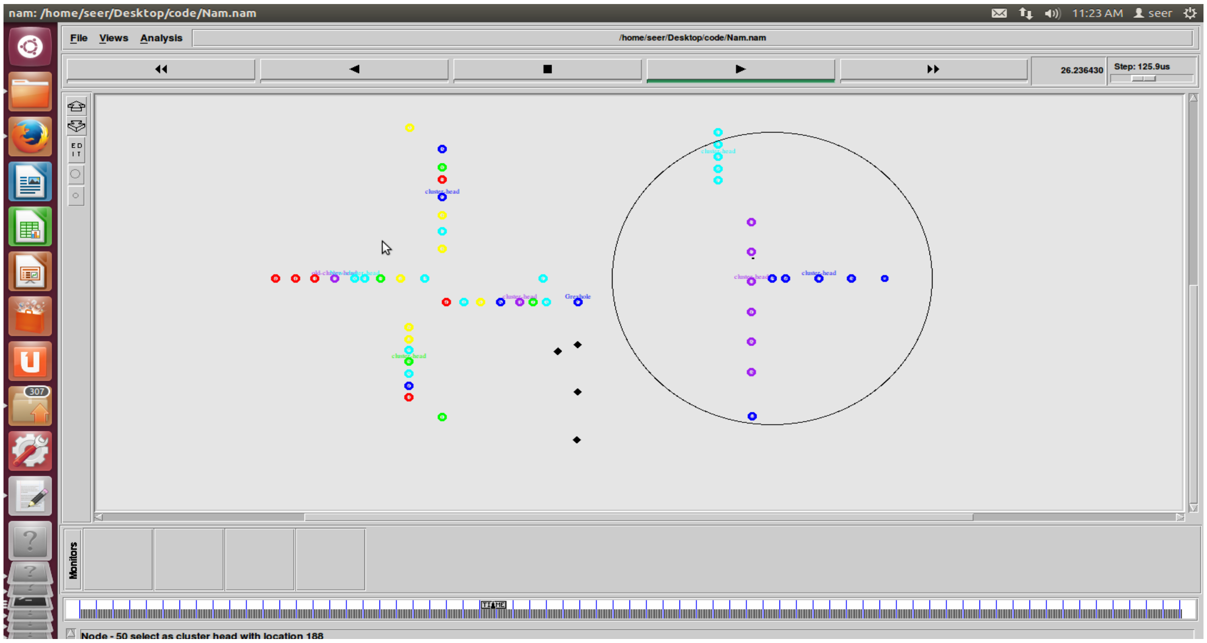
The fig 12 is use to represent the Data monitoring during CBR i.e. Constant Bit Rate.



```
Node - 50 select as cluster head with location 188
Predict car - 21 changing direction wrong prediction for car-21 350
Predict car - 8 select as cluster head with futuer postion predict location 383
```

Fig 13. Gray Hole Attack Detection

The fig 13 is use to represent the detection of Gray Hole Attack.



Node - 50 select as cluster head with location 188

Fig 14. Broadcasting of Malicious Node on the network

The disrupting of the network by malicious nodes may cause problem in the transmission of valid information to the nodes available in the range. To detect the malicious nodes available in the network for avoiding the collision neighbor nodes information has been captured.

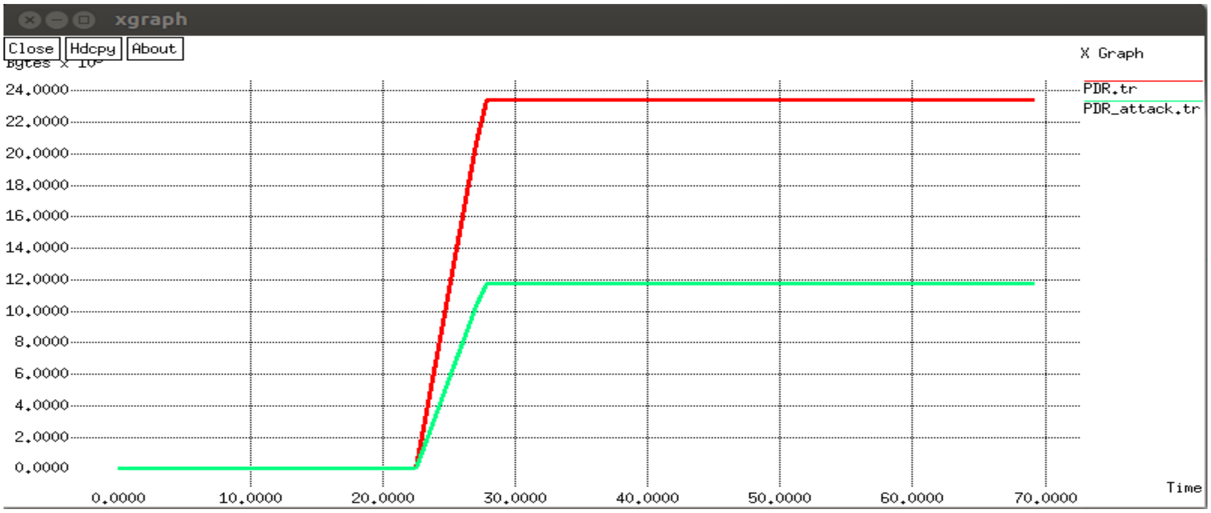


Fig 15. PDR

Fig 15 shows that there is very less loss which shows that network is performing well. PDR for existing work which is represented by green line is more as compare to current one. X Graph shows bytes at x axis and time in milliseconds at y axis.

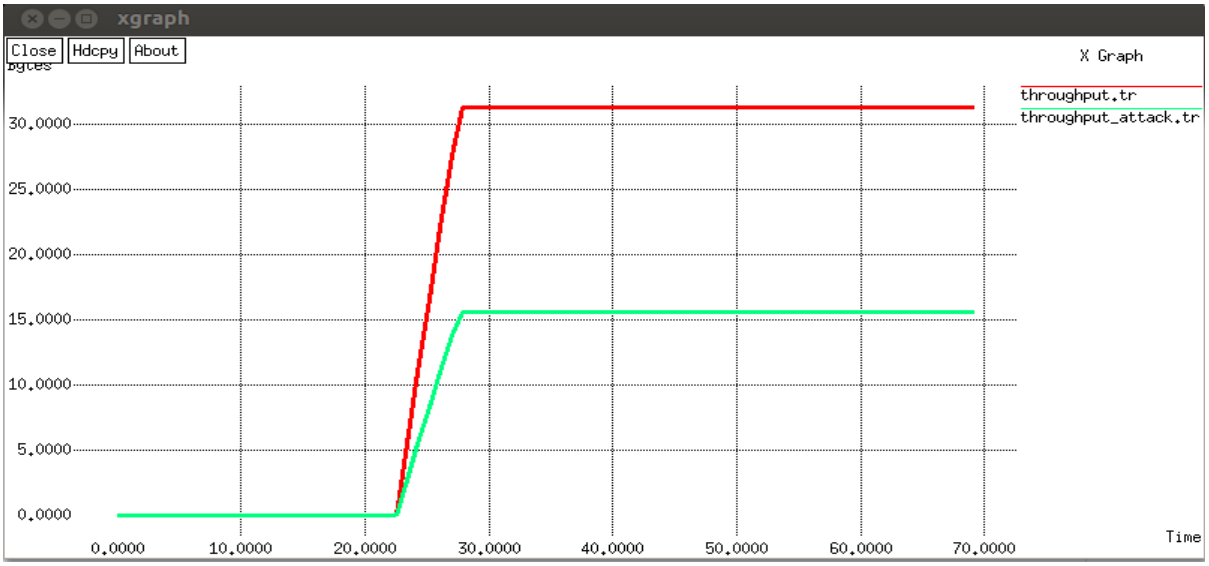


Fig 16. Throughput

Fig 16 shows the calculated throughput for the nodes. The red line in this graph represents the current workload, and the green line represents existing workloads that are very minor in comparison to the current workload.

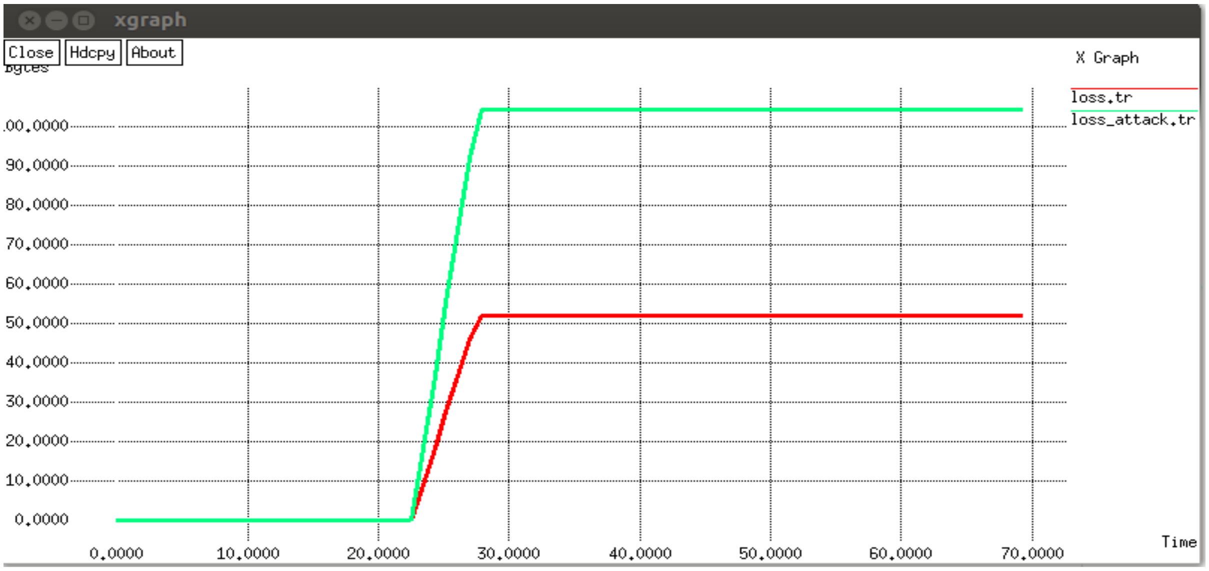


Fig 17. Packet Loss

Fig 17 shows that the network is performing well, because there are very few losses. However, the loss for current work, indicated by the green line, is significantly greater than the loss for new work.

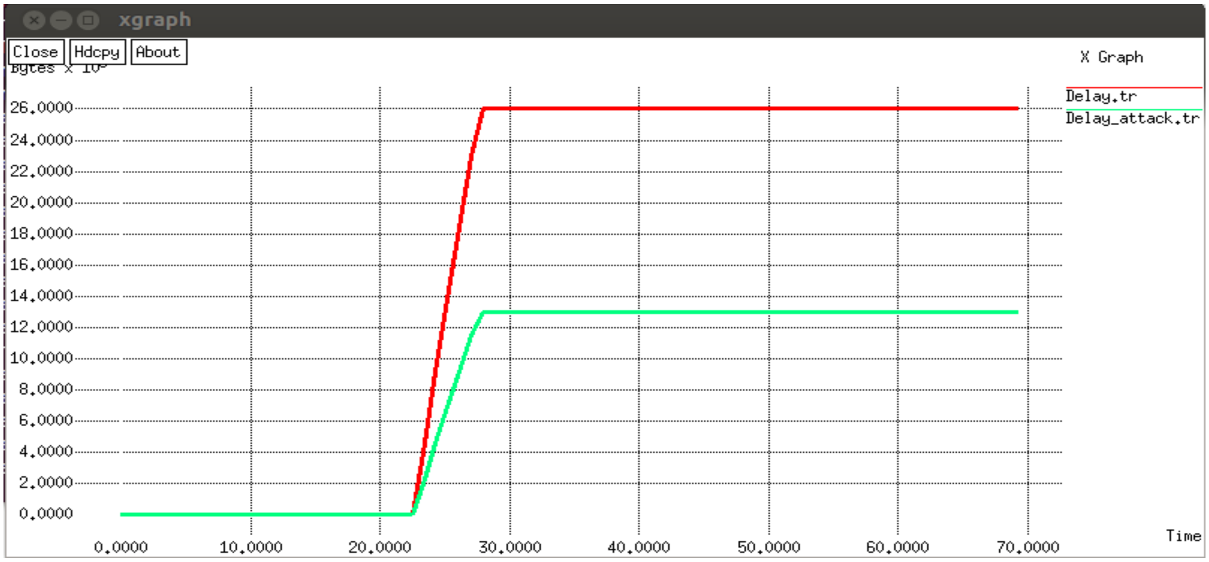


Fig 18. Time Delay

Graph in fig 18 indicates that the delay for this network is extremely low, indicating that network performance is good, while the delay for old work (shown by the green line) is relatively high in comparison to current work.

7. CONCLUSION

The field of VANET deals with vehicular networks. Various types of attacks are occurred in VANET. Environment safety message have to be transmitted in real time so that collision between different vehicles can be avoided. By performing attacks create an innumerable prudent identity for disturbing the network. The disrupting of the network by malicious nodes may cause problem in the transmission of valid information to the nodes available in the network. To identify malicious nodes available in the network for avoiding the collision neighbor nodes information has been captured. We used PDR, PMOR & neighboring information. At last we evaluate various parameters PDR, Packet loss, delay and throughput for performance evaluation & based on these factors, we infer that our approach produces superior outcomes.

8. FUTURE WORK

Future work would be conducted on comparing the various data security mechanisms. The future work is to avoid these attacks by using cryptographic methods over the network for the security of the network from these attacks. A feasible future expansion of this system would be to investigate various attacks using different AI approaches such as Fuzzy Petri Nets (FPNs).

REFERENCES

[1] S. Verma, “Impact of Gray Hole Attack in V ANET,” no. September, pp. 4–5, 2015.

[2] B. Sharma, M. Satya, P. Sharma, and R. Singh Tomar, “A Survey: Issues and Challenges of Vehicular Ad Hoc Networks (VANETs) under responsibility of International Conference on Sustainable Computing in Science, Technology and Management,” Accessed: Aug. 27, 2021. [Online]. Available: https://ssrn.com/abstract=3363555.

[3] F. Domingos *et al.*, “Data Communication in VANETs : Survey , Applications and Challenges To cite this version : HAL Id : hal-01369972 Data Communication in VANETs : Survey , Applications and Challenges,” 2016.

[4] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, “Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures,” no. March,

2019, [Online]. Available: http://arxiv.org/abs/1903.01541.

[5] A. M. Malla, “Security Attacks with an Effective Solution for DOS Attacks in VANET Security Attacks with an Effective Solution for DOS Attacks in VANET,” no. November, 2015, doi: 10.5120/11252-6467.

[6] M. Ali *et al.*, “Classification of Security Attacks in VANET : A Review of Requirements and Perspectives,” vol. 06038, pp. 1–7, 2018.

[7] Deeksha, A. Kumar, and M. Bansal, “A review on VANET security attacks and their countermeasure,” *4th IEEE Int. Conf. Signal Process. Comput. Control. ISPCC 2017*, vol. 2017-Janua, pp. 580–585, 2017, doi: 10.1109/ISPCC.2017.8269745.

[8] T. Zaidi and S. Faisal, “An Overview : Various Attacks in VANET,” *2018 4th Int. Conf. Comput. Commun. Autom.*, pp. 1–6, 2018.

[9] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, “Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks,” *Computers*, vol. 5, no. 3, 2016, doi: 10.3390/computers5030016.

[10] F. Khan, K. Sani, F. Elahi, and J. Copeland, “Recovering VANET Safety Messages in Transmission Holes,” pp. 0–4, 2013.

[11] A. Kumar and R. P. Nayak, “An Efficient Group-Based Safety Message Transmission Protocol for VANET,” pp. 270–274, 2013.

[12] A. Kumar, V. Varadarajan, A. Kumar, and P. Dadheech, “Microprocessors and Microsystems Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm,” *Microprocess. Microsyst.*, no. October, p. 103352, 2020, doi: 10.1016/j.micpro.2020.103352.

[13] A. Fiade, “Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network),” pp. 6–10.

[14] C. Science and C. Science, “Review of Potential Security Attacks in VANET,” pp. 3–6.

[15] R. Kaur, “Vehicular Ad-hoc Network-A Literature Review on Simulation Tools,” *WECON Conf.*, vol. 1, no. February, pp. 21–27, 2015.

[16] C. Guleria, “Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network,” *2018 4th Int. Conf. Comput. Commun. Autom.*, pp. 1–4, 2018.

[17] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, “VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead,” *J. Sensors*, vol. 2018, 2018, doi: 10.1155/2018/6576841.