Section: Research Paper
ISSN 2063-5346

IMPLEMENTATION OF SECURITY MECHANISM AGAINST ROUTING ATTACK IN VANET

Kirti
Research scholar, Kalinga University, Raipur
Email id. : kirtinandal3@gmail.com

ABSTRACT

This work provides the concept of mobility based VANET network in which all nodes are dynamically provided. This work presents the concept of network reconfiguration with Sybil attack detection and handling in VANET. It presents the concept by prediction based routing under shortest path in network. It also provides the concept of detection and prevention of Sybil attack in this network. Among multiple types of attacks, the main aim of the present study will be Sybil attack, which is a well-known attack. It is most vulnerable in open & broadcast network schemes. The use of Sybil attack decrease the system performance by creating malicious nodes. So, it is necessary to detect and prevent from these types of attacks. The proposed work presented the cases by taking different number of nodes with simulation time 50 ms. The work is being evaluated in terms of throughput and end to end delay with different number of nodes and simulation time.

Keywords-VANET, Vehicular Networks, Sensor Nodes, Routing Attack etc.

1. INTRODU CTION

WHO (World Health Organization) reports that the percentage of fatal car accidents has increased internationally by 2.2 percent. 1.35 million people die in automobile accidents every year. Because emergency medical assistance is frequently interrupted in road accidents, human lives are lost in many circumstances. According to the Golden Hour Principle, the period immediately following a catastrophic injury is known as the "golden hour," and there is a good probability that rapid emergency and surgical treatment can save a person's life during this time. The response time of emergency medical services can be sped up to reduce mortality risk by one-third.

Vehicular Sensor Networks (VSNs) are wired sensor system networks that collect data and use it to clear and resurface roadways. Modern automobiles use a variety of sensor systems, including actuators, GPS devices, and micro-integrated computers. As a result, a lot of vehicles are able to collect and process data. Additionally, automobiles can interact with other vehicles or roadside networks by using networking protocols such as Wireless Application Protocol (WAP), Next-Generation Telemetric Protocol (NGTP), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).

Vehicular Adhoc Network (VANET) (MANET) is a critical component of Mobile Adhoc Network. Automobiles serve as nodes in this system, facilitating data transmission between them. It has capabilities like mobility and sensor space utilization. It takes advantage of wireless networks to deliver data over distances of up to 1000 meters. Due to these restrictions, the VANET is supported by a defined foundation that contributes to specific VANET administrations and grants access to specified entities. Artificial brains are now used

more frequently than natural brains because of modern technological advancements. With the use of artificial intelligence, humans produce clever technical devices. IoT stands for "Internet of Things," which is a three-phase paradigm that emphasizes communication, cost savings, and automation through the use of technology. The rise of IoT offers a creative answer that can aid in enhancing many parts of the farming industry. Due to the deployment of smart technologies in rural areas, data collection could become simpler in this decade. This is a result of network advancement at all layers, which now allows for improved communication. The application of this technology to increase productivity has become a popular topic in contemporary studies [1]. The fixed frames are sent to common locations such as street edges, government buildings, dangerous intersections, or locations with hazardous weather. The VANET construction can be seen in Fig. 1 below.

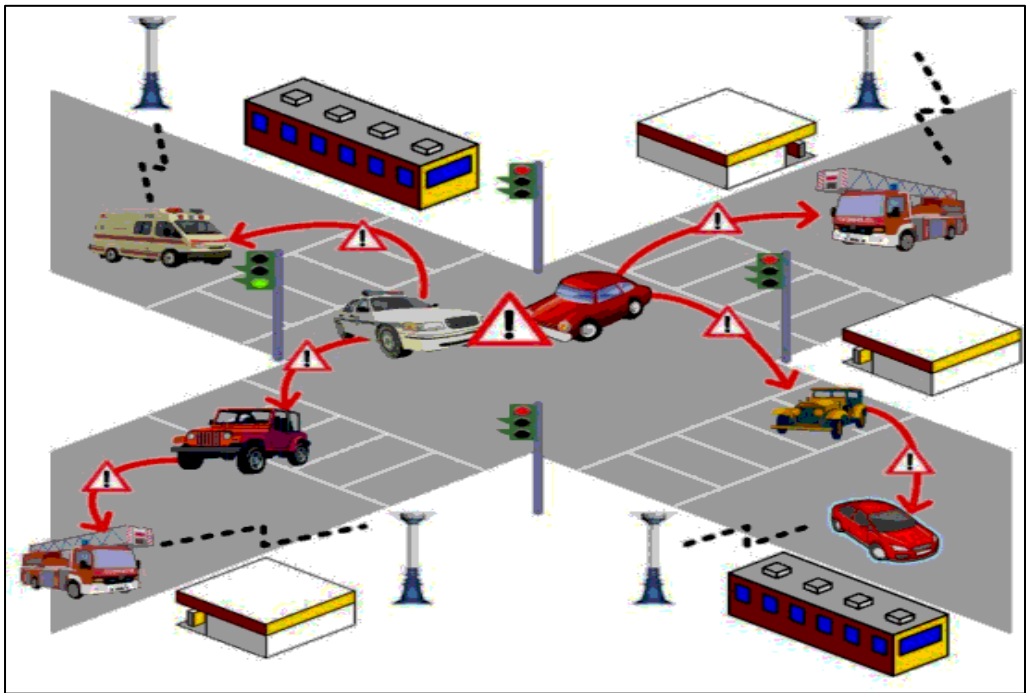

Fig 1: Structure of Vehicular Ad-hoc Network [1]

The majority of cars today come with GPS and sophisticated navigation systems. More businesses are creating technology geared toward electric vehicles. They are developing a battery-powered driving mechanism for the car. As technology advances, this pattern will persist in the future. VSN has the potential to alter both the system and the technology of transportation because of its virtually endless power supply. On the other hand, before it can be implemented, VSN must solve various challenges related to its architecture, implementation, network scalability, efficiency, and deployment over large-scale networks.

1.1 Characteristics of VANET

The use of VANET offers a number of beneficial uses for safety-related or unrelated purposes, such as automatic road safety alerts and file sharing with another vehicle. Through a network, a roadside infrastructure development facility, or vehicle to vehicle communication, they can connect with one another [3]. The network reconfiguration system is shown in fig 2 below, in which S is the source, D is the destination and Ij is intersection points.

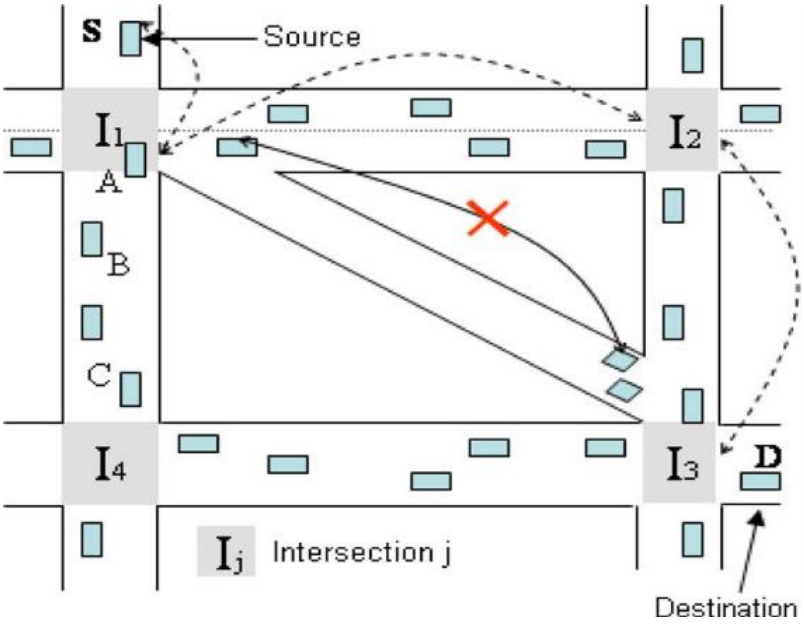

Fig 2: Network Communication in VANET [2]

The following [2] is a list of the primary advantages:

- By using technology and the Internet of Things, water waste can be reduced.
- Monitoring the land and taking the appropriate safety measures
- May promote greater productivity
- It makes use of technology to lessen the need for labour
- Soil management-related parameters can be tracked
- aids in agricultural disease control identification

Additionally, it improves the system's efficiency and cost. It includes some significant elements, including:

- Sensing Devices
- Technology for Communication
- Internet
- Processing & Storage Devices

2. ROLE OF SENSOR NODES IN VANET

The Internet plays a significant part in modern life and is becoming more and more popular as a result of technological improvement. The Internet has a complex network with several layers. These layers are employed in the transmission and receipt of data. The Internet offers a very quick means of information sharing between corresponding networks. The vast majority of the vehicles in VANET are referred to as "nodes." Each has a sensing gadget that allows them to communicate more quickly. The biggest issue with this network is the route instability, which has an impact on system overhead. Sensing nodes' primary responsibilities include surveying the immediate area and communicating with other adjacent devices. Due to connection unreliability, data forwarding presents the biggest obstacle in this situation. All vehicles are moving more quickly, and connection problems are frequent.

2.1 Attacks in VANET

- In VANET, the congestion problem is of greater importance than in other networks because higher delays might occur. The car has only one feature in the system and exhibits malevolent conduct in the network. The network system's attitude toward technology makes it susceptible to a variety of dangers. The system's many attacks are outlined below [3]:
- An attack known as an alternation attack involves changing certain information using any systemic method. This information can cause system malfunction and lower system performance.
- A fabrication attack is brought on by this type of flaw, which the attacker exploits to send fake data into a sensor system to detect the entrance. The information could not be accurate, and there is a good chance that the transmitter is not who the framework thinks he or she is.
- In a malware attack, someone enters another system without authorization. Corrupted files have the potential to harm the system. It is a highly frequent form of system attack.
- In a masquerading attack, the attacker who actually becomes interested in the sensor network makes use of this flaw. The attacker makes an effort to gain in by pretending to be another vehicle node and using a false identity. This could be done and used for concealment through message generation, replay faults, or adjustment faults.
- In a wormhole attack, two or more nodes are involved in the transmission of harmful data. Data broadcasting via a network can be useful.
- In a Sybil attack, a single node is used to represent numerous identities that can all be affected at once. Its main objective is to gain network dominance for some illicit activity, and it has the potential to unleash malicious activity.

3. LITERATURE REVIEW

Chen *et al.* provided a modern feature that will improve the current technology in automobiles while remaining low-cost. They formerly settled on a technology recognized as the Smart Crash Prediction System (SAPS), which decreases the number of car crashes while also improving passenger safety. The present research is advancing this approach by combining Google Assistant with SAPS. A planned system combines many embedded devices in automobiles to track different factors like distance, speed, and safety features such as seatbelts, airbags, door locks, and handbrakes, among others. Real-time data is saved in the cloud, or the car will respond to distinct scenarios based on previous data [1].

Chinnaswamy *et al.* presented that an architecture built on an SDN (software-defined network) solution to advance QoS (quality of service) in dynamic IOV networks, which is vital when vehicles are reporting car crashes to one another, was developed. Reenactment in LED on the Ns-2 stage can demonstrate that the proposed model increases security while communicating and encourages sensor nodes to coordinate in the remote system. This will also cause the malignant nodes to be isolated from the dynamic information sending and directing [2].

Shamshirband *et al.* presented that a real-time vehicle system with IOT capabilities will predict collisions and respond to changing circumstances. Furthermore, the car is more secure than ever before thanks to RFID keyless entry authentication. It investigated the protection issues and factors that are basic to be considered for safeguarding security in SIoV conditions from alternate points of view, including the protection of an individual, conduct and activity, correspondence, information and picture, contemplations and emotions, area and space, and affiliation [3].

Deka *et al.* presented that the "Social Internet of Vehicles" (SIoV) is one use of SIoT in the vehicular area that has developed the current "Wise Vehicle Framework" (ITS). Further, the paper talks about the square chain-based answers for saving security for SIoV. Another examination objective was the impact of alteration factor usage on anticipated danger factors to diminish the street vehicle-train crash hazard at the intersections [4].

Goni and Lawal proposed a car accident monitoring algorithm that used the ADXL345 accelerometer and acceleration device to detect a collision and a heart rate device to track the passenger's health and send an emergency SMS or voice call to family. The purpose of their paper is to implement an IOT-based system that aids in the detection and notification of car accidents [5].

Sanyal *et al.* presented a fog computing-based solution for developing a low-priced mobile device to minimize the time it takes to record a road accident. To identify an injury, the device uses an Android program that takes data from mobile sensors. Their research presented here takes advantage of advanced smart phone features and fog computing to suggest and improve delay-aware accident detection and response systems and a low-cost ERDMS (Emergency Response and Disaster Management System). For the detection of accidents, an Android application is being built that makes use of mobile sensors [6].

Kumar *et al.* introduced a routing scheme for finding the best possible paths. The routing scheme was centered on community routing standards and a data cluster structure. They introduced how smart cities will track the evolution of vehicle connectivity. This paper also discussed how to use a multi-mediator scheme to reduce the shortcomings associated with IOT rollout and application in a smart city setting [7].

Balan et al. presented an IOT-based car crash detection system that used an ADXL345 accelerometer to track collisions and GPS to identify and relay accident locations to a nearby ambulance via the internet. They also discuss the possibility of equipping a vehicle with technology that can identify and alert emergency responders in the event of an accident. When a car accident occurs, someone must immediately seek assistance, such as by dialing 911 for emergency services [8].

Khan & Jain have proposed a discovery model that comprises a lot of base-include classifiers that utilize fractional unique element space just as an information mining classifier. The proposed model combines the element selection strategy for location rate advancement with the information mining procedure to reduce the number of false alerts, similar to a collaborative effort of abuse identification and abnormality recognition. According to the exploratory results, the half-and-half model has a better way of dealing with execution while actualizing the recognition definition with both low FPR on typical framework utilizations and high DR on vindictive projects [9].

Chaqfeh and Lakas have proposed a novel framework that can possibly fault the system and wreck it totally. As a result, some safety efforts are embraced in VANET engineering to improve street wellbeing and travel accommodations; these are accomplished by providing self-sorting and decentralized conditions to communicate traffic information. This could be accomplished without requiring a fixed framework. Reproduction results demonstrated the productivity of our telecom approach in accomplishing low communication overhead while keeping up the high information conveyance proportion [10].

3.1 Challenges Faced By VANET

The VANET is experiencing a lot of challenges. These are primarily technical issues with a few business-related ones [11].

1. Technical challenges make it difficult to plan new conventions or modify existing conventions because there hasn't been a unique vehicle convention created for vehicular organizations up to this time. Since a message won't be retransmitted in the event that two

cars are passing one another while travelling in the other direction, these data should typically be error-free [12].
2. There are numerous business-related issues in Business Challenges that have an impact on the functionality of the VANET system. Some antique cars lack the most advanced smart technological equipment and are out-of-date. Therefore, creating smart markets that have smart sensing vehicles on the market is the key difficulty [13].

4. RESEARCH METHODLOGY

In wired networks, the main issue is the loss of data and the large amount of delay in the network. Due to this, wireless networks are preferable to wired networks. For vehicle communication, VANET is very popular and has advanced technological features. It comprises a large number of nodes that can communicate with each other at the same time on the same network. This network is low-cost and provides high bandwidth as compared to other networks. It has a large number of mobile nodes that communicate with one another and are all connected on the same channel. There are various attacks that can affect the performance of a network. One of these attacks is the Sybil attack, which can generate multiple identities at a time and affect the performance of the system. The objective of this work is listed as follows:

- To design network reconfiguration with mobility in VANET.
- To design security mechanism against Sybil attack that preserves the security and privacy of VANETs.

This work presents the concept of network reconfiguration along with the concept of detection and prevention of the Sybil attack in VANET by prediction-based routing. It uses the Grey Wolf Optimization (GWO) for enhancing the performance of the system. The GWO is a type of particle intelligence algorithm for achieving proper exploration. In existing work, a merged technique to prevent Sybil attacks in VANETs is presented. In existing work, a security phase mechanism was presented as a useful solution for having a Sybil attack in the system. It used the concept of vehicle-to-vehicle communication with Sybil nodes. The existing work provided performance in terms of end-to-end delay and throughput parameters, with a simulation time of 50 ms. In the proposed work, it uses the concept of pre-existing knowledge of all nodes via a training dataset. All nodes that already have a location are added to the database, which is then updated on the fly. In the worst-case scenario, a Sybil attack is a type of false attack that can provide nodes with multiple identities at the same time. These kinds of attacks are easy to pull off in a VANET because the network is open and always changing.

4.1 Sybil Attack

In a peer-to-peer network, a Sybil attack employs a single node to manage numerous active false identities (also known as Sybil identities) concurrently. By controlling the vast majority of the network's influence, this kind of attack seeks to weaken the legitimacy or power of a well-respected system. This effect is made possible by the false identities. Threat actors have the potential to carry out unauthorized actions in the system after a successful Sybil attack. In a severe attack on vehicular ad hoc networks (VANET) [14], known as a "Sybil attack," the attacker maliciously assumes or steals many identities and uses them to disrupt the VANET network's functionality by spreading bogus identities. The communication between moving cars in the VANET network occurs via inter-vehicle communication, while the communication between moving vehicles and RSUs occurs via roadside-to-vehicle communications.

Structure Based Detection Technique

- In a Sybil attack, a false vehicle node creates a false identity to take over the control of the whole VANET and provides false information to harm the vehicle.
- It employs the concept of a roadside unit (RSU) to detect Sybil attacks, with two vehicles passing by multiple RSU at the same time.
- All nodes will be issued different IDs by RSU, and if any vehicle shows the same duplicate ID, then it is treated as a false attack and will be stored in a faulty bag in the database [30].
- The first step in this method is to collect the packet from the vehicle, then calculate the distance between the vehicles and identify and group the Sybil nodes.
- Each node has information about its neighboring node and exchanges information with each other on a continuous basis.
- If these nodes observe the same type of information repeated, then this node acts as a Sybil attack node. This method is fast and helpful for large network databases.

Prediction Based Routing Protocol

- Calculate weight of each vehicle node
- Detect the neighbor node by Structure based method
- calculate distance between nodes by distance formula

  $$\boldsymbol{dist} = \sqrt{(\boldsymbol{Xs} - \boldsymbol{Xd})^2 + (\boldsymbol{Ys} - \boldsymbol{Yd})^2} \quad \text{(i)}$$

where $(\boldsymbol{Xs}, \boldsymbol{Ys})$& $(\boldsymbol{Xd}, \boldsymbol{Yd})$ denotes the sender & receiver location respectively.

- calculate angle of neighbor node and destination node by

  $$\boldsymbol{\theta} = \mathbf{cos}^{-1}\left(\frac{\boldsymbol{v} * \boldsymbol{LsLd}}{\boldsymbol{v} * \boldsymbol{LsLd}}\right) \quad \text{(ii)}$$

  where v is velocity of current node.
  Ls & Ld are the distance length from sender and receiver respectively
- Find the shortest distance between nodes and predict the path
- If path found ok, then proceed
  else choose 2nd shortest path.

In this protocol, it uses vehicle dynamic information and time to predict the information. It observed the dynamic topology and helped to transmit the packet in better way. It observed their location and angle also that helped to track vehicle position and movement

4.2 System Evaluation Metrics

All nodes are mobile in nature in this system. These nodes have initial 100 % energy for utilize their work. The system is analysed on the basis of energy consumption, delay and throughput.

1. End to End Delay

The end to end delay is defined as the time taken by packet to travel from sender to receiver. It is total time taken by data to transmit to reach its destination. It can be measured in msec or seconds.

2. Throughput

It is defined as the rate at which message is communicated from one end to another end. It is measured in msg/sec. It is also rate of successful delivery of message to destination.

5. RESULTS & DISCUSSION

This result shows the performance of system when vehicle node in system are 30 with same area. All nodes are deployed randomly and follow the same routing and detection methods as used previously. These figures show the routing from sender to receiver via shortest path.

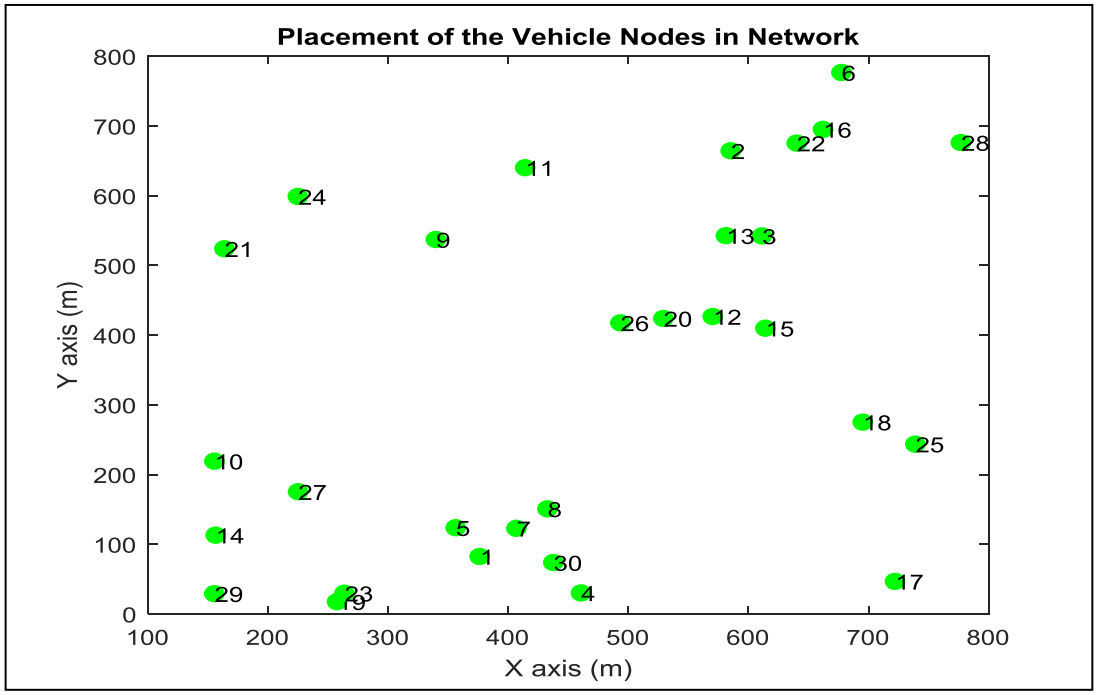

Fig 3: Placement of Vehicles in Network

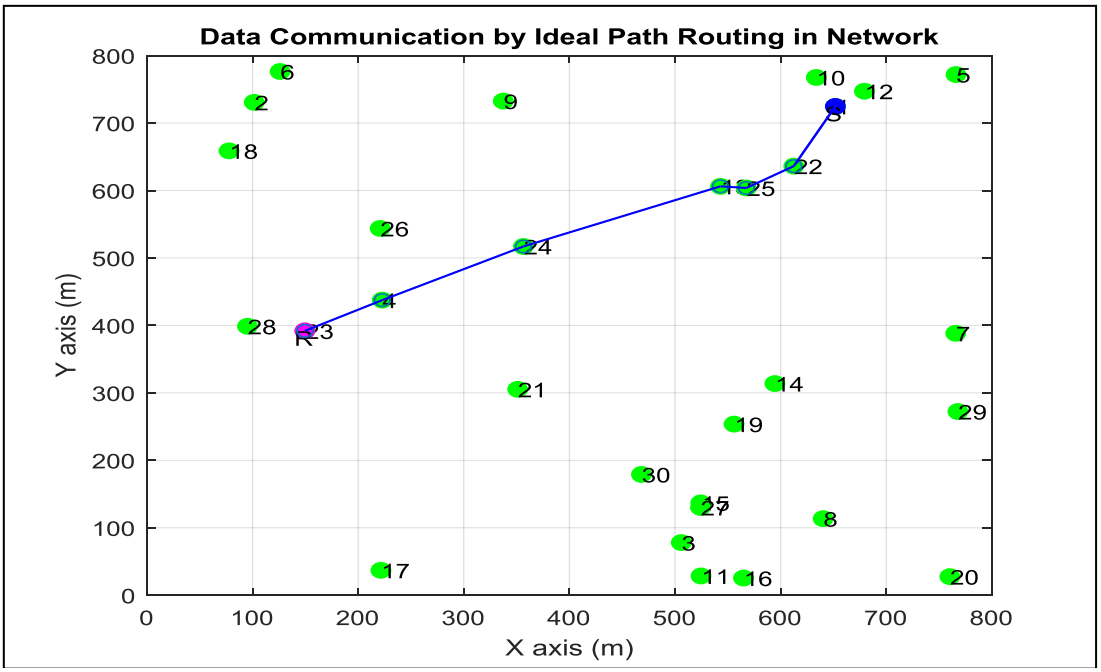

Fig 4: Data Communication by Ideal Path Routing in Network

Fig 3 & 4 shows the performance comparison of system with nodes are 30 only. Throughput is no. of packets transferred successfully in phased manner and end to end delay is the time taken by user to send packets from sender to receiver successfully. This data is shown in

Table 1 and results are better in terms of performance parameters at 50 ms. The proposed results provide 512 packets at 50 ms simulation time.

Table 1: Performance Comparison of System for N=30

Simulation Time	**50 msec**	**75 msec**	**100 msec**	**125 msec**	**150 msec**
Delay (Proposed)	0.12	0.10	0.08	0.05	0.03
Throughput (Proposed)	524	525	526	527	528

6. CONCLUSION

This work provides the concept of mobility based VANET network in which all nodes are dynamically provided. It also provides the concept of detection and prevention of Sybil attack in this network. It also uses the GWO method to optimize the performance of system. The use of Sybil attack decrease the system performance by creating malicious nodes. So, it is necessary to detect and prevent from these types of attacks. The lifetime of node is a metric that can help to measure the life of a node with active performance. The existing work used the concept of two way symmetric key system having Sybil attack in network. It affected the performance of system in terms of end to end delay and throughput. The proposed system worked in drawbacks of existing system to improve their performance metrics. To detect Sybil attack, it uses the concept of road side unit (RSU) that two vehicle are passing by multiple RSU at same time. The proposed work presented the cases by taking different number of nodes with simulation time 50 ms. The work is being evaluated in terms of throughput and end to end delay with different number of nodes and simulation time. The proposed results show better as compared to existing results.

In future, Finding the route lifetime prediction through smart sensing technique and High level security mechanism by controlling attacks.

REFERENCES

[1] Chen, R., Haung, Y., & Hsieh, C. "*Ranger intrusion detection system for Wireless Sensor Networks with Sybil attack based on Ontology",* New Aspects of Applied Informatics, Biomedical Electronics and Informatics and Communications, 2010.

[2] Chinnasamy,A., Prakash,S., &Selvakumari,P. "*Enhance trust based Routing Techniques Against Sinkhole Attack in AODV based VANET*", International Journal of Computer Applications, 65(15), 0975-8887, 2013.

[3] Shamshirband, S., Anuar, N., Kiah, M., Rohani, V., Petković, D., Misra, S., & Khan, A., "*Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks",* Journal of Network and Computer Applications, 42, 102-117, 2014.

[4] Deka, R., Kalita, K., Bhattacharya, D., &Kalita, J., "*Network defense: Approaches, methods and techniques. Journal of Network and Computer Applications*", 57, 71-84, 2015.

[5] Goni, I., & Lawal, A., "*A Propose Neuro-Fuzzy-Genetic Intrusion Detection System*", International Journal of Computer Applications, 115(8), 2015.

[6] Sanyal, S., Das, N., & Sarkar, T., "*Survey on host and network based Intrusion Detection System*". Acta Technica Corviniensis-Bulletin of Engineering, 8(1), 17, 2015.

[7] Kumar S., Thriveni, J., Venugopal, K., Manjunatha, C., & Patnaik, L., "*Reinforcement based Cognitive Algorithms to Detect Malicious Node in Wireless Networks"*, International Journal of Computer Applications, 2015.

[8] Balan, E, Priyan, M., Gokulnath, C., & Devi, G., "*Fuzzy based intrusion detection systems in MANET*", Procedia Computer Science, 50, 109-114, 2015.

[9] Khan, J. A., & Jain, N. "*Improving intrusion detection system based on KNN and KNN-DS with detection of U2R, R2L attack for network probe attack detection*", International Journal of Scientific Research in Science, Engineering and Technology, 2(5), 209-212, 2016.

[10] Chaqfeh, M., & Lakas, A., "*A novel approach for scalable multi-hop data dissemination in vehicular ad hoc networks"*, Ad Hoc Networks, 37, 228-239, 2016.

[11] Rupareliya, J., Vithlani, S., & Gohel, C. "*Securing VANET by preventing attacker node using watchdog and Bayesian network theory*", Procedia computer science, 79, 649-656, 2016.

[12] Chaudhary, A., Tiwari, V., & Kumar, A. , "*A New Intrusion Detection System Based On Soft Computing Techniques Using Neuro-Fuzzy Classifier For Packet Dropping Attack In Manets*", International Journal of Network Security, 18, 514-522, 2016.

[13] Prathima, E., Venugopal, K., Iyengar, S., & Patnaik, L., "*SDACQ: Secure Data Aggregation for Coexisting Queries in Wireless Sensor Networks"*, International Journal of Computer Science and Network Security (IJCSNS), 17(4), 205, 2017.

[14] Hasrouny A., Hamssa A., "*VANET Security Challenges And Solutions: A Survey*." Vehicular Communications, 7-20, 2017.

[15] Tyagi, P., & Dembla, D., "*Performance Analysis And Implementation Of Proposed Mechanism For Detection And Prevention of Security Attacks In Routing Protocols of Vehicular Ad-Hoc Network (VANET)"*, Egyptian informatics journal, 18(2), 133-139, 2017.

[16] Safi, Q., Luo, S., Wei, C., Pan, L., & Chen, Q. "*PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs"*, Computer Networks, 124, 33-45, 2017.

[17] Pandey, P., Jain, M., & Pachouri, R., "*DDos Attack On Wireless Sensor Network: A Review*", International Journal of Advanced Research in Computer Science, 8(9), 2017.

[18] Azim, M., Salah, H., & Ibrahim, M., "*Black Hole attack Detection using fuzzy based IDS*", International Journal of Communication Networks and Information Security, 9(2), 187, 2017.

[19] Poonia, D., & Sharma, M., "*Detection and Prevention of Denial of Services Attack based on Signal Strength and Reputation Mechanism*", International Journal of Communication Networks and Information Security, 202-207, 2017.

[20] Qahatani, M., & Mostafa G., "*Trust modeling in wireless sensor networks: state of the art*", International Conference on Automation, Computational and Technology Management, pp. 191-197, 2018.