Secure Routing Protocol for VANET using Hashing with Session Key

Muqtadir
Research Scholar Rayalaseema University
PP. COMP SCI & ENGG. 0384
Kurnool,Andhra Pradesh,India
mabdulmuqtadir@gmail.com
.
.
Dr. Syed Abdul Sattar
Director R & D,
Nawab Shah Alam Khan College of Engg. & Tech. (NSAKCET),
Hyderabad
. Telangana, India

Abstract:- Vehicular ad hoc network is the novel technology of wireless communication based on wireless ad-hoc network. Communication among the vehicles play an important role to provide safe and covenant journey to drivers and passengers. Creating communication path between vehicles is an active research and challenging area in VANET. In literature reactive prediction based routing protocol have been developed to cope with dynamic position of vehicles and frequently changed network topology. However, these networks routing protocols are vulnerable towards malicious attacks, which transmit false control messages lead to cause the accident and disturb the performance of system. In this paper we develop a secure reactive prediction based routing protocol by message digest and password based session key. Performance results are shows that proposed routing protocol create the routing path by mitigating misbehaving node and improve the packet delivery and throughput by reducing the packet loss.

1. Introduction

Vehicular Ad-Hoc Network [1] is developed to provide communication between vehicles based on mobile ad hoc network technology. This network used to develop towards the emerging application such as intelligent transport system. Here, vehicles communicate with another vehicle regarding status of traffic flow and road side navigation to overcome the existence of unsafe situation. This system is used to enhance the traffic management, provide on board information and free parking places, multimedia sharing.

Mobile hoc network is a network that composed of mobile devises animatedly varying network topology without central coordinator and infrastructure. One special type of MANET with mobile vehicles is known as Vehicular ad-hoc network. This network is one of the evolving technology composed of set of vehicles furnished with communication devices known as on board unit (OBU), and number of static units at road side known as road side unit (RSU). The VANET network architecture is shown in figure1. Sometime during communication, vehicles uses the RSU as gateway between them to enable communication. Every vehicle's OUB has network interface creates the wireless communication medium and create the connection with another vehicles and RSU in its communication range and also it can connect with wired or wireless interfaces to which application units could be fixed.

By enabling communication between vehicles or between vehicles to road side unit, VANET can substance widespread of applications in traffic monitoring, reducing accidents passenger infotainment, and vehicle traffic optimization, that's why VANET receive the attraction towards the academia, industrial and government sectors.

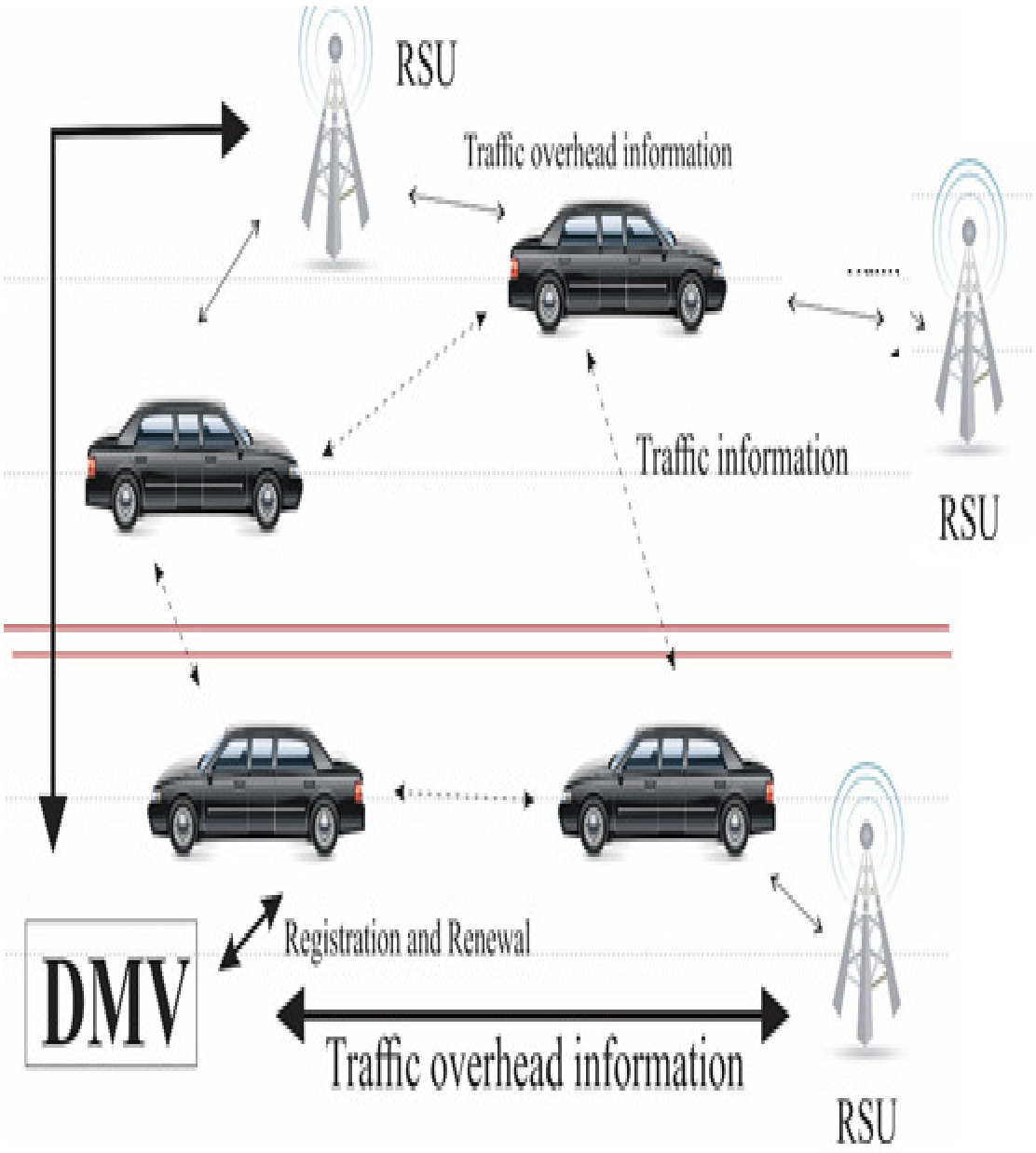

Figure1:- VANET architecture

Vehicle ad hoc network has characteristics such as not a stable infrastructure for communication. It must be establish the communication in an ad hoc basis, and may not uses the central coordinator. Topology of network unpredictably changes due to mobility of vehicles. Communication session time is also very less, while memory and battery is not an issue. Potential data Communication in VANET is impossible, as this network environment communication entities are facing building obstacles for communication.

Routing is the method for finding the optimal route between communication entities, and forwarding the information through the elected route in a particular time interval. Elected route may contain number of hops between communication entities. However finding and managing optimistic path between communicating entities is challenging in VANET due to its characteristics such as high mobility and dynamic network topology [2]. In literature number of position based routing protocols have been designed, such as General Packet Radio Service, Greedy Perimeter Coordinator Routing, geographical opportunistic source routing and Greedy Routing. Secure routing is one of the challenging task in VANET, as active and passive attacks are making considerable damage to the performance of network.

These attacks cause the routing control packets alteration and data packets dropping and also provide the way for malicious nodes (drivers) to enter into the network easily, who can disturb the network protocol specifications and degrades the network performance. Thus, in this work we design a secure reactive-prediction based routing protocol by message digest and password based session key, which find the secure path between communication entities by following contributions.

1. End to end password based key agreement
2. Creating the message digest of control packets with hashing by source
3. Compute the routing path by prediction based method [3].
4. Verify the message digest of control packets at destination node.

The rest of the work is ordered as follows: next section designates the related work of the paper and followed by existing prediction based algorithm, section 3 explain the proposed work and performance analysis explained in section 4. Our work ends with conclusion

2. Background

In general, VANET needs an optimistic routing path establishment between communication entities, due to its high mobility and dynamic network topology. Basically routing in VANET is divided into two types i.e., topology based and position based. These routing protocols design principles must consider the dynamic network topology and high mobility of vehicles and entrance of new vehicles as well as exit of existing vehicles.

The main aim behind the VANET technology design is to provide the safety to vehicles and passengers by relaying on information communication between vehicles. In order to provide reliable communication between communication entities is achieved through secure routing protocols of network layer, as malicious attackers or misbehaving nodes used to transmit the false information through the routing path. In this network false information is directly impact to vehicle accidents and business losses. To overcome the issue, in literature various routing protocols have been designed to provide reliable communication between vehicles. One of the category of security based routing protocols is trust-based secure routing protocols.

. Trust based routing protocol aim is to establish secure routing path between communication entities based on trust computation of nodes or links or network. These protocols must compute the trust based on real time monitoring to get trust related information and also act as a safeguard to protect the network environment from false information propagation, so as to enhance the network performance and reduce the damage to the vehicles or business. Let consider, if the vehicle (node) receives the false information regarding road or traffic then it increases the traffic jams and leads to traffic jam. Trust based routing protocols must consider the following considerations to compute the trust value

- High mobility of vehicles
- Mobility of vehicles are random
- Less delay for communication, so that the position information of vehicle is informed either other vehicle or road side unit very quickly
- Traffic condition of road is not static
- Time and location information of vehicles are accurate

In literature number of trust based routing protocols are designed [2] to establish confidential communication to prevent the accidents. The first important issues in trust based routing protocols are facing due to nodes high mobility. The most important thing is how to faith the getting information, as neighboring node is quickly varying its position, as nodes computed trust is based on the received information of its neighbor. These protocols causes the problem of oversampling [4], Oversampling is a condition where the node detecting two or more nodes, with their equal opinions by not knowing their influences of one another. Thus there is a requirement of routing protocol which must be overcome the problem of oversampling.

2.1 Prediction Based Routing Protocol [3]

This protocol is an extension of existing MANET reactive routing protocol such as AODV. This protocol improved the AODV routing mechanism with two factor optimization in route finding mechanism to support it in vehicular ad hoc network. These two factors are high mobility of the vehicle and direction of the vehicles. Initially protocol allows the stable vehicles to participate in route finding process i.e., forwarding the route request packets, as these vehicles have stable links with other vehicles. Later it computes the most stable routes for packet communication by two factor optimization. Thus this method creates the stable route with less overhead.

In order to make two factor optimization to achieve stable route with less overhead, it includes the mobility and direction vehicle. The mobility and direction of vehicle is obtained through GPS. If the vehicles are in large speed in different directions, then their communication link is easy to break and it valid for least time interval. Vehicles only communicate with one another only when they present in the communication range of each other. Thus vehicles with comparatively same velocity can stay in radio range for extended duration and their link also be live for long time and we can say that it is stable. At the same time vehicles moving in different direction will move from communication range of one another. Thus this protocol is created the route based on the direction and speed of the vehicles. Thus this protocol creates the route based on the prediction of the route lifetime i.e. stable or not.

3 Proposed Work

Proposed work consist of two phases. First phase is password based authenticated key agreement between communication entities based on chaotic maps, which is explained in our existing work [5]. We are assuming that each node present in a network have the session key with chaotic maps based Deffi-Hellman problem [6]. Then we design a message digest with session key method used to secure the prediction based routing protocol during the route finding process. Message digest value is computed with the help of MD5 [7] or appropriate hash algorithm with agreed session key. The algorithm is explained as follows.

1 Route request packet of prediction based algorithm's route request field is added with an extra field and this field is included with an extra field for digest value.

Route request packet of Prediction based algorithm's fields

2 Source node computes the hash value of the route request packet by appropriate hash algorithm

$$Digest\ value = Hash\ Function\ (Route\ Request\ packet)$$

3 Then the source node adds the digested value to route request packet

Route request packet of Prediction based algorithm's fields
Digest

4 Then the source broadcast the RREQ packet until it reach the destination, reaming route creating process is followed by prediction based protocol specification.

5 Whenever RREQ packet received by the destination or an intermediate node then it verify the digest value by using its session key as follow. First it removes the digest value and adds its session key to RREQ packet and compute the digest value and compare it with received digest value, if both are match then the packet during the communication did not alter.

"Digest value of received packet $Is\ compared\ with$ Digest value computed by destination"|

6 Then destination create the route replay packet. And computed its message digest value and included it in RREP packet and unicast this packet to source node along with computed path

Route replay packet of Prediction based algorithm's fields
Digest

7 Source need to validate the RREP packet, with its session key by the following the step 5.

Proposed routing protocol route calculation process is followed by existing prediction based routing protocol with the message digest extension. Flow of protocol is shown in figure 2.

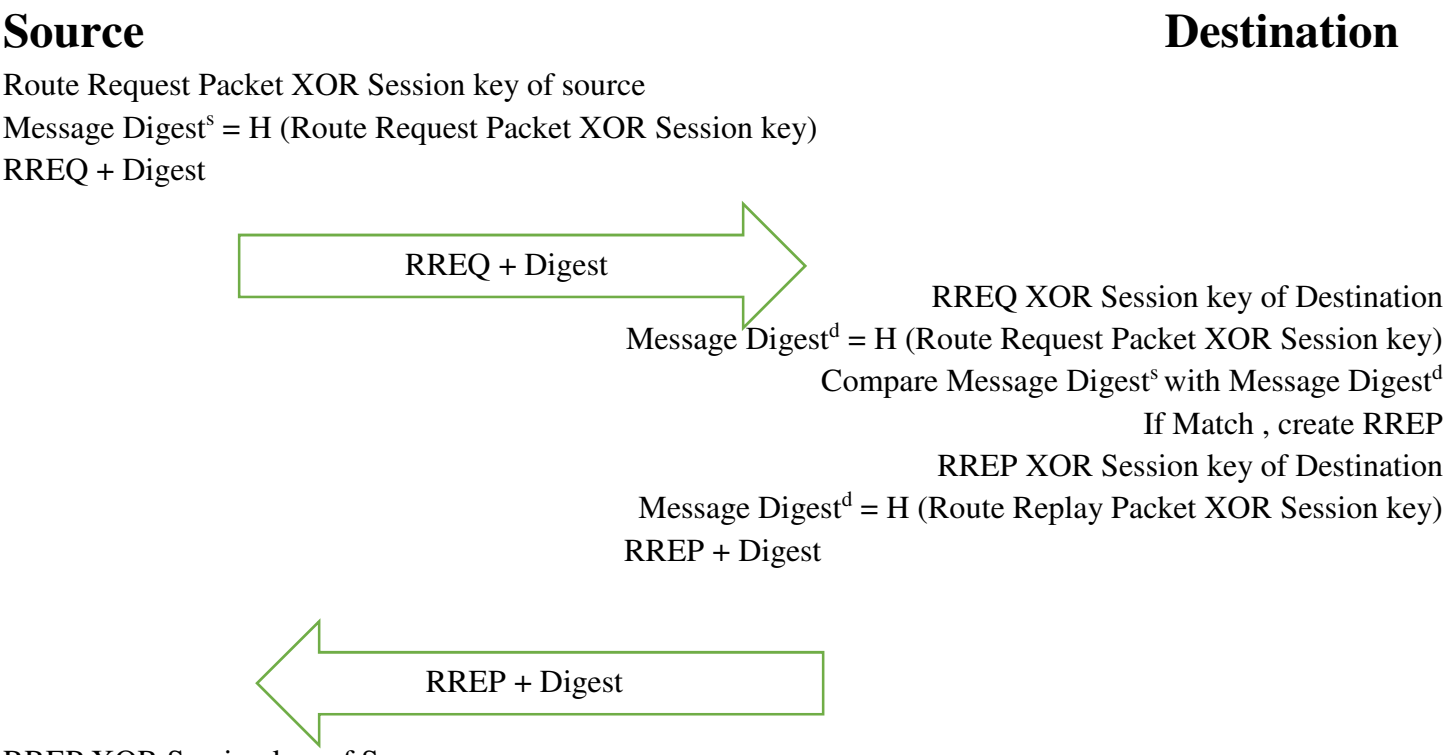

Figure 2 :- Proposed protocol steps for computing secure routing path with hashing

3. Performance Analysis

Performance of proposed work is carried out by network simulator NS 2.35 [9] and compare its performance with existing routing protocol in the identical environment. The main objective of the performance evaluation of proposed work is to find the effect of misbehaving nodes in the network performance. In our simulation we consider the variable nodes (Vehicles) moves based on random mobility model concept in random direction. Nodes are equipped with sufficient energy and buffer for communication and connected by 801.11 Medium access Card with identical data rate of 2 Mbps. We also consider there is an attacker node [8] who is capable of altering routing protocol control packets so as to attract the traffic towards it during route selection process, and drops the packets in data forwarding phase.

We also consider that the there is a authenticated key agreement algorithm which is responsible for providing session key between communication entities through chaotic maps Diffie Hellman key method. In order to measure the performance, we considered the following performance metrics. Simulation parameters are shown in table1.

Throughput:- it is a network performance metric to calculate how much data packets transmitted from source to destination in a particular time interval.
Packet Delivery Fraction:- It is the ratio of amount of data packets received by destination to amount of data packets transmitted by source multiplied by hundred.

Table 1:- Simulation parameters for Performance calculation

Network parameters	*Values*
Simulation duration	1,200 s
Number of nodes	10 to 100 nodes
Link layer	Logical link
MAC	802.11
Mobility	Random waypoint (60 mph - 40 mph)
Network layer	PBR-AODV,proposed
Communication	Two-ray ground
Queuing	Drop-tail priority
Battery	Sufficient
Traffic	Constant bit rate
Road highway length	2200 m

Packet delivery fraction of performance calculation is shown ion figure 3. It is clearly indicate that performance of proposed work overcome the misbehaving node from routing path. Where in existing protocol did not have the procedure to overcome the problem of misbehaving node mitigation. Similarly performance of throughput is shown ion figure4.

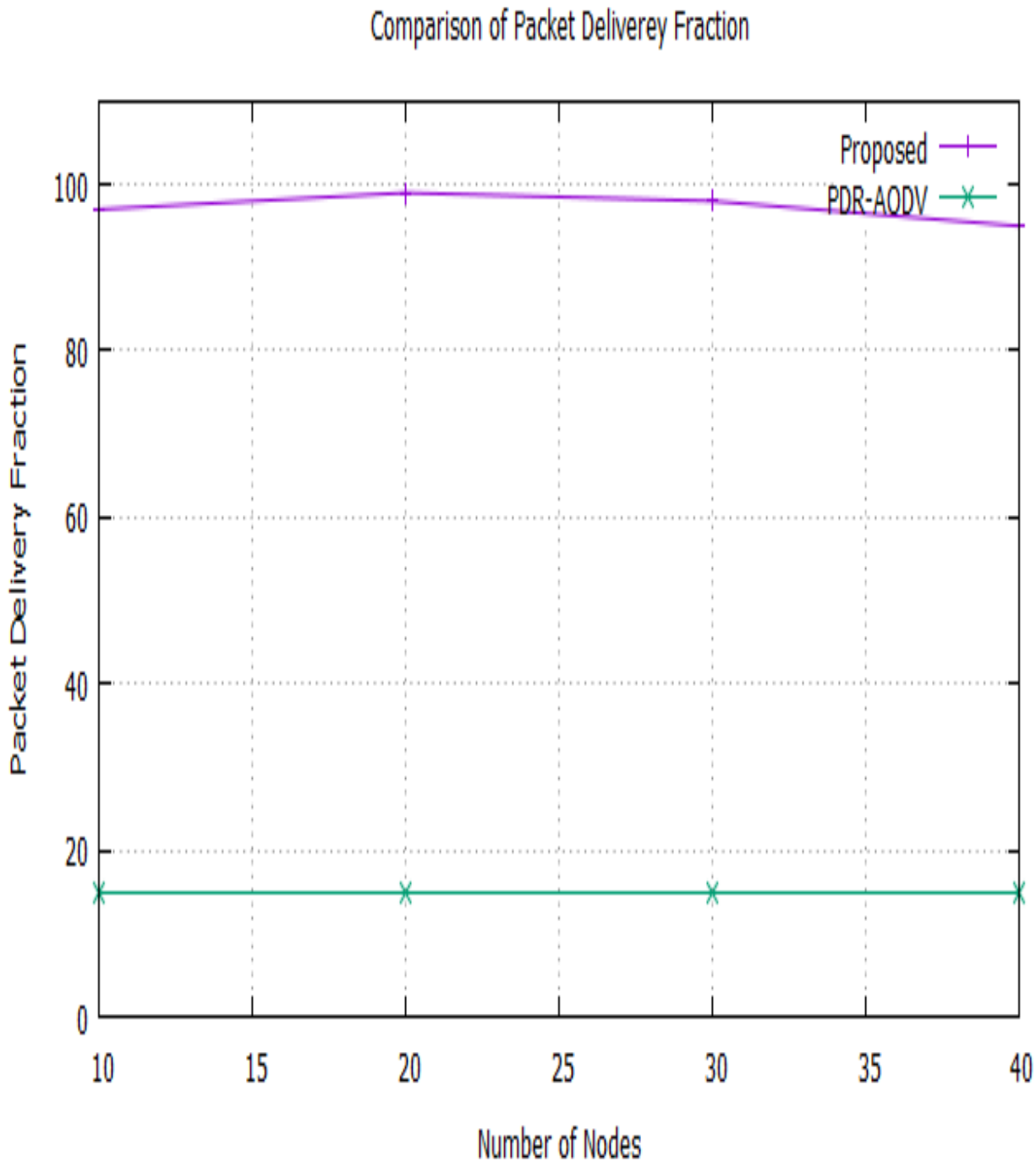

Figure 3 ;- Performce comparison of packet delivery fraction

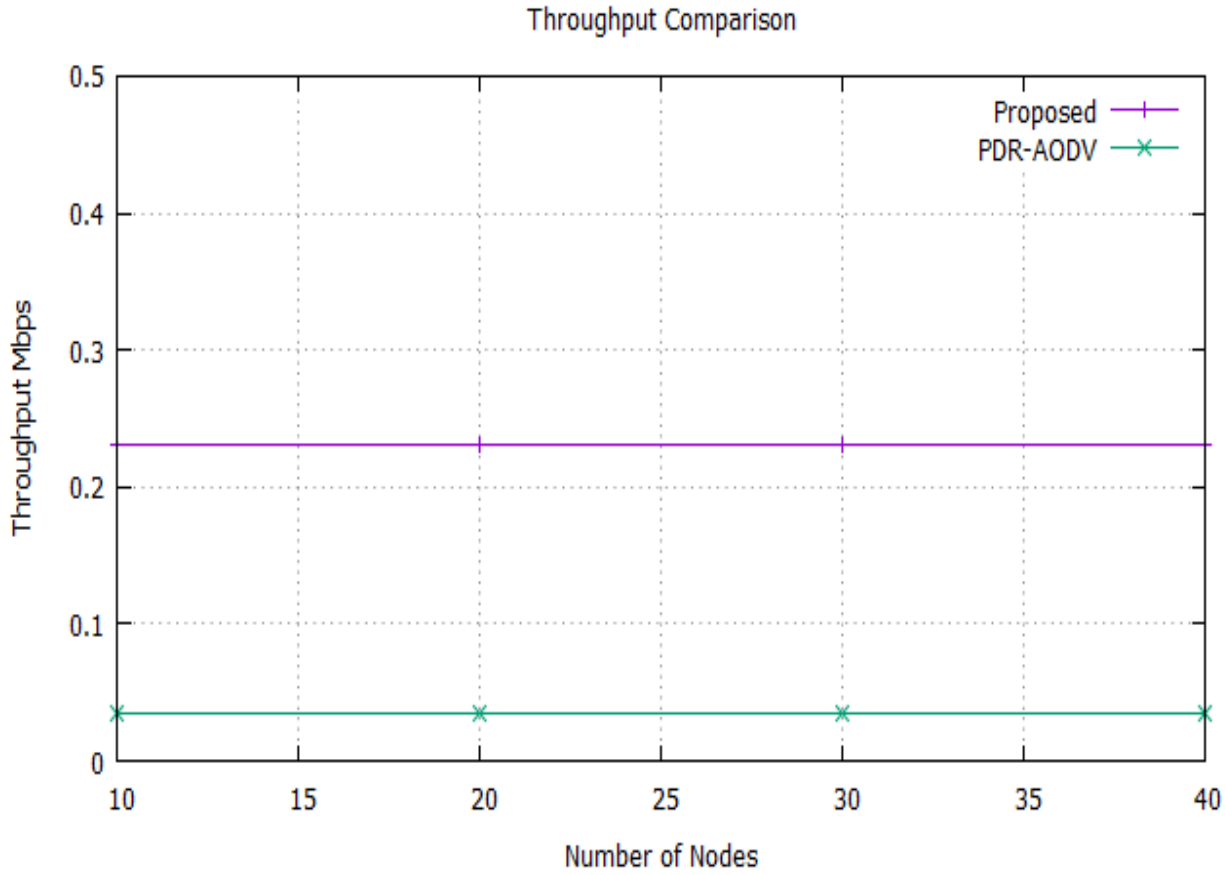

Figure 4 :- Throughput Performance comparison

4. Conclusion

VANET is the novel technology of wireless communication based on MANET. Communication between vehicles play an important role to provide safe and covenant journey to drivers and passengers. Creating communication path between vehicles is an active research and challenging area in VANET. In literature reactive prediction based routing protocol have been developed to cope with dynamic position of vehicles and frequently changed network topology. However, these networks routing protocols are vulnerable towards malicious attacks, which transmit false control messages lead to cause the accident and disturb the performance of system. This work design a secure reactive prediction based routing protocol by message digest and password based session key. Performance results are shows that proposed routing protocol mitigate the misbehaving node from routing path there by improve the packet delivery and throughput.

References

1. Al-Sultan, Saif, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. "A comprehensive survey on vehicular ad hoc network." *Journal of network and computer applications* 37 (2014): 380-392.
2. Li, Fan, and Yu Wang. "Routing in vehicular ad hoc networks: A survey." *IEEE Vehicular technology magazine* 2, no. 2 (2007).

3. Ding, Ben, Zehua Chen, Yan Wang, and Hui Yu. "An improved AODV routing protocol for VANETs." In *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*, pp. 1-5. IEEE, 2011.
4. Huang, Zhen, Sushmita Ruj, Marcos Cavenaghi, and Amiya Nayak. "Limitations of trust management schemes in VANET and countermeasures." In *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, pp. 1228-1232. IEEE, 2011
5. Muqtadir, syed abdul sattar "Network security based on chaotic maps authentication in VANET" JOURNAL OF APPLIED SCIENCE AND COMPUTATIONS , Page No:280-292, volum5 issue 12 December 2018.
6. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. *Indian Journal of Science and Technology*, *9*(26).
7. Lakhtaria, Kamaljit, Bhaskar N. Patel, Satish G. Prajapati, and N. N. Jani. "Securing AODV for MANETs using message digest with secret Key." *arXiv preprint arXiv:1004.0777* (2010).
8. Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on*, pp. 421-425. IEEE, 2015.-
9. Issariyakul, T. and Hossain, E., 2012. Introduction to Network Simulator 2 (NS2). In *Introduction to Network Simulator NS2* (pp. 21-40). Springer, Boston, MA.
10. Eastlake 3rd, D., and Paul Jones. *US secure hash algorithm 1 (SHA1)*. No. RFC 3174. 2001.