Find Secure Location using AODV trust calculation in VANET

Kumud Dixit[1] Krishna K Joshi[2]
[2]Assistant Professor
[1,2]Department of CSE/IT
[1,2] MPCT Gwalior, India

Abstract— Vehicular Ad-hoc Network (VANET) is an emergent technology and is popular research area. VANET is basically a network with each other, by devices here referring as "vehicles". The communication among these vehicles is very fast thus forms ad-hoc network, VANET is highly dynamic in nature, attacks are easily deployed in it. Vehicles communication is based on Trust. Trust between vehicles is very essential in such scenarios, vehicle while communicating depend on trust created by other vehicles. If they do not trust on each other than the path for communication is not proper. Trusted Location Selection in Vehicular ad-hoc Network have problem that if number of malicious node increase in network so all vehicle follow wrong route or there is no method to identify this problem by existing work. Overcome with existing work we propose a "Find secure location using AODV trust calculation in VANET" in this thesis we create three scenario and for these scenario we calculate trust for each vehicles trust calculation is done either direct or indirect method and in case of when direct or indirect trust not working trust calculated by trusted authority.

Key words: AODV, VANET

I. INTRODUCTION

In recent years, along with the development of wireless ad-hoc network and wireless sensor technology, Vehicular ad hoc network (VANET) has now become one of the promising and attractive fields of research. With a sharp increase in the number of vehicles safe driving and to reach at destination on time has now become more challenging task to do. Roads are very saturated; reasonable speed and safety distance are hardly maintained by drivers. For solving this problem it is possible to provide traffic information timely to the vehicles so that they can utilize this information to analyze vehicular network. This can be achieved by sharing information of vehicular network among vehicles. Since all the vehicles are mobile in nature, a mobile network is needed which is self-organized, self-manageable and capable of operating without fixed infrastructure support.

VANET is a hybrid technology of wireless ad hoc networks more precisely a network that can be formed by establishing communication among vehicles with the aim to improve driving security and traffic management. VANET is a very promising approach and application of mobile ad hoc network allows vehicles to communicate with nearby vehicles and nearby roadside units but different with other networks due to its some unique features. This is achieved with embedding sensors on vehicle. Road side units (RSUs) work as cellular base to distribute information with vehicles but can-not be treated as central access points. There are some of the basic features of VANET like self-organization, self-management, dynamic nature, low bandwidth, shared radio transmission criteria etc. Apart from these features such as no restriction of network size, real time critical, predicted mobility patterns and highly dynamic topology make a VANET environment more challenging for designing efficient routing protocols.

Wireless Access for Vehicular Environment (WAVE) is a novel type of wireless access particularly devoted to V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) communications. Vehicles and infrastructure (roadside unit and trusted authority) are major components of VANET and when these components are equipped with WAVE communication devices it forms a highly dynamic, self-organizing ad hoc network. These protocols are used for information sharing like sensitive messages regarding accidents prevention ,trusted route selection ,entertainment services, real time traffic updates etc.

II. SCENARIO DEFINITION

A figure is presented below depicts a general scenario of VANET. In this figure, we have shown number of vehicles are communicating with near-by vehicles and Road side authorities to form a VANET. Now these vehicles exchange information about events such as an occurrence of an accident, obstacle, traffic jam or weather related conditions during travelling with the help of sensors equipped with it. A second major component of VANET is a fixed infrastructure bodies having specific processing capacity and Internet service connection which used to act as cellular base for distributing data with the vehicles in their way. There are basically two types of infrastructure over the road which takes part in communication shown. First one is a RSU, which is situated over the road in a particular interval and used to communicate near-by vehicles, other RSUs and with the BS (base station). Second one is a base station which is usually connected to the Internet through internet technology. There are basically two types of communication in VANET as shown in figure as first one is V2V (vehicle to vehicle) communication in which vehicles used to exchange information over the shared wireless channel and second one V2R (Vehicle to Road side unit) communication in which vehicles used to communicate with RSU to exchange important messages. In this way all the entities are working well in this network, but like other networks we can-not imagine VANET without maliciousness. These malicious nodes are used to attract the whole network towards itself by spreading bogus or fake information, dropping valid packets or flooding the network with dummy-nodes, for instance [8].

The prime motto of this research [8] is to find and separate such malicious entities by means of a reliable trust and reputation computation mechanism. This research model will provide a trust based routing of an information and enable users to differentiate whether the information received from another (maybe previously unknown) vehicle is reliable or not.

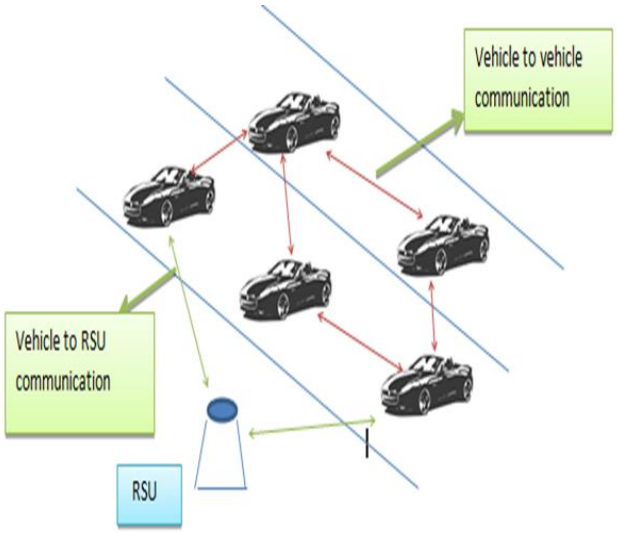

Fig 1: Vehicular Ad-Hoc Network

III. Problem Definition

In VANET, vehicles communicate with each other in hop by hop fashion through wireless channel so this life critical and sensitive information is broadcasted by vehicles to other vehicles to make real time decisions accordingly. But we cannot imagine any network without the presence of malicious vehicle in the network. This may trap a vehicle taking wrong decision with dire consequences. Moreover, an attacker vehicle can inject fake information with different identities. An attacker vehicles can also refuse to take part in communication or simply drop out all the packet information without forwarding further to the other node or destination as shown in fig 3. In the figure below there is a black-hole attack in VANET where, for an example node A wants to send data packets to node C but does not know the route to C. Therefore, A initiates the route discovery process. As a malicious node, B claims that it has active route to C and pretends that it must be next-node if A wants to send packets to C.in this way B drops out whole packet and refuses to take part in communication. Black-hole attack usually occurred in V2V (vehicle to vehicle) communication [11].

So there is a need that messages and vehicles be trusted, especially during V2V communication. The trust management system should accurate and transparent, scalable, resilient to security but should not be very complex. By having all these properties, the trust evaluation should be possible in limited real time [8].

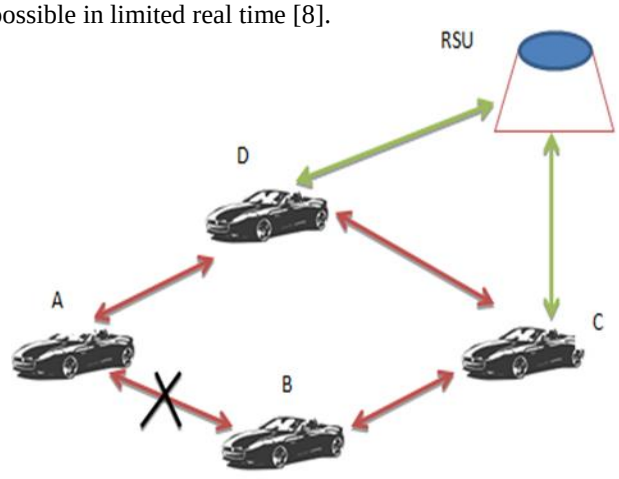

Fig2: Blackhole Attack in Vanet

The trust establishment process in a VANET must take into consideration the direct messages, indirect and forwarded messages from vehicles to other vehicles, its own observation of the whole network, and recommendations of other vehicles about a vehicle, messages and the nature of messages. All these must be used in the trust establishment of a vehicle and the associated messages before forwarding messages sent to it. This necessitates a method that will take all the parameters into consideration and also able to generate trust values in the absence of a majority of the parameters especially in indirect communication or lack of direct trust in critical time. It should be expected to easily detect a malicious behavior and delist that vehicle from communication range and not communicate to that vehicle in future.

IV. Trust Establishment Issues of VANET

In VANET environment, vehicles used to move with very high speed and also change their topologies dynamically around dense area or urban area. So as per the traffic environment, density of vehicles and different types of road, speed of vehicles is varied. It becomes very difficult to react on location in this real time network for vehicles with high speed. VANET is decentralized, real time and open system environment so, at any time any vehicle can integrate and leave the network. But there is not any effective technique to communicate next time with a specific vehicle within network. If any fake message is distributed in real time can result in dire consequences and decrease the performance of network. So, it is important to establish trust of messages and vehicles. Usually, on highways vehicles have high mobility i.e. 60-100 km/hr. as it requires high transmission power from vehicle to vehicle. All the information regarding positions and time should be very accurate. So it requires a long term relationship between peer to peer. Vehicle's position and information is sent to RSU and other neighbours for establishing trust values of vehicles and messages.

Trust is a set of relations based on previous interactions made by all entities in the network. It creates safe and secure driving environment in VANET with the prime aim to calculate trust value at their neighbouring nodes for securely disseminating information to the destination. Decentralization, accurate, scalable, resilient to security threats and independent mobility patterns are some of the design requirements which should be considered while making trust model in VANET. There is a classification of Trust establishment approaches is given below in figure.

A. Infrastructure models

Certified Central Authority (CA) provides certificates to all other nodes/vehicles that provide authentication to particular peers/vehicles. The presence of RSU is necessary in infrastructure models for communication [10].

B. Self-Organizing models

Self-Organization models are classified in three sub categories: Direct trust model, indirect trust model, Hybrid trust model [10].

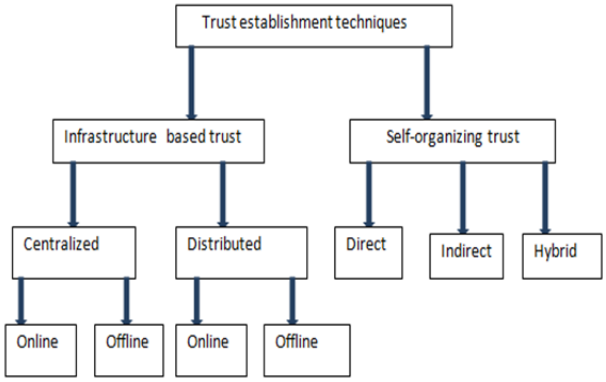

Fig.2: Trust establishment models

V. LITERATURE SURVEY

In VANET, trust establishment to exchange safety, non-safety and control messages among all entities of VANET is very hard to implement and manage in real time. A malicious vehicle has an intention to inject fake messages and share with neighbour nodes. There are various procedures have been proposed to establish trust in vehicular environment. Our Researchers are making their best efforts in designing, developing and implementing the trust establishment and computation in VANET. Basically trust can be defined as a set of relations among entities that participate in a protocol. These relations are based on the evidences generated by the previous interactions of entities within a protocol.

Sonam Soni et al [1] proposed a trust computation and establishment in VANET[1]. They have presented a trust based secure location finding mechanism which have two steps of computation of trust i.e. direct and indirect trust computation. However, direct trust is evaluated with the help of RSU and TA and indirect trust is evaluated with the help of watchdog scheme. Proposed Results show that this approach is quite applicable for the actual situation of VANET.

Deepika Saraswat [2] presents an AHP (analytical hierarchy process) is decision making technique to prevent dire consequences in VANET environment. This is a three step process to calculate trust value of vehicles to prevent maliciousness. First step is a reputation based computation of trust based upon previous interaction records of vehicle. In second step direct ranking trust computation method is used by Perron-Frobenius theorem.in the third step an indirect rank is computed which is based on evaluation of the number of authentication certificate exchange in a specific time period of vehicles with in communication range. When computation of all three trusts is done, then it computes AHP-trust which is a summation of all three trust values calculated earlier.

Chaurasia et al [3] proposed a reputation assisted trust evaluation framework. In this they have categorized a trust in two types, first one is static trust that depends on organization of received messages and Second one is dynamic trust that depends on number of vehicles are moving on the road.

Ming-Chin Chuang et al [4] proposed a TEAM (trust-extended authentication mechanism) for VANET .this mechanism is decentralized scheme of lightweight authentication .this approach uses a transitive trust relationship among vehicles to improve authentication procedure during communication.

Mayuri Pophali et al [5] designed a trust model to build a trust by applying an idea of an opportunistic forwarding model, this model applies a trust mechanism which enhances the security of routing of packet into the network and Makes less vulnerable from malicious attack.
Muthukumar.S et al [6] proposed a signal based trust model that aims to sensor internal attacker from transferring false messages in privacy-improved VANET. To approximate the reliability and performance of the planned scheme, they have conducted a set of simulation under alteration attacks, bogus message attacks and black-hole attacks.

VI. PROPOSED WORK

This proposed work is focused on the selection of trusted location in AODV based VANET. A proposed algorithm is categorized in two scenarios first one is sparse environment and other one is dense environment. Because these two environments carry different features so according to that routing strategies are developed. In Sparse (highway) scenario density of vehicles is comparatively low, vehicle speed is high, obstacle are less, vehicle speed variance is low .Where as in dense environment, vehicle density is high,vehicle speed is low as compare to sparse environment due to buildings and various types of obstacles.

The proposed algorithm is divided in two environments: first one is sparse environment and second one is dense environment.

Notations used in the Algorithm

- Count1- Count 1 is a number of vehicles are saying the location is present.
- Count2-Count2 is a number of vehicles are denying the location is present.
- RREP-Route Reply Packet
- RREQ-Route Request Packet
- TA-Trusted Authority
- RSU-Road Side Unit
- BS-Base Station

A. Sparse environment

In sparse environment there are two cases as follows

Case 1- Calculation of trusted location using Vehicles
Source vehicle broadcasts its route request message (RREQ) for finding the secure location within the communication range in the network. Source vehicle receives the route reply message (RREP) from various vehicles then source vehicle computes ratio of vehicles to find out that weather a particular location is trusted or not.

Case2-Calculation of trusted location using RSU-
Source vehicle now asks to RSU about location. Source vehicle will receive location information from RSU and that information will be fully trusted by RSU. If the prerecorded information is not present then RSU sends Reply packet to TA (as police vans, ambulance and post office vehicles) and ask for suggestion. Now TA will send reply to RSU and then RSU will send message to source vehicle.

Algorithm<Trusted location selection>

- CASE 1:

Source vehicle broadcasts RREQ
RREQ is received by neighbouring vehicles within its communication range
Vehicles send reply with RREP

```
For each (RREP)
 {
if (trusted_ location= =true)
{
 count1 ++;
}
else
{
count2 ++;
 } }
Compute Ratio (count1/count2)
If (count1>>count2)
 {
Path is trusted
}
else if (count2>> count1 )
{
Can-not follow the path
if(count1 ≤ count2)
{
Ask for suggestions about location
 }
```

– CASE 2:

```
Source vehicle asks about location to RSU
RSU get the RREQ packet from source
If (pre-recorded info. present)
{
RSU sends location information to source vehicle
}
else
{
RSU sends reply packet to TA and ask for its suggestion it will send reply to RSU with the help of reply packet.
RSU send message to the source node.
}
Dense environment
```

– Case1:

Step1: In this approach if we want to enquire about the vehicle or event then it will send query directly to the RSU.
Step2: If RSU is busy it will send a busy interruption to the vehicle in which enquires it.
Step3: on receiving the interruption it sends the query to TA and finally to its neighbours.

– Case2:

Step1: RSU will initialize trust value for every vehicle which comes under its communication range.
Step2: On receiving trust value it will be incremented by 1 and on receiving false value trust value will be decremented by 2.
Step3: RSU will submit these values to the BS (base station).
Step4: On the basis of the calculated value of trust values base station will calculate the result.
If trusted value of a vehicle is less than T.V. (predefined value) then it is considered to be malicious.
else
do nothing
for further communication this malicious vehicle will not be used.

VII. SIMULATION SETUP AND RESULTS

The proposed Algorithm is implemented in NS-2 simulator and executed on a Pentium(Core i3) processor with 4 GB RAM,running at 2.40 GHz under Red Hat Enterprise Linux. Parameter settings.

Parameter	Value
Number of Nodes	Value (10,30,50)
Topography Dimension	2000m x2000m
Propagation Model	Two Ray Ground
Traffic type	CBR
Packet size	1500
Mac type	802.11 MAC Layer
Channel	Wireless
Interface Queue	Drop tail
Protocol Type	AODV
Queue length	50
Link Layer Type	LL
Antenna Type	Omni directional
Mobility Model	Static
Network Interface Type	Wireless Phy
Start time	0.0ms
Stop time	100ms

Tabel:1

A. Packet Delivery Ratio

This metric is used to simulate the performance of routing protocols. It can be defined as total number of incoming packets and total received packet by the destination. This illustrates the level of delivered data to the destination. In this case the PDR for the BASE algorithm is shown by the red color and in the case where we implement our algorithm, the PDR graph is shown by the green color. And we can clearly see that our algorithm increases the packet delivery ratio. This Graph is drawn between number of packets in Y-Axis and time in milliseconds in X-Axis.

1) Low environment (no. of nodes=10 nodes)

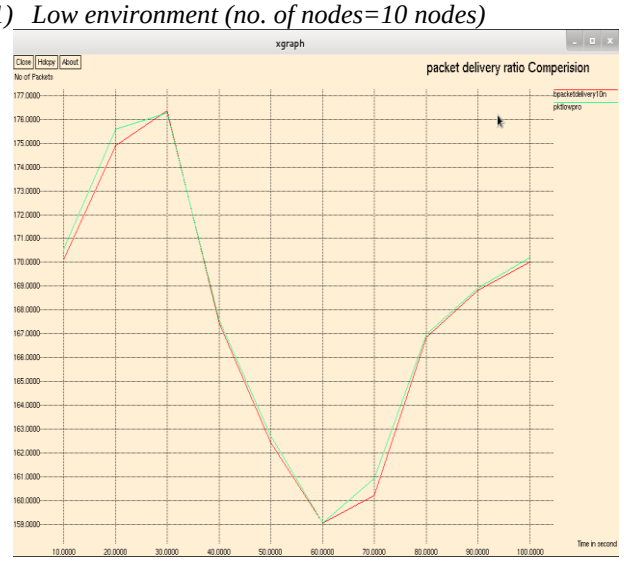

Fig. 4: Packet Delivery Ratio graph for low environment (10 nodes)

2) Dense environment (no. of nodes=50 nodes)

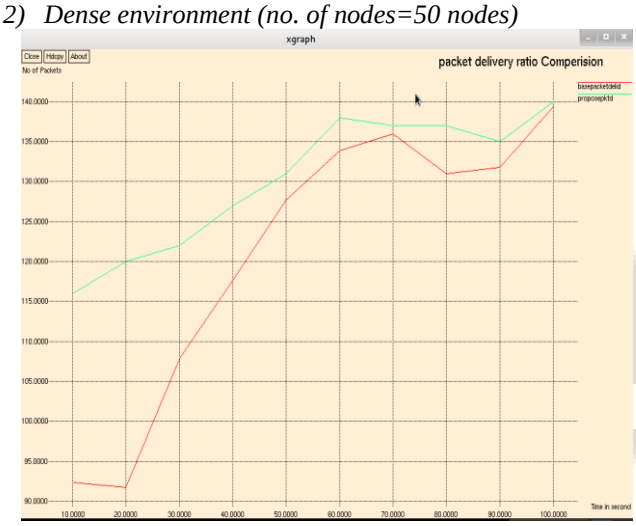

Fig. 5: Packet Delivery Ratio graph for low environment (10 nodes)

3) End to end delivery

This metric is basically used to describe the average time taken by source to transmit a packet to the destination. This time is always measured in milliseconds.The delay caused by discovery of path in routing is included in it.It counts only the number of data packets delivered successfully to destination. The end to end delay for the base algorithm is shown by the red color and in the case where we implement our algorithm in the black-hole infected vehicular network; the graph is shown by the green color. This Graph is drawn between time in second in X Axis and End to end Delay (in milliseconds) in Y-Axis.

∑ (arrive time – send time) / ∑ Number of connections

a) Low environment (no. of nodes=10 nodes)

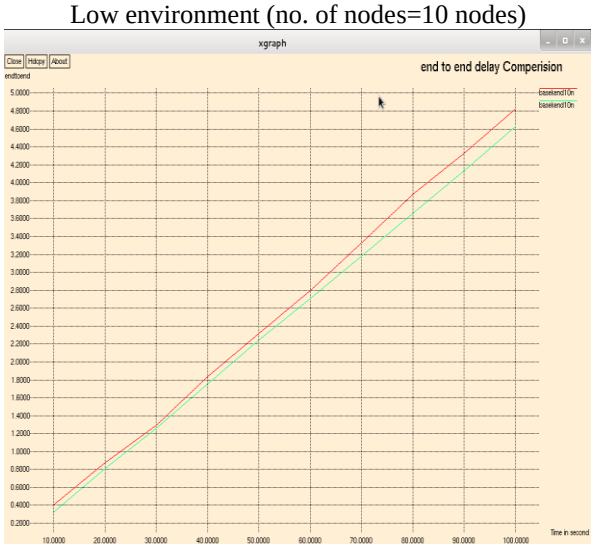

Fig .6: End to End delivery graph for low environment (10 nodes)

b) Dense environment (no. of nodes= 50 nodes)

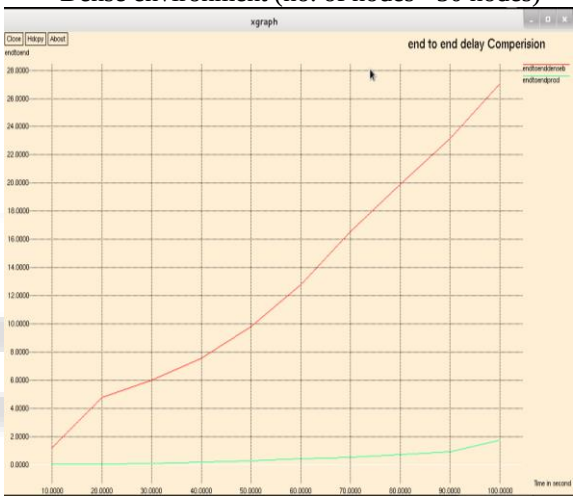

Fig .7: End to End delivery graph for low environment (50 nodes)

4) Throughput

This metric is basically used to describe the total number of bits send to the physical layer per second. So it is always measured in bps. It describes total data received by the receiver divided by the total time it taken. It is applied broadly to systems ranging from various aspects of computer and network systems to organizations. Basically this graph is used to describe the Throughput in Kbps. In this case the Throughput for the base algorithm is shown by the red color and in the case where we implement our algorithm in the black hole infected vehicular network, the graph for throughput is shown by the green color. This Graph is drawn between time in second in X Axis and throughput in Y-Axis.

a) Low environment (no. of nodes=10 nodes)

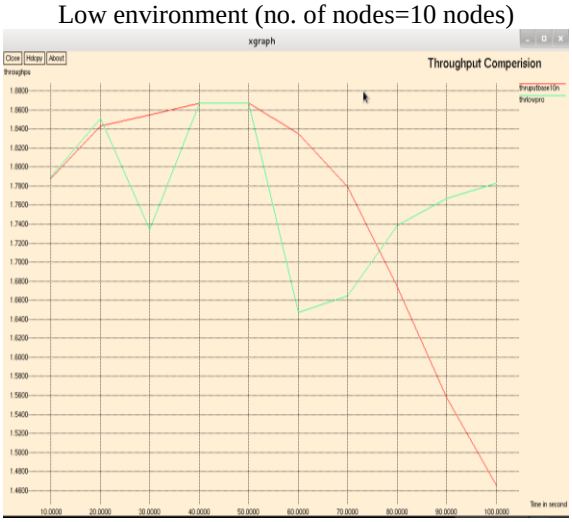

Fig .7: Throughput graph for low environment (10 nodes)

b) Dense environment (no. of nodes=50 nodes)

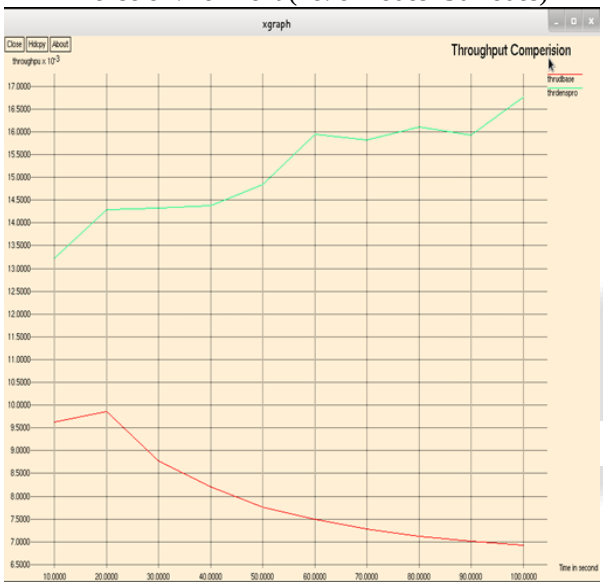

Fig .8: Throughput graph for low environment (10 nodes)

VIII. CONCLUSION

Trust is essential in such network. On basis of this trust vehicles communicate in efficient and proper manner. The possibilities of collisions are reduced if vehicles trust each other. Trust forms safe and secure driving environment in VANET. The proposed approach focused on the selection of trusted location in AODV based VANET. A proposed algorithm is categorized in two scenarios first one is sparse environment and other one is dense environment. Because these two environments carry different features so according to that routing strategies are developed. This approach provides improved results in terms of throughput, packet delivery ratio and end to end delay.

Future work

We can enhance this trust model by dividing whole network into grids by deciding number of vehicle at a particular time stance. Now in each grid we put one trusted authority so, this makes very effective to find malicious behavior. By applying this trust model over grid can get better performance of trust based routing.

REFERENCES

[1] SonamSoni, Kapil Sharma and Brijesh Kumar Chaurasia "Trust Based Scheme for Location Finding in VANETs" V. Lakshminarayanan and I. Bhattacharya (eds.), Advances in Optical Science and Engineering, Springer Proceedings in Physics 166, DOI 10.1007/978-81-322-2367-2_53.

[2] DeepikaSaraswat, Brijesh Kumar Chaurasia, "AHP Based Trust Model in VANETs" 2013 5th International Conference on Computational Intelligence and Communication Networks.

[3] Brijesh Kumar Chaurasia, ShekharVerma, Geetam S Tomar, "Trust Computation in VANETs" 2013 International Conference on Communication Systems and Network Technologies.

[4] Ming-Chin Chuang and Jeng-Farn Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks" IEEE SYSTEMS JOURNAL, VOL. 8, NO. 3, SEPTEMBER 2014.

[5] MayuriPophali, ShraddhaMohod, T.S.Yengantiwar,"Trust Based Opportunistic Routing Protocol for VANET Communication" International Journal Of Engineering And Computer Science ISSN: 2319-7242 ,Volume - 3 Issue -8 August, 2014 Page No. 7408-7414.

[6] Muthukumar.S, KarthickSelvan.R, "Identifying the Misbehavior Nodes Using TrustManagement in VANETs" International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) Vol. 2 Issue Special 1 Jan-March 2014.

[7] NiravJ.Patel, RutvijH.Jhaveri, "Trust based approaches for secure routing in VANET: A Survey"International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[8] Fe´ lix Go´mezMa´rmol, Gregorio Martı´nezPe´ rez ," TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks" Journal of Network and Computer Applications 35 (2012) 934–941.

[9] David Antolino Rivas, Manel Guerrero Zapata, "Chains of Trust in Vehicular Networks: a Secure Points of Interest Dissemination Strategy," Journal of Network and Computer Application Vol. 10 Issue 6, pp. 1115-1133

[10] Wex, Philipp, Jochen Breuer, Albert Held, T. Leinmuller, and Luca Delgrossi, "Trust issues for vehicular ad hoc networks.", In Vehicular Technology Conference, 2008, VTC Spring IEEE, pp-2800-2804. IEEE, 2008.

[11] EmanFarag Ahmed, RehamAbdellatifAbouhogail and Ahmed Yahya, "Performance Evaluation of Blackhole Attack on VANET's Routing Protocols" International Journal of Software Engineering and Its Applications Vol.8, No.9 (2014), pp.39-54.

