www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue -8 August, 2014 Page No. 7408-7414

Trust Based Opportunistic Routing Protocol for VANET Communication

Mayuri Pophali[1], Shraddha Mohod[2], T.S.Yengantiwar[3]

[1]Tulsiramji Gaikwad-Patil College of Engineering & Technonogy, Nagpur
mayuri.pophali@gmail.com

[2]Tulsiramji Gaikwad-Patil College of Engineering & Technonogy, Nagpur
Shraddhamohod2010@rediffmail.com

[3]Tulsiramji Gaikwad-Patil College of Engineering & Technonogy, Nagpur
yengantiwar@rediffmailmail.com

Abstract: ***Vehicular ad-hoc network (VANET) has created their importance in network area, because of their special characteristics. The important characteristics of VANET are high mobility, self organization, no restrictions on network size all these characteristics made VANET environment a challenging for developing efficient routing protocols. For the better performance in network VANET require a special support, which made a network fast, secure and efficient, the best solution to that is an Opportunistic routing. This paper build a trusted opportunistic forwarding model in VANET, it incorporates trust mechanism into OR and to enhance the security of routing and protect the network from malicious attack. This paper focuses on the ratio of throughput, delay and security must be good more than existing protocols. In this paper, TMCOR and TOMCOM routing protocol are proposed, which are trusted minimum cost opportunistic unicast routing protocol and multicast routing protocol.***

Keywords: VANET, Degree of Trust, Trusted Opportunistic Routing.

1. Introduction

VANET is the special kind of network, where the communication nodes are vehicles, such a kind of network deal with a number of mobile nodes which are scattered on different roads .Basically, the purpose behind the development of VANET is lack of communication infrastructures in rural and sparse areas. VANET faces many difficulties in routing, which are:-security, privacy, routing, connectivity, and quality of services. To address these difficulties VANET uses Opportunistic routing. The main goal for routing protocol is to provide optimal paths between network nodes via minimum overhead. Many routing protocols have been developed for VANETs environment, which has different aspect likewise they have classified. This paper focus on that problem which are faced during routing, to solve these problem apply opportunistic routing in VANET minimize the attack of malicious node and makes the routing environment safety.

The basic idea of opportunistic routing is that, it allows any node that overhears the transmission and a nearest node perform forwarding, while the others will simply drop the packet [4]. There are several benefits of Opportunistic routing, main benefits are only two First is that, it can combine several weak links into one strong link and Second one is the link quality.

Opportunistic routing exploits these occurrences to skip some hopes and increases the throughput at the same time. By involving multiple neighboring nodes in packet forwarding opportunistic routing exploits the broadcast nature of wireless medium. This packet forwarding reliability improves throughput and energy efficiency.

In this paper, VANET uses the opportunistic routing very deeply and efficiently which results improve the performance of routing.

In this paper, a model is build, which will calculate a degree of trust and then apply this model to opportunistic routing in VANET, called the model as trust model. Trust model makes a relationship between all neighboring nodes and recommend trust degree [2]. And it also identifies selfish and malicious nodes efficiently and solves the security problems of node failure.

2. Related Work

Trust makes a bonding in between those entities which will participate in various protocols. Trust relations are based on evidence created by previous interactions of entities within a protocol. George Theodorakopoulos and John S. Baras [1] presented a scheme for evaluating trust evidence in ad-hoc network.

Yan Lindsay Sun, Wei Yu, Zhu Han, K. J. Ray Liu [2]Presented a framework for information theoretic to measure

trust in ad-hoc network. They develop four axioms to address the meaning of trust and establish trust relationship with third parties. As a result reduction in the packet loss and attack of malicious node reduces.

To increases the reliability of single transmission opportunistic routing takes an advantage of wireless communication. In packet forwarding when packet is forwarded from source to destination at that time necessary to relay on next hop node to forward a packet. Instead of that, opportunistic routing pre-determines a set of node relay with priority order and then select the highest priority node for forwarding that packet. Final aim is to reach packet to destination safely with minimum overhead. For that, design proper routing matrix for opportunistic routing this is done by [3] M. Lu and J. Wu. Due to simultaneous transmission, some time it is very difficult to handle the traffic in Opportunistic Routing. Z. Zhong, J. Wang and S. Nelakuditi [4] do some experiment first the captures the no of transmission between the node pair in opportunistic environment, then accordingly the select nodes and priorities them.

In this case each node contributes to packet delivery, and this helps to handle multiple interactive traffic flows. Graphical Opportunistic Routing scheme involve as many as available next-hop neighbors into the local forwarding, and give the nodes closer to the destination higher relay priorities. K. Zeng, W. J. Lou, J. Yang and D. R. Brown III [5] studied Graphical Opportunistic Routing scheme, and analyzed the trade-off among the packet advancement, reliability and MAC coordination time cost in GOR.

K. Zeng, W. Luo and H. Zhai, [6] studied the impact of multiple rates, interference, candidate selection and prioritization on the maximum end-to-end throughput of OR.

Taking into consideration of wireless interference, proposed a new method for constructing transmission conflict graphs, and present a methodology for computing the end-to-end throughput bounds (capacity) of Opportunistic Routing. The capability of supporting multiple channel rates, which is common in wireless systems, has not been carefully studied for GOR. K. Zeng, W. Lou and Y. Zhang [7] studied the multi-rate GOR (MGOR), to incorporate the rate adaptation and candidate selection algorithm efficiently forwards the packet to the destination with higher throughput than the corresponding geographic routing.

S. Biswas and R. Morris [8] introduced a new protocol named as "ExOR"; the performance of this protocol is superior to previous traditional routing protocols.

Opportunistic routing and network coding are two different ideas, which may not co-relate. S. Chachulski, M. Jennings,

S. Katti and D. Katabi [9] combine these ideas in a natural fashion to provide opportunistic routing without node coordination. Design a system, MORE tests on a 20-node show that MORE provides both unicast and multicast traffic with significantly higher throughput than both traditional routing and prior work on opportunistic routing.

S. Marti, [10] improve the throughput in ad-hoc network, in presence of node that are ready to forward the packet but fail, Here watchdog is used to identify misbehaving nodes.

Protocols have different methods to find and maintain routes in VANET for either unicast, broadcast or multicast communication. A number of simulations and testing have been done on most protocols in each category to evaluate the protocols' performances in a vehicular ad hoc network. In this paper the performance evaluation between unicast and multicast routing protocols implemented in a vehicular environment that is based on Manhattan grid model for transmission between one sender and multiple receivers. Unlike multicast transmission in geocast routing, the multiple receivers for the paper scenario are not located in a specific geographic region. Performance is evaluated in term of average end-to-end delay, throughput, packet delivery ratio and routing overhead. The results reveal a consistent performance for multicast protocols as the number of receiving nodes increases during the transmission. The main objective is to evaluate whether a multicast routing protocol can outperform a unicast routing protocol for these multiple transmissions. The simulation is done in a vehicular environment that is based on 600 x 700 m Manhattan grid model with 150 vehicles, and is executed for 300 seconds.

Unicast Routing Protocols

MANET routing protocols such as Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) can still be implemented in VANET. Both AODV and DSR are reactive protocols. DSR uses source routing, where the data packet carries a complete route that needs to be transmitted from a source to a receiver. On the other hand, AODV depends on the routing table in the intermediate nodes that is dynamically established for the next-hop information.

Multicast Routing Protocols

Multicast transmission in VANET is normally a transmission from a single source to multiple destinations within a specific geographic region, and usually handled by geocast routing. ODMRP is on-demand mesh-based routing protocol. It creates a forwarding group, which is a mesh of nodes that are responsible in forwarding multicast packets to any group member via

flooding; another multicast routing protocol that is often used for comparison is Adaptive Demand-Driven Multicast Routing (ADMR) protocol. ADMR uses tree topology in creating multicast trees or links between the sources, receivers and forwarding nodes. Forwarding nodes are not receivers; their only purpose is to forward the multicast packets from the source to the receivers in the multicast forwarding tree.

Manhattan grid model

VANET simulation is implemented in a 600 x 700 meters grid model of city environment, which is based on Manhattan Grid mobility model, also known as City Section Mobility Model .This model is based on several assumptions. The first assumption is that there are two directions in every street. For vertical direction, mobile node can move either to north or south, whereas for horizontal direction, it is either east or west. Based on this model, it is also assumed that mobile node can only move in the horizontal and vertical lines on the streets.

Figure 3 shows the city model that is used for the simulation. The distance between each intersection is by 300 x 200 meters. Traffic lights are used in a number of intersections to replicate the natural city environment. For simplicity, the types of vehicles do not affect the result of the simulation. The Manhattan grid model is shown below:-

In this paper also used a tool called MOVE (Mobility Model generator for Vehicular Network) [8], which provide a graphical user interface to set the simulation scenario the

simulation scenario. This tool is able to generate mobility trace using SUMO engine and convert it to NS-2 configuration to generate the network traffic trace.

3. Opportunistic Trust Forwarding Model

Trust is the key element in creating a trustable VANET environment which would help promote a safer road environment. TCG defines trust as "An entity can be trusted if it always behaves in the expected manner for intended purpose". Putting "trust" definition in the context of VANET, it would mean that "all components of the network (vehicles and infrastructure) are behaving in an expected manner (trusted communication between the nodes in network) and serve the users and save human lives".
In this paper, opportunistic routing mainly focus on two factors that are cost and security. At the same time they integrate analysis of cost and secure factor. Opportunistic routing helps to make up the security deficiency with trust mechanism. To design a high trust VANET these trust mechanism can be considered as a guidelines.

3.1 Degree of Trust

Although some existing approaches play good roles in improving security of other networks, trust management in VANET still remains a challenging field. Trust depends on observation of the object and third party recommendations. Trust makes a relationship between two parties' one party, known as a thruster and the party known as the trustee.
Here the trust is relates with two different nodes which may have different properties, but they are in their vicinity. These nodes participate in forwarding packet with their recommendations only. Trust is based on the fact that "Trusted entity will not have malicious behavior". The need of trust is to decrease the attack of malicious node. Trust identify malicious node easily. The main characteristics about trust are that: It is subjective, time dependent and asymmetric.

Asymmetric means two nodes do not need to have a similar trust on each other. Different nodes have different opinion about the same node is subjective. It grows and decays over the period of time means that different perception about nodes at different time is time Dependent.
The trust can be divided into two types: - 1.Direct Trust 2.Indirect Trust In case of direct trust, the two different parties is in direct relationship like Mother and Son. In case of indirect trust, two different parties are in relationship but not directly like Grandmother and grandson. In Vehicular ad-hoc network (VANET), trust relationship build from direct interaction with some node is Direct Trust. Trust relationship can be formed from recommendation from other trusted nodes or a chain of nodes about some node is Indirect Trust. When a packet is forwarded from source node to destination node, it follows some path called it as trust path. Mainly the trust paths are created by the nodes in indirect trust. These recommendations are used in trust evaluating process.

Direct trust means node i directly observe node j with a past direct interaction between them i.e. Node 1 has an direct trust on node 2 if they have direct interaction .These interactions are introduced with several constraints: time aging factor, reward factor and penalty factor. There are several interactions between nodes in the network, some are positive and some are negative. These interactions are called as successful and failed interactions. These impacts of interaction are distinguished by penalty factor for trust evaluation process. When neighbor node not only transmits a packet to all its next hops, but also forward devotedly is the successful interaction. But in case of fail interaction the neighbor node does not forward packet correctly due to some attack. These factors are used to save our network from various attacks like black hole attack, gray hole attack and modification attack. And safely continue trust evaluation process. These reward and penalty factor encourage corporation within VANET by providing some measurement to the benevolent and cooperating nodes.

The trust process is totally depend upon the judgment and recommendation specified by node i and node k for node j. And the level of similar recommendation is the Similarity.
When the similarities are higher about some other node means the opinion towards each others are same, i.e. node i and k have same opinion towards each others. Here, lets s (i, k) denote the similarity of node i and k, its formula is as follows:

The most similar nearest neighbor is node which as highest similarity among the other node in a network and it is nearest node also. The strategy behind the selection of that particular node is considering all the similarities between nodes i and its neighbor node and then select one node.
If node finds to be with highest similarity of neighbor then that node will be more reliable and more trustful also. And it will be the best recommender also. So, the trust degree between for node i and node j can be computed indirectly by node i and most similar nearest neighbor. Likewise by using some reference and trusted nodes can calculate the indirect degree.

Indirect trust degree can be calculated with the help of recommendation from most similar nearest neighbors is a recommendation trust degree. Then combine the direct trust degree of most similar nearest neighbor, Describe the recommendation trust level more reliably and trustfully.
The formula of $T^r(i, j)$ as:

In a network, nodes generally monitor the behavior of their neighbors in respect to different trust metrics and finds direct trust value per neighbor. This process is called as trust evaluation process. The trust management is necessary to deal with both malicious and selfish misbehaving nodes. The maliciousness refers to malicious nodes performing trust related attacks to disrupt operations built on trust. A node's trust value is based on direct trust evaluation and indirect trust information like recommendations. The trust of one node toward another node is updated upon encounter events.

Degree of trust is the sum of direct and indirect trust degree between two nodes.
The performance of the network is consistent during some period, so the trust relationship between nodes can be easily fore from direct trust along with indirect trust.

3.2 Opportunistic Routing Cost

The single routing cost is referred to as all feasible existing opportunistic routing in R. Let R denote the existing opportunistic routing from source to destination.
Route in R is $r = (s, n_1, n_2, n_k, d)$
The trust forwarding list is denoted by

$$L = \{n1, n_2, n_k, d\}$$

The sum of all existing feasible routing cost with an emerging probability across the opportunistic routing is the opportunistic routing cost *COR*(*R*).

The cost of opportunistic routing in network is denoted by *COR*(*R*). *p*(*r*) can be estimated by factors such as the nondeterministic outcome of link layer transmissions, network layer protocol mechanisms and the topology of the network. These depend on congestion in network, packet sending rate and interference of channels such a practical conditions of the network.

4. Trusted Opportunistic Forwarding Mechanism

The above definitions help you to derive minimum cost opportunistic routing. In that simply choose the optimal forwarder and calculate node cost to the destination and priorities each node in trust forwarding list.

It can ensure that all the routes in the network must follow minimum cost opportunistic routing, and also avoid malicious attack which are to be happen when malicious node present in a network. Strictly refuse malicious node to join any network.

4.1 Unicast Routing Protocol

Unicast routing refers to information delivery from a single source to a single destination using the wireless multi hop scheme; where the intermediate nodes are used to forward data from the source to the destination or by using the store and forward scheme. It is the most class that widely used in the general ad hoc networks. This scheme required the source vehicle to hold its data for a time and then forward it. There are many unicast routing protocols proposed for VANETs; most of the topology-based routing protocols belong to a unicast class. Unicast forwarding means a one-to-one communication, i.e., one source transmits data packets to a single destination. This is the largest class of routing protocols found in ad hoc networks.

There are several unicast protocols such as proactive, reactive and hybrid routing protocols.

Proactive Protocols keep track of routes for all destinations in the ad hoc network are called Proactive protocols or Table-driven Protocols, as the routes can be assumed to exist in the form of tables. As in VANET, nodes have high mobility and moves with high speed. Proactive based routing is not suitable for it. Proactive based routing protocols may fail in VANET due to consumption of more bandwidth and large table information.

Reactive Protocols acquire routing information only when it is actually needed. The Advantage is that due to the high uncertainty in the position of the nodes, however, the reactive protocols are much suited and perform better for ad-hoc networks. Some of the Reactive Routing Protocols are Associatively Based Routing (ABR), AODV (Adhoc on-demand Distance Vector), and DSR (Dynamic Source Routing). DSR uses source routing, where the data packet carries a complete route that needs to be transmitted from a source to a receiver.

Dynamic Source Routing (DSR) is an On Demand unicast routing protocol that utilizes source routing algorithm. In source routing algorithm, each data packet contains complete routing information to reach its dissemination. Additionally, in DSR each node uses caching technology to maintain route information that it has discovered.

Here we designed a network consisting of 5o nodes and divides that node into four different layers first layer consist of single node second layer having 7 nodes, third layer having 14 nodes, fourth layer having 28 likewise network formed. In unicast routing protocol packet transferred between single sources to single destination. And path between source destination pair are decided previously.

4.2 Multicast Routing Protocol

DSDV

Multicast transmission in VANET is normally a transmission from a single source to multiple destinations within a specific geographic region, and usually handled by geocast routing. In this project we are using two multicast protocols DSDV and AODV. The C. Perkins and P. Bhagwat developed DSDV routing protocol in 1994. It is table driven routing scheme for ad-hoc mobile network based on classical Bellman Ford routing algorithm with some improvements. Solving routing looping problem, increases convergence speed and reducing control overhead message was the main contribution of this algorithm. In DSDV nodes transmit update periodically to its neighbour node with the information of its routing table.

In DSDV, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Using such routing table stored in each mobile node, the packets are transmitted between the nodes of an ad hoc network. Each node of the ad hoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network. When network topology changes, each mobile node advertises routing information using broadcasting or multicasting a routing table update packet.

DSDV routing protocol maintain a routing table that store cost metric for routing path, address of next hop up to the destination and the destination sequence number assigned by the destination node. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges and the node changed routing table information into event triggered style and send updates to its neighbour nodes. The “full dump” and “incremental update” is two ways in DSDV for sending

Information of routing table updates. As like name “full dump” the complete routing table is send in update message while incremental update contains only the entries with metric that have been changed since last update was sent. This algorithm is suitable for small ad-hoc networks but the regularly updating routing table, less bandwidth and essentially requirement of new sequence number at the time of network topology change shows the shortcoming of this protocol and make it unsuitable for long and highly dynamic network environment like VANET.

AODV

This protocol same as DSDV routing protocols with significant differences. In AODV when a node sends a packet to the destination then data packets only contains destination address. On the other hand in DSR when a node sends a packet to the destination the full routing information is carried by data

packets which causes more routing overhead than AODV. The AODV establishes a route when a node requires sending data packets i.e. on-demand. For finding path from source to destination node in AODV algorithm the source node sends a route request packet to its neighbors and this process is repeat till the destination node path is not found. The sequence number of packet is check at every intermediate node to produce a loop free path. If a node finds that number in its routing table than node discard the route request packet otherwise store record in it stable. It has the ability of unicast & multicast routing and uses routing tables for maintaining route information. It doesn't need to maintain routes to nodes that are not communicating.

AODV uses only symmetric links between neighboring nodes because the route reply packet follows the reverse path of the route request packet. If one of the intermediate node realize path broken than it send information to its upstream neighbor and this process is execute until source node not get this message and after it again source node transmit the route request packet to neighbors node for finding new path. The AODV has the advantage of establishing on-demand route in between source and destination node with the lower delay in connection setup and does not require much memory for communication but there are several disadvantage with this protocol like if the source node sequence number is very old than the intermediate nodes can lead to route inconsistency. Heavy control overhead if there has multiple route reply packets for a single route request packet. It consumes extra bandwidth because of periodic beaconing.

5. Result and Discussion

Here we evaluate the performance of original AODV, DSDV routing protocol we use the open network simulator NS-2. Nodes follow a random waypoint mobility model, travelling at a variety of speeds over a 1000 x 80 meters area for 200seconds of simulated time.

Table 1. Simulation Parameter

Parameters	*Meaning*	*Value*
Area	Road area	1000 m × 80m
N	Number of nodes	70
R	Transmission radius of each node	250 m
S	Maximum node speed	20 m/s
P	Data packet size	512 byte
α	Weighting factor of $Td(i, j)$	0.6
β	Weighting factor of $Tr(i, j)$	0.4
Δt	Time interval of trust update	0.5 s
T	Simulation time	200 s
M	Number of malicious nodes	1~20
Threshold	Threshold of trust degree value	0.5

5.1 Performance Metrics

Packet Delivery Ratio:

It is calculated by dividing the number of packets received at the destination node by the total packets sends by the source node. It specifies the packet loss rate, which limits the maximum throughput of the network and the delivery ratio performance. The high packet delivery ratio presents better performance of a protocol.

$$\text{Packet delivery ratio} = \frac{\text{Packets received by the destination node}}{(\text{Packets received} + \text{Packets dropped})}$$

Average end-to-end delay of data packets:

It is defined as the average end-to-end delay of data packets within a network. The sum of all time differences between the packet sent and received divided by the number of packets, gives the average end-to-end delay. The lower the end-to-end delay the better the application performance. Delay can be defined as: Packet Delay = packets receive time – packets send time.

Packet delivery fractions (PDF):

The ratio of data packets generated by CBR sources to the packets delivered. This metric characterizes both the completeness and correctness of the routing protocol and also the reliability of routing protocol by giving its effectiveness.

5.2 Simulation Results

The simulation of the vehicular ad hoc network consists of 50 mobile nodes with movement. The figure below shows that the position of node in network before starts the simulation. Here nodes are divides into four layers at very fist layer single node located which is source node and all other nodes are destination nodes. In second layer seven nodes are there, in third layer 14 nodes, in fourth layer 28 nodes. Likewise total 50 nodes are divided.

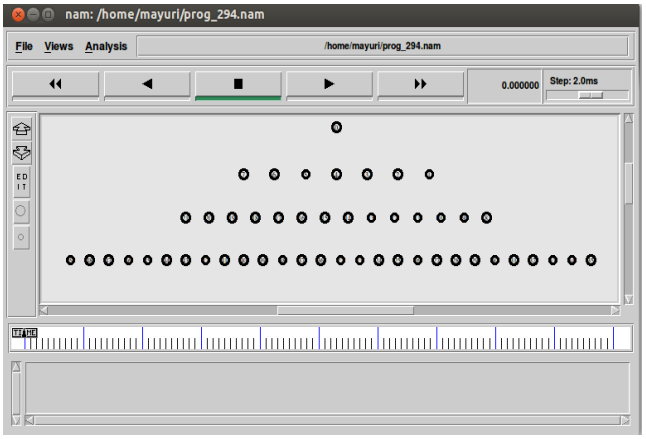

Figure 1: Node position in Network

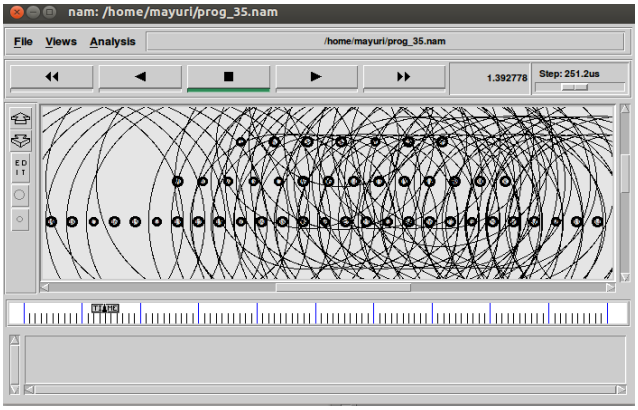

Figure 2: Node **Movement**

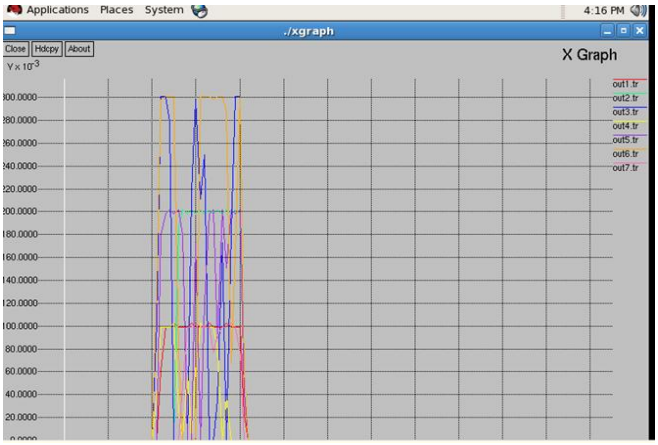

Figure 3: X Graph

The above figure is an X Graph of seven nodes present in second layer of a network. These seven nodes decides the performance of routing because all the nodes below the second layer connected directly or indirectly to that layer so instead of taking the performance of all node we just take that seven node performance which give a very detail idea about a network.

Packet Delivery Ratio of DSDV and AODV

The average Packet Delivery ratio of the DSDV & AODV protocols in the scale of network is plotted in Fig.10 & 11, in which y-axis represents the packet delivered. Observing the throughput comparison in different routing protocols we found that, the On-demand protocol AODV performed particularly well, delivering over 85% of the data packets regardless of mobility rate. While DSDV could not achieve good packet delivery ratio when moves more frequently. This result is valid for each of the cases with different simulation -time and number of nodes. Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV Destination-Sequenced (Distance Vector Routing (DSDV) is a table-driven routing protocol– DSDV). The performance of DSDV is better with more number of nodes in comparison with the performance of AODV, which is consistently uniform. In terms of dropped packets, DSDV's performance is the worst.

The performance degrades with the increase in the number of nodes. AODV performs consistently well with increase in the number of nodes.

5.3 Comparative Analysis

Many of the researchers evaluate the performance of routing protocol like AODV, DSDV in the VANET environment using different evaluation methods means on the basis of different performance metric or using different simulators for this purpose.

In routing protocol AODV and DSDV performance analyze in highway scenario on the basis of Packet loss, Packet Delivery Ratio and End-To-End Delay. Many routing protocols like EX-OR showed that network nodes can achieve superior performance than the traditional forwarding by opportunistically forwarding the received data packets. In the same fashion, here we analysed the performance of protocol AODV and DSDV in VANET environment [16]. Result shows that proposed method produce satisfactory results in comparison of other, by using routing protocol AODV and DSDV.

Analyze the routing performance on the basis of performance metric of throughput, average packet latency. The AODV protocol performs better in comparison of DSDV routing protocol shows in the simulation work results. The performance of AODV, DSDV evaluated at the basis of Packet loss, Packet Delivery Ratio and End-To-End Delay performance metric. For this work they used NS2 Simulator. The different simulators are also used to perform the analysis of routing protocols. The major advantage of NS2 is the open source model saves the cost of simulation, and online documents allow the users easily to modify and improve the codes.

The NS2 simulator use to compare the performance of AODV, DSDV routing protocol and in the same fashion of work .NS-2 simulator used to analyze performance of AODV, DSDV routing protocol on basis of packet loss and security gain more effectively.

The Performance of the routing protocol in VANET Network is analyzed with respect to Packet Loss, End-To-End- Delay, Packet De-livery Ratio and Routing Overhead. The results shown in graphs with some average values computed from all simulation runs. These graphs have shown the performance of AODV and DSDV Multicast routing protocol in VANET environment in terms of packet delivery ratio, end to end delay and packet loss %.

Two On-demand (Reactive) routing protocols namely Ad-hoc On Demand Distance vector Routing(AODV) and Dynamic Source Routing (DSR) and one Table driven (Proactive) namely Destination Sequenced Demand vector(DSDV) is used.

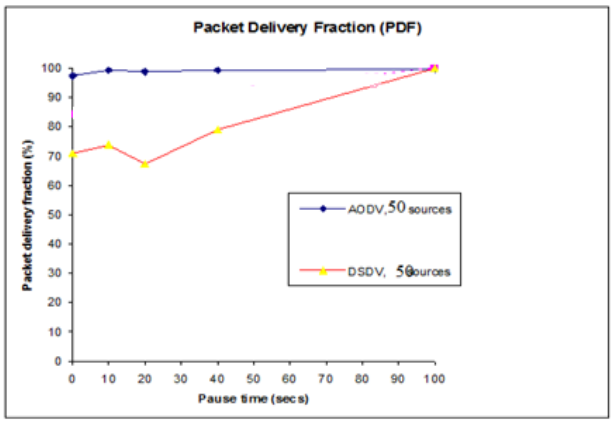

Figure 4: Pause Time Vs Packet Delivery Fraction

Figure 4 shows packet delivery ratio with pause time varying from 0 to 100(sec) for DSDV and AODV routing protocols. The pink line shows the graph for DSDV and the blue line shows the graph for AODV protocol. PDF is the ratio between the number of packets originated by the application layer sources and the number of packets received by the sinks at the final destination. It will describe the loss rate that will be seen by the transport protocols, which in turn affects the maximum throughput that the network can support. This simulation chooses 0, 10, 20, 30, 40, 50, 60, 70, 80 and 90seconds pause time. This simulation generates 50 nodes. Figure shown above at pause time 0 seconds (high mobility) environment, AODV outperforms DSDV and DSR in high mobility environment, topology change rapidly and AODV can adapt to the changes quickly since it only maintain one route that is actively used.
DSDV deliver less data packet compare to AODV because in rapid change topology it is not as adaptive to route changes in updating its table. DSR does not have mechanism in knowing which route in the cache is stale; data packet is forwarded to broken link.

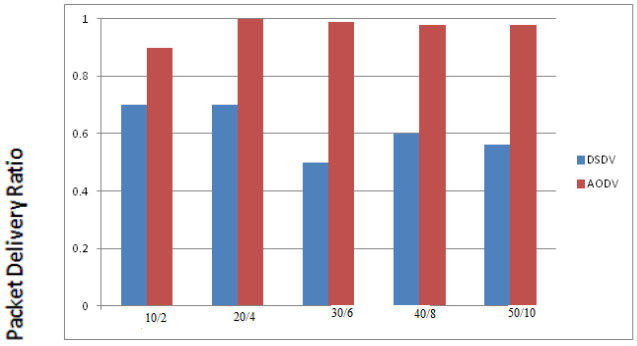

Figure 5: No. of Nodes/Connection Vs Packet Delivery Ratio
Figure 5 shows packet delivery ratio of AODV, DSDV and DSR routing protocol in the opportunistic VANET environment. It is observed that DSR protocol shows better result than AODV and AODV is better than DSDV. The packet delivery ratio of DSDV is less compare to AODV and DSR.
Scenario 1:
In this scenario, number of nodes connected in a network at a time is varied and thus varying the number of connections, through which the comparison graphs of AODV, DSDV and DSR, is obtained.
End-to-End Delay:
All three protocols show same delay for small number of nodes, but the delay decreases with increasing nodes for DSDV network.

Packet Delivery Ratio:
Performance of AODV remains
constant for increasing number of nodes, whereas for DSDV it is more than that of DSR.
Throughput:
The performance of AODV, DSDV and DSR remains almost constant for increasing number of nodes but AODV and DSR shows better than DSDV.

6. Conclusion

In this paper, build a trusted opportunistic forwarding model mainly based on the concept of opportunistic that: "a node forwards a packet in opportunistic mode".The trusted opportunistic unicast routing protocol and multicast routing protocol TMCOR and TMCOM outperforms existing protocol in terms of throughput, cost of routing and resisting malicious attack, this is shown in simulation results. Improvement in the performance of routing is to be done by minimizing the packet loss and reduce the attack to malicious node by comparing a trust value of a node and judging a node behavior and do not allow any node to join a network In future work, planning to implement more elaborate models for attacker's behavior and concentrate on low trust value node to detected their bad behavior. Next plan is to present this trust model in three dimensional ways. To verify the performance of TMCOR and TMCOM in real environment, we have to conduct the simulation extensively and analysis rigorously.

Acknowledgement

The work is supported by the national natural science foundation of china (Project No. 60970117, 61173137), Fundamental research founds of national university, Wuhan University (Project No. 3104002, 2011211- 02020007).

References

[1] G. Theodorakopoulos and J. S. Baras, 2006. On Trust Models and Trust Evaluation Metrics for *Ad Hoc* Networks, IEEE Journal on Selected Areas in Communications.

[2] Y. Sun, W. Yu, Z. Han and K. J. R. Liu, 2006. Information Theoretic Framework of Trust Modeling and Evaluation for *Ad Hoc* Networks, IEEE Journal on Selected Areas in Communications.

[3] M. M. Lu and J. Wu, 2009. Opportunistic Routing Algebra and its Applications. In the Proceedings of INFOCOM.

[4] Z. Zhong, J. Wang and S. Nelakuditi, 2006. Opportunistic Any- Path Forwarding in Multi-Hop Wireless Mesh Networks.

[5] K. Zeng, W. J. Lou, J. Yang and D. R. Brown III. 2007 On Throughput Efficiency of Geographic Opportunistic Routing in Multihop Wireless Networks.

[6] K .Zeng, W. Luo and H. Zhai, 2008.On End-to-End Throughput of Opportunistic Routing in Multirate and Multihop Wireless Network .*IEEE INFOCOM*'08.

[7] K. Zeng, W. Lou and Y. Zhang, 2007.Multi-Rate Geographic Opportunistic Routing in Wireless *Ad Hoc* Networks .IEEE Milcom.

[8] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," *ACM SIGCOMM*, Vol. 35, No. 4, 2005, pp. 133-144.

[9] S.Chachulski, M. Jennings, S. Katti and D Katabi.2007.Treading structure for the randomness in wireless opportunistic routing.ACM SIGCOMM computer communication.

[10] S. Marti, *et al.*, 2000. Mitigating Routing Misbehavior in mobile Ad Hoc Network. In the proceeding of MobiCom'00.