Trusted Opportunistic Forwarding Model in VANET

Mayuri Pophali
Tulsiramji Gaikwad-Patil
College of Engineering and
Technology, Nagpur

T.S.Yengantiwar
Tulsiramji Gaikwad-Patil
College of Engineering and
Technology, Nagpur

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

Trusted opportunistic routing, VANET, Degree of trust.

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 than 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.

3. PROPOSED SYSTEM

In this paper, a network is designed in which nodes are mobile in nature. The challenging thing in such an environment is to send data to from source to destination safely with minimum time. For that, here opportunistic strategy is used which supports a vehicular ad-hoc network. In short, in this paper a model named as “Trusted Opportunistic Model” is build.

3.1 Simple Opportunistic Trust Forwarding Model

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.

3.1.1 Trust Mechanism

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.

Definition 1 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.

From the below formula [1] state that, T_{new}^{d} ***(i, j)*** is in the range of o to 1. The time aging factor TF represents during the period Δt trust changes with time, i.e. $TF = \Delta t / (\Delta t + 1)$. The positive impact for the trust in Successful interactions during the time period ΔT is denoted by the reward factor RF. Whereas the negative impact for the trust in failure interactions during the time period Δt is denoted by the penalty factor PF .So, *RF* and *PF* satisfy the following conditions: $1 \geq RF > PF \geq 0$, $RF + PF = 1$. *T*he period between the current time and the time of last interaction and between the two nodes i and *j is* Δt *where* ($\Delta t \geq 0$).The number of successful or failed interactions during the time period Δt *is denoted by s and f.* The forwarding Successful or failed probability is S and F respectively.

So, direct trust degree can be calculated as follows denoted by:-

$$T_{\text{new}}^{d}(i,j) \begin{cases} 1 - TF * T_{\text{old}}^{d}\ (i,j) & (s = 0 \text{ or } f = 0, T_{\text{old}}^{d}\ (i,j) > 0) \\ 1 - TF * (RF * S - PF * F) * T_{\text{old}}^{d}\ (i,j) + (RF * S - PF * F) & (s = 0 \text{ or } f = 0, T_{\text{old}}^{d}\ (i,j) > 0) \\ 0 & \text{otherwise} \end{cases} \qquad (1)$$

Definition 2 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:

$$S(i,k) = \frac{\sum_{u\in CN(i,k)}(\mathrm{T^d}\ (i,u) - \overline{T_i}) * (\mathrm{T^d}\ (k,u) - \overline{T_k}\ )}{\sqrt{\sum_{u\in CN(i,k)}(\mathrm{T^d}\ (i,u) - \overline{T_i})^2} * \sqrt{\sum_{u\in CN(i,k)}(\mathrm{T^d}\ (\mathrm{k,u}) - \overline{T_k})^2}} \qquad (2)$$

The above formula (2), *s* (*i*, *k*) ranges between 0 and 1.Where the common neighbor nodes for nodes i and k are denoted by CN (*i*, *k*) .and the direct trust degree of node i, k to u are denoted by T^d (*k*, *u*) and T^d (*i*, *u*). T_i and T_k denote the average direct trust degree of node *i* and node *k* that are put on their common neighbor nodes in *CN* (*i*, *k*) respectively. Calculate the similarities between nodes i and its neighbor node with the help of formula (2).

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.

Definition 3 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 $\mathrm{T^r}$(i, j) as:

$$T^r(i,j) = \frac{\sum_{k\in m} T^d\ (k,j) * s(i,k)}{\sum_{k\in m} s(i,k)} \qquad (3)$$

So, the above formula should satisfy this condition:

$0 \leq \mathrm{T^r}(\mathrm{i, j}) \leq 1$

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.

Definition 4 The degree of trust is the sum of direct and indirect trust degree between two nodes. It can be computed as follows:

$$T\ (i, j) = \alpha \times \mathrm{T^d(i, j)} + \beta \times \mathrm{T^r(i, j)} \qquad (4)$$

Where *T* (*i*, *j*) denotes the trust degree between node *i* and *j* (0 ≤ T (*i*, *j*) ≤ 1)

The corresponding weighting factor for direct trust degree *Td* (*i*, *j*) and indirect trust degree *Tr* (*i*, *j*) are denoted by *α* and *β*, trust degree can be determined by the practical situation. α + β = 1. Then set up the condition: 1 > *α* > *β* > 0, if network is prone to estimate the direct trust. At the network initialization time every node in the network familiar with every other node in the network. So, the network only considers the direct trust degree for trust degree (*α* = 1, *β* = 0) instead of indirect trust. 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.

3.1.2 Opportunistic Routing Cost

Definition 5 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 cost of *r* relative to *R* denoted by *Cr*, the sum of the fore link costs in *r*. The cost of *r* relative to *R* denoted by *Cr*, the sum of the fore link costs in *r*.

$$\mathrm{C}_{\mathrm{r}} = \sum_{i\in r} d_{i,J(i)} = d_{s,J(s)} + d_{n1,J(n_1)} + \cdots + d_{n_{k,J(n_k)}} \qquad (5)$$

From the above formula (5), j(i) denotes the trust neighbor forwarding list of node i ∈ r. d_i is an consecutive fore link cost. j(i) depends upon the entire trust forwarding list rather than on the effective forwarder in *J*(*i*) that is used. Some influences such as interference of wireless channel, remaining energy consumption of each node and dynamic topology etc. single route may suffer from these influences. . The *r* emerges with a certain probability, Denoted by *p*(*r*). The broadcast nature of wireless network can generate the |*R*| size of opportunistic routing. So, the cost of opportunistic routing can be calculated by *COR*(*R*).

Definition 6 The sum of all existing feasible routing cost with an emerging probability across the opportunistic routing is the opportunistic routing cost *COR*(*R*).

Thus *COR*(*R*) is expressed as:

$$\mathrm{COR(R)} = \sum_{r\in R} \mathrm{p(r)} \times \mathrm{C}_{\mathrm{r}} \qquad (6)$$

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.

3.2 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. Express the trust opportunistic forwarding mechanism as:

$$\mathrm{Min}_{\nabla \mathrm{R}}\ \mathrm{COR(P)}$$

The most similar nearest neighbors' are more reliable, they are best recommender and trustful also. These trust nodes consists of trust neighbor forwarding list Jr *R* (*i*) of each node i in a route r. The trust degree between node i and node k is denoted by *T* (*i*, *k*). *T* (*i*, *k*) ≥ T_{hreshold}. T_{hreshold} represents the trust threshold of network. The actual forwarder is selected by using highest trust degree node and lowest cost to reach destination in the J_r R (i). As the *COR*(*R*) achieves the minimum gradually, trust forwarding list can be formed by selecting the forwarding nodes from the trust neighbor forwarding list of each node in this minimal cost routing.

3.3 Unicast Routing Protocol

For calculating Trust Degree and Updating the Direct Trust Degree described some algorithm below. With the help of these two algorithms calculating and updating trust degree among the nodes in a distributed way becomes possible. The detailed process is showed in **Algorithm 1** and **Algorithm 2.**TMCOR is Trusted Minimum cost Opportunistic Routing, which is depicted in **Algorithm 3.** A filtering neighboring node algorithm in **Algorithm 4.**This algorithm is to prevent our network from malicious node or link and avoid the malicious node joining the forwarding list.

Algorithm 1. Calculating trust degree (*i*, *j*).

```
Input: node $i$ and its neighbor $j$
Output: T ($i, j$)

//Initialize and compute the trust degree between node $i$ and its neighbour $j$.
Node $i$ collects related information to construct the local topology;
Calculate the direct trust degree based on the neighbour table and historical interactive event with neighbour of node $i$;
If there is no interaction between $i$ and its neighbour $j$ then
{
Trust degree of node $i$ and $j$ is initialized by the direct trust degree as $T (i, j) \leftarrow T^d (i, j) \leftarrow 0.5$;
Store the direct trust degree and the current time in the local information table;
}
Else if there is interaction between $i$ and its neighbour $j$ then
{
Updating DirectTrustDegree($i, j$);
Store the direct trust degree and the current time in the local information table;
Node $i$ calculates the similar direct trust degree of its neighbours to $j$ by formula (2), the similarity $\tau$ satisfies the condition, $\tau \geq 0.6$;
Node $i$ calculate the indirect trust degree with its neighbour $j$ by formula (3);
Calculate the total trust degree of node $i$ and $j$ by formula (4);
}
else
$T (i, j) \leftarrow 0$; end if;
```

Algorithm 2. Updating direct trust degree (*i*, *j*).

```
Input: node $i$ and its neighbour $j$.
Output: $T^d_{new} (i, j)$.

//Updating the direct trust degree between node $i$ and its neighbour $j$.
if ( (Node $i$ and $j$ are connected) and $T^d_{old} (i, j) > 0$)
        then $T^d new (i, j)$ is updated by formula (1);
else
if ((Node $i$ and $j$ are not connected) and $T^d old (i, j) \leq 0$)
        then $T^d new (i, j) \leftarrow 0$;
else
Node $i$ collects its neighbours' information by sending HELLO packets during period $T$;
end if
```

Algorithm 3. Trusted minimum-cost OR (*G*, *d*).

```
Input: graph $G$ and
node $d$. Output: $S$

for each node $i$ in $V$
    do Filtering NeighborMNodes ($G$ ,$i$)
      $D_i \leftarrow \infty$;
      $F_i \leftarrow \Phi$;
end for
$D_d \leftarrow 0$;
$S \leftarrow 0$;
$Q \leftarrow V$;
while $Q \neq \Phi$ do $j \leftarrow$EXTRACT-LEAST-COST($Q$);
      $S \leftarrow S \cup \{j\}$;
          for each edge ($i, j$) in $E$
              do $J \leftarrow F_i \cup \{j\}$;
              if $D_i > D_;$ then $D_i \leftarrow d_{i,j} + D_j$;
                    $F_i \leftarrow i$;

              end if
               end for
end while
```

Algorithm 4. Filtering NeighborMNodes (*G*, *i*).

```
Input: graph G & node i.
Output: the new graph
G(E,V)

 for each edge ($i, j$) in $E$
      if Calculating TrustDegree($i$,$j$) <$T_{threshold}$
            then $E \leftarrow E$-edge($i$,$j$);
             $V \leftarrow V$-{$j$};
       end if
end for
```

4. EXPERIMENTAL WORK

To evaluate the performance of routing protocol TMCOR which is trusted minimum cost opportunistic unicast routing protocol use a simulator. Here the simulation is based on IEEE 802.11b of MAC layer. In VANET vehicles move from random starting point to random ending point is the destination along the road. In a network source and destination pairs are randomly spread. The simulation environment for such a network consists of the 10 source node, around 1~20 malicious node spread over the entire network and 4 CBR packet generation rate. Traffic sources are Constant-Bit Rate (CBR). **Table 1** contains a list of other related parameter.

4.1 Result Analysis

Here, the performance is evaluated as compare TMCOR scheme with ExOR in terms of Throughput, Security gains and average end-to-end Delay. Throughput is the number of packet transmitted per unit time in between source and destination pair. Average end-to-end Delay is the total average delay caused by the entire packets that are transmitted successfully. A security gain is the increment of security performance caused by adopting the way in the aspect of resisting the malicious attack.

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

Figure 1 shows that the throughput of the two protocols verses number of malicious nodes. The results shows that as the no of malicious nodes increases throughput of two protocols are reduces. There is little higher of throughput than ExOR protocol. TMCOR (from 179 KB/ Sec to 60 KB/s), ExOR (from 156 KB/ Sec to 40 KB/Sec). This is happen because the attack of malicious node reduces in TMCOR by comparing its trust degree value.

.**Figure 2** Shows that security gains verses malicious nodes. The lifetime of Network is about the network time, as the network run during long time interval as it suffers from many different malicious nodes. When malicious nodes are 20 the security gain is 0.8.

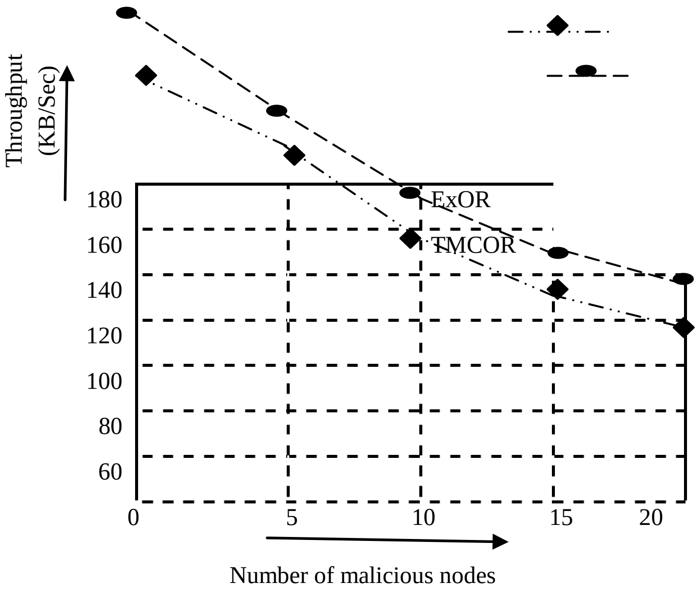


Figure 1: Number of Malicious nodes Vs Throughput

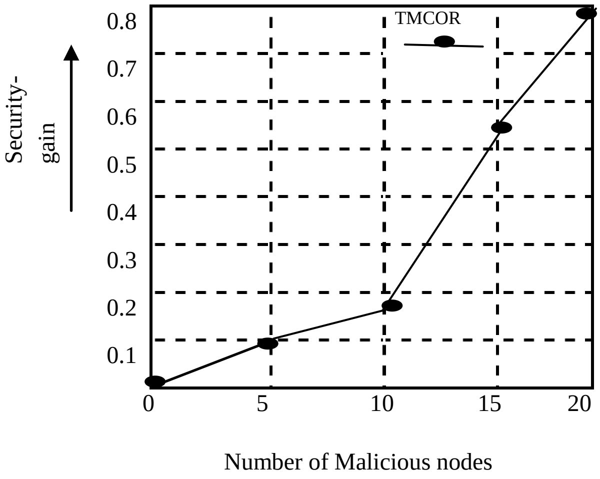


Figure 2: Number of Malicious nodes Vs Security gains

Figure 3 shows that average delay verses nodes speed. By 29.9% TMCOR achieves higher average delay than ExOR. Because of the cost of TMCOR has additional delay overhead than of ExOR. It collects information of trust degree and updating the trust degree.

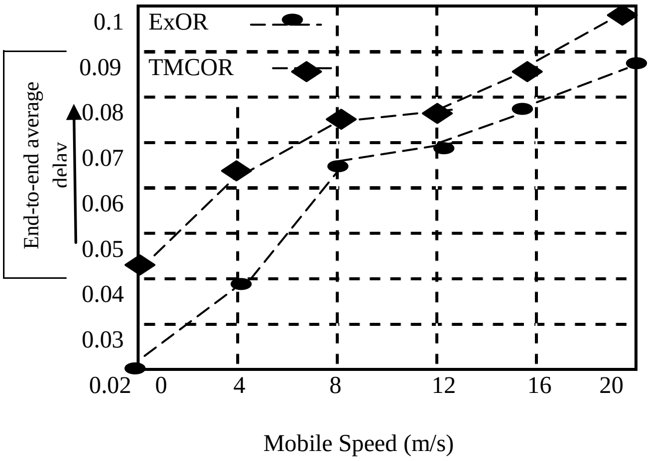
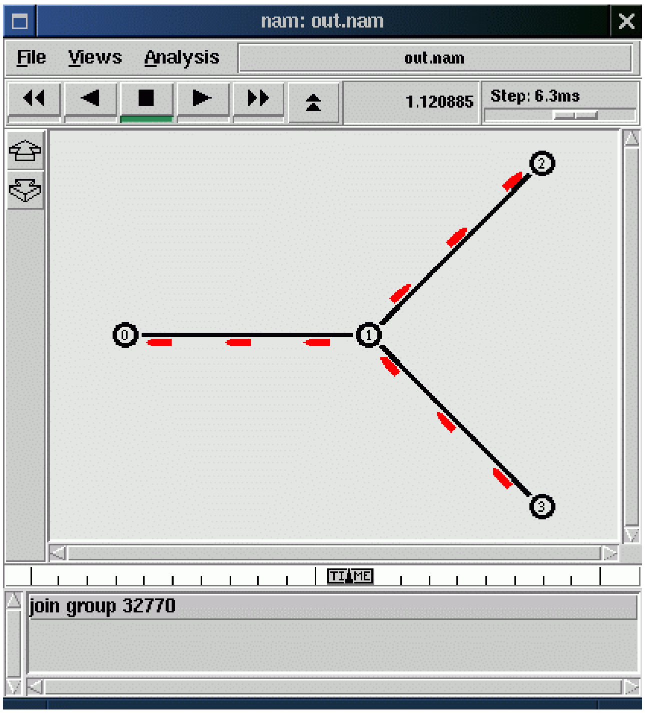


Figure 3: Mobile Speed Vs End –to-end average Delay

A network consist of number nodes, out of these some are connected and others are not means that connected node performs transmission in between them and other are not. Likewise network formed. The first step to design a model is to create network, which consists of number of nodes. Then create a communication link between nodes for communication. Network Simulator-2 discrete event network simulator, used for the simulation of network protocols with different network topologies. The ns2 interface is shown in figure-4 below.



join group 32770

Figure 4: ns2 Simulator interface

5. 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, planning to conduct the simulation extensively and analysis rigorously furthermore, this idea can be integrated with Quality assurance and network coding.

6. ACKNOWLEDGMENTS

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).

7. 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.