Trust Enhanced Secure Multi-Path DSR Routing

Poonam
Department of Electronics & Computer Engineering
Indian Institute of Technology Roorkee, India

K. Garg
Department of Electronics & Computer Engineering
Indian Institute of Technology Roorkee, India

M. Misra
Department of Electronics & Computer Engineering
Indian Institute of Technology Roorkee, India

ABSTRACT

Ad-hoc networks establish communication in improvised environments without requiring any fixed infrastructure. These networks are inherently prone to security attacks, with node mobility being the primary cause in allowing security breaches. Therefore, it is required that the nodes cooperate for the integrity of network operation. However, nodes may refuse to cooperate by not forwarding packets to others for selfish reasons and/or not wanting to exhaust their resources. Due to high mobility of nodes in the network, detecting misbehavior is a complex problem. Nodes have to share routing information in order for each to find the route to the destination. This requires nodes to trust each other. Thus we can state that trust is a key concept in secure routing mechanisms. A number of secure routing protocols based on trust have recently been proposed. However, all these protocols use the traditional route discovery model, where a node drops RREQ packet if its own ID is in the source route of the packet, or if it has previously processed the packet. A misbehaving node takes advantage of this vulnerability and forwards the RREQ fast, so that the RREQ received from other nodes are dropped and the path discovered includes itself (the misbehaving node). In this paper, we present a unique trust based method which is not vulnerable to this behavior. In our method, each node broadcasts a RREQ packet if it is received from different neighbors. A secure and efficient route to the destination is calculated as a weighted average of the trust value of the nodes in the route, with respect to its behavior observed by its neighboring nodes and the number of nodes in the route. We evaluate the misbehaving node detection rate and the efficiency of our method along a number of parameters. Results show that our method increases the throughput of the network while discovering a secure route.

Categories and Subject Descriptors

C.2.1. [Computer-Communication Networks]: Network Architecture and Design—distributed networks, wireless communication; C.2.2 [Computer Systems Organization]: Computer Communication Networks—Network Protocols, Routing Protocols.

General Terms

Algorithms, Performance, Reliability, Security.

Keywords

Trust, Misbehaving nodes, Dynamic Source Routing, Path Trust.

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes organized to create a temporary connection between them. Neither pre-defined network infrastructure nor centralized network administration exists to assist in the communication in MANETs. Nodes communicate with each another via direct shared wireless radio links. Each mobile node has a limited transmission range. Nodes wishing to communicate with other nodes outside their transmission range employ a multi-hop strategy.

There are two types of MANETs: closed and open [1]. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior [2]. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission [3]. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

Since routing is a basic service in such a network and a prerequisite for other services, it has to be reliable and trustworthy. In order to mitigate the adverse effects of routing misbehavior, the misbehaving nodes need to be detected so that these nodes can be avoided by all well-behaved nodes.

Our proposed solution finds a secure, trustworthy path from source to destination. Such a path is free from any misbehaving nodes. We consider both the trust value of the nodes in the path and also the number of hops involved to search for a path from source to destination. Hop count is also given consideration as the shorter the path lesser is the delay.

In our solution we have used a different approach for RREQ packet broadcasting. In the traditional DSR protocol [1] when a node receives a RREQ packet, it checks if it has previously processed it. If so it drops the packet. A misbehaving node takes advantage of this and forwards the RREQ fast so that the RREQ from other nodes are dropped and the path discovered includes itself. Our solution is not vulnerable to this behavior. In our method, each node broadcasts a RREQ packet if it is received from different neighbors. Therefore at the destination we have multiple paths incorporating different nodes, which further lead to the discovery of the most secure path, avoiding misbehaving nodes.

The rest of this paper is organized as follows. In Section II we provide abrief introduction to traditional DSR protocol. In Section III the related work is given, followed by a detailed description of our solution in Section IV. In Section V we evaluate the efficiency of our method through exhaustive simulation. An analysis of the proposed method is also presented. Finally, the last section concludes the paper and gives suggestions for further work in this area.

2. DSR Protocol

DSR is the next generation pure reactive routing protocol for MANETs. It was proposed for the first time by Johnson and Maltz [5] in order to provide routing with minimum overhead while adapting to the network dynamics. DSR is undergoing fast evolution thanks to the many optimizations integrated into it. DSR is based on a pure reactive approach and operates using two simple and complementary mechanisms: route discovery and route maintenance.

2.1 DSR Basic Routing Scheme

DSR uses the source routing concept where the source node puts the whole route in the data packets. Intermediate nodes belonging to this route do not use any data structure to store routing tables. This facilitates the routing task, without adding any additional overhead to the network. Route discovery uses two types of control messages: the route request (RREQ) and the route reply (RREP) packets. The source node floods the network with RREQ packets to reach the destination node. When receiving an RREQ packet, an intermediate node checks if it is itself the destination. If this is true, a RREP packet (which includes the accumulated route in RREQ packet during its ‘‘travel’’) is returned to the source. If the intermediate node is not the destination, this node checks if it has already received a copy of the packet or if the accumulated header route of the RREQ is saturated. If this is true, the RREQ packet is dropped. Otherwise, the intermediate node adds its own address in the RREQ packets’ source route and rebroadcasts the same message to all its direct neighbors If no MAC acknowledgment is received when transmitting a data packet to the downstream node of a link, the upstream node declares the wireless link as ‘‘being broken.’’ In which case, the node updates its cache and then sends a RERR (route error packet) to the source node. The RERR packet contains the broken link (the upstream node and the downstream node). If this packet arrives at the source node, it updates its cache, seeks for a new route toward the same destination. If such a route does not exist in the cache, a new route discovery procedure is initiated for reaching that destination.

3. RELATED WORK

Much research work has been done to make the route discovered by Dynamic Source Routing (DSR) secure.

A Trust based multi path DSR protocol is proposed by Poonam et al. [11] in which uses multi-path forwarding approach. In this approach each node forwards the RREQ if it is received from different path. Through this method detect and avoid misbehaving nodes which were previously included due to vulnerability in DSR route discovery. In the traditional DSR protocol [5] when a node receives a RREQ packet, it checks if it has previously processed it, if so it drops the packet. A misbehaving node takes advantage of this vulnerability and forwards the RREQ fast so that the RREQ from other nodes are dropped and the path discovered includes itself. In their protocol each node broadcast the packet embedding trust information about the node from which the packet is receive. At the source node a secure and efficient route to the destination is calculated as weighted average of the number of nodes in the route and their trust values.

The Watchdog and Pathrater mechanism [6] has been specifically designed to optimize the forwarding mechanism in the (DSR) protocol [5]. The mechanism basically consists of two components: Watchdog and Pathrater. The Watchdog is responsible for detecting selfish nodes that do not forward packets. The Pathrater assigns different ratings to the nodes, based upon the feedback that it receives from the Watchdog. These ratings are then used to select routes consisting of nodes with the highest forwarding rate. The range of the ratings varies from 0.0 to 0.8, where 0.5 signifies a node as neutral. These values are updated periodically by 0.01 every 200 ms. During route selection, these ratings are averaged over all nodes present in a particular path and the route with the maximum rating is selected.

A Trust based routing is proposed by Pirazada [8] in which the trust agent derives trust levels from events that are directly experienced by a node. A Reputation agent shares trust information about nodes with other nodes in the network. A Combiner computes the final trust in a node based upon the information it receives from the Trust and Reputation agents. Trust is computed using direct and indirect information. The trust value is propagated by piggybacking the direct trust value of the nodes along with RREQ packets [9]. Each time a packet is sent or forwarded, the forwarding node scans the routing tables for all alternate paths leading to the destination. It compares the direct trust value of all next hops in this path and selects the one with the highest trust value.

Wang et al. [13] have also proposed a Routing Algorithm based on Trust. They have assumed that the trust values of all nodes are stored at each node in advance. Trust for the route is calculated at the source node based on the weight and trust values are assigned to the nodes involved in the path at the source node. Weights are assigned by the source node ranging from 0 to 1. The protocol uses the path with the largest trust value of route and least packet delay from among multiple route options, as metrics, unlike the standard DSR protocol that only uses minimum hop count.

The Trust-embedded AODV (T-AODV) routing protocol [10] was designed to secure an ad hoc network from independent malicious nodes by finding a secure end-to-end route. In this protocol, trust values are distributed to the nodes a priori. In the route discovery phase the RREQ packet header contains a trust_level field, in addition to the other fields. Each intermediate node rebroadcasts the RREQ after modifying the trust_level by including the trust level of the node that sends it the RREQ to. All the RREP PACKET are sent by the destination. The source node selects the route with the highest value of the trust_level metric.

CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad hoc NeTworks) [2] adds a trust manager and a reputation system to the Watchdog and Pathrater scheme. The trust manager evaluates the events reported by the Watchdog (monitor in this case) and issues alarms to warn other nodes regarding malicious nodes. To verify the source of alarms, a mechanism similar to Pretty Good Privacy [3] is employed. The reputation system maintains a black-list of nodes at each node and shares them with nodes in the friends-list. The CONFIDANT protocol implements a punishment based scheme, by not forwarding packets of nodes whose trust level drops below a certain threshold.

In the TDSR [14] model, trust among nodes is calculated as a combination of direct trust and indirect trust. The direct trust score is modified when misbehavior has occurred by a number of times exceeding a threshold. The indirect trust score is modified when a node receives a message reported by neighbor nodes. If the trust score of a node in the table has deteriorated so much as to fall out of a tolerable range. Such nodes are added to the blacklist. In the route Discovery phase, when node A sends a RREQ packet to node B, B looks up its blacklist to find whether the node A is in it. If not, it forwards the packet.

Narula et al. [7] proposed a novel method for message security using trust-based multi-path routing. The Pizarda model [8], [9] is used for assigning trust levels to the nodes in the network. The trust level is assigned in discrete form, from -1 to 4, which signify complete distrust to complete trust. The paths between the source and destination are found using DSR. The trust levels assigned to the nodes are used to define the maximum number of packets which can be routed via these nodes. Nodes having lower trust values are given lesser number of encrypted parts of a message, making it difficult for malicious nodes to access the information in the message. A node with trust level 0 is not given any message and all the packets received from a node having trust level as -1 are dropped. A node with trust level 4 can read the message. Hence, only those nodes that are completely safe can read the message. The authors have used message encryption and decryption as proposed in [4].

All the existing models have one or more of the following limitations. Most of the methods use the traditional DSR request discovery model, in which a node drops a RREQ packet, if it has previously processed it. A misbehaving node takes advantage of this and forwards the RREQ packet fast so that the RREQ received from other nodes, which arrive later, are dropped and the path discovered includes itself. Most of the trust based routing protocols have used forward trust model to find the path from source to destination. In this model trust is embedded only in the RREQ packet when it is forwarded. So each node evaluates only its previous node and the source node evaluates all the nodes involved in path. But we believe that the trust is asymmetric, so mutual trust information should be used. In watch dog and pathrater approach the trust values are not updated based on node behavior, rather they are updated periodically. Such periodic updates are not able to quantify the misbehaving nodes. Therefore the path discovered includes misbehaving nodes. All of these possible vulnerabilities have been taken care of in [11]. The authors have designed a secure routing protocol, called Trust based multi path DSR protocol, which depends on two-way effort of the node by embedding trust to find an end-to-end secure route free of misbehaving nodes. This protocol has a drawback routing overhead is very high compared to traditional DSR due to broadcasting of RREQ packet. The other drawback is that all the one hop neighbors of destination after receiving first RREQ propagate to destination and also among them. Then this results in discarding the RREQ packet from most of the other paths to the destination node.

4. TRUST ENHANCED SECURE MULTI-PATH ROUTING PROTOCOL

DSR routing model in which dropping of the subsequent RREQ packet in done, as it may lead to following problems:

1. In the traditional DSR protocol [5] when a node receives a RREQ packet, it checks if it has previously processed it. If so it drops the packet. A misbehaving node takes advantage of this and forwards the RREQ fast so that the RREQ from other nodes are dropped and the path discovered includes itself.
2. RREQ packets from non congested paths arrive quickly compared to the paths with congested or highly mobile areas of the network. This results no path through congested or highly mobile area. But if such areas are recovered quickly and there exists a shorter path including such area, then such shorter path may not be utilized.
3. The other drawback is that all the one hop neighbors of destination after receiving first RREQ propagate to destination and also among them. Then this results in discarding the RREQ packet from most of the other paths to the destination node

To address the above problems, we proposed following modification to the traditional DSR and present efficient trust based multi-path routing protocol (TMDSR). TMDSR discovers multiple paths between two nodes. This is essential for an ad hoc network to be able to tolerate attack-induced path failures and provide robust packet delivery [15]. Selecting the route to use depends on the needs of the application. If the application requires robustness, it can send the same packet through multiple paths. If it requires load balancing among the nodes, it can choose different paths to send data packets.

The assumption of our protocol is that each node creates a Trust Table as shown in table 1. This table maintains a trust value for its immediate neighbors. In our protocol we have assumed that each node stores the trust value of its immediate neighbors.

Table 1: Trust table

Immediate neighbor	Trust value
A	0.62
B	0.77

The trust value is assigned in the range from 0 to 1. A well behaved node is assigned trust value >= 0.5, while a malicious node is assigned trust value < 0.5. We do not consider physical layer and link layer attacks, like jamming attacks, in this paper. To decrease the routing overhead and increase the network performance all the one hop neighbors of destination unicast the RREQ packet. In DSR there is no procedure to know the one hop neighbors of destination as no next hop table is maintained. Therefore to address the above problem we maintain neighbor table as shown in table 2 at every node in MANETs. This table is used to maintain all the one hop neighbors of the intended destination. It has two fields which are destination Id in which we store the destination Id to whom the RREQ packet is designated and the other field is one hop neighbor which store the hop neighbor of the specified destination. This table is created when a new RREQ packet is received at each intermediate node.

Table 2: Neighbor table

Destination ID	**One hop neighbors**
30	29
30	21

4.1 Route Discovery at source node

When a source node wants to transmit a data packet to a destination node, to which it does not have a known path. It initiates a route discovery process by broadcasting RREQ packet. The RREQ packet header is modified by adding a *p_trust* field, so that it now contains the following fields: source IP address, destination IP address, a sequence number and *p_trust*:

$$RREQ: \{IPd, IPs, Seq\ num\} || p\_trust \qquad (1)$$

Where

IPd and *IPs* are IP addresses of the destination and source nodes,

Seq num is the sequence number maintained by the source node for each destination node and increases monotonically for each route request.

"||" indicates concatenation and

p_trust denotes the trust value of the path up to that node and is initialized as 0 at source node.

After broadcasting the RREQ packet, the source node sets a timer whose time period T which is equal to 1-way propagation delay. It is determined by using formula given below:

$$T = 2*TR/S + C \qquad (2)$$

Where TR = maximum transmission range.

S = Speed of the wireless signal.

C = constant value, TR/2*S as used in our simulation.

The time value of timer indicates the time needed to receive a RREP packet from one hop neighbors. Acceptance of RREP packet depends on the arrival time and the path length between source and destination node.

The possible arrivals for RREP packet could be before or after the timer expires. If RREP packet arrives before the timer expires then it is accepted if path length is equal to 1 else it is rejected. As this RREP packet may be forged RREP packet from a malicious node. But if it arrives after timer expires then it is accepted if path length is greater than 1. As now the RREP packet has traversed along the path containing only legitimate nodes from source to destination. RREP packet is rejected if path length is 1 as it is from malicious node

4.2 RREQ processing at intermediate nodes

When an intermediate node receives the RREQ packet, it is processed only if the packet is received from a different path, is not from the one hop neighbors of destination and does not include one hop neighbor of destination. So an intermediate node delays the forwarding of RREQ by time equal to 1-way propagation delay after receiving the RREQ packet. The delay D is calculated using formula given below.

$$D = TR/S + C \qquad (3)$$

Where TR = maximum transmission range.

S = Speed of the wireless signal.

C = constant value, TR/2*S as used in our simulation.

If the intermediate node overhears a RREP packet with hop count equal to 1 before the timer expires, then intermediate node and the node that forwarded the RREQ packet are both one hop neighbor of destination. So the neighborhood table is updated by storing intermediate and forwarding node as one hop neighbor of the specified destination.

The RREQ is forwarded in unicast manner if the intermediate node is one hop of destination forward the RREQ else it is broadcasted. This ensures lesser routing overhead as unicast the RREQ packet by such intermediate node decrease routing packets in the network. Unlike previous approaches which are based on broadcast and hence ignore the path from one hop neighbor of destination, the protocol proposed in this paper consider such path as it uses unicasting of route discovery packet from one hop neighbor of destination which lead to detect most trustworthy path. So the increase in detection rate of misbehaving node lowers the packet drop attack which indirectly increases throughput of the network.

Each RREQ packet is modified to include the trust value of the node from which packet is received. So when B broadcasts a RREQ packet and node A receives it, it updates the *p_trust* field as:

$$p\_trust = p\_trust + T_{AB} \qquad (4)$$

where T_{AB} is trust value that is assigned by node A to B and signifies how much node A trusts B.

4.3 RREP at Destination node

When a destination node receives RREQ it immediately sends RREP. At the destination, *p_trust* contains information about the trust of all nodes involved in the path.

The RREP packet header is modified such that it contains two fields p_trust and n_trust in addition to other fields. The updated RREP PACKET is:

$$RREP : \{IPs, IPd, Seq\ num\} || p\_trust || n\_trust \quad (5)$$

Where *p_trust* is assigned from the RREQ packet received at the destination and *n_trust* is initialized to 0. It has the same significance as *p_trust* in the RREQ packet and denotes the trust value of the path up to that node from the destination.

4.4 RREP processing at intermediate nodes

When an intermediate node receives a RREP PACKET, it checks if it is the intended next recipient. If yes, then it modifies field *n_trust* in the same manner as *p_trust*. Each node updates it by including the trust value of the node from which it received the packet.

So when node x receives RREP PACKET from y, it updates *n_trust* as:

$$n\_trust = n\_trust + T_{xy} \quad (6)$$

Then intermediate node forwards the RREP PACKET along the route in source route of RREP PACKET.

If an intermediate node overhear a RREP PACKET and it is not the intended next recipient, then it adds the first node in source route of RREP PACKET to neighbor table. The first node in source route is the one hop neighbor of destination.

4.5 Path decision at source node

When the RREP packet reaches the source node, the most secure path is selected by it. It calculates the path trust based on the trust values *p_trust* and *n_trust* received in the RREP packet and the number of nodes in the path. The path selected is the one which has the maximum path trust.

Trust value of i_{th} path:

$$path\_trust_i = ((p\_trust + n\_trust)/2) * w_i \quad (7)$$

where $$w_i = 1/n_i / \sum_{i=1}^{n} 1/n_i \quad (8)$$

and $$path\_trust_{s-d} = \max(path\_trust_i) \quad (9)$$

where:
n_i is the number of nodes in i_{th} path.
n is the total number of paths from s to d.
w_i is the weight assigned to the i_{th} path.
$path\_trust_i$ is the trust value of the i_{th} path.
$path\_trust_{s-d}$ is the trust value of the path selected as the most trust-worthy path.

4.6 Illustration

To illustrate how to calculate Path trust in DSR Route Discovery, consider the network shown in Figure 1 below.

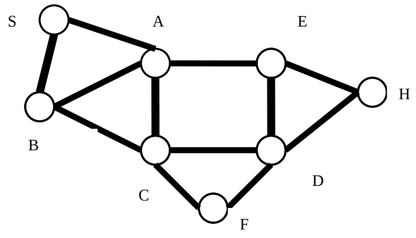

Figure 1. An ad hoc network

Consider that source node S has to send data to destination node D. S does not have a path to D, so it initiates route discovery by sending RREQ to its neighbors. Let the RREQ packet reach node D from the path S-A-E-H-D. Each intermediate node modifies *p_trust* by including the trust value of the node from which it received the packet. When the RREQ packet reaches node D, the value of p_trust is given by:

$$p\_trust = T_{AS} + T_{EA} + T_{HE} + T_{DH}$$

Now RREP is sent from node D to S from the path D-H-E-A-S with *p_trust* as in RREQ packet received at D and *n_trust* initialized to 0. Each intermediate node will update *n_trust*.

So at S *n_trust* will be:

$$n\_trust = T_{HD} + T_{EH} + T_{AE} + T_{SA.}$$

Therefore $path\_trust_{s-d} = (p\_trust + n\_trust)/2 * w_n$

Or $path\_trust_{s-d} = ((T_{AS} + T_{SA} + T_{DH} + T_{HD} + T_{EH} + T_{HE} + T_{AE} + T_{EA})/2) * w_{n.}$

Hence $path\_trust_{s-d}$ contains mutual trust information of all the nodes involved in the path from S to D.

5. PERFORMANCE EVALUATION

In this section we discuss the performance of the proposed method based on simulation using some metrics defined here.

5.1 Simulation

We have used the QUALNET network simulator (version 4.5) developed by Scalable Network Technologies Inc. [12] to evaluate the effectiveness of the proposed method. Different scenarios are defined in a 400 * 400 m square area with 30 nodes. The source and destination nodes are randomly selected. In each scenario, each node moves in a random direction using the random waypoint model [1] with a speed randomly chosen within the range of 0–20 m/s. The transmission range of each node is 100 m. we assume that there are 0-40% malicious nodes in the network.

5.2 Metrics

To evaluate the performance of the proposed scheme, we use the following metrics:
Percentage of detection: It is defined as the ratio of the number of nodes detected as malicious and the actual number of such nodes present in the network.
Routing Overhead: It is defined as the time number of RREQ packets transferred taken to find a secure path from source to

destination, in the presence of malicious nodes.

Throughput: it is the ratio of the number of data packets received by the destination node to the number of packets sent by the source node.

5.3 Results

In this section we show the results for the proposed protocol (TMDSR) and compare these with those obtained from standard DSR protocol and trust based multipath DSR, by varying the number of malicious nodes in the network.

Figure 1 show that TMDSR is able to detect more misbehaving nodes compared to trust based multi path DSR. TMDSR is able to explore more routes to destination as RREQ packet is unicasted. Therefore more number of path are available at source and trustworthy path is selected based on the path trust. The percentage of detection is less than 100 due to node mobility which results in link breakage. When there is a link breakage the next trustworthy path is selected. But the behavior of some node may change during this time and it may start misbehaving. This information is available only with the intermediate nodes, which are unable to make any routing decisions. Thus the path selected may include such nodes, which remain undetected.

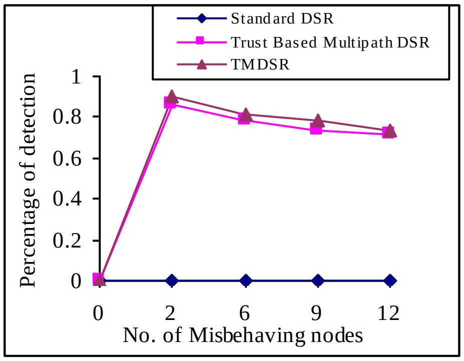

Figure 1. Percentage of detection

Figure 2 shows that the routing overhead of TMDSR is more than DSR when there are no malicious nodes in the network. Because in TMDSR, a RREQ packet is processed if it is received from different path while in DSR a node drop the packet if is has seen it previously no matter for the path. But as the number of nodes increases in the packet are dropped which induces new route discovery. In TMDSR misbehaving nodes are detected and excluded from the path the route discovery is delayed which indirectly decreases the routing overhead. Unlike DSR approaches which is based on broadcast of RREQ our protocol uses unicasting of route discovery packet from one hop neighbor of destination. This unicasting of RREQ introduces very less additional routing overhead on standard DSR in the network.

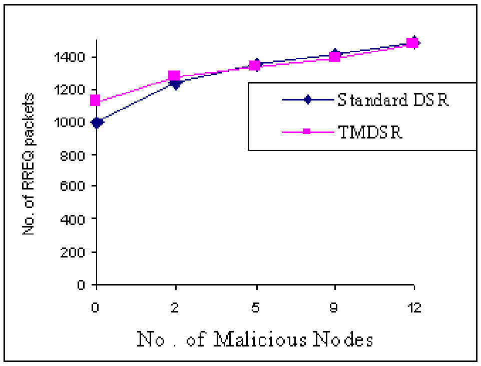

Figure 2. Routing Overhead

The throughput of TMDSR is more compared to DSR and Trust based multipath DSR. Throughput for all the methods degrades with the increase in number of misbehaving nodes in the network as shown in Figure 3.

However, the decrease is steeper in DSR as it discovers the shortest path without detecting any misbehaving nodes which induce packet drop.

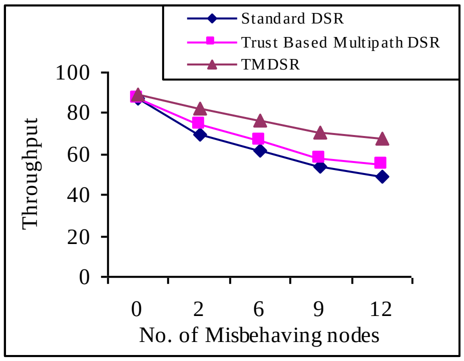

Figure 3. Throughput

TMDSR uses unicasting of route discovery packet from one hop neighbor of destination unlike both approaches which are based on broadcast and hence ignore the path from one hop neighbor of destination. Therefore TMDSR is able to explore more routes to destination and is able to find the most trustworthy route excluding malicious nodes.

6. CONCLUSIONS AND FUTURE WORK

In this paper proposed, an efficient trust based multi-path routing protocol (TMDSR) has been proposed to find a secure and trustworthy path with minimized routing overhead. The technique discovers the shortest secure path from source to destination by embedding trust information in RREQ and RREP packets. The route discovery packets are unicasted from one hop neighbor of destination so that it introduces very less additional routing overhead in the network. Results demonstrate that the proposed TMDSR protocol provides better throughput in the presence of as high as 40% of misbehaving nodes in the network. Moreover the protocol is able to detect 90% of misbehaving node in the network. Unicast based approach introduces very less additional routing overhead on standard DSR in the network.

The future work is directed to prevent node congestion and provide load balancing using alternate routes discovered by the proposed protocol.

7. REFERENCES

[1] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y.C. and Jetcheva, J. G. 1998 A performance comparison of multihop wireless ad hoc network routing protocols. In proceeding of International Conference Mobile Computing and Networking (MobiCom), ACM Press, 85–97.

[2] Buchegger, S. and Boudec, J. 2002. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes—Fairness In Distributed Ad hoc NeTworks. In Proceeding ACM Workshop Mobile Ad Hoc Networking and Computing (Switzerland, 2006). 226-236.

[3] Garfinkel, S.1995 PGP: Pretty Good Privacy. O'Reilly and Associates.

[4] Haniotakis, T., Tragoudas, S. and Kalapodas, C. 2004. Security enhancement through multiple path transmission in ad hoc networks. IEEE Communications Society, 4187-4191.

[5] Johnson, D. B., Maltz, D. A., Hu, Y. C. and Jetcheva, J.G. 2003. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet draft IETF RFC 3561, http://www.ietf.org/rfc/rfc3561.txt.

[6] Marti, S., Giuli, T. J., Lai, K. and Baker, M. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In Proceeding of Sixth Annual International Conference Mobile Computing and Networking (MobiCom). ACM Press, New York, NY, 255-265.

[7] Narula, P., Dhurandher, S. K., Misra, S. and Woungang, I. 2007. Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing. Elsevier Journal of Computer Communications, 760-769.

[8] Pirzada, A. A., Datta, A. and McDonald, C. 2004. Propagating trust in ad-hoc networks for reliable routing. In Proceeding of IEEE International Workshop Wireless Ad Hoc Networks (Finland, 2004). 58-62.

[9] Pirzada, A. A., Datta, A. and McDonald, C. 2004. Trust-based routing for ad-hoc wireless networks. In Proceeding of. IEEE International Conference Networks (Singapore, 2004). 326-330.

[10] Pissinou, N., Ghosh, T. and Makki, K. 2004. Collaborative trust-based secure routing in multihop ad hoc networks. Networking (Athens, Greece 2004). Lecture Notes in Computer Science, vol. 3042, 1446-1451.

[11] Poonam, Garg, K., and Misra, M. 2010. Trust based multi path DSR protocol. In Proceedings of Fifth International Conference on Availability, Reliability and Security, (Poland, February, 2010). 204-209.

[12] QUALNET simulator, Available from: <http://www.scalable-networks.com>.

[13] Wang, C., Yang, X. and Gao, Y. 2005. A Routing Protocol Based on Trust for MANETs. In Proceeding of Sixth Annual International Conference on Grid and Cooperative Computing (Beijing, China). Lecture notes in computer science, vol. 3795, 959-964.

[14] Yong, C., Chuanhe, H. and Wenming, S. 2007. Trusted Dynamic Source Routing Protocol. IEEE International Conference on Wireless Communications, Networking and Mobile Computing (Athens, Greece 2007), 1632-1636.

[15] Zhou, L. and Haas, Z. J. 1999. Securing ad hoc networks IEEE Network Magazine, vol. 13, no. 6, 1-12.