# DIRECT TRUST ESTIMATED ON DEMAND PROTOCOL FOR SECURED ROUTING IN MOBILE ADHOC NETWORKS

**N.Bhalaji** bhalaji.80@gmail.com
*Assistant professor/department of information technology*
*Hindustan University*
*Chennai-603103, Tamilnadu, India*

**Druhin mukherjee, Nabamalika banerjee**
*School of CSE*
*SRM University*
*Chennai-603203, Tamilnadu, India*

**A.Shanmugam**
*Principal*
*Bannari Amman Institute of Technology,*
*Sathyamangalam-638401, Tamilnadu, India*

## Abstract

Adhoc network is a collection of wireless nodes communicating among themselves over multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous techniques have been proposed for the secure routing, in this paper we propose a more reasonable and unambiguous equation for trust evaluation. Our scheme is distributed and effective without reliance on any central authority. In this paper we focus on improving the security of most commonly used Dynamic Source Routing Protocol (DSR).We improve the routing security of the existing DSR protocol by enhancing the concept of trust value, the selection of a secure route will be based on these trust values. Ns-2 simulations are performed to evaluate the impact of applying trust value based route selection to the DSR protocol.

**Keywords:** Adhoc, DSR, Security, Trust

## 1. INTRODUCTION

Adhoc networks are a collection of mobile hosts (or they can also be called as nodes), which form a temporary network. There is no fixed infrastructure in an adhoc Network and each host have a wire less interface and communicate with each other over radio or infrared. Because of node mobility the network topology changed frequently. All nodes of these wireless networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are useful in the emergency operations and in which persons need to share information and data quickly. The security for routing protocols should be an important component in MANET. The network operations can be easily jeopardized if countermeasures are not embedded into basic routing protocol functions of MANET at the early stages of their design. Wireless mobile ad hoc network routing protocols have to be thoroughly tested and analyzed in term of their operations. Simulation experiments are the main tool for testing MANET routing protocols. Simulation experiments need to be conducted before any real implementation. The wireless and mobile nature of MANET brings new security challenges in the network design. Mobile nodes in MANET communicate with each other via open and shared broadcast wireless channels, so they are more vulnerable to security attacks. In addition, their infrastructure-less nature means that centralized security control is hard

to implement, so the network needs to rely on individual security solutions from each mobile node participating in the network. Our goal in this paper is to present the trust- based route selection to the existing implementation of the DSR routing protocol [1] of MANET to improve the security aspects of the routing protocol. We also perform detailed simulation study for the proposed secure routing protocol for MANET.
The main contributions of this paper are:

- Improving the security of the existing DSR protocol by enhancing a trust-based route [2]selection
- Comparing the implemented routing protocol with the existing DSR protocol, using simulations.

The remainder of this paper is organized as follows. Related work is discussed in Section 2, followed by a description of the proposed Trust based DSR protocol in Section 3. The simulation setup and corresponding results are outlined in section 4. Future work is outlined in Section 5 and conclusions are drawn in Section 6.

### 1.1. On demand routing protocol

The protocols for the adhoc network are classified based on different characteristics [2] such as

- Routing information update mechanism
- Use of temporal information for routing
- Routing topology and
- Utilization of specific resources.

The on demand routing protocol belongs to the first category of protocols which updates the information and are of reactive in nature. They obtain the necessary path when it is required, by using a connection establishment process. The most commonly used protocols under this category are Dynamic Source Routing [1] and AODV [3]. For our simulation study we consider DSR as a reference protocol.

## 2. RELATED WORK

### 2.1. DSR Protocol

Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by Broch, Johnson, and Maltz [1]. In a nutshell, it works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link.
The author in [4] developed and applied trust based routing to the DSR protocol. The idea behind this approach is to store information of the trust that one node has to the other nodes. These trust values are adjusted based on the experiences of the nodes, such as packet drops or acknowledgements receipts. The routes are evaluated based on some heuristic that uses the trust Values of the nodes as criteria. The performance study in [4] showed that this implementation had a higher throughput than standard DSR when the number of malicious nodes is slow. However it showed that DSR protocol outperformed the trust based routing in situations with a high number of malicious nodes. The malicious nodes should have very low trust values. In this paper, we improve the DSR protocol by enhancing the trust-based routing solution when exist a high number of malicious nodes in the network.
The authors in [5] evaluate the performance of some trust-based reactive routing protocols in a mobile network with varying number of malicious nodes. By doing many simulations, they demonstrate that the performance of theses protocols varies significantly even under similar attack, traffic, and mobility conditions. However, each trust-based routing protocol has its own peculiar advantage making it suitable for application in a particular extemporized environment.

Current ad hoc routing protocols are basically exposed to two different types of attack: active attacks [6] and passive attack. The active attack occurs when the malicious node bears some energy costs in order to perform the threat, whereas passive attacks are mainly due to lack of cooperation, with the purpose of saving energy selfishly. Mobile nodes that perform active Attacks with the aim of damaging other nodes by causing network outages are considered to be malicious nodes, where mobile nodes that perform passive attacks with the aim of saving battery life [7] for their own communications are considered to be selfish nodes. Malicious nodes can disrupt the functions of a routing protocol by modifying its information or by sending false routing information through the entire network. On the other hand, selfish nodes can severely degrade network performance and eventually partition the network by simply not participating to the network operation.

## 3. NEW TRUST BASED ROUTING SCHEME

This section presents the improvement of the trust based Route selection to be applied to the DSR protocol in order to enhance the security of the routing protocol. The purpose of applying the Trust based route selection to the DSR protocol is to fortify the existing implementation by selecting the best and securest route in the network. In difference to the process of route selection in the DSR protocol which involves the selecting of the shortest route to the destination node, in our proposed Protocol we choose the most reliable and secure route to the destination based on the trust values of all nodes that found in the administrator of the trust unit. A separate acknowledgement module is there to monitor the received acknowledgments and adjust the trust values for the nodes on the route. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes. This trust value will be adjusted based on the experiences that the node has with its neighbor nodes. When a node receives data packets or acknowledgements from its neighbor node, the trust value for this neighbor node will be upgraded. Neighbor node that is encountered for the first time will have an initial trust value assigned based on trust formation strategy. If a route contains known nodes, the trust values of these neighbor nodes are used to assign the initial trust value. If a requested acknowledgement was not received, the trust value for this neighbor node should be decreased.

### 3.1. Components of the proposed protocol

The proposed protocol consists of the following components.

**1. Trust Unit**
**1.1. Initialiser**
**1.2. Upgrader**
**1.3. Administrator**
**2. Monitor**
**3. Router**

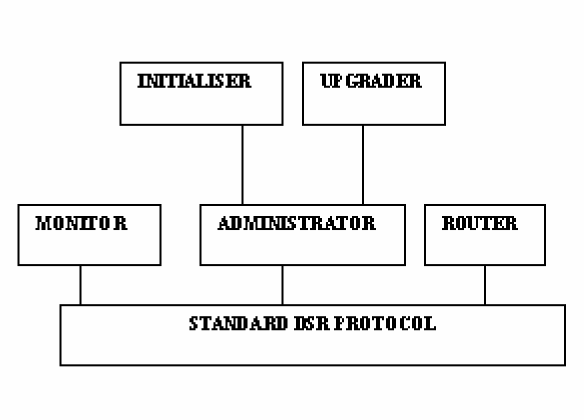

**FIGURE 1:** Components of Relationship Based DSR

**Trust Unit**

***Initialiser Module***: This module is used to assign a trust value for unknown new mobile nodes in the network. It would be best to assign a low trust value in an environment with many malicious nodes. If a route contains known nodes, the trust value of these nodes is used to base the assignment of the initial trust value for the new node.

***Upgrader Module:*** The upgrader module of trust unit is used to implement the Functions for upgrading trust. The updating of the trust values will depend on a given node experience in a given situation. We use the following equation to upgrade the trust value for each node encountered in the route the function for upgrading trust depends on two parameters, previous trust values and the nature of Experience. It is calculated as below

***$T = \tanh [(\Delta+W)*Te]$***

*Where*
*T: The upgraded trust value*
*Te: The existing trust value*
*W: The weight of the experience. For acknowledgement related operations it is assumed to be 1 and for data forward and receiving it takes 0.5.*
*Δ: assumes +1 for positive experience and 0 for negative experience.*

The positive and negative experience is calculated based on the acknowledgment. If the acknowledgement is received within the time frame then it's counted as positive experience else if its not received with in the stipulated time it is counted as a negative experience.

***Administrator:*** The Administrator module of the trust unit stores trust information about all known nodes during run time, and it offers methods to query for information about stored trust values. So it is used as the interface between the existing DSR protocol on one hand and the Initialiser and Upgrader modules on the other hand.

***Monitor:*** The purpose of the monitor module is to adjust the trust values from the received acknowledgements. Since the trust values are used on routing selecting decisions, it is important that a missing acknowledgement is detected fast. When an acknowledgement is received, the trust upgrader module upgrades the trust values for nodes on the stored route. If a requested acknowledgement is not received, the packet is considered dropped, so the trust values should be adjusted in a negative way.

***Router:*** The router module is responsible to evaluate routes based on trust values of nodes. In this paper we are going to discuss about different routing strategies which we are going to apply over the proposed protocol and test its performance in presence of malicious nodes.

***Route selection strategy 1:***

The first route selection strategy will return the average trust value of all nodes on the route. Based on this value the route is rated and the route with highest rating is preferred.

***Route selection strategy 2:***

The second one is extension to the first. In order to favor shorter routes average of the trust values is divided by the number of nodes. Thus the route with high value are given high ratings and subsequently selected for the routing.

## 4. SIMULATIONS AND RESULTS

In our simulations we use performance metric to compare the trust based DSR protocol fortified with the above route selection strategies under the presence of the malicious nodes and the standard DSR. The throughput is considered for our experiment which is defined as a important metric for the determination of the routing protocol performance [8].

*Throughput*: This gives the fraction of the channel capacity used for data transmission

Throughput = Total amount of Data received correctly / Total time

For the performance analysis of the protocol extensions, a regular well-behaved DSR network is used as a reference. We then introduce compromised stranger nodes into the network which doesn't forward the packets. The simulation is being implemented In Network Simulator 2 [9], a simulator for mobile adhoc networks.

| PARAMETER | VALUE |
|---|---|
| Application traffic | CBR |
| Radio range | 250 m |
| Packet size | 512 bytes |
| Transmission rate | 4 packets/s |
| Pause time for nodes | 60 s |
| Maximum speed | 1 m/s |
| Simulation time | 600 s |
| Number of nodes | 25 |
| Area | 1000 m * |

| | |
|---|---|
| | 1000 m |
| Available bandwidth | 1 Mb/s |

The speed of 1 m/s corresponds to slow moving. For a simulation that last 600 seconds, approximately 30000 CBR packets are sent. This number is considered high enough to eliminate any deviations influence on the results. With 1 Mb/s bandwidth, a packet size of 512 bytes and a transmission rate of 4 packets/s, congestion of the network is not likely to occur.

The following graphs illustrate the performance of the different routing strategies and their throughput values. The route selection performance of standard DSR protocol is shown below and it assumes all the nodes are functioning proper and does not bother about the malicious behaviour of the nodes. No trust enhancements are used in the route selection of the DSR protocol.

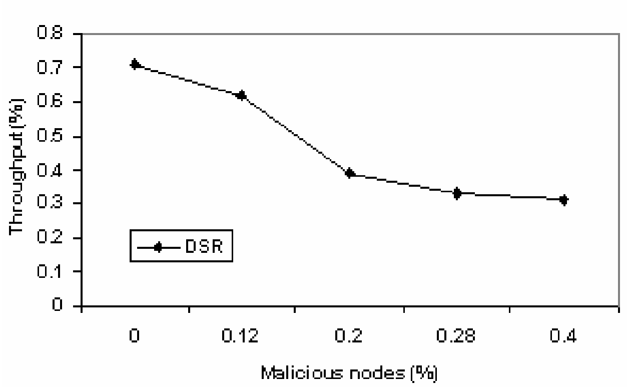

**FIGURE 2:** Throughput of Standard DSR

The following graph is the result of employing the route selection strategy 1 which is based on the average trust value of nodes. The highly rated routing path is selected and thus the following graph shows some improvement over the standard DSR.

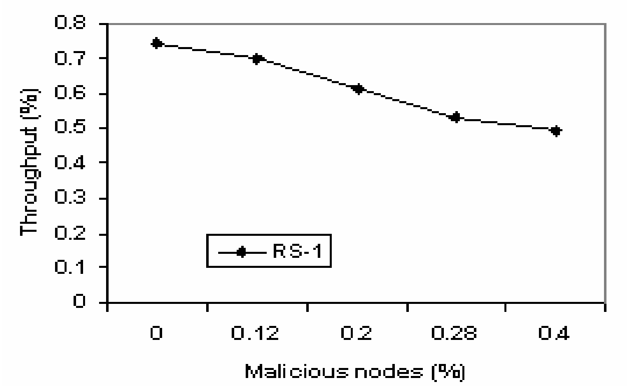

**FIGURE 3**: Throughput of Route Selection strategy-1

Then we conduct another simulation to analyse the performance of the routing protocol when provided with the scheme of Routing strategy -2 which we have discussed in the previous section. This method determines the rating of the route based on the values obtained from dividing the average of the trust values by the number of nodes. This figure also gives better performance than the standard DSR.

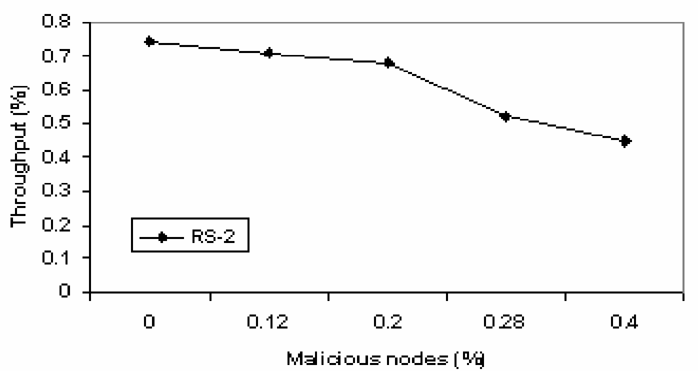

**FIGURE 4:** Throughput of Route selection strategy-2

The throughput obtained by using all above routing techniques are compared and the results reveal that the routing performed with fortified trust values yield better results than the standard DSR routing.

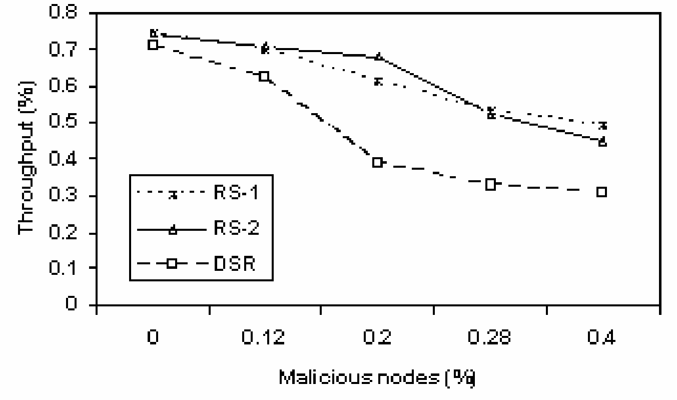

**FIGURE 5:** Comparison of throughput

## 5. FUTURE WORK

In this paper we proposed a two routing schemes based on the trust values of the nodes. In future instead of using only the trust values, the experience factor may be considered for calculating the rating of the route. the proposed scheme may also be tested under different attack scenarios.

## 6. CONCLUSION

We presented improvement in mobile adhoc routing over on demand type of protocol namely Dynamic Source Routing protocol and analysed the performance of the proposed scheme and compared it with the existing DSR protocol. Ns-2 simulator [9] was used for the analysis of the performance. The results show that the proposed trust based routing performs better than the existing standard DSR.

## 7. REFERENCES

1 D. Johnson, D. Maltz, Y. Hu, and J. Jetcheva. "*The dynamic source routing protocol for mobile ad hoc networks. Internet Draft, Internet Engineering Task Force*" Mar. 2001.http://www.ietf.org/internetdrafts/ draft-ietf.

2 C. Siva Ram Murthy and B. S. Manoj, "*Ad Hoc Wireless Networks: Architectures and Protocols*" Prentice Hall, 2004.

3 C.E.Perkins and E.M.Royer, "*Adhoc On-Demand Distance Vector Routing*" proceedings of IEEE workshop on mobile computing systems and Applications 1999, pp. 90-100, February 1999.

4 John Keane, "*Trust-based Dynamic Source Routing in Mobile Ad Hoc Networks*", MS thesis, Department of Computer Science, Trinity College Dublin, September 2002.

5 A. Pirzada, C. McDonald and A. Datta,"*Performance Comparison of Trust-based Reactive Routing Protocols*", IEEE Transactions on Mobile Computing, Vol 5(6), pages 695-710, 2006.

6S. Murphy, "*Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt*, October 2002. https://forum.eviloctal.com/redirect.php?tid=1992&goto=lastpost

7 Djamel Djenouri, Nadjib Badache "*New power-aware routing protocol for mobile Adhoc network*" International journal Adhoc and ubiquitous computing, volume 1.No.3, 2006. pp 126-136. DOI: 10.1504/IJAHUC.2006.009882.

8 J. Broch, D. Johnson, D. Maltz, Y. Hu, J.Jetcheva, "*A Performance Comparison of Multihop Wireless Ad Hoc Networking Protocols*", Proceedings of 4th ACM/IEEE International Conference on Mobile Computing and Networking, 1998.

9 Kevin Fall, Kannan Varadhan: *The ns manual*, http://www.isi.edu/nsnam/ns/ doc/index.html