RESEARCH ARTICLE

ISSN: 2321-7758

Design and Analysis of Trust Based Modified DSR Routing Protocol in Mobile Ad-Hoc Networks

MUNESH DEVI[*1], DAYAL CHADRA SATI[2], MOHIT BANSAL[3], RAVI KANT[4]

[1]M.Tech Scholar BRCM CET BAHAL Bhiwani(HR.)

[2]Assistant Professor BRCM CET BAHAL Bhiwani(HR.)

[3]Assistant Professor GIET Sonipat(HR.)

[4]Assistant Professor, Department of Electrical Engineering, IITM,Murthal, Sonepat, India

MUNESH DEVI

ABSTRACT

A mobile ad-hoc network is a self-configuring network or infrastructure-less network of mobile nodes connected by wireless links which together form a random topology. Due to absence of centralized control, multi hop communications and dynamic network topology, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in wired network or infrastructure based networks. Nodes in mobile Ad Hoc Network (MANET) do not depend on a central infrastructure but relay packets originated by other mobile nodes. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. For individual nodes it might be advantageous not to cooperate, though. In this research paper, we propose a new approach based on relationship among the mobile nodes which makes them to cooperate in an infrastructure-less environment. The faith unit is used to calculate the faith values of each node in the network. The calculated faith values are being used by the relationship estimator to determine the relationship status of mobile nodes. The proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the MATLAB.

©KY Publications

INTRODUCTION

A mobile ad-hoc network is the collection of two or more devices equipped with wireless communications [3] [1]. Mobile ad hoc networks (MANETs) are composed of a set of stations (nodes) communicating through wireless channels, without any fixed support.[7]. Due to recent advances in computing and communication technologies, MANETs have become the networks of choice for various types of applications such as military operations and crisis management, healthcare services [6]. Such devices can communicate with another device that is immediately within their radio range. Main characteristics of mobile ad hoc network are:

- Dynamic topology- the nodes in the network can move arbitrarily, the topology of the network also changes.
- The bandwidth of the link is constrained and the capacity of the network is also varies tremendously. Because of the changing topology, the output of each relay node will vary with the time and then the link capacity will change with the link change.
- Power limitation in mobile devices is a serious factor. Because of the mobility characteristic of

the network, devices use battery as their power supply. As a result, the advanced power conservation techniques are very much necessary in designing a system.

- The security is limited in physical aspect. The mobile network is easier to be attacked than the fixed network.

A MANET is a collection of mobile nodes sharing a wireless channel not having any centralized control or established communication backbone which is shown in figure 1. MANET has dynamic topology and every mobile node has limited resources such as battery, Processing power and on-board memory. This kind of infrastructure-less network is useful in situation in which ordinary wired networks is not feasible like battlefields, natural disasters etc. One of the challenging designs task in wireless Ad Hoc networks is supporting mobility in Mobile Ad Hoc Networks (MANETs). The mobility of nodes in MANETs increases the complexity of the routing protocols and degree of connection's flexibility [4]. A key challenge in MANET is that communication has to be carried out with changing network topology due to node mobility [3] [8].

Fig.1. Ad-hoc Network

Classification of Routing Protocols

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network [2]. The studies on various aspects of routing protocols have been an active area of the research for many years[3] [9]. Routing is the most fundamental research issue in MANETs. The merit of the routing protocol can be analyzed through metrics-both qualitative and quantitative.[10]. To provide complete security in both phases of a MANET, we require secure routing protocols, since nodes involved in the routing cannot by themselves ensure the secure and undisrupted delivery of transmitted data [3]. In

MANET, there are different types of routing protocols each of them is applied according to the network circumstances. Figure 2 & figure 3 shows the basic classification of the routing protocols in MANETs.
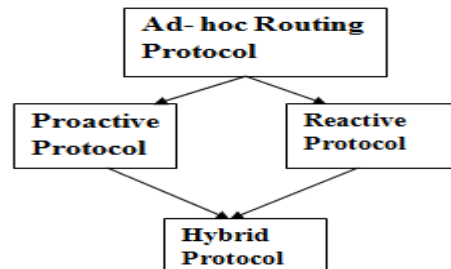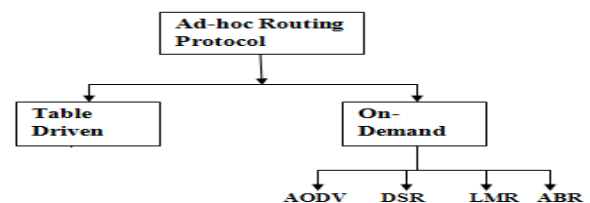

Fig. 2. Classification of Routing Protocol

Fig.3. The Family Tree of Routing protocol

Proactive Routing Protocols

Proactive routing protocols are also called as table driven routing protocols. In this protocol every node maintain routing table which contains information about the network topology even without requiring it. This feature although useful for datagram traffic, incurs substantial signaling traffic and power consumption. Routing is the most fundamental research issue in MANETs. The merit of a routing protocol can be analyzed through metrics-both qualitative and quantitative. The routing tables are updated periodically whenever the network topology changes. Proactive protocols are not suitable for large networks as they need to maintain node entries for each and every node in the routing table of every node. These protocols maintain different number of routing tables varying from protocol to protocol. There are various proactive routing protocols. Example: DSDV, OLSR, WRP etc [3].

Reactive Routing Protocols

Reactive routing protocol is also known as on demand routing protocol. In this protocol route is discovered whenever it is required Nodes initiate route discovery on demand basis. Source node sees its route cache for the available route from source to destination if the route is not available then it

initiates route discovery process. A proactive routing protocol is also called "table-driven" routing protocol [5].The on- demand routing protocols have two major components:

Route discovery: In this phase source node initiates route discovery on demand basis. Source nodes consults its route cache for the available route from source to destination otherwise if the route is not present it initiates route discovery. The source node, in the packet, includes the destination address of the node as well address of the intermediate nodes to the destination [3] [1].

Route maintenance: Due to dynamic topology of the network cases of the route failure between the nodes arises due to link breakage etc, so route maintenance is done. Reactive protocols have acknowledgement mechanism due to which route maintenance is possible Reactive protocols add latency to the network due to the route discovery mechanism. Each intermediate node involved in the route discovery process adds latency. These protocols decrease the routing overhead but at the cost of increased latency in the network. Hence these protocols are suitable in these situations where low routing overhead is required. There are various well known reactive routing protocols present in MANET for example DSR, AODV, TORA and LMR.

Dynamic Source Routing (DSR)

DSR is the next generation pure reactive routing protocol for MANETs. It was proposed for the first time by Johnson and Maltz. in order to provide routing with minimum overhead while adapting to the network dynamics. Dynamic Source Routing (DSR) is a reactive protocol based on the source route approach. In Dynamic Source Routing (DSR), shown in Figure 4, the protocol is based on the link state algorithm in which source initiates route discovery on demand basis [3].
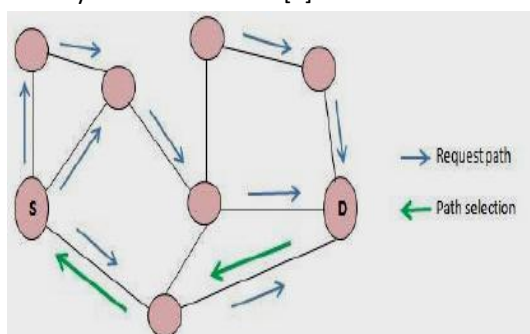

Fig.4. Dynamic Source Routing (DSR)

The sender determines the route from source to destination and it includes the address of intermediate nodes to the route record in the packet. DSR was designed for multi hop networks for small Diameters. It is a beaconless protocol in which no HELLO messages are exchanged between nodes to notify them of their neighbors in the network.[1].

Proposed Methodology

In this proposed method they have designed a new protocol using MATLAB which is called as modified DSR & its output parameters like time & distance are compared with normal DSR. After comparison it is found that Modified DSR protocol takes less time to cover more distance with more trust. The modified DSR is dependent on trust value of the nodes & during path selection it takes all the trusted values. As the modified DSR takes less time & cover more distance the efficiency of the system is improved. The normal DSR protocol does not consider the trust values of the nodes during path selection. It randomly takes any node in the path & finds the shortest path using Dijkstra algorithm. This trust based protocol depends upon the trust values or faith values of the nodes & during path selection it takes the maximum nodes with the trust value or faith value more than 0.5. A trusted node is the one whose trust value is high or we can say that above 0.5 otherwise it will be considered as not trusted node.

Programming Steps:

1. Various input parameters like no of nodes are taken.
2. Select the source node & destination node.
3. After the selection of source & destination node X-co–ordinate, Y co-ordinate & trust matrix is specified for normal DSR.
4. In normal DSR trust value of all the nodes considered equal.
5. Based on trust value of the nodes shortest path is selected from source to destination.
6. Computation time is also calculated from starting to the end.
7. Same steps are followed for trust based modified DSR except in trust based DSR trust value is defined for each node.
8. Also computation time is calculated for trust based modified DSR.

9. In the path selection maximum trusted nodes are selected.

10. A node is said to trusted if its trust value is more than 0.5 otherwise it will be considered as not trusted nodes.

11. In the result it has analyzed that the trust based modified DSR protocol selects maximum node with trust.

12. It is also analyzed that it takes less computation time & covers more distance.

Block Diagram of Modified DSR Protocol
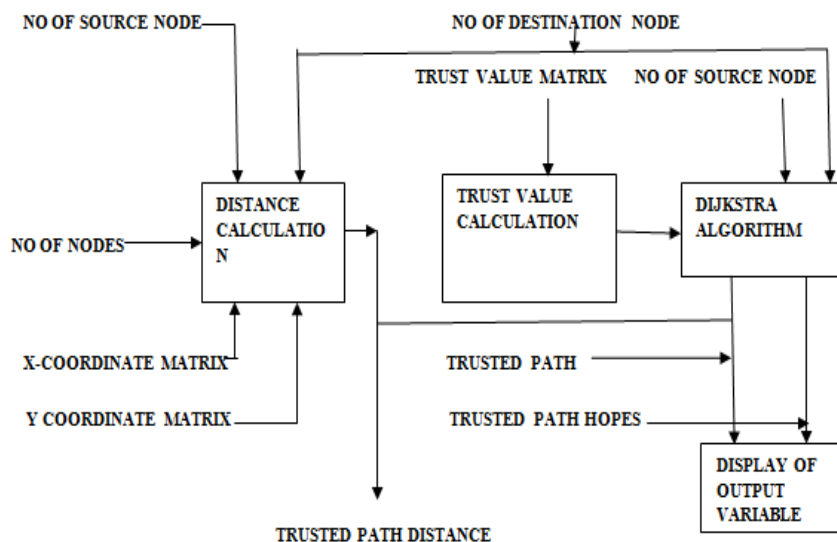
Fig.5. Block diagram of modified DSR

SIMULATION & RESULT

Normal DSR Route: The following figure shows the shortest path selected by normal DSR protocol.
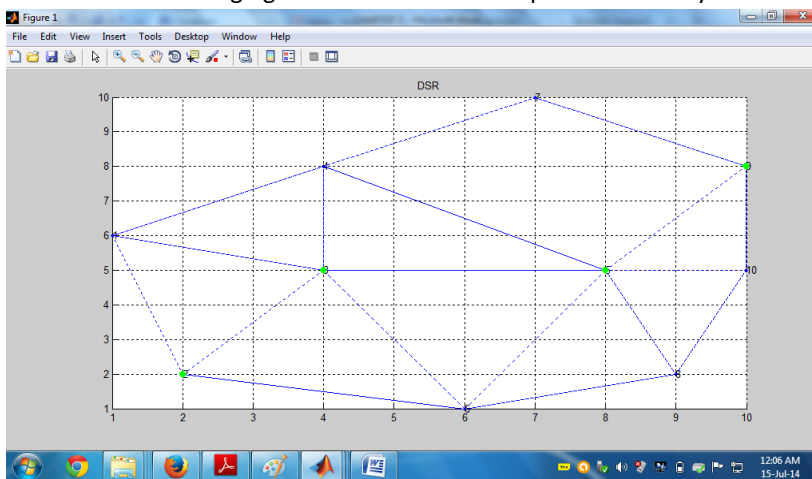
Fig.6. Route selected by Normal DSR

4.2 Route with Trust Based modified DSR

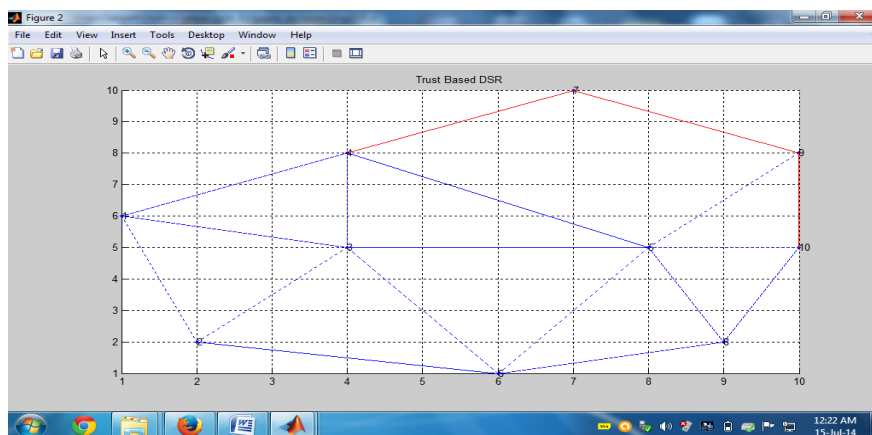The following figure shows the route selected by trust based modified DSR protocol.

Fig.7. Route selected by Trust Based modified DSR

Comparison of Distance

The following figure shows distance comparison between normal DSR & trust based modified DSR protocol. As from this figure it is clear that trust based modified DSR protocol covers more distance.
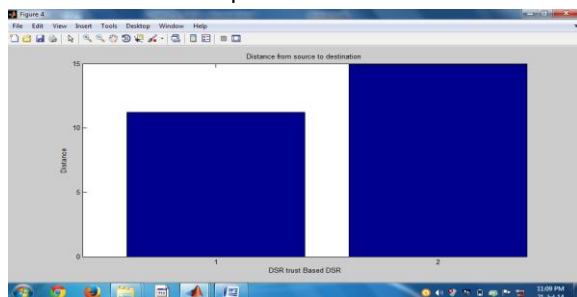

Fig.8. Comparison between distance covered by normal DSR & trust based DSR

Time Comparison

The following figure 8 shows comparison between normal DSR & trust based modified DSR protocol. As from this figure it is clear that trust based modified DSR protocol takes less time as compared to normal DSR.
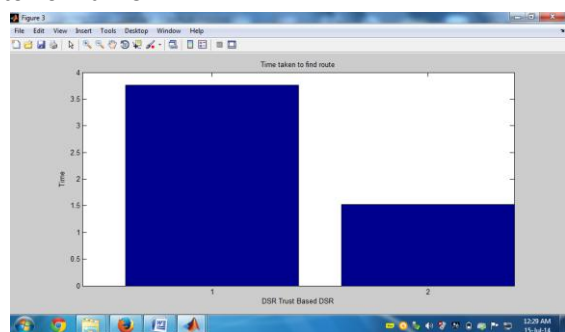

Fig.9.Computation of Time comparison between normal DSR & trust based DSR

CONCLUSION

This paper is conclude that the modified DSR is having better performance than normal DSR. In this it has seen that in modified DSR the path taken by Dijkstra algorithm is the shortest path having trust values more than 0.5. It covers more distance in small span of time as compared to normal DSR. The Route Selection time which is also known as computation time is the time taken by the protocol to select the path from source to destination is also less in modified DSR as compared to normal DSR

Future Scope

In future the mobility of nodes during the path selection can be included. More number of parameters like mobility, delay, bandwidth etc can be included. Further the efficiency of the mobile ad-hoc Networks can be improved by detecting misbehaving nodes.

REFERENCES

[1]. Dr. S.S. Dhenakaran and A. Parvathavarthini, "An Overview of Routing Protocols in Mobile Ad hoc Network", International Journal of Advanced Research in Computer Science & Software Engineering Volume 3 ,Issue 2, February 2013.pp 251-259.

[2]. Poonam, K. Garg and M.Misra, "Trust Enhanced Secure Multi-path DSR Routing" , International Journal of Computer Applications(0975-8887)Volume 2 – No. 2, May 2010.pp 63-69.

[3]. Poonam Gera, Kumkum Garg and Manoj Mishra "Trust-based Multi-Path Routing For Enhancing Data Security in MANETs", International Journal of Network Security, Vol. 16, No. 2 pp. 102-111, March. 2014.

[4]. Ammar Odeh, Eman Abdelfattah and Muneer Alshowkan, "Performance Evolution of AODV and DSR Routing Protocols in MANET Networks". International Journal of Distributed and

Parallel Systems(IJDPS) Vol. 3, No. 4, July 2012.pp 13-22.

[5]. Amit N. Thakare and Mrs. M. Y. Joshi," Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks". IJCA Special issues on "Mobile Ad hoc Networks" MANETs, 2010. pp 211-218.

[6]. Issac Woungang , Mohammed S.Obaidat, Sanjay Kumar Dhurandher and han-Chieh Chao, Chris Liu. "Trust-Enhanced Message Security Protocol for Mobile Ad hoc Networks",IEEE ICC 2012-Communication and Information System Security Symposium. PP. 988-992.

[7]. T. Nirmal Raj, S. Saranya, S. Arul Murungan and G. Bhuvaneswari "Secured Multi Path Routing with Trust Establishment Using mobile Ad hoc Networks" International Journal of Scientific & Engineering Research, Volume 3, Issue 1, January-2012.pp 1-5.

[8]. S. Gopinath, Dr. S. Nirmala, N. Suresh Kumar "Misbehavior Detection: A New Approach for MANET /International Journal of Engineering Research & Applications Volume 2, Issue 1, Jan-Feb 2012, pp.993-997.

[9]. Sunil Taneja and Ashwani Kush "A Survey of Routing Protocols in Mobile Ad HocNetworks" International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.pp.279-285.

[10]. Akshai Aggarwal,, Savita Gandhi and Nirbhay Chaubey." PERFORMANCE ANALYSIS OF AODV,DSDV AND DSR IN MANETS ".International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011 DOI .pp.167-177.