ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Trust and Route Maintenance Collaborative Approach for DSR

Er. Srishty Tanwar, Er. Sahil Batra

Student M. Tech, Dept. of CSE, Geeta Institute of Management and Technology, Kurukshetra, India

Assistant Professor, Dept. of CSE, Geeta Institute of Management and Technology, Kurukshetra, India

ABSTRACT: Mobile ad-hoc networks (MANET) is a field of vast applicability and have the research area of many researchers from the last decade or so. The field also involves other organization for the advancement of hardware involved as well as the other software and routing strategies. The MANET has the applicabilities in defense, exploration of the remote area, and many other real life scenarios because of the structure and its nature. The MANETs with the advancement in the area also facing new challenges day by day as the old one is removed or solved. One of the major issues for this type of the network remain the security. Security is the prime motive of any network working in any area without security the network applicability may have no significance at all. The security mechanism is proposed by many researchers and also implemented in the area. Still advancement continues in the area of security of the network, with this approach, exploring the area of security, in this work, a modified trust based network routing scheme is purposed and implemented. The proposed approach considers the best suited candidates for the transmission between the source and destination. In this effort sometimes, the path adopted may not be the shortest but due to security requirements and structure of the proposed algorithm the adaptation is made.

KEYWORDS: MANET, TRUST UPDATE, SECURE DSR,ROUTE SECURITY

I. INTRODUCTION

Mobile adhoc networks (MANETs)[1] are usually formed by a group of mobile nodes interconnected via wireless links, which agree to cooperate and forward each other's packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is honest and cooperative. That means, if a node claims it can reach another node by a certain path or distance, the claim is trusted/true; similarly, if a node reports a link break, the link will no longer be used. While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces vulnerability several types of denial of service (DoS) attacks [5], particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it. Due to the lack of physical protection and reliable medium ac mechanism, packet dropping attack represents a serious threat to the routing function in MANETs. A foe can easily join the network and compromise a legitimate node subsequently start dropping packets that are expected to be relayed in order to disrupt the regular communications. Consequently, all the routes passing through this node fail to establish a correct routing path between the source an destination nodes.

Related work

Watchdog and Pathrater components to mitigate routing misbehavior have been suggested by Marti, Giuli and Baker [20]. They observed increased throughput in MANETs by complementing DSR protocol with a watchdog for detection of denied packet forwarding and a Pathrater for trust management and routing policy, rating every path used. This enables every node to avoid any malicious node in its routes as a reaction. Ratings are maintained for all the nodes in the network, and the ratings of actively used nodes are updated periodically. The drawback of this system is that there is no reward and no punishment for the participants. Consequently, the selfish nodes still can forward their packets via others, while they are relieved of forwarding the packets of others. So that it becomes even advantageous to be selfish. This drawback is addressed in the subsequent systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

II. PROPOSED ALGORITHM

A. *Design Considerations:*

- The study focus on analysis of routing process.
- Analyzing the effects of changing the routing strategy to follow the trust instructions for the network.
- Simulating the trust scenario for the network.
- Analysis of result with the help of plotting of different graphs to follow the objectives. Ensuring the parameter analysis of the network.

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to maximize the network security by increasing the transmission security using trust management scheme. The proposed algorithm is consists of three main steps.

Step 1: The state of the simulation consists of node deployment and forming the network base. After which it create a source node with the help of cbr agent and creation of destination node with the help of null agent. These will not function until they are attached in pair, or source is attached to any destination.

Step 2: In the next step of proposed strategies, check if the trust value of nodes is available, if it is available, Select the shortest path with nodes having trust value(max. possible). This forms the path basis and provides the desired category for the path formation. Once, this is done to complete the communication process.

Step 3: If network is in its initial stage, that will be unable to have any trust value for any node, it this scenario, Select the shortest path for communication, start communicating through it, If the ack is received, update the trust values of nodes and again go to selection process . but if the ack is not received in that case a different path is choose, which is different from shortest path and this process continues until we get the desired path. After the completion of communicative tasks, the network stops.

III. PSEUDO CODE

```
Step 1: Deploy the nodes and form the network with the desired number of nodes.
Step 2: Create source node with the help of cbr agent and destination node by using null agent.
Step 3: Connect the desired pair of source and destination.
Step 4: If trust value >0
            Select the shortest path with nodes having trust value(max. possible)
        Else
            Include the shortest path with max. number of trusted nodes
Step 5: if available trust =0
            Select the shortest path
            If ack
            Update the trust values of nodes and go to step 4
            Else
            Select another path possible between source and destination
Step 6: stop communication.
```

IV. SIMULATION RESULTS

The Mobile Ad hoc networks may also experience packet loss due to parameters employed but that is reduced in case of proposed work implementation.

1 Throughput:

The average rate at which the total number of data packet is delivered successfully from one node to another over a communication network is known as throughput. The result is found as per KB/Sec. It is calculated by

Throughput= (number of delivered packet * packet size) / total duration of simulation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

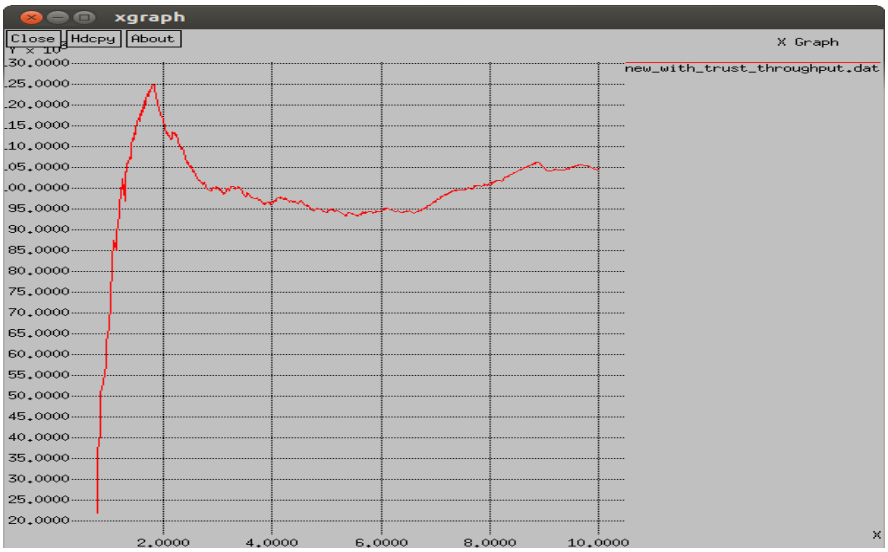

Fig 1: Throughput of Proposed algo.

This is the throughput graph of proposed algo and analysis that the values of throughput remains higher for the proposed algorithm for the complete plot.

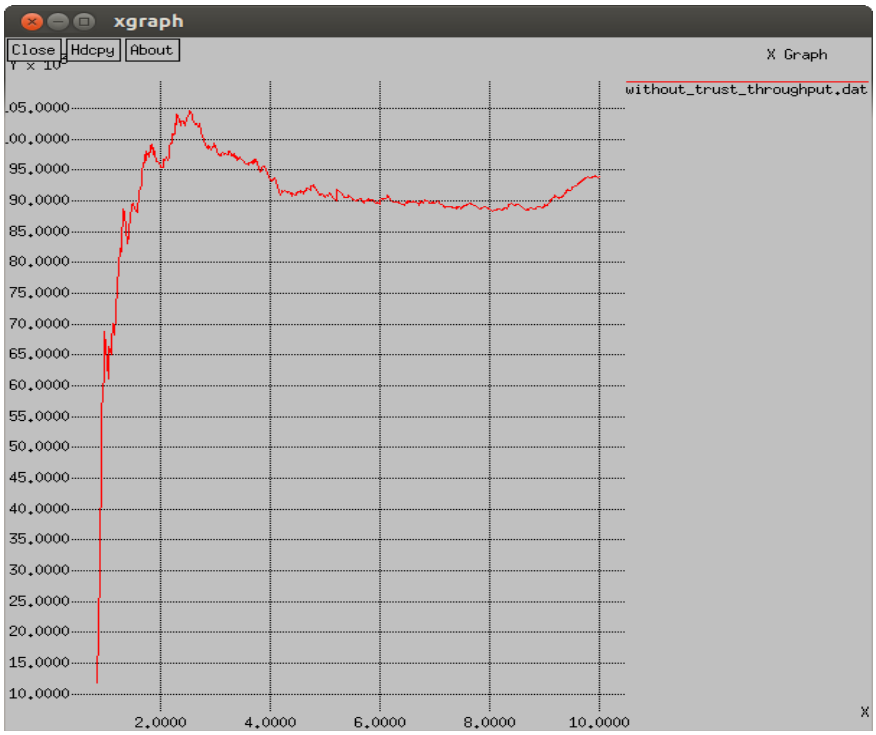

Fig 2:Throughput of simple DSR protocol observed

Above figures Fig 1 and Fig 2 shows the plot for throughput of the proposed algorithm and simple DSR. The values attained by these are different. Simple DSR attains a maximum value of 1.05 x 10^3 Kbps while the proposed algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

is capable of attaining 1.25 x 10^3 Kbps value for the throughput. Further the values attained by these two algorithms also differ. By comparing the values in the plot it comes as the analysis that the values of throughput remains higher for the proposed algorithm for the complete plot.

2 Packet delivery Ratio (PDR): This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation. It also describes the loss rate that of the packets, which in turn affects the maximum throughput that the network can support.
PDR= (Packets Received / Packets Sent)

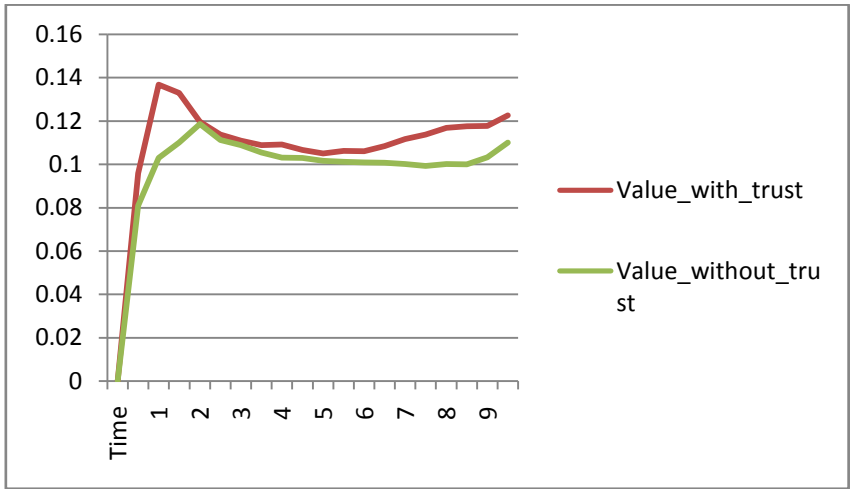

Fig 3: Comparison of PDR of Proposed algo with DSR

Fig 3 shows the comparison of PDR for the two algorithms, proposed having modifications in the DSR and simple DSR i.e. DSR as the standard one, without any modifications.The PDR for the Proposed algorithm remains higher than that of simple DSR and as the simulation is done in the same environment and under same parameters for the network, the plot proves the higher performance metric for the Proposed algo.

4 Packet Drop Ratio It is the ratio of the number of packet sent and the number of packets which are not received to the destinations

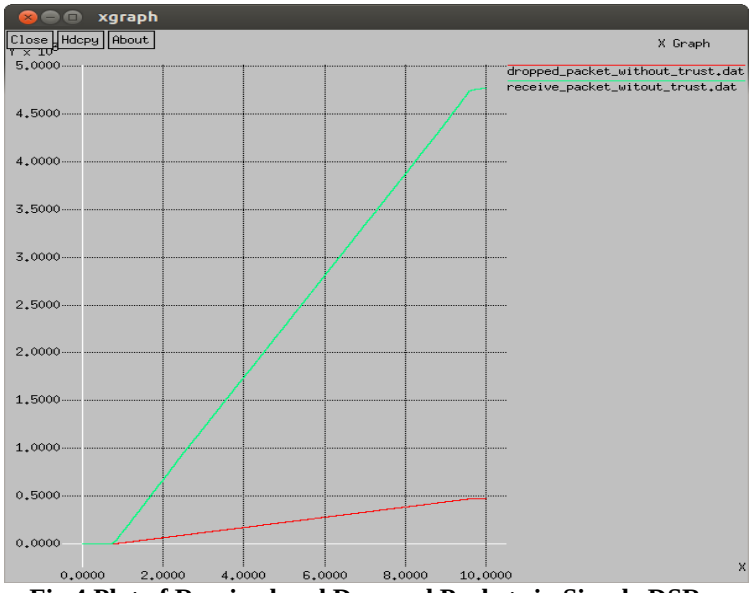

Fig 4 Plot of Received and Dropped Packets in Simple DSR

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

In Fig 4 , the line plot for the dropped packet is high due to which the slop for received packet is not so high which indicate that a large no of packets are dropped in this case.

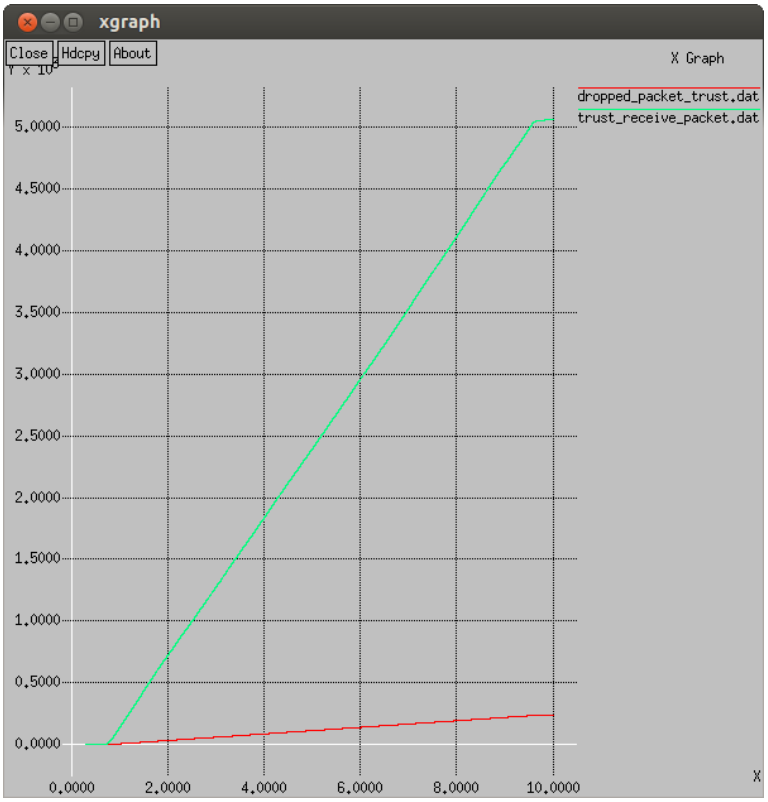

Fig 5: Plot of Received Packets and dropped packets in case of Proposed algo.

Fig 4 and Fig 5 provides the plot of received packets and dropped packets in case of simple dsr and Proposed algo. The line plot with higher slop provides the higher value indication while the line plot with lower slop indicate a less value. while in Fig 5 , the line plot of dropped packets have a very less slop due to which the line plot for the received packets have the higher slop.
So, the analysis provides the information that a high no. of packets are dropeed in case of simple DSR while a low no. of packets are dropped in case of Proposed algorithm. As a consequence high number of packets are received in case of Proposed algo. as compared to Simple DSR protocol.

V. SUMMARY

Here we show the different parameters average value for different parameters studied in case of simple DSR and the proposed algo implemented under DSR.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

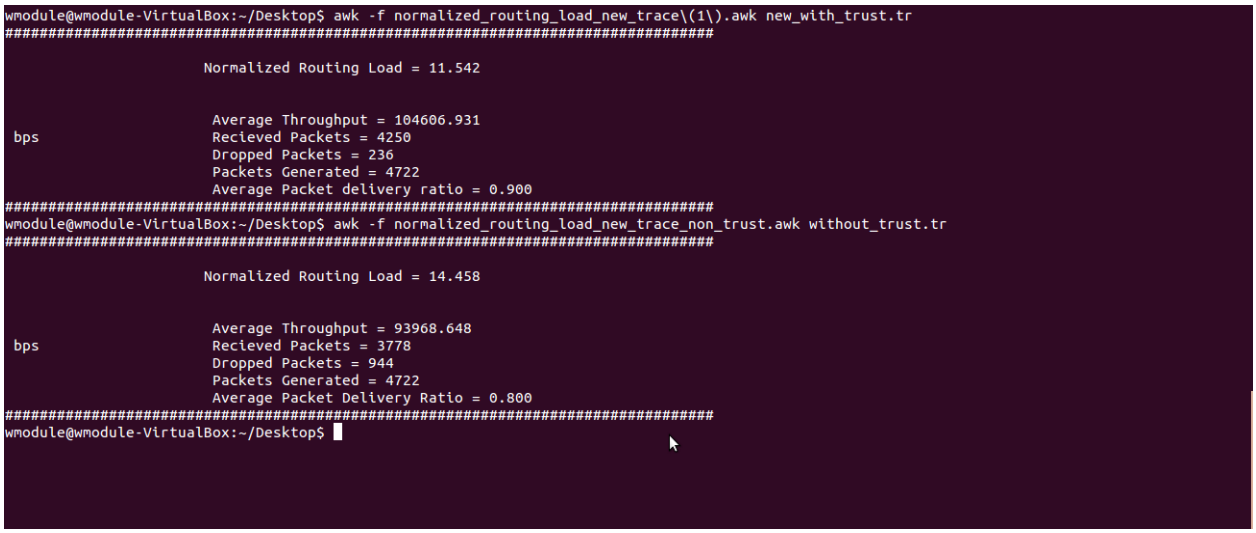

Fig 6 : Parameter studied in case of Proposed and simple DSR

Fig 6 provides the values of Normalized Routing load, Average Throughput, Received Packets, Dropped packets, Packets Generated and Average Packet Delivery Ratio. Firstly the result shown is for the proposed algo. and after that the results are shown for simple DSR protocol i.e. without trust.

VI. CONCLUSION AND FUTURE WORK

In this study, MANETs are susceptible to adversaries who can compromise nodes. The routing protocol is critical to MANETs performance. Therefore security is crucial, but it is also a hard task due to the nature of such networks. Trusted routing protocols are one means of providing security. A comprehensive work focusing on adapting reputation and trust-based systems for MANETs along with a critical evaluation of their strength and weaknesses is presented. This thesis presents an trust based on demand routing protocol called TBD. TBD depends on the self monitoring of each node to find out its trust value. The nodes trust values moves across the network during the route discovery messages without flooding the network with extra messages. The advantages of TBD are examined via simulation done over a network. The results show that TBD can effectively improve the energy efficiency and data delivery ratio. TBD has a better routing packet overhead than DSR because it does not require flooding the network with trust values inquiries.

REFERENCES

1. Sourish Mitra, Mounita Das, Rupa Mitra, Priyanka Maity, Alolika Banerjee(Department of Computer Science & Engineering, Gurunanak Institute of Technology, India), "Route maintenance and Scalability improvement of DSR, based on Relay node identification after locating Link-failure over MANET", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 21-27 www.iosrjournals.org
2. QI HAN, ABDULLAH GANI , NOR BADRUL ANUAR, OMAR ZAKARIA Faculty of Computer Science and Information TechnologyUniversity of Malaya, 50603, Kuala Lumpur, MALAYSIA, "Improving ACK Reply of DSR Protocol for Mobile Ad Hoc Network", Proceedings of the 8th WSEAS Int. Conf. on ELECTRONICS, HARDWARE, WIRELESS and OPTICAL COMMUNICATIONS
3. Thiyam Romila Devi, Rameswari Biswal, Vikram Kumar, Abhishek Jena,M.Tech, School of Electronics, KIIT University, Odisha, India,"IMPLEMENTATION OF DYNAMIC SOURCE ROUTING (DSR) IN MOBILE AD HOC NETWORK (MANET)", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308
4. Prof. M.Neelakantappa, Dr.B.Satyanarayana, Dr. A.Damodharam, Professor, BITS , Kunool,AP,India," Performance Improvement Techniques for Dynamic Source Routing Protocol in Mobile Ad Hoc Networks", International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009
5. Sharmin Sultana, Salma Begum, Nazma Tara, Ahsan Raja Chowdhury Department of Computer Science & Engineering, University of Dhaka, Dhaka, Bangladesh," Enhanced-DSR: A New Approach to Improve Performance of DSR Algorithm",International Journal of Computer Science and Information Technology, Volume 2, Number 2, April 2010
6. G.Lavanya, A. Ebenezer Jeyakumar," An Enhanced Secured Dynamic Source Routing Protocol for MANETS", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume X, Issue-4, September 2011
7. *David B. Johnson, David A. Maltz, Josh Broch,* Computer Science Department Carnegie Mellon University," DSR: The Dynamic Source Routing Protocol for
8. Multi-Hop Wireless Ad Hoc Networks"
9. Frank Kargl, Alfred Geiß, Stefan Schlott, Michael Weber, University of Ulm, Germany," Secure Dynamic Source Routing"

Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks"