A Secure Trust Based Routing Protocol for MANET

Ranjana Sharma
(Pursuing M. Tech, CSE)

Er. Anuradha Panjeta
(Assistant Professor, CSE)

Shree Siddhivinayak Group of Institutions,
Kurukshetra University, India

Abstract: **The aim of this piece of work is to compile a case study on MANET with a full proof solution to not only detect the malicious behaviour but also demolish it using reputation mechanism to multi Dynamic Source Routing protocol and also to detect the black hole attack in the node and to mitigate it by increasing throughput. The reputation is carried out on NS-2.34 and the performance is evaluated in the end on Throughput, Routing overheads, PDR ratio and Data Packets dropped.**

Keywords: DSR, Security, Trust, Routing, Attacks, Reputation.

This Paper carries various sections- Introduction is explained in section I, section II contains related work, section III comprises of Proposed Work, section IV described the Simulation Results and in the end Conclusion and Future Scope has been described under section V.

I. INTRODUCTION

Mobile Ad hoc Network is a vast network of various mobiles connected by wireless links also we may refer it as infrastructure less network. The routes between nodes may potentially contain multiple hops [11]. All devices in MANET work as a router and are free to move anywhere in any direction, though nodes mobility may cause the change in routes. The basic characteristic of MANET is dynamic topology. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. MANET is a network made up of various wireless mobile nodes which collectively work together to make transmission attainable between any of the nodes in the system [2]. Nodes communicate with each other with the direct shared wireless radio links [4]. Due to open and dynamic nature, this network is quite susceptible to number of malicious attacks. Information is transmitted from source to destination in the route via other nodes in the form of packets [1]. There are certain things which should be taken care of our Route selection, Request initiation, topology etc used in the system. Many routing protocols have been proposed to handle the network with large number of hosts also with limited resources like energy and bandwidth but no security consideration have been made, and then many routing protocols which are developed to secure the network.

Characteristics of MANET:

- Infrastructure less IP based network
- Autonomous behaviour- each node act as a host as well as a router
- Self-directed and decentralized wireless system
- Dynamic network topology- any nodes can leave and join network any time
- Highly reliable, stable and efficient
- Mobile and spontaneous behaviour
- This can be setup at any place and time
- Cheaper than wired network
- Good Network scalability

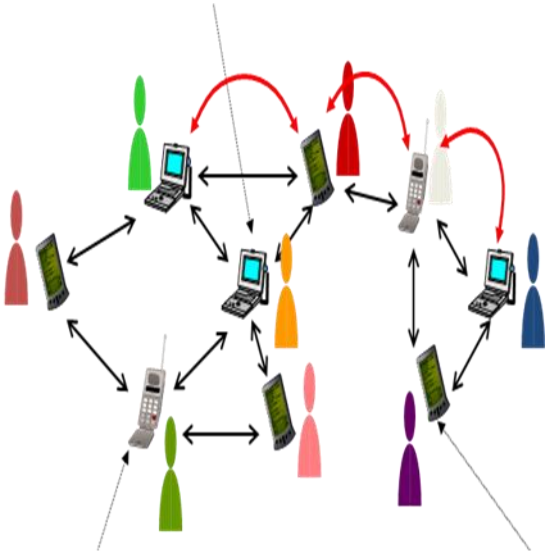

Fig. 1: Various nodes connected in MANET

Applications

- Education
- Tactical networks
- Emergency services
- Commercial and civilian
- Home and enterprise networking
- Entertainment
- Home applications
- Coverage extension

DSR protocol:

A reactive routing protocol that uses source routing to send packets is Dynamic Source Routing Protocol, here reactive means that it only requests a route when it needs one and does not require that the nodes maintain routes to destinations that are not communicating. It uses source routing, which means that the source must know the complete hop sequence to the destination. 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.

The DSR protocol operates in two procedures:

Route Discovery

Route Discovery is used whenever a source node requires a route to a destination node. First, the source node looks up its route cache to check whether if it already contains a route to the destination r not? Source sends the data packet only if the source finds a valid route to the destination. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message.

Route Maintenance

Route Maintenance is used to remove route breaks. When a node confronts a fatal transmission issue at its data link layer, it demolishes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. On receiving a route error message, it removes the hop in error from its route cache.

Advantages:

1. Route is found only when required.
2. All nodes get route cache information.
3. It reduces overhead.

Disadvantages:

1) Route mechanism does not repair the broken links.
2) Higher connection setup delay.
3) Inconsistency may appear in route construction phase.
4) If in case overhead occurs in this routing protocol, path length is directly affected.

II. Related Work

Nilesh N. Dangare.et.al (2015) Mobile ad-hoc network (MANET) is used widely today. The work of MANET is totally depends on the cooperation of various nodes in the network. As we compared with the wired network, wireless network has various advantages, such as MANET doesn't require any infrastructure; it is decentralized system and dynamic in nature. Hence MANET is popular in various areas such as Military application, wireless sensor network, Public network and more. But these advantages of MANET may become disadvantages: As its openness, decentralized and dynamic nature, it is highly prone to various attacks. That's why security is the challenging job in MANET. Various existing system for detection of attacks is in-efficient and may require more computation and space as in cryptography technique. In this paper, the focus is given on the Trust based approach to mitigate the attack. In Trust based approach, the most trusted path is selected rather than the shortest path [1].

R. Menaka.el.al (2013) Collaboration and cooperation is critical and challenging in managing trust in a distributed Mobile Ad Hoc Network (MANET). This is also critical in achieving mission and system aims like reliability, availability, scalability, or re-configurability. Defining and managing trust in a MANET requires consideration of interactions between composite social, information and communication networks and also considers resource constraints like computing power, energy, bandwidth, and dynamics. This paper discusses concepts and properties of trust and provides a survey of MANET developed trust management schemes. The accepted classifications, potential attacks, and trust metrics in MANETs are discussed [7].

Mohammed S. Obaidat.el.al (2012) Securing the routing of message in mobile ad hoc networks (MANETs) is still a challenging issue. This paper proposes an enhanced trust-based multipath Dynamic Source Routing (DSR) protocol (so-called ETBMDSR) to securely transmit messages in MANETs. The author's method consists in a combination of soft-encryption, novel trust management strategy, and multipath DSR routing. Simulation results are presented to validate our proposal, showing that our ETB-MDSR scheme outperforms a recently proposed Trust-Based Multipath DSR message scheme (TB-MDSR), in terms of route selection time [9].

Isaac Woungang.et.al (2012) Mobile ad hoc network (MANET) is a collection of mobile nodes that communicate with each other without any fixed infrastructure or a central network authority. From a security design perspective, MANETs have no clear line of defence; i.e. no built-in security. Thus, the wireless channel is accessible to both legitimate network users and malicious attackers. In this paper, a novel scheme for Detecting Black hole Attacks in MANETs (so-called DBA-DSR) is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes. Simulation results are provided, showing that the proposed DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput, chosen as performance metrics, when black hole nodes are present in the network [6].

Mehdi Keshavarz.et.al (2012) Free-riding by packet dropping is one of the most important issues for the establishment and survivability of the open multi-hop wireless networks. In this paper, we focus on the data packet dropping in a rather dense Mobile Ad-hoc network. To encounter this situation, we propose a scheme based on using MAC-layer acknowledgements to detect and punish packet dropper nodes. The author used simulation-based results to evaluate the performance of our scheme. All simulations have been performed using NS-2 [8].

R. Sudha.et.al (2011) Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV and TORA However, the majority of these MANET secure routing protocols did not provide a complete solution for all the MANETs' attacks and assumed that any node participating in the MANET is not selfish and that it will cooperate to support different network functionalities. Much work is going on to provide security to the network. One of the solution to the problem is ARAN –(Authenticated routing protocol) which is a secure protocol and provides Integrity, availability, Confidentiality, Authenticity, Non repudiation, Authorization &Anonymity but an authenticated selfish node can infer to this protocol performance and can disturb the network by dropping packets. This paper discusses Temporal table based schemes that can be applied to ARAN to detect selfish node and improve the performance [4].

Ramasamy Mariappan.at.al (2011) In this paper, the author presented new protocol design scenario like Re - Pro Routing Protocol (RPRP) for Broadcasting in wireless mobile Ad-hoc Network and a comparative performance for Mobile Ad hoc Networks protocols like as Ad-hoc On-Demand Distance Vector Routing protocol focusing on the effects of changes such as the increasing number of receivers or sources and increasing the number of nodes. Although some simulation results of MANET protocols have been published before, these protocols have not been compared in isolation. A systematic performance evaluation of these protocols is done by performing certain simulations and the trust methods are one of the security methods in mobile Ad-Hoc networks and these methods are prone to security risks but have found their acceptance due to efficiency over computationally expensive and time consuming cryptographic methods. The major problem with the trust methods is the period during which trust is growing and is yet to reach the requisite threshold. This paper also proposes security mechanism dependent upon Electronic Code (EC) combined with permutation functions. The proposed mechanism has low time complexity, is easier to implement, computationally inexpensive and has very high brute force search value [5].

Poonam, K. Garg.et.al (2010) 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 secure routing is a must for such networks. 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, the author presented a unique trust based method which is not vulnerable to this behaviour. In this method, each node broadcasts a RREQ packet if it is received from different neighbours. 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 behaviour observed by its neighbouring nodes and the number of nodes in the route. The author evaluated the misbehaving node detection rate and the efficiency of our method along a number of parameters. Results show that his method increases the throughput of the network while discovering a secure route [2].

SHEN Ming-yu.et.al (2010) This paper published by the author describes the Authentication Test Theory of strand space firstly and the theory is expended because of the demands of mobile ad hoc network routing protocol security analysis. By analyzing the existing security DSR routing protocol leaks, a new Ariadne-S protocol model is proposed based on Ariadne routing protocol. And finally it is proved that the returning routing information from the process of routing finding are secure and credible by using strand space model [3].

III. PROPOSED WORK

My proposed work is to apply reputation mechanism to DSR and evaluate its performance. In this work we also considering the malicious nodes, those are not only silently dropping the packet, but also attacking the routing layer. We are dealing with more aggressive routing level attack, in which a black hole actively replying the route discovery requests advertise itself as attractive route having shortest number of hops to destination and higher DSR sequence number.

Basic Algorithm to Mitigate Black Hole Attack

```
1. Source Node broadcasts fake RREQ;
2. IF Source Node receives RREP for fake RREQ
3. Source Node checks the RREP packet for the address of
   the node
   Initialized RREP and marks the node as malicious;
4. Else
5. Continue sending the normal RREQ;
6. IF RREP from Destination Node
7. Consider the route to be safe and start routing the data
   packets;
8. Else IF RREP from Intermediate Node
9. Send an Acknowledgement to the Destination Node along
   the route;
10. IF reply to the Acknowledgement is received
11. Consider the route to be safe and start routing the data
    packets;
12. Else
13. Restart the process to identify malicious node;
```

IV. SIMULATION RESULTS

In this section we examine the performance of various parameters like PDR, Throughput etc using Reputations in DSR over Base DSR.

The values used for various parameters of the simulation experiments are described in the Tables and so on graphs are made so as to show the betterment done.

Table I: Comparative Values for Evaluating Throughput in the Simulation Experiment

Pause Time	DSR	RepDSR
0	0.5	0.7
100	0.6	0.9
300	0.75	0.9
600	0.75	0.9
900	0.6	0.8

GRAPH I: EVALUATING THROUGHPUT OVER INCREASING PAUSE TIME

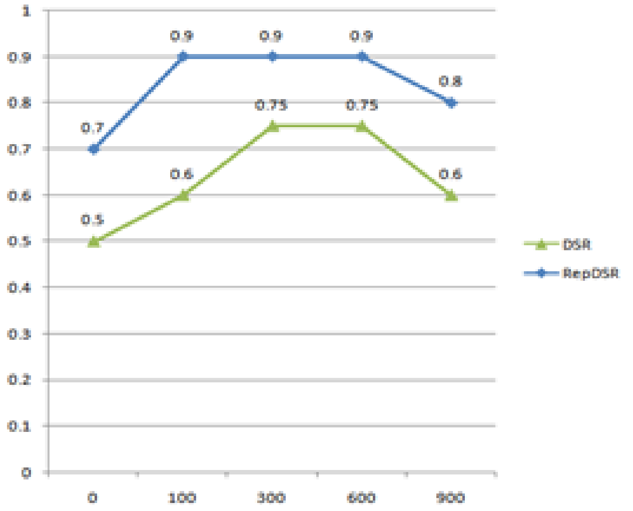

Fig. 2: Graph showing better Throughput

This graph shows that Repudiation DSR has higher throughput than normal DSR used previously over increasing pause time.

Table II: Comparative Values for Evaluating Routing Overheads in the Simulation Experiment

Pause Time	DSR	RepDSR
0	0.9	0.7
100	0.8	0.6
300	0.4	0.2
600	0.3	0.1
900	0.25	0

GRAPGH II: EVALUATING ROUTING OVERHEADS

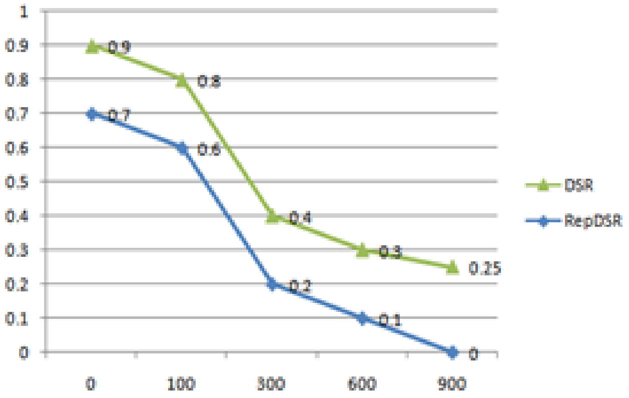

Fig. 3: Graph showing less Routing Overheads

In this graph, we may notice that RepDSR has comparatively less routing overhead in comparison with base DSR. Lesser the routing overhead more efficient the system will be.

Table III: Comparative Values for Evaluating Data Packet Drops in the Simulation Experiment

Pause Time	DSR	RepDSR
0	9000	8800
100	10000	9800
300	11800	8200
600	10000	8000
900	12200	9000

GRAPH III: EVALUATION OF DATA PACKET DROPS

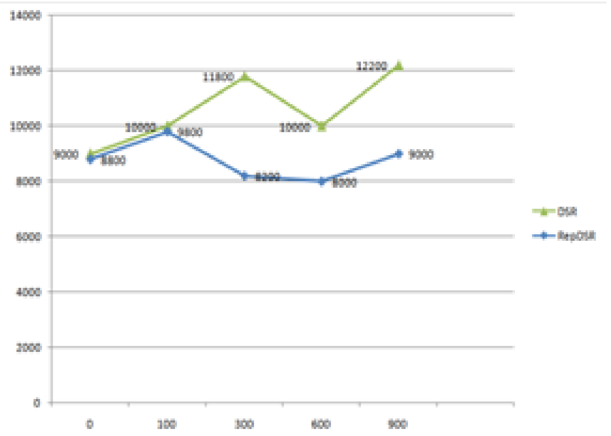

Fig. 4 Graph showing Less Data packets dropped

In this graph, we may notice that data Packet dropped in RepDSR is comparatively lesser than DSR. Thus we come up with much reliable system.

Table IV: Comparative Values for Evaluating Packet Delivery Ratio in the Simulation Experiment

Pause Time	DSR	RepDSR
0	75	75
100	70	70
300	68	72
600	68	72
900	60	72

GRAPH IV: EVALUATION OF PACKET DELIVERY RATIO

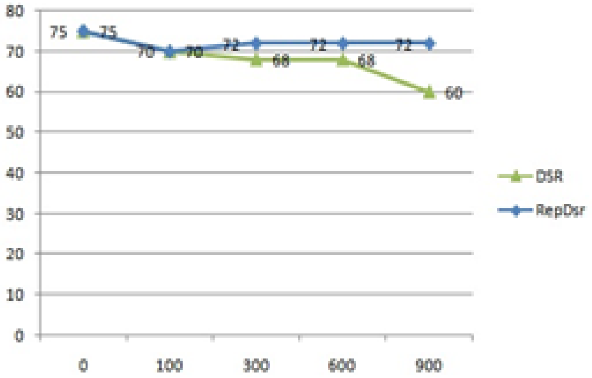

Fig. 5: Graph displaying high PDR in RepDSR

This graph shows that Repudiation DSR has higher Packet delivery Ratio than normal DSR used previously over increasing pause time.

V. CONCLUSIONS & FUTURE WORK

DSR is enhanced using NS2 simulator by the concept of Repudiation and not only detecting but also mitigating the malicious nodes from the system. The proposed evaluation is done and is shown on various metrics: Throughput, Packet Delivery Ratio, Data Packets Dropped and Routing overheads. The RepDSR is compared with Base DSR and gave better outcomes.

This evaluation can be extended further by evaluating the rest of the metrics like Average Delay, Network Resource Load etc.

REFERENCES

[1] Nilesh N. Dangare M. Tech. (CSE) BDCOE, R. S. Mangrulkar Associate Professor Head Comp. Engg, BDCE, “Design and Development of Trust Based Approach to Mitigate Various Attacks in Mobile Ad-hoc Network”, International Journal of Computer Applications (0975 – 8887) International Conference on Quality Up-gradation in Engineering, Science and Technology (ICQUEST2015).

[2] Poonam, K. Garg, M. Misra, Indian Institute of Technology Roorkee, India “Trust Based Multi Path DSR Protocol”, 2010 International Conference on Availability, Reliability and Security.

[3] SHEN Ming-yu, LI Cang-yuan, School of Computer & Information. Hefei University of Technology Hefei, China, “Research and Analysis On Secure DSR Routing Protocol Based on Strand Space”, 2010 International Conference on Electrical and Control Engineering.

[4] R. Sudha, S.Lecturer, CSE, Dr.Pauls Engineering College. Villupuram, Dr. D. Sivakumar, Professor & Head Department of IT, Adhiparasakthi Engineering College. Melmaruvathur, “A Temporal table Authenticated Routing Protocol for Adhoc Networks”, 978-1-4577-1894-6/11/$26.00©2011 IEEE.

[5] Ramasamy Mariappan Sangameswaran Mohan Professor, Department of CSE Department of CSE Adhiparasakthi Engineering College, Melmaruvathur, “Re-Pro Routing Protocol with Trust Based Security for Broadcasting in Mobile Ad hoc Network”,978-1-4673-0671-3/11/$26.00©2011 IEEE.

[6] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, Mohammad S. Obaidat, “Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks”, 978-1-4673-1550-0/12/$31.00 ©2012 IEEE.

[7] R. Menaka, Dr. V. Ranganathan, “A Survey of Trust related Routing Protocols for Mobile Ad Hoc Networks” International Journal of Emerging Technology and Advanced Engineering,ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.

[8] Mehdi Keshavarz, Mehdi Dehghan, "MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks" 978-1-4673-0682-9/12/$31.00 ©2012 IEEE.

[9] Isaac Woungang, Mohammed S. Obaidat, Sanjay Kumar Dhurandher, Han-Chieh Chao, Chris Liu, "Trust-Enhanced Message Security Protocol for Mobile Ad Hoc Networks" 978-1-4577-2053-6/12/$31.00 ©2012 IEEE.

[10] Priyanka Goyal, Sahil Batra and Ajit Singh “A Literature review on Security Attack in Mobile Adhoc Networks” International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010

[11] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma “Review of Various Routing Protocols for MANETs” International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011

[12] Gurpinder Singh, Asst. Prof. Jaswinder Singh “ MANET: Issues and Behavior analysis of Routing Protocols”, IJARCSSE, ISSN: 2277 128X, Volume 2, Issue 4, April 2012

[13] Hrituparna Paul, Dr. Prodipto Das ‘Performance Evaluation of MANET Routing Protocols”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012

[14] Ankur O. Bang , Prabhakar L. Ramteke “MANET : History,Challenges And Applications” IJAIEM, Volume 2, Issue 9, September 2013

[15] Aarti ,Dr. S. S. Tyagi “ Study of MANET: Characteristics, Challenges, Application and Security Attacks”, Volume 3, Issue 5, May 2013