



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Enhanced More Secure Trust Based Routing Scheme for DSR Protocol in MANETs

Ankita Sahu, Vikas Sejwar
Department of CSE / IT,
Madhav Institute of Technology and Science, Morar, Gwalior,
Madhya Pradesh, INDIA.

Abstract: A Mobile Ad hoc Network (MANET) is a group of movable hosts with wireless network interfaces that structure a temporary network without the support of any permanent infrastructure or central administration. A MANET is also referred as an infrastructure less network because the mobile nodes in the network dynamically locate paths among themselves to transfer packets provisionally. In this paper we evaluate the routing paths of nodes to some features before to transmit data to these routes. Experimental results show that our gateway based DSR improves network performance to much extent.

Keywords: Mobile ad hoc network security; Trust feature; DSR Protocol; RREP; RREQ;

I. Introduction

Mobile Ad hoc Networks (MANET) are placed to set up wireless communication in improvised scenario without a predefined centralized administration or infrastructure [1]. MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes [2]. MANET is a self organizing network of mobile nodes forming a temporary network. MANET has many salient features which make it different from other networks and enforce many constraints on it. These features include lack of infrastructure, dynamic topology, bandwidth constraint, power constraint etc. The most challenging task in such a dynamic network is routing. Many routing protocols have been proposed and optimized till date and constantly undergoing further evolution. DSR (Dynamic Source Routing) [3, 4] is the most famous and basic routing protocol which works on on-demand paradigm. In this paper the basic functionality of DSR is appended with some intelligent decisions which ultimately lead to energy conservation. Thus this modified approach is called IDSR (Intelligent Dynamic Source Routing).

II. Dsr Overview

Wireless routing can be broadly classified into two types: Proactive and Reactive. DSR [3, 4] is a reactive protocol i.e. it works only when a node wishes to send data or whenever there is a link failure. This is called "on - demand" approach of routing protocol. This method is effective in contrast to proactive protocols which use table based approach producing large routing overhead. DSR is based on source routing [5, 6] in contrast to hop-by hop routing. In source routing the source collects the complete knowledge of the path to be travelled by the packet. The source appends this path information in the packet header. Thus every packet generated by source has complete path information specifying the identity of all the intermediate nodes to be visited before reaching its destination. The traditional DSR consists of two phases: Route discovery and Route maintenance.

A. Route Discovery

This phase allows a source to dynamically discover a path to the destination node. The process begins with generation of RREQ (Route Request) packet. It contains Request ID, sequence number, source ID, destination ID. This packet is then broadcasted to all the neighbor nodes. A node which receives this packet appends its own ID in packet header and forward RREQ to its neighbors. Finally RREQ packet reaches its destination. The destination node generates RREP (Route Reply) and sends it to the reverse path travelled by RREQ packet. Each node maintains a route cache and caches the path when RREP travels through them.

B. Route Maintenance

This phase works whenever there is a link breakage/failure in the network. An intermediate node upon discovering a link failure generates RERR (Route Error) packet and sends it to the source using the path stored in its cache. All the intermediate nodes delete their cache entry for the failed link upon receiving RERR. Traditional DSR works quite efficiently but there is always a scope of improvement. If any one of the internal nodes dies out of energy while the communication is established then the whole process will be interrupted and

again the path has to be chosen for the specified source to destination. Moreover traditional DSR is based on minimum hop count; it does not bother about the nodes' residual energy and treat all nodes equivalent.

III. Related work

Mittal *et al* [7] developed the routing protocol which can deal with single and cooperative black hole attack and also without degrading the performance of such networks. The approach provides a feasible solution for the Black hole node detection within the network by making use of "reputation tables" and assigning reputation values to the participating nodes. It improved the routing security of the existing association based DSR protocol using the concept of reputation of nodes value, by identifying and isolating black hole nodes working in a group. Xu Xiang *et al.* [8] performed a work, "Providing Efficient Secure DHTs Routing". Authors propose a secure protocol which consists of two phases: detecting malicious nodes and bypassing them. Author present a novel efficient routing strategy called tracer routing to control routing progress, accompanied by a node-ID based signature scheme. Combine these two; the source of every query can verify each step and malicious nodes can be identified. Authors also present a scheme to create a secure path to bypass malicious nodes.

Yanzhi Ren *et al.* [9] performed a work, "Detecting Black hole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording". In this paper, Authors present a technique that provide the security from history records of packet delivery information at each contact so that other nodes can detect insider attacks by analyzing these packet delivery records. Author evaluated Presented approach through extensive simulations using both Random Way Point and Zebranet mobility models. Presented results show that Presented method can detect insider attacks efficiently with high detection rate and low false positive rate.

Lanjun Dang *et al.* [10] performed a work, "DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks". In this paper, Authors present a new distributed anonymous secure routing protocol with good scalability for mobile ad hoc networks. The proposed protocol addresses the problems of anonymous routing and later anonymous data transmission via a dynamic identity pseudonymity approach based on Incomparable Public Keys. Good scalability is achieved by using Diffie-Hellman key exchange scheme and symmetric key cryptography, instead of public key cryptography.

Saurabh Gupta *et al.* [11] performed a work, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network". In this paper, Authors propose a protocol for avoiding black hole attack without the constraint of special hardware and dependency on physical medium of wireless network. BAAP forms link disjoint multi-path during path discovery to provide greater path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network.

Rajesh Yerneni *et al.* [12] performed a work, "Enhancing performance of AODV against Black hole Attack". In this paper, a method is proposed called Secure-Ad hoc on demand Distance Vector (SAODV) algorithm that mitigates black hole attack by analyzing destination sequence number and validating the destination by random value. Simulation results show that the proposed protocol provides better security by increasing the packet delivery ratio when compared to AODV in presence of black hole attacks.

IV. Proposed Methodology

In this section, we present our friendship-based framework proposed to secure DSR .

Proposed Technique

- 1) In proposed technique for DSR, Start with source node sends RREQ to their neighbor's.
- 2) All nodes update their Routing table.
- 3) Here we calculate the trust from $[f-(d+m)]/f$
- 4) If value for trust is greater than trust worthy path.
- 5) Malicious node, do not accept RREQ.
- 6) In that condition do not listen the node.

Two algorithms are used here forward and reverse routes respectively in DSR protocol.

STEPS OF OUR ALGORITHM:

STEP 1:

S is the source node. D is the intended destination

STEP 2:

S sends the data packets to neighbors and update its routing table as per the forwarding packets number

STEP 3:

The neighbors also forward the routing packets further and the trust value is calculated as per the following formula of step 4

STEP 4:

Trust parameters

f= number of packets forwarded

d=number of packets dropped

m=number of packets misrouted

4.1: Collect data for f,d,m.

4.2: Calculate total number of packets which were dropped or misrouted i.e (d+m)

4.3: Calculate total number of packets which were successfully reached to the destination i.e (f-{d+m})

4.4: Calculate direct trust by using formula

$$\text{Trust (t)} = [f - (d + m)] / f \dots\dots\dots(1)$$

STEP 5:

If the value of the calculated trust exceeds the obtained value then it does not forward it to the next nodes and considers it as malicious. So the path becomes malicious gateway path. All neighbors are informed not to forward data packets via that route.

STEP 6:

If the obtained value is less than the threshold then the packets are forwarded and that gateway or path is considered as path of maximum trust.

STEP 7:

In case when maximum values are trust values then obtained maximum valued data packets are forwarded first and considered as path or gateways of that route.

V. Simulation Result

Nasty nodes create the following types of attacks against data and control packets:

1. Modification Attack. These attacks are carried out by adding, altering or deleting IP addresses from the ROUTE REQUEST, ROUTE REPLY, ROUTE ERROR and Data packets that pass through the malicious nodes.
2. Black Hole Attack. In this attack the malicious node drops all packets, which it is supposed to forward.
3. Grey Hole Attack. Here the malicious node selectively dumps data and control packets at random intervals. All malicious nodes work in a non-colluding manner. Each malicious node sporadically alters its attack profile by randomly switching between the three types of attacks.

metrics used include:

1) *Packet Drop*:

It is a kind of denial of service attack in the packets i.e. the packets that were dumped by malicious nodes without any notification.

2) *Packet delivery ratio (PDR)*:

The PDR in this simulation is defined as the ratio between the number of packets sent by constant bit rate sources and the number of received packets by the CBR sink at destination. It describes percentage of the packets which reach the destination.

$$\text{PDR} = \Sigma \text{CRB PktRecv} / \Sigma \text{CRB PktSent}$$

3) *Packet forwarding*:

It is defined as the forwarding or direction of the packet traffic to the further nodes or neighbors to reach the destination

4) *Packet Sent*:

This is the correct forwarding of the packets to the group of nodes (multicast and broadcast) between the control packets and the data packets received during the simulation time.

5) *Packet Receive*:

It is the fraction of packets that were obtained by nodes after the multicast or broadcast.

6) *End to End Delay*:

It is defined as the difference between two time instances: one when packets generated at the sender and the other, when packet received by the receiving application.

The results are shown as:

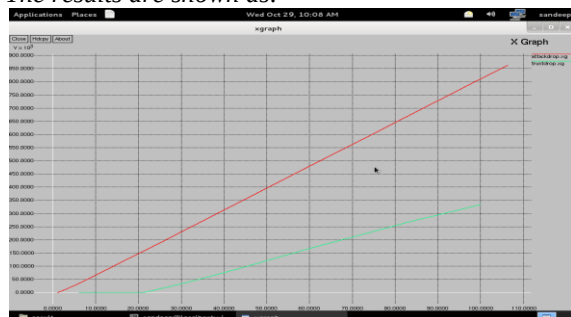


Fig. 1: Packet drop

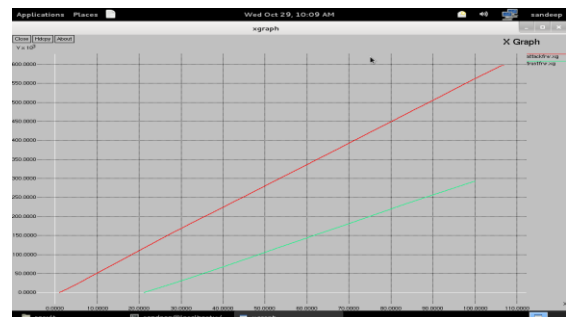


Fig. 2: Packet forward

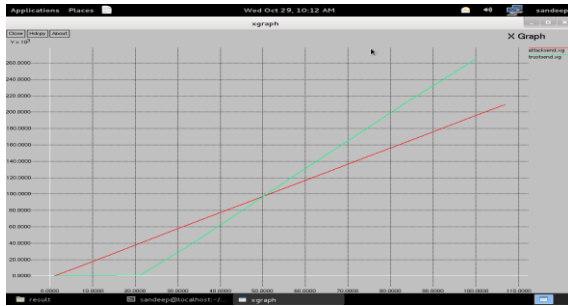


Fig. 3: Packet send

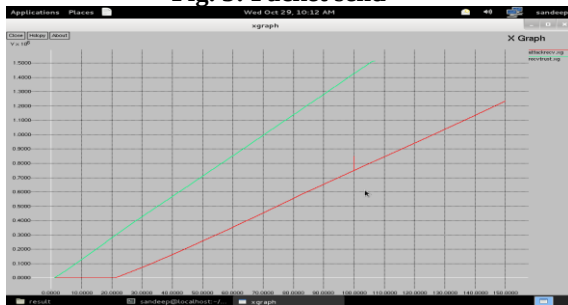


Fig. 4: Packet receive



Fig. 5: Pdr (Packet delivery ratio)

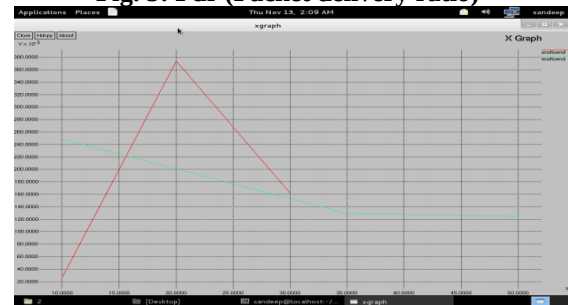


Fig. 6: End to End Delay

VI. Conclusion

In last few years, MANETs has gained much more attention in research community. There are many active research projects concerned with MANETs. MANETs are wireless networks that use multi-hop routing in place of static networks infrastructure to provide network connectivity. MANETs applications is mostly used in dynamic military and civilian systems. In MANETs the network topology usually varies with time. MANET is facing new challenges in routing protocols because traditional routing protocols may not be suitable for MANETs. In this paper, an overview of DSR in MANETs is present. Using DSR, the overhead is reduced and also eliminate the malicious node. By this trusted route between source and destination is created, that provide secure communication network. In simulation result we have found that the throughput of our proposed protocol remains notably higher than that of the standard DSR protocol in the presence of malicious nodes.

References

- [1] Zhao, Z., Hu, H., Ahn, G. J., and Wu, R. Risk-aware response for mitigating MANET routing attacks. IEEE Conference In Global Telecommunications (GLOBECOM 2010), December 2010, pp. 1-6.
- [2] Mohapatra, P., Li, J., and Gui, C. QOS in Mobile Ad hoc Networks. IEEE Wireless Communications, June 2003, 10(3), pp. 44-52.
- [3] D. B. Johnson and D. A Maltz, "Dynamic Source Routing in ad hoc wireless networks." in Mobile computing (Imielinski and Korth,), eds vol. 353. Kluwer Academic Publishers, 1996.
- [4] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", Experimental RFC 4728, Internet Engineering Task Force (IETF), February 2007.
- [5] Roy C. Dixon and Daniel A. Pitt., "Addressing, bridging and source routing". IEEE Network, 2(1):25-32, January, 1988.
- [6] Mittal, S., and Taluja, H. Analysis of Cooperative Black Hole Attack Using Dynamic Source Protocol. International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), August 2012, 2(8), pp. 139-142.
- [7] Xu Xiang," Providing Efficient Secure DHTs Routing", 2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 © 2009 IEEE (pp 510-514)
- [8] Yanzhi Ren," Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", 978-1-4244-7265-9/10@2010 IEEE .
- [9] Lanjun Dang," DASR: Distributed Anonymous Secure Routing with Good Scalability for Mobile Ad Hoc Networks", 2010 IEEE Asia-Pacific Services Computing Conference 978-0-7695-4305-5/10© 2010 IEEE (pp 454-461)
- [10] Saurabh Gupta," BAAP: Blackhole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCT)-2011 978-1-4577-1386-6/11©2011 IEEE (pp 468-473)
- [11] Rajesh Yerneni," Enhancing performance of AODV against Black hole Attack", CUBE 2012, September 3-5, 2012, Pune, Maharashtra, India. Copyright 2012 ACM 978-1-4503-1185-4/12/09 (pp 857-862) .
- [12] Yang H, Meng X, Lu S (2002) Scane: Self organized network-layer security in mobile ad hoc networks. In Proceedings of the 1st ACM workshop on Wireless security, WiSe '02, pp 11-20, New York, NY, USA. ACM