Impact of Malicious Node in MANETs

Anshu Chaturvedi
Department of Computer Applications
MITS, Gwalior, India

ABSTRACT

MANETs are known to possess unique and many vulnerable features. In such a case, security is again another crucial issue to be tackled. The attacks can affect the performance of the network critically. This paper therefore proposes a solution for maintain the optimum performance of the network even in presence of malicious nodes by modifying the existing DSR protocol. The simulation is performed in NS-2. The results of the scheme show that the network performance is not affected and proposed solution handles it well.

Keywords

Adhoc network, Security, Malicious, throughput, performance.

1. INTRODUCTION

An ad hoc network is formed spontaneously by a group of two or more mobile devices incorporating wireless interfaces. These devices, also referred to as Nodes, may communicate directly if they are within radio range of each other. However for communication outside this range they have to depend on some other nodes to relay the messages. Nodes in MANET are free to join, leave or change their current location and thus move around arbitrarily. Consequently, we have a network with frequently changing network topology. Unlike wired environments, there is no primary network infrastructure to carry out routing functions also. Rather, each node needs to serve the functions of a router as well to forward messages sent by other nodes. The dynamic and infrastructure less nature of the ad hoc network pretence many peculiar problems and challenges.

The nodes in MANET are of heterogeneous nature. This ultimately leads to amplify the vulnerability of MANET. The data capturing or interfering with the communication is possible because of the open accessibility of MANET's connective links. On the other side, these unwanted interactions consume power and consequently lessen the survivability of the network. Security in MANET is itself a crucial aspect with its own hindrance because of the vulnerable features of Ad hoc networks and therefore in this work we are trying to evaluate security issues related to malicious nodes.

Unlike wired networks where an attacker is required to go through some type of authentication before gaining physical access to the network or has to bypass through several lines of defence at firewalls and gateways, attacks on a wireless network are easy to launch, since they do not involve physical boundaries. Furthermore, it is easier to launch attacks on MANETs than on infrastructure based wireless networks because there is no central base controlling identity of participant nodes.

In order to achieve an adequate performance in such an environment, It is required that routing protocols should be able to handle both the dynamic nature of the environment, and probable existence of malicious nodes which do not cooperate with other nodes and try to disturb the normal working of the network. The mobility of the nodes can lead to breakage of existing links and discovered paths after a while. Many existing proposals deal well with the dynamic nature of ad hoc networks, conversely, the majority of these routing protocols to not take security in consideration and presuppose that all nodes in the network are cooperative and trustworthy. In this regard, the proposed scheme makes some changes by introducing two modules in the DSR routing protocol to handle these malicious nodes. The simulation results of the modified DSR shows that these changes are giving better performances than the original DSR. Hence, the proposed scheme is efficient enough.

2. RELETED STUDY

In general scenario of security numerous solutions are given by researchers in Mobile ad hoc network. The authors in [1] have given a proposal to use threshold cryptography for offering security to the network. A method is designed in [2] that try to provide equal authority to issue certificates to the members of the ad hoc group, and thus assures equal participation of all the nodes. Secret sharing based ad hoc routing protocol is proposed in [3] but the assumptions made here are unfortunately erroneous. Fundamentally, it is that each node cannot copy the MAC address of numerous other nodes. A common structure for secure ad hoc routing is designed in [4]. In [5] the authors have discussed the routing security issues in MANETs and have given a solution of black hole problem. The security concerns associated with multihop network connectivity are identified and a discussion of the challenges to security design is given in [6]. A suggestion Random Walker Detector (RWD) [7] also works on monitoring the node's action to ensure if a node is under attack or not.

In this regard, there can be certain nodes that behave selfishly, i. e. the nodes take part in the normal route discovery but forward packets according to their choice. In other words, these nodes selectively forward packets in order to save their battery. A lot of work is being done over selfish nodes as well. Yet the selfish routing also suffers with certain problems [8]. It is this that the routing decisions here are taken in node's local viewpoint and do not take into consideration the global network scenario. Consequently, the system gets suboptimal behaviour. [9] Depicts some of the research work that dealt with finding out the consequences of selfish routing on network's efficiency. [10] Shows the result of how selfish routing can hamper with the performance of network.

Apart from these certain specific protocols such as SEAD (Secure Efficient Ad Hoc Distance Vector Routing Protocol) [4], SAR (Secure-Aware Ad Hoc Routing protocol) [11], ARAN (Authenticated Routing for Ad Hoc Networks) [12], ES-AODV (Efficient Security Ad-Hoc On-Demand Distance Vector) [13] are also proposed that intend to provide security to the network with the utilization of concepts like certification system, cryptography and other security solutions.

The security solutions to monitor malicious behaviour in ad hoc network also include Intrusion Detection System [14]. The database of IDS maintains the profiles consisting of the normal behaviour of a node. These IDS are based on anomaly and existence of any anomaly in the profiles maintained validates an attack. .

3. PROPOSED WORK

This paper proposes modification to the standard DSR protocol to handle security related issues. It consists of two modules namely: - Identifier and Verifier. The role of the Identifier is to detect malicious behaviour of neighbouring node. For this purpose, it utilizes the promiscuous mode, i.e. the node can listen to all the packet transmission of neighbouring nodes. The identifier looks for some malicious activity such as packet dropping, performed by these nodes and sets a suspicious flag for such nodes. It then send request to the verifier. The verifier then collects the trust values from all the nodes in the network and decides whether to continue communication with such nodes or not. The detailed working of the identifier and verifier is given next.

Identifier:

The module identifier is based on the promiscuous mode working. It maintains the table of packets forwarded to the next node. The structure of the table is as given below. It stores Sequence number Sq of the packet, Time t at which the packet was sent and packet p itself.

Sq	***t***	***p***

Fig 1: Structure of the table stored

Whenever identifier listens a packet from it's neighbor, it matches the sequence number Sq of the listened packet with that of the packet stored in the table. If a match is found, it sends a message to the verifier to increment and update the trust value for the node from which the packet was listened. Now it removes that packet entry from it's table. A time out period t-out is defined by the identifier. If a match is not found and a timeout has occurred, it sets the suspicious for such nodes. Also it asks the verifier to decrement the trust value for such nodes and look for the status of such nodes. It is also possible that the identifier is not able to listen to the packet because the neighbor node has moved out of the range. For such situations also, this work informs the verifier with the suspicious flag set for such nodes.

Verifier:

The verifier maintains two tables trust value table for the neighboring nodes and route error table for the nodes for which RERR message is generated. The structure for the tables is given below.

Node_ID	***Trust_value***

Fig 2: Structure of the trust table

Node_ID is the address of the neighboring node, Trust_Value is the value of trust for that node. The initial trust value is set to zero and can reach upto a maximum value of forty. The value of the trust is updated by verifier with an increment and decrement of two for forwarding and not forwarding of the packet by the neighbor respectively.

From_ID	***To_ID***	***Sq***

Fig 3: Structure of the Route Error table

The route error table stores the link failure information. From_ID and To_ID are the addresses of the nodes within which the communication is not possible because of the broken link and for which the RERR message is generated.

Whenever the verifier receives a node with it's suspicious flag set from the identifier, it matches the address of the suspicious node with that of To_ID in the route error table. If there is a match, the verifier does not take any action. The reason for this is that the node might have gone out of the range and this mobility causes the flag to be set as suspicious for that node. Otherwise, the verifier will send a trust request message TREQ with TTL value set to seven. The TREQ is not broadcasted to the complete network because this could flood the network with TREQ and lead to increase in network overhead. The value of TTL is set to seven because it is possible that neighbours of the suspicious node will fall within this range and can provide better opinion about that node, since neighbour is considered to be those which are at a one hop distance from the concerned node. A calculation timer is also used to limit the waiting time for the trust reply TREP to arrive at the requesting node. When the calculation timer expires, the verifier calculates the average of the trust values received so far and if that average is less than the defined threshold, it deletes that node form the route cache.

4. SIMULATION & RESULTS

In order to evaluate the performance of proposed work, the Network Simulator (NS2) version 2.34 with wireless extension is used.

The proposed work is done with DSR as mentioned earlier. A network area with 1000m x 1000m is simulated with the number of nodes 50. The simulation time is 900 seconds. The nodes are mobile that moves within the network space according to the Random Waypoint model. The traffic patterns used are TCP connections with a data rate of 10 packets per second. Total 30 connections are used.10%-50% of the total number of nodes was chosen randomly as malicious nodes. Those malicious nodes drop the data packets.

Table 1: Simulation Parameters

Parameters	Value
Number of Nodes	50
Maximum Speed	10m/s
Simulation Area	1000*1000
Simulation Duration	900 seconds
Traffic Type	TCP
Source-Destination Pairs	30 connections
Data Size	512 bytes
Pause time	0 , 100, 250, 400, 500 seconds
Available bandwidth	2 Mbps

Table 2: Values of Other Parameters

Tout	0.5 seconds
Initial Trust	0
Threshold value of trust	-0.85
TTL value of TREQ packet	7

Since the initial trust value of all the nodes is kept at 0, therefore the trust value of the malicious node collected from various nodes at any time will be 0 or less than that. Keeping this observation in consideration, we considered three values of average threshold, which determines the maliciousness of a node. These values are -0.5, -0.85 and -0.9. We performed several simulations by varying pause times from 0-500 seconds keeping number of malicious nodes 50% of the total nodes and observe the network throughput as performance metric at these three threshold values. The graph is as discussed below:

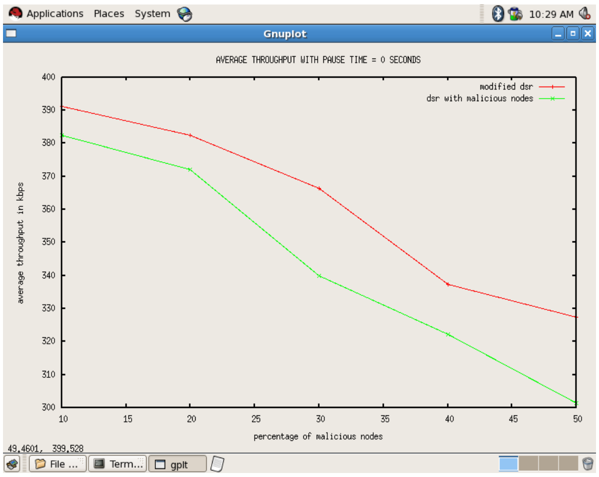

Fig 4: Average Throughput Vs Number of Malicious Nodes with pause time = 0 seconds

Figure 4 shows average throughput against number of malicious nodes when the pause time is 0 seconds. We can see that the throughput decreases with the increase in number of malicious nodes but is always greater than the throughput value observed with standard DSR with malicious nodes. The highest value of throughput is achieved when there are only 10% of malicious nodes and lowest value is attained at 50% of malicious nodes. The reason for this is clear from the graphs of detection efficiency. It is clear from the graphs that at number of malicious nodes 10%, detection efficiency is 100% therefore throughput will increase and at 50% number of malicious nodes detection efficiency is 72% means not all the malicious nodes are detected, therefore throughput decreases.

In figure 5 average throughputs is measured against number of malicious nodes at pause time 250 seconds. The figure shows that average throughput of modified DSR is again better than that of standard DSR with malicious nodes. The throughput of the modified DSR is fluctuating at some points. Also throughput value is not increased with pause time so much. The reason for this may be that at these places the good nodes(that are not malicious)may be deleted in more amount with the malicious nodes within the given simulation time, which is quite possible also. Therefore the throughput value at these points is reduced. But the overall throughput is superior to standard DSR with malicious nodes.

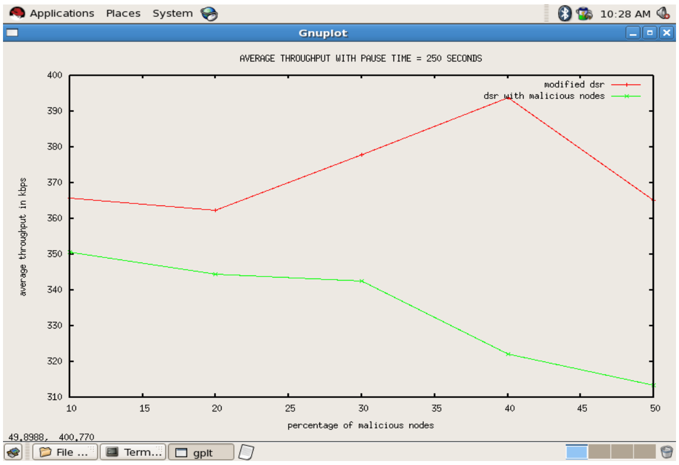

Fig 5: Average Throughput Vs Number of Malicious Nodes with pause time = 250 seconds

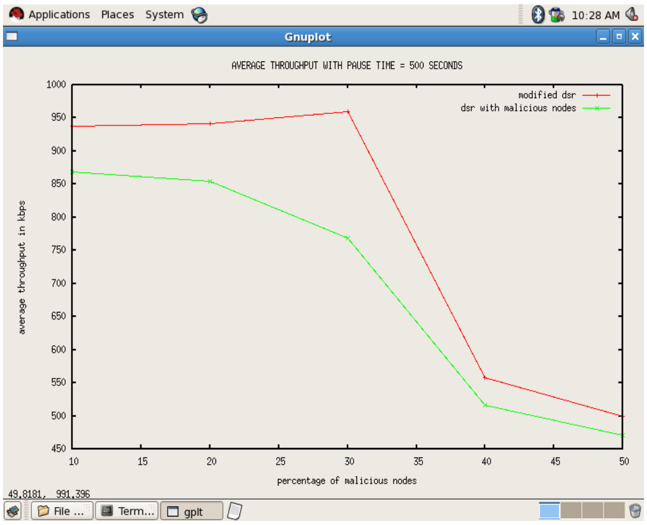

Fig 6: Average Throughput Vs Number of Malicious Nodes with pause time = 500 seconds

Figure 6 depicts the average throughput comparison of modified DSR and Standard DSR with malicious nodes at pause time 500 seconds. It is clear from the graphs that modified DSR again outperforms standard DSR with malicious nodes in terms of throughput. As pause time increases, the network tend to becomes stationary therefore malicious nodes are less detected and the behavior of modified DSR tends to be like standard DSR with malicious nodes. Moreover as the network becomes stationary although malicious nodes are less detected but chances of deletion of good nodes also become less therefore value of throughput is increased from pause time 0 and 250 seconds like it has maximum throughput value about 950 kbps.

5. CONCLUSION

The proposed work deals with the issue of security handling without affecting the network performance. Thus, it is a good scheme in which further enhancement can be done to integrate other issues also.

6. REFERENCES

[1] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044

[2] J.-P. HuBaux, L. Buttyan, and S. Capkun., "The quest for security immobile ad hoc network," In Proc. ACM MOBICOM, Oct. 2001.

[3] J. Kong et al., "Providing robust and ubiquitous security support for mobile ad-hoc networks," In Proc. IEEE ICNP, pages 251–260, 2001

[4] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks", In Proceedings of ACM MOBIHOC 2001, pp. 299-302, October, 2001.

[5] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH,USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[6] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-1284

[7] Panos,C Xenakis,C and Stavrakakis,I - A Novel Intrusion Detection System for MANETs International Conference on Security and Cryptography (SECRYPT) 2009.

[8] Orda, A. and Libman, N. The designers' perspective to atomic noncooperative networks. IEEE/ACM Transactions on Networks, 7(6) pp. 875-884, 1999.

[9] Qiu, L. Yang, Y.R. Zhang, Y. and Shenker, S. On selfish Routing in internet like environments. In Proceedings of ACM SIGCOMM'03, Aug 2003.

[10] Roughgarden, T. The price of anarchy is independent of the network topology. In Proceedings of the 34th Annual ACM Symposium on the Theory of Computing, 2002.

[11] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD:Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.

[12] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks", In Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP' 02), pp. 78-87, November 2002.

[13] Alfawaer,Z. And Al Zoubi,S. , "A Proposed Security Subsystem for Ad Hoc Networks" International Forum on Computer Science Technology and Applications, IEEE 2009.Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

[14] Sahu, S and Shandilya, S K - A Comprehensive Survey On Intrusion Detection In Manet, International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 305-310July-December 2010.