International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011

MADSN: Mobile Agent Based Detection of Selfish Node in MANET

Debdutta Barman Roy[1] and Rituparna Chaki[2]

[1]Department of Information Technology, Calcutta Institute of Eng. & Mgmt , Kolkata, India
barmanroy.debdutta@gmail.com
[2]Department of Computer Science and Eng., West Bengal University of Technology, Kolkata, India
rituchaki@gmail.com

ABSTRACT

Mobile Adhoc Network (MANET) is highly vulnerable to attacks due to the open medium dynamically changing network topology, co-operative algorithm, lack of centralized monitoring and management point. The fact that security is a critical problem when implementing mobile ad hoc networks (MANETs) is widely acknowledged. One of the different kinds of misbehavior a node may exhibit is selfishness. Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. Because of open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. There can be two types of selfish attacks –selfish node attack (saving own resources) and sleep deprivation (exhaust others' resources. In this paper, we propose a new Intrusion Detection System (IDS) based on Mobile Agents. The approach uses a set of Mobile Agent (MA) that can move from one node to another node within a network. This as a whole reduces network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. Besides, it has been established that the proposed method also decreases the computation overhead in each node in the network.

KEYWORDS

MANET, Mobile Agent, Selfish Node, IDS

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous system, in which mobile hosts connected by wireless links are free to move randomly and often act as a router sometimes [4,5].Therefore the limited wireless transmission range of each node gets executed by multi-hop packet forwarding. That is here nodes within each other's radio range communicate directly via wireless links while those are far apart uses other nodes as relays. This kind of network is well suited for the mission critical applications such as emergency relief, military operations where no pre-deployed infrastructure exists for communication. Due to the lack of authorization facilities, volatile network topology it is hard to detect malicious nodes [4, 5], MANETs are highly vulnerable to attacks. Finally, in

A MANET nodes might be battery-powered and might have very limited resources, which may make the use of heavy-weight security solutions undesirable [7, 8, 9, 10 and 11].
Many different types of attacks have been identified. This paper deals with the Denial of service attack (DoS) by a selfish node; this is the most common form of attack which decreases the network performance.

DOI : 10.5121/ijwmn.2011.3416

A selfish node does not intend to directly damage other nodes, but is unwilling to spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. The reason behind this is 'saving one's own resource' by saving of battery power, CPU cycles or protecting wireless bandwidth in certain direction. A selfish node wants to preserve own resources while using the services of others and consuming their resources. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and last but not least energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

According to the attacking technique the selfish node can be defined in three different ways [1]

SN1: These nodes take participation in the route discovery and route maintenance phases but refuses to forward data packets to save its resources.

SN2: These nodes neither participate in the route discovery phase nor in data-forwarding phase. Instead they use their resource only for transmissions of their own packets.

SN3: These nodes behave properly if its energy level lies between full energy-level E and certain threshold T1. They behave like node of type SN2 if energy level lies between threshold T1 and another threshold T2 and if energy level falls below T2, they behave like node of type SN1

One immediate effect of node misbehaviors and failures in wireless ad hoc networks is the node isolation problem due to the fact that communications between nodes are completely dependent on routing and forwarding packets. In turn, the presence of selfish node is a direct cause for node isolation and network partitioning, which further affects network survivability. Traditionally, node isolation refers to the phenomenon in which nodes have no (active) neighbors; however, we will show that due to the presence of selfish node, a node can be isolated even if active neighbors are available [2].

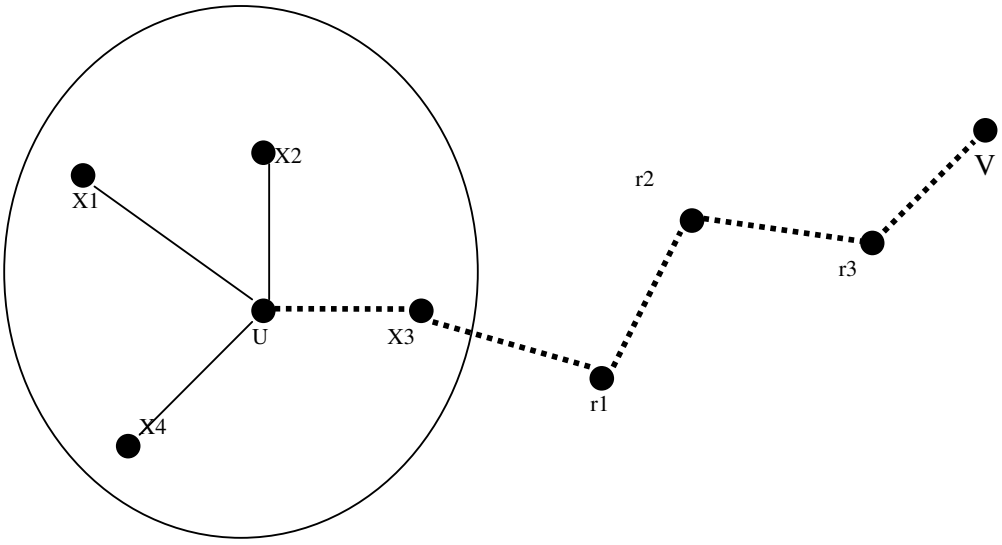

Fig 1: Node isolation due to selfish neighbors

In Figure.1, suppose node x3 is a selfish node. When node u initiates a route discovery to another node v, the selfish neighbors x3 may be reluctant to broadcast the route request from u. In this case, x3 behaves like a failed node. It is also possible for x3 to forward control packets; however, the situation could be worse since u may select x3 as the next hop and send data to it. Consequently, x3 may discard all data to be forwarded via it, and then communications between u and v cannot proceed. When all neighbors of u are selfish, u is unable to establish any communications with other nodes at a distance of more than one-hop away. In this case, we say that a node is isolated by its selfish neighbors. Note that selfish nodes can still communicate with other nodes (via their cooperative neighbors), which is different from failed nodes.

2. RELATED WORK

Several methods proposed to defend these attacks have been studied. These can be classified into three types: reputation based scheme, credit based approach and game theoretic approach [1] [3] [6]

2.1 Reputation Based scheme

In a reputation based scheme [1] watchdog and path rater approach the IDS overhear neighbors' packet transmission promiscuously and notify misbehavior to the source node by sending a message. The source node collects the notifications and rates every other node to avoid unreliable nodes in finding a path. Though the scheme is easier to implement but it depends only on promiscuous listening that may results false identification.

CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks), in this scheme the IDS performs task in a distributed ways the monitor node promiscuously observes route protocol behavior as well as packet transmission of neighbor node. The Trust manager sends ALARM messages on detection of misbehavior. The Reputation system: maintains a rating list and a blacklist for other nodes. The Path manager ranks paths according to the reputation of nodes along each path. This scheme uses both direct and indirect observations from other nodes. In this scheme the adversary nodes are black listed but not removed from the network. As the detection depends on the other nodes that reduces the reliability of the IDS because any one of the above mentioned nodes may provide false result that may blacklisted a nonadversary node.

CORE (Collaborative Reputation) approach, here the source node observes usual packet transmission and the task specific behavior of neighbor nodes and rate the node by using the positive reports from other nodes. The malicious node with bad reputation rate is isolated. But in this approach reputation of node is not changed frequently, thus the nodes temporarily suffering from bad environmental conditions are not punished severely

2.2 Credit based scheme

Sprite Simple, cheat-proof, credit based system; here the node s send CAS (Central Authorized Server) a receipt for every packet they forward, CAS gives credits to nodes according to the receipt. This approach is useful as it is easy to implement but the major problem is scalability and message overhead.

Ad hoc-VCG(Vickery, Clarke and Groves) scheme ,this is a two phase approach in the Route Discovery phase destination node computes needed payments for intermediate nodes and notifies it to the source node or the central bank. In the Data Transmission phase actual payment is performed .This scheme is fully depends on the report of the destination node.

2.3 Game Theoretic scheme

In game theoretic scheme the IDS compares node's performance against other node based on a repeated game. This scheme is easy to implement but it needs fair comparison among nodes other wise it may falsely identify a node as adversary node.

3 MOTIVATIONS

The initial motivation for our work is to address limitations of current IDS systems by taking advantage of the mobile agent paradigm. Specifically, we address the following limitations of the earlier proposed IDS

False Positive Rate: The IDS reduces the False Positive rate that may arise in Reputation based scheme, which effectively increase the network performance.

Scalability: The process scalability of the credit based approach or any centralized approach is much lower. By using Mobile Agent the scalability may increase that enhance the network performance.

Interdependencies: In the Credit based scheme the IDS depends on the report of the destination node that make the network not convenient that require for MANET.

Centralized Authorization: Due to centralized authorization of previous IDS the IDS can not perform efficiently. In Mobile Agent based IDS the computation is done in distributed manner that increase the efficiency of the IDS.

4 PROPOSED WORK

Our objective is to find out the malicious node that performs the DOS by selfish node in network. The assumptions regarding the proposed work are listed below

4.1 Assumption

The following assumptions are taken in order to design the proposed algorithm.

1. A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2. Every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.
3. The source node generates mobile agent after a specific period of time.
4. The mobile agent moves towards forward path created using RREQ and RREP.
5. The agent calculates the packet receive and forward by a node.
6. If the agent discovers a malicious node, instead of moving forward, it sends a report to the source node.

4.2 Architecture

Architecture of a Mobile agent based system:

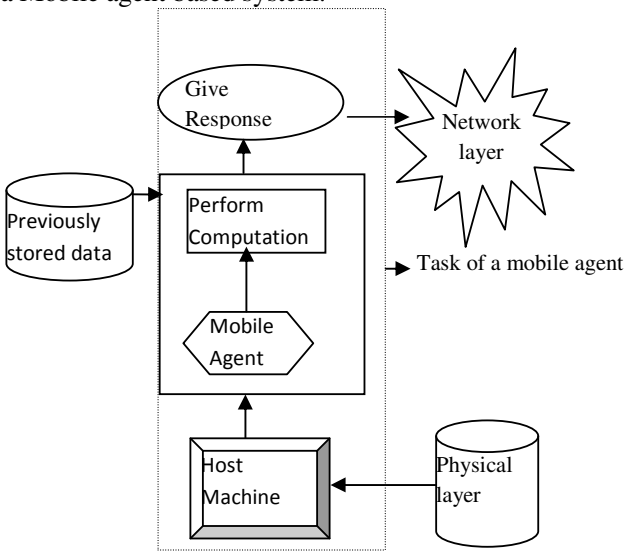

Fig 2: Architecture of proposed Mobile Agent IDS

From the above figure, it is observed that the mobile agent performs three tasks. At first the mobile agent (MA) has to collect the raw data from the host machine then it computes the packet delivery ratio (P_{dr}) after computation it compares the resultant P_{dr} with the predefined one and then gives responses to the source node accordingly.
The Mobile Agent maintains the following table to perform the computation and comparison with threshold value

Table 1: Data structure of the Mobile Agent

Source node ID	Destination Node ID	HOP count	$THRESOLDP_{dr}$

The table contains the source node id, destination node id that will be initiated by the source node. The HOP count field in the table denotes number of HOP between source node and destination node. $THRESOLDP_{dr}$ signifies the number of packet drop to be considered for any node in the forward path. The forward path is generated by the AODV routing protocol.

4.3 Methodology

The network is modeled based on the de-bruijn graph as follows:
Node Sequence: The Node sequence describes a set of nodes where the link among the nodes are created in such a way that when the node n with bit sequence (a0n a1n a2n…. akn) is connected with a node m having a bit sequence (a0m a1ma2m…. akm) where 1<=m,n<=r-1], then (ajm = ai n +1) where 1<=i,j<=k-1. Each node has in-degree and out-degree r. k is the diameter of the network represent as graph [12]. Here, the degree depends on the number of nodes in the forward path but for sake of simplicity the rank is always kept two. For a network where the number of nodes in the forward path including source and destination node is 7 the degree (d) should be computed as
C=7, r=2
We consider that d for which the following conditions
are satisfied
1. (2d –C) is minimum
2. 2d >C
i) d=1 2d =2 2<7
ii) d=2 2d=4 4<7
iii) d=3 2d=8 8>7 and 2d-1=1
iv) d=4 2d=16 16>7 2d-1=9
For the first two computations 2nd condition is not satisfied for the 4th computation 1st condition is not satisfied so the degree is taken as 3.The digits are {0,1,2}

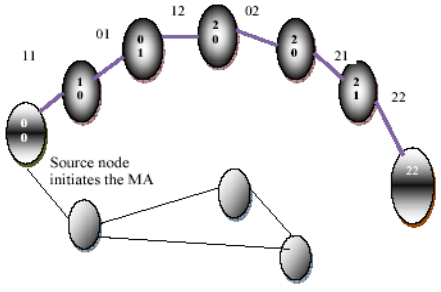

Fig 3: Nodes have unique ID compute by debrujin graph

Definition1: Packet Receive Counter: The number of packet that a node i receive from a neighbor node j is denoted as CPR (i,j)(Packet Receive Counter),1<=i,j<=N,where N is the total number of node in the network and i≠j and CPR (i,j)>=1.
Definition2: Packet Forward Counter: Total number of packet that a node i forward to its neighbors j is defined as CPF (i,j) (Packet Forward Counter) where 1<=i,j<=N-1 and i≠j.
Definition3: Packet Delivery Ratio (Pdr (i, j)): This is defined as the ratio of CPF (i, j) (Packet Forward Counter) of each node i for each neighbor j to the CPR (i, j) (Packet Receive Counter), 1<=i, j<=n and i≠j

CPR(i,j)= CPR(i,j)+1…… (1)
CPF (i,j) = CPF (i,j) + 1 ……(2)
Pdr(i,j)= CPF (i,j)/CPR(i,j) ……..(3)

If this Pdr(i,j)> THRESHOLDPdr(i,j) , It mark the i^{th} neighbor as malicious node and inform source node

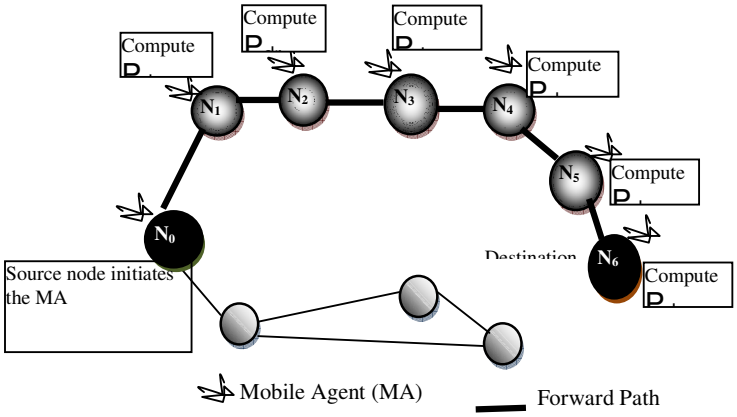

Fig 4: A network Without Malicious Attack The MA moves from source node N_0 to Destination Node N_6 by the forward path.

The figure 5 describes the situation when the network is under DoS attack by a selfish node. Here the node N2 sends acts as a malicious node RREQ messages to the node N2.The node N2 is a node in the forward path from source to destination node. N2 behaves as selfish node and refuse to forward packet to the neighbor node N3. When the MA comes to the node N2 it observes that the node behaves as malicious node by computing Pdr(N2,N3). This value is greater than THRESOLDPdr (N2, N3) and it send MMSG (Malicious Message) to the source node.

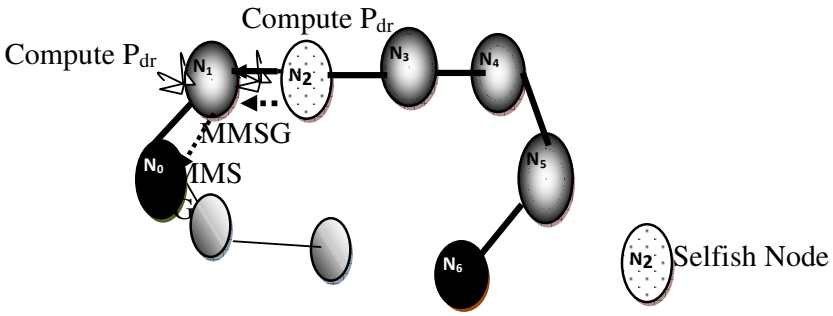

Fig 5: A network With the Malicious Attack

4.4 Algorithm:

In the figure 4 the source nodes N_0 generates the mobile agent and send it to the closest neighbor N_1. The MA at N_1 compute CPR (i, j) according to the equation 1. MA then calculates CPF (i, j) using equation 2, and then computes P_{dr} (i, j) using equation 3. If the Pdr (i, j) is greater than $THRESHOLDP_{dr}$ (i, j), then MA readily informs the source node via the intermediate nodes. From figure 4 it is observed that the MA reaches the destination node only when the network is free from DoS attack by a selfish node. The source uses the same path for others packets to be sent.

/* The following algorithm depicts the task of a mobile agent*/

Begin

Step1: the source node N0 sends packet to the destination node N6

Step2: Start Timer T

Step3: Wait for the acknowledgement from destination node

Step 4: increase T by unit time

Step 5: if T>Tout then

Goto step 6

Else

Goto step 3

Step 6: The node S generates Mobile Agent(MA) and provides it's own ID and send it to the next hop node

Step7: The mobile agent observe for i^{th} node the number of packet receive from neighbor node j and compute CPR(i, j

Step 8: MA compute CPF(i,j)for the ith node

Step 9: MA compute Pdr(I,j) for the ith node at tth instance

Step 10: If the ratio is less than threshold for ith node

Then

The agent moves to the next hop node

decrase hop count by 1

Else

Agent reports the malicious activity to the source node

End

6 PERFORMANCE ANALYSES

6.1 Simulation Metric

Simulation metrics are the important determinants of network performance, which have been used to compare the performance of the proposed scheme in the network.

End to End Delay (D): The End to End Delay (D) is defined as the time of reception of the packet by the destination node (T_d) and the time of generation of the packet by the source node (T_s) for a sequence of packet $P_{seq.}$

For the packet sequence P^1_{seq} $D_1 = T^1_d - T^1_s$
For the packet sequence P^2_{seq} $D_2 = T^2_d - T^2_s$
For the packet sequence P^n_{seq} $D_n = T^n_d - T^n_s$

$$\text{Average End to End Delay} = \frac{\sum_{i=1}^{n} Di}{Npkt}$$

Where N_{pkt} is the total number of packet

Number of data packets Received: This parameter computes the total number of data packet received by any node in the forward path. If the number of received packets increases, the throughput would increase.

Cumulative Sum of Receiving Packet: This is defined as the sequence of partial sums of all packets received by the destination node.

$$CU_{Sum} = \sum_{i=1}^{n} N^i_{pkt}$$

Where n is the total number of packet sends at i^{th} instance to the destination node

6.2 Performance Evaluation

From figure 6, we observe that the performance of the network in presence of malicious node degrades than the network with mobile agent. Due to presence of mobile agent the network performance improves as the network is prevented from the malicious node. Initially the Average Throughput of Receiving Packet is same implies that he network is free from network at that time instant. As the packet size increases the throughput decreases means due to packet overhead the throughput decreases.

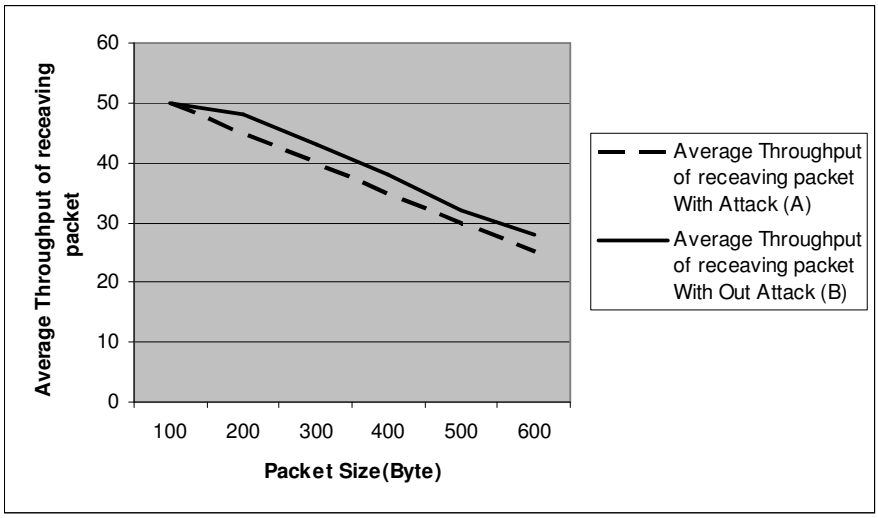

Fig 6 Average Throughput of Packet receive when the network is under attack and in presence of mobile agent

From figure 7, it is observed that cumulative sum of number of receive packet is more in presence of mobile agent. Series A describe the performance of the network with attack and series B describes the performance of network in presence of mobile agent.

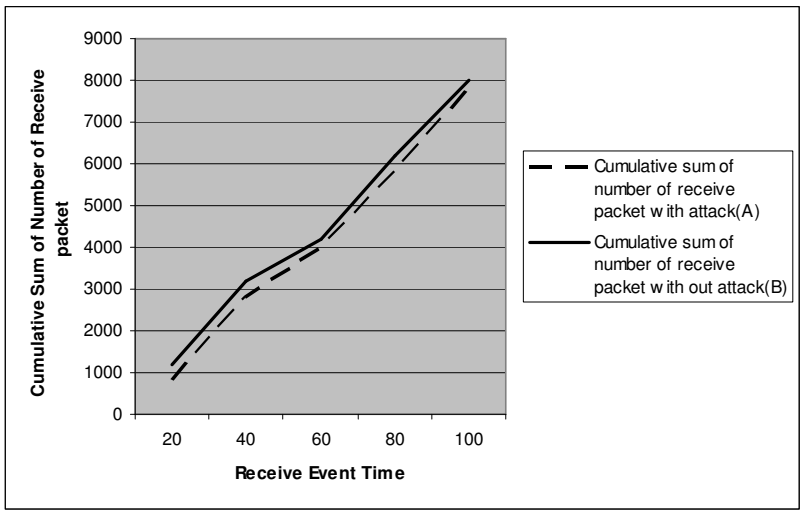

Fig 7 Cumulative Sum of number of Receive packet when the network is under attack and in presence of mobile agent

In figure 8, series "A" denotes average Throughput of Forwarding Packet from source to destination node in presence of malicious node attack in network. Series "B" indicates the Throughput of Forwarding Packet in presence of mobile agent in the network. At the simulation time instance 40sec the throughput is maximum indicating that at this moment the packet forward by the intermediate nodes are maximum in presence of malicious node. The source and the destination nodes are very close to each other in the network at this time instance.

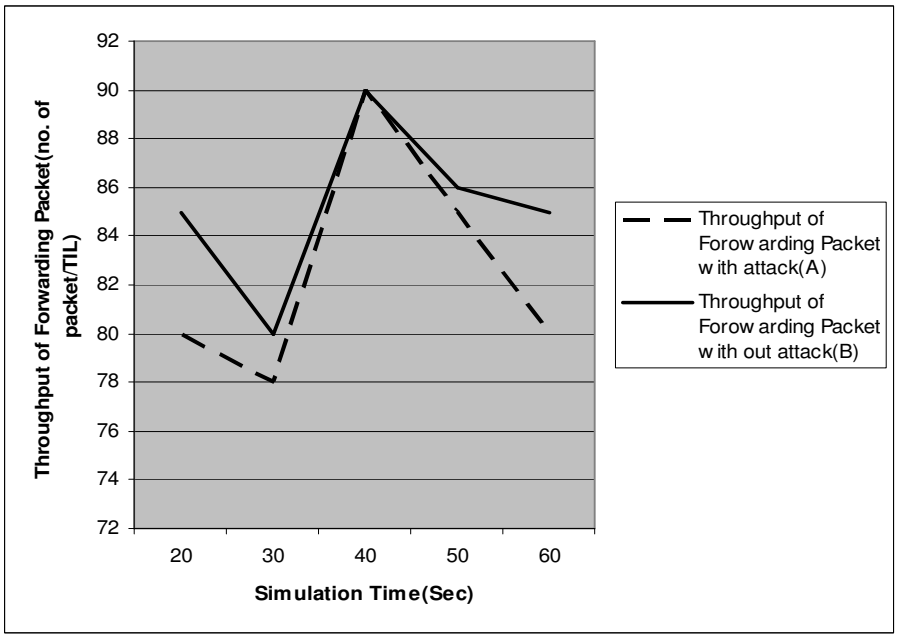

Fig 8 Throughput of forwarding packet when the network is under attack and in presence of mobile agent

From figure 9, we observe that the performance of the network in presence of selfish node degrades than the network without any attack. When the network is under attack in presence of mobile agent then the performance of the network remain same as that in case of the network without attack.

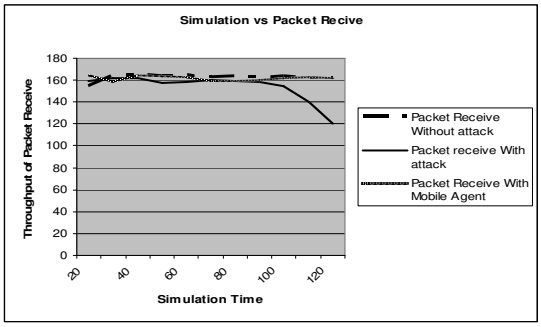

Fig 9 Throughput of Packet receive when the network is under attack and in presence of mobile agent

In figure 10, the series "a" indicates the average end to end delay in presence of DoS attack in the network. In series "b" the end to end delay increases as the packet size increases but the performance is better than that is shown in series "a". The pick of the graph denotes that at that point due to network congestion the delay is maximum.

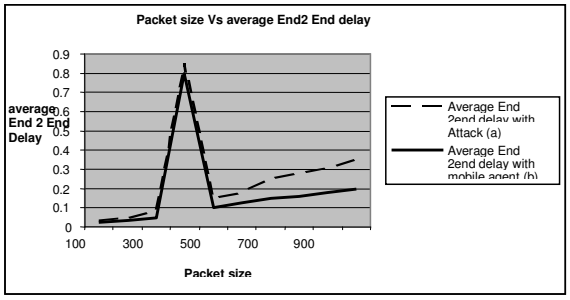

Fig 10 End 2 End Delay under attack and in presence of mobile agent

7 CONCLUSIONS AND FUTURE WORK

The mobile ad-hoc network suffers from several types of intrusions, out of which, the denial of service attack by a selfish node is the one of them. The mobile agents travel through the network, gathering vital information. This information is then processed by the mobile agent itself. The choice of threshold value is very important to help the detection of the attacker as early as possible. The computation complexity of the MA is kept minimum so that computation overhead can be reduced. In this paper we only focus on the DoS attack caused by selfish node by refusing the packet delivery to the neighbor node. The computation overhead of our algorithm is much less as the computation is done by the MA when the source node notices that the destination node does not response in correct time. The nodes are also free from performing the computation. This feature of our proposed scheme increases the efficiency of each node thereby increasing the overall performance of the network.

8 ACKNOWLEDGMENTS

This research is supported in part by the Computer Science and Engineering Department of University of Calcutta. We would like to thank Dr. Nabendu Chaki for fruitful discussions and endow with valuable suggestion.

REFERENCES

[1] A. S. Anand, M. Chawla, Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010

[2] T.V.P.Sundararajan1, Dr.A.Shanmugam2, Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET, International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010

[3] 3. P.K.Suri and Kavita Taneja,Exploring Selfish Trends of MaliciousDevices in MANET In Journal Of Telecommunications, Volume 2, Issue 2, May 2010.

[4] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks, (IJNSA), Vol 1, No 1, April 2009

[5] Sukla Banerjee, Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks in Proceedings of the World Congress on Engineering and Computer Science 2008WCECS 2008.

[6] Xiaoxin Wu David K. Y. Yau,Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach, ASIACCS'07, 2007.

[7] Marko Jahnke, Jens Toelle, Alexander Finkenbrink,. Alexander Wenzel, et.al;Methodologies and Frameworks for Testing IDS in Adhoc Networks; Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks; Chania, Crete Island, Greece, Pages: 113 - 122, 2007

[8] Y.-C. Hu, A. Perrig, D. B. Johnson; Wormhole Attacks in Wireless Networks; IEEE Journal on Selected Areas of Communications, vol. 24, numb. 2, pp. 370-380, 2006

[9] Yang, H. and Luo, H. and Ye, F. and Lu, S. and Zhang, U.; Security in Mobile Ad Hoc Networks: Challenges and Solutions; Wireless Communications, IEEE, vol. 11, num. 1, pp. 38-47, 2004

[10] Y.-C. Hu, A. Perrig; A Survey of Secure Wireless Ad Hoc Routing; Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

[11] Y.-C. Hu, A. Perrig, D. B. Johnson; Packet leashes: a defense against wormhole attacks in wireless networks; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, pp. 1976-1986, 2003

[12] Rituparna Chaki, Uma Bhattacharya dsign Of New Scalable Topology for Multihop Optical Network, IEEE TENCON 2000.

Authors

Debdutta Barman Roy received her M. Tech. Degree in Software Engineering from the West Bengal University of Technology in 2007. She is at present working as a Lecturer at Calcutta Institute of Engineering and Management, Kolkata, West Bengal. Her research interests include the field of Computer Networking, and Wireless Mobile Ad hoc Network

Rituparna Chaki is a Reader (Associate Professor) in the Department of Computer Science & Engineering, West Bengal University of Technology, Kolkata, India since 2005. She received her Ph.D. in 2002 from Jadavpur University, India. The primary area of research interest for Dr. Chaki is Wireless Mobile Ad hoc Networks. She has also served as a Systems Manager for Joint Plant Committee, Government of India for several years before she switched to Academia. Dr. Chaki also serves as a visiting faculty member in other leading Universities including Jadavpur University. Dr. Chaki has about 20 referred international publications to her credit.

.