BAIDS: Detection of Blackhole Attack in MANET by Specialized Mobile Agent

Debdutta Barman Roy
Calcutta Institute of Engineering and Management
West Bengal, India

Rituparna Chaki
West Bengal University of Technology
West Bengal, India

ABSTRACT
The inbuilt flexibility along with easy set-up and low maintenance cost causes MANETs to be increasingly useful in catastrophe management, battlefield surveillance; etc. The infrastructure-less performance of MANET has made it more vulnerable to intrusion than ever before making the security of network all the more acute. As the previously used security systems fail to protect the MANET from insider attacks, the need for an Intrusion Detection System (IDS) becomes evident. IDS based on Mobile Agents is long been used for securing the MANET. The prior works seem to suffer from computational overhead leading to performance. This paper proposes a mobile agent based IDS in order to reduce the overheads. The use of distributed ID consists of multiple mobile agents which assist over a large network and to make communication with each other, or with a central server that provide advanced network monitoring, incident analysis, and instant attack data. This as a whole reduces the network bandwidth usage by moving data analysis computation to the place of the intrusion data & sustains on the heterogeneous platforms.

Keywords: MANET, BLACK HOLE, MOBILE AGENT

1. INTRODUCTION
Mobile wireless ad hoc networks are essentially different from wired networks, as they use wireless medium to communicate, do not rely on fixed infrastructure, and can place them into a network quickly and competently[1]. In a Mobile Ad Hoc Network each node serves as a router for other nodes, which allows data to travel, utilizing multi-hop paths, beyond the line of sight without relying on wired infrastructure. Security in such networks, however, is a great concern [2, 3, 4 and 5]. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. Lack of any centralized control makes deployment of traditional security mechanisms almost impossible. The absence of clear network entry points also makes perimeter-based defense mechanisms such as firewalls almost useless. Devices in a MANET are normally battery-powered and might have very restricted resources, which may make the use of heavy-weight security solutions undesirable [6, 10, 11, and 7].
IDSs implemented using MAs is one of the new paradigms for intrusion detection. MAs are a particular type of software agent, having the capability to move from one host to another. [15] A software agent can be defined as ". a software entity which functions continuously and autonomously in exact environment able to carry out activities in a flexible and intelligent manner that is responsive to changes in the setting. Ideally, an agent that functions continuously would be able to learn from its experience" by Bradshaw. In addition, we do expect an agent that inhabits an environment with other agents and processes to be able to communicate and co-operate with them, and perhaps move from place to place in doing so. The Mobile agents offer several potential advantages when used in ID systems that may overcome limitations that exist in IDS that only employ static, centralized components [6]

- Reducing Network Load
- Overcoming Network
- Autonomous Execution
- Platform Independence
- Dynamic Adoption
- Static Adoption (Upgradability Scalability)
- Robust and fault-tolerant behavior
- Security
- Code Size
- Performance

MAIDSs are also encountered with some demerits like Mobile Agent solutions may not be fast enough to meet the needs of IDS. One of the major challenging difficulties facing MAIDS is improving the speed with which they can identify adversary activities. Mobile agents have proved to improve significantly the detection performance. Effective detection of autonomous attacks is still very low. Also, agents are often written in scripting or interpreted languages which are easily ported between different platforms. Their modes of performance are still very low compared to native codes. Another problem is to protect the protector (MAIDS) from attacks.

The rest of this paper is organized as follows. Related works are presented in section 2. BAIDS architecture is described in section 3. The implementation procedure and evaluation of the design are presented in section 4. In section 5 conclusion is presented.

2. RELATED WORK
The research in a field significantly benefits from a good taxonomy. The aims of the efforts in several classifications have also been quite diverse. Few only try to survey the field and find it easier with labels on the systems and others try to use the taxonomies for a deeper understanding [8].
Despite these previous efforts, intrusion detection still lacks a widely applicable and accepted taxonomy. This may in part be because of it being a young research field; part of it being fast paced and may be part of it owing to its inherent complexity .Figure 1 shows classification of a typical intrusion detection system.

Current MA-IDSs

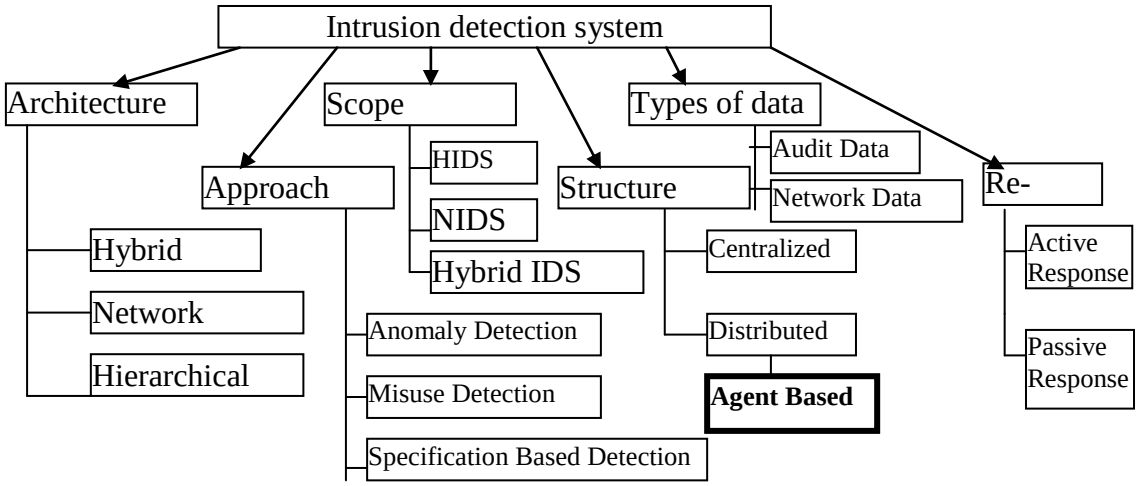

Figure 1: Taxonomy of Intrusion Detection System

Mobile agents have been proposed as a technology for the detection applications. Since agents are the independently executing entities, there is the potential that new revealing capabilities can be added without completely halting, the renewal and restarting the IDS.

The following is the research that has been done in the area of MA-IDS, focusing on architecture and mode of the data collection, security and their strengths and weaknesses.

DSCIDS - Architecture this paper is based on a hierarchical architecture with Central Analyzer and Controller (CAC) as the heart and soul of the DIDS [9]. The CAC usually may consists of a database and web server which allows for the interactive querying by the network administrator for the information of attack and initiate preventive measures. The authors tested the model using different soft computing the techniques which must consists of neural network, fuzzy inference system, and the approximate reasoning and the derivative free optimization techniques on a KDD cup of dataset. The test data is then passed through the saved trained model to detect intrusions in the testing phase.

Strengths: The problem faced with hierarchical architecture is being solved by allowing a free communication between the layers. A well comparative analysis of several soft computing algorithms with additional machine learning techniques, is being carried out which serves as references for researchers in the field

Problems: The agents are not well distributed. The complete description of how the agents detect intrusions based on the soft computing algorithms proposed is not well discussed.

MSAIDS – Multi-Level and Secured Agent-based Intrusion Detection System [10] focused on the following points (i) improving IDS performance (ii) detection of autonomous attack using its architecture (iii) Reduction in false alarm (iv) IDS agents' security architecture provides the methodology where intrusion is done at two levels. The first is the Lower Level Detection (LLD), which has the data agents

and processing agents. The data agents move around the nodes in the network to collect associated information. The processing agents also known as Node 1 agent is responsible for construction of the first level database from the collected information and for data cleansing, classification and the formatting. The Node-2 agent is responsible for data mining and first level intrusion detection and communicates about the possibility of intrusions to the interface agent through the alarm agent.

The Upper Level Detection (ULD) is known as validation level is involved in separate intrusion detection process. At the ULD, the lower level agents gather data from the data agents and inform the Controller and Protector (CP), which acts as the Facilitator agent about the nature of the gathered data. The CP also ensures proper communication and the delivery of service among agents. The data gathered are then used to update the ULD database; the ULD does not check for intrusion if there is no signal from the LLD. In Data Collection the types of data collected is the application messages, the events of authentication system calls, and TCP connections. The techniques an Apriori algorithm is modified to extract way by the first level and second level agents. Mobile Agent-Based Intrusion Detection Systems 674 Security.

MSAIDS maintains security of agents by using asymmetric cryptosystem of the Aglet's framework. In addition to this, agents' states are recorded and authenticated before they are initiated. Response any suspected intrusion is reported by the Interface Agent to the Site Security Officer (SSO). The action to be taken by the SSO is not stated.

Strengths In addition to securing mobile agents, the use of recorded state mechanism, which has been proved effective, is a plus in this work. The agents are well coordinated.

Problem 1. The activities at the ULD could still integrate with the LLD to form one-level architecture and have the CP at the ULD since detection of intrusion at each level is still based on same algorithm. It took 0.14 seconds to report an intrusion at the LLD and 0.75 seconds at the ULD.

2. The architecture presented does not provide adequate security for the database, which could be vulnerable to changes by the attackers.

Mobile Agent for Network Intrusion Resistance by H. Q. Wang [11]

Architecture the designed system framework includes the following components: (i) Manager: Centre of controlling and adjusting other components and it maintain information about their configuration information. The manager receives intrusion alarms from host monitor MA and executes the intrusion responses using intrusion response MA. (ii) Host monitor MA: this is established on every host in network. If the intrusions occur confirmatively, the host monitor MA will appeal to the manager and report about the suspicious activity

directly. After receiving the appeal, the manager distributes a data gathering MA patrolling other hosts in the network to gather information. If a distributed intrusion is found, the manager will assign an intrusion response MA to respond intelligently to every monitored host. The database stores the node configuration of detecting system.
Strengths it changes the hierarchical system structure of the traditional distributed IDS.
Problem There is a control center carrying out the major part of the intrusion detection, if the location of this center is being discovered, then the system collapses.
An Adaptive Intrusion Detection and Defense system based on Mobile agents. [12]
Architecture: It comprises of the following components: (i) Main Intrusion detection Processor - Responsible for the monitoring network segments (hosts) and acts as a central intrusion detection and processing units - Responsible for collection and correlation of IDS data from distributed IDS mobile agents. - Acts as a secure, trusted repository for the mobile agents to obtain latest information about attacks that they should look for and to update the severity lists.
(ii) Mobile Agent Platform (MAP) the MAP can create and interpret, execute, transfer and terminate/kill agents. The main platform which is a small server program that resides on each host is responsible for accepting requests made by network users and generating IDS mobile agents plus transmitting them into the network to do intrusion detection functions.
(iii) Mobile IDS agent each host has a mobile IDs agent roaming all its hosts at all times. This agent is responsible for detecting intrusion based on data gathered by sniffing on the network traffic.
Strengths The mobile agents in this work are fully managed and network resources utilization is saved when there is no attack.
Problems High false positive rates, so many attacks could be missed when the severity level is between 3 and 5. Also, the security of the whole system is not discussed.
MAIDS - Architecture for distributed Intrusion detection using Mobile Agents [13]
Architecture The architecture includes four components: Manager, Assistant Mobile agent, Response mobile agent and Host Monitor Agent. The host monitor agent which resides on every host cooperate three subagents namely the network detection subagent (for network access), the file detection subagent (for file operation) and user detection subagent for privilege operation. If the intrusion can be determined at the certain monitored host, HMA reports the intrusion directly to the manager, otherwise it asks manager for aid and it only records the suspicious activity. Manager is the center for controlling and coordinating all the other components. It should maintains configuration information about all the components including HMA, MA platform, The Assistant MA, and Response MA. Manager is responsible for creating, leaving, accepting and removing MAs according to the host's request and environment.
Strengths the evaluation criterion is based on 3 categories: Intrusion detection ability evaluation which reported that 94.1% attacks can be detected. The system performance result is also taken where the use time of CPU is less then 1% and approximately 5% memory is exhausted and lastly, the mobile agent performance is taken where the interval from the leave of Host Monitor agent or Manager to their return is taken. It was reported that it took a long time that agents migrated with authentication and encryption though the transportation of these agents was very fast.
Problems the security of the location of the manager is not reported, hence if this is found by attackers, the IDS would be in a dangerous situation.
APHIDS - A Mobile Agent-based Programmable Hybrid Intrusion Detection System by Deeter
Architecture APHIDS works with the known network based architecture by placing an agent engine at every location. It is appreciated as a distributed layer which operates on top of a set of distributed agent engines. APHIDS architecture takes the benefit of the mobile agent model to implement a system capable of effective, flexible distribution of analysis and monitoring tasks, as well as integration of existing detection techniques.
Strengths APHIDS makes its Analysis Agent lightweight in order to save the bandwidth during the transfer of log data. The use of Distributed correlation scripts in capturing the expert knowledge of security administrator by automating the standard investigative procedures that are performed in the response to an incident.
Problem The security of the agents is not considered.

3. PROPOSED METHODOLOGY

Adversary nodes in a wireless mobile ad hoc network may target to exploit features of the MAC layers. The common of the security mechanisms in such networks have been focused in the network layer [14]. Few researches have been done on the MAC layer security. The role of MAC layer in wireless ad hoc networks is important as it is liable for the continuation of the communication between nodes and the scheduling of the access in a shared radio channel. MAC layer is affected in direct way by almost every anomaly, since it is placed in the first layers of the protocol stack. Indeed, the data delivery ratio or throughput may be affected by malicious behavior or misuse of the shared medium due to increased routing load. The control overhead for each delivered data packet may also increase.
In this paper, we propose specialized agent based black hole intrusion detection system. Moreover, we propose a possible response technique to detect the malicious node. The present architecture of the suggested IDS could be either distributed or cooperative or distributed and hierarchical [1].

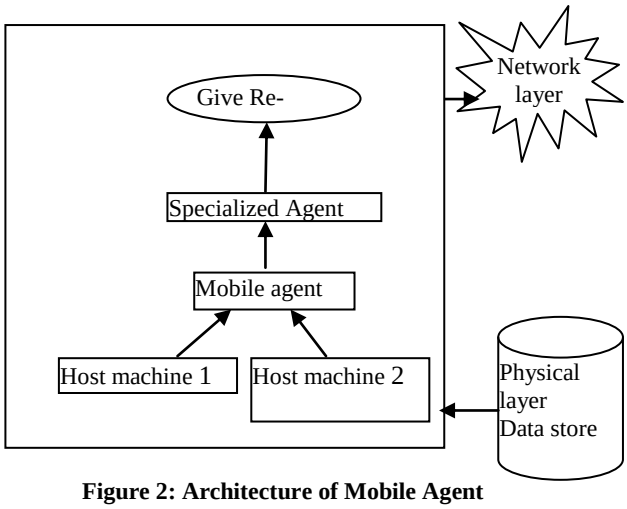

Figure 2: Architecture of Mobile Agent

Our objective is to find out the malicious node that performs the wormhole attack in network.
We have assumed that the MANET consists of clusters of nodes. The assumptions regarding the organizations of the MANET are listed in section

3.1. Assumptions

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 being assigned to a new node collaboratively by existing nodes.
3. The source node during sending packets creates a mobile agent with life time of maximum hop count to the destination
4. Any node in the route from source to destination can create new mobile agent if any malicious behavior is being observed by it.
5. The mobile agent is called after a period o time where the time period must be predefined.

Table 1. Data Definition

Black_agent (S_{id} , $D_{,id,}$ $H_{c,\,ount}$ TH_R)	*The black hole detector agent*
S_{id}	*Source node ID*
D_{id}	*Destination Node ID*
H_{count}	*HOP Count*
TH_R	*Thresold value of no. of packet forwarded by the node (P_f) and no. of packet receive by the node (P_r)*
N_{id}	*Node IDof i^{th} node*
R_i	*Ratio of no. of packet forwarded by the node (P_f) and no. of packet receive by the node (Pr) for node i*

Mobile Agent Based Detection

Figure3 shows a network consisting of ten nodes. The sending path between source node S and destination node D is marked by (dotted lines) all nodes.

S creates a Mobagent (source_id, present_node_id) and send it through the forward path to the destination node D. The Mobagent calculates the Confidence Ratio R which is the ratio of number of packet forwarded by the node i (P_f) and number of packet receive by the node i (P_r)

$$R^i=P_f^i/P_r^i,$$

where P_f^i is the total number of packets forwarded by the i^{th} node and P_r^i is the number of packet received by the i^{th} node.

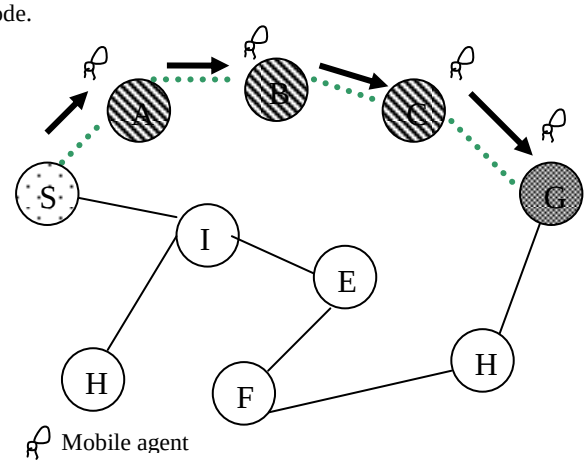

Fig 3: Source node create Mobagent and send it to the destination node

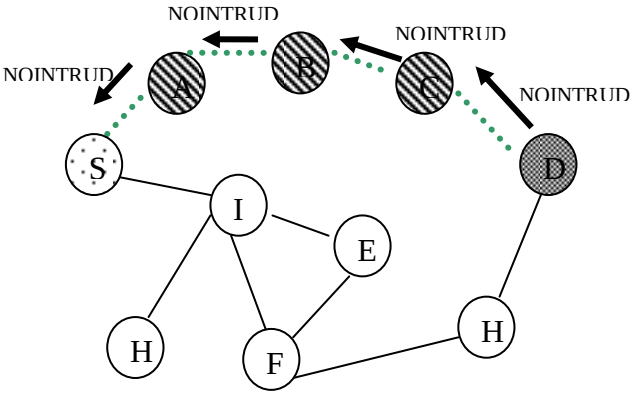

Fig 4: Destination node D sends acknowledgement to the source node S

In the absence of any malicious node, the destination node D receives the Mobagent within timeout. The "NOINTRUD" signal is sent by D to the source node to confirm the absence of any intruder, as shown in figure 4.

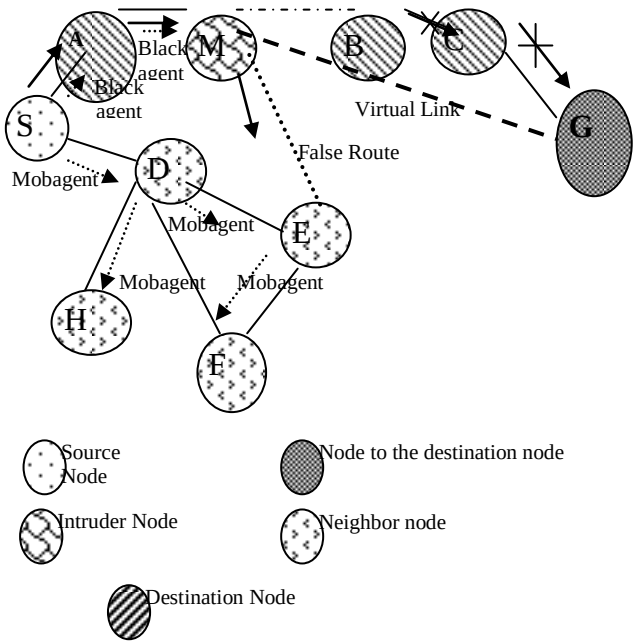

Figure 5: Scenario of mobile agent traversing through the network with intrusion attack

Figure 5 shows that the network is attacked by a malicious node M. After a period of time the source node S again create a Mobagent and send it for destination node D. Now, the MOBAGENT sends k number of data sequences to the M which is malicious node and waits till time-out for return data streams. The counter Pr and T_{delay} are incremented whenever a data stream is returned to D. Then D sets P_f to k, which define the number of packets returned to D is the actual number of packets forwarded. Then the MOBAGENT calculates the confidence ratio R^i For the ith node. Where

$$R^i = (P_f^i / P_r^i)*(1/T_{delay})$$

Here. MOBAGENT observes that R^i is less than ThR^i . Then it readily informs the node A and the source node S.
In the figure 6 the flow chart describe the functionality of mobile agent and black agent as described in figure 4 and figure 5

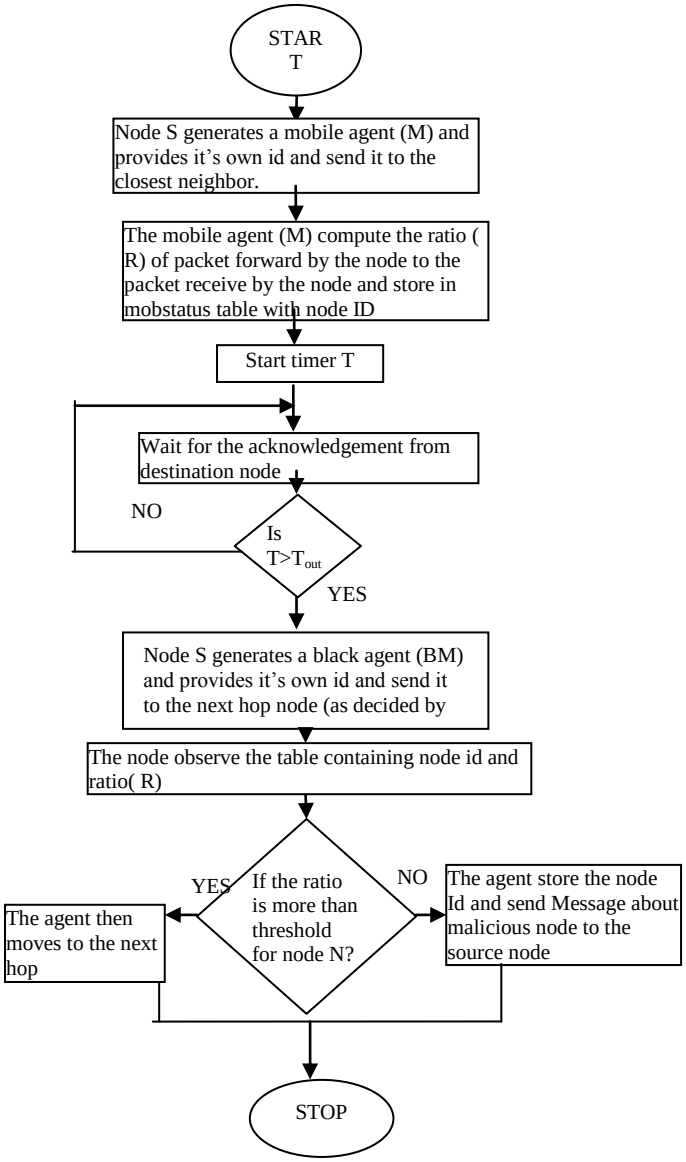

Fig 6: Flow Chart of proposed methodology

4. PERFORMANCE ANALYSIS

4.1 Metrics

Metrics: The metrics used to evaluate the performance are given below.
Packet Delivery Ratio (P_r): The ratio between the numbers of packets originated by the application layer sources (P_s) and the number of packets received by the sink at the final end (P_d).

$$P_r = P_d / P_s$$

Node mobility (N_m): It signifies how fast the node is being changing it's position in the network.

$$Pr \ \alpha \ 1/N_m$$

$$Pr=constant/N_m$$

Average End-to-End Delay: This is average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at present intermediate nodes, retransmission delays at the MAC layer.
We have used NS2 ver 2.29.2 with Cygwin-1.5.21

Table 2: Simulation Parameters

Simulator	NS2
number of mobile node	15
number of malicious node	1
routing protocol	AODV
maximum bandwidth	2Mbps
Traffic	CBR(constant bit rate)
maximum connection	50
maximum speed	10-100mps
pause time	5s

4.1.1 Throughput Of Packet Delivery

In figure 7 the packet delivery ratios measured with respect to number of transaction the number of transaction indicates number of flows initiated during a particular duration of time from same or different sources to same or different ends. The packet delivery ratio increases by using BAIDS compare to BHIDS. In BHIDS the communication overhead is much more than in BAID. The network is mobile in the nature at the transaction 1 and 2 the source and destination comes closer to each other so their communication using mobile agent rises the overhead. The distance from the adversary node and that of destination node become very closer to each other. Mobile agent based detection of attacks becomes more complex, leading to the degradation of the performance.

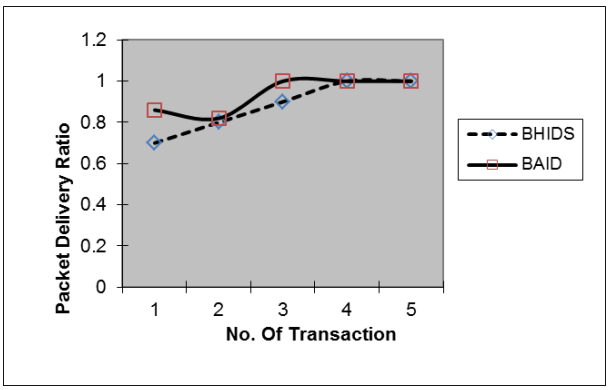

Figure -7 Packet Delivery Ratios vs no. of transaction

4.1.2 Packet Delivery Ratio

In figure 8 the packet delivery ratios measured with respect to Node mobility. In the plot it is observed that performance of the BAID is better than that of BHIDS. In BAID the overhead due to communication is less than that of BHIDS. At the higher mobility the performance is better implies that at that instance the network is free from adversary node.

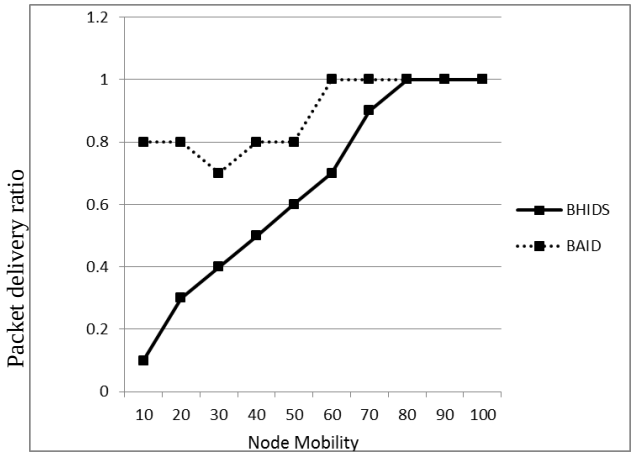

Figure-8: Packet Delivery ratio Vs. Node Mobility

5. CONCLUSION

The design of our algorithm has shown that MA technology is an efficient tool for building IDS infrastructure. Since this technique has shown an improvement in comparison with some previous works, multi-level intrusion detection using mobile agents has proven to be efficient. In this paper we proposed BAIDS, an IDS for detecting the blackhole attack using the specialized mobile agents. From the simulation experiment we can conclude that when the source and the destination become closer to each other then the use of MA is not effective. In future, our algorithm has to be tasted in the simulated environment with about 100 nodes and more than one malicious node. Once this has been done, concept of MA can be extended to the detection of sleep deprivation attacks

6. REFERENCE

[1] Debdutta Barman Roy, Rituparna Chaki "MADSN: Mobile Agent Based Detection of Selfish Node in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011

[2] Debdutta Barman Roy, Rituparna Chaki,Nabendu Chaki"a new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks ",International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009

[3] Chaki, Rituparna; Chaki, Nabendu; "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network"; Proc. of the 6th Int'l Conf. on Computer Information Systems and Industrial Management Applications (CISIM '07); pp. 179 - 184, ISBN: 0-7695-2894-5, June 2007

[4] 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

[5] 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.

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

[7] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: 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

[8] Saidat Adebukola Onashoga, Adebayo D. Akinde, and Adesina Simon Sodiya" A Strategic Review of Existing Mobile Agent- Based Intrusion Detection Systems", Issues in Informing Science and Information Technology Volume 6, 2009

[9] Abraham, A., Jain, R., Thomas, J., & Han, S. Y. ". D-SCIDS: Distributed soft computing intrusion detection system". Journal of Network and Compute Application, 30,pp 81- 98,2007

[10] Adesina Simon Sodiya" Multi-level and Secured Agent-based Intrusion Detection System", Journal of Computing and Information Technology - CIT 14, 3, 217–223 doi:10.2498/cit.2006.03.05

[11] H.Q. Wang, Q.Wang, Q. Zhao, G.F.Wang, R.J.Zheng and D.X.Liu "Mobile Gent for Network Intrusion Reistance" , Advance Web and Network Technology and Applications Lecture notes in Computer Sci ence,vol. 3842/2006. 965- 970 ,2006

[12] Eid, M., Artail, H., Kayssi, A., & Chehab, A. " An adaptive intrusion detection and defense system based on mobile agents Innovations in Information Technologies (IIT'2004)

[13] Li, C., Song, Q., & Zhang, C." MA-IDS: Architecture For distributed intrusion detection using mobile agents". 2nd International Conference on Information Technology for Application (ICITA, 2004).

[14] Aikaterini Mitrokotsa, Rosa Mavropodi, Christos Douligeris "Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks", Ayia Napa, Cyprus, July 6-7, 2006