IMPACT OF SINKING BEHAVIOR IN MOBILE ADHOC NETWORK

Usha G[1] and Dr.Bose S[2]

[1]Department of Computer Science &Engineering, Anna University, Chennai, INDIA.
Ushag2@gmail.com

[2]Department of Computer Science &Engineering, Anna University, Chennai, INDIA.
sbs@cs.annauni.edu

ABSTRACT

Mobile adhoc networks suffer for lack of security because of its mobility of the nodes and the network is vulnerable to most of the intrusion behaviour. In this paper we analyze one of the most vulnerable behaviours known as Sinkhole behaviour. We designed architecture to effectively analyze this attack on MANET. We consider various performance metrics and attributes to understand the behaviour of this attack. From the results we can understand that this attack causes damage to the communication of Manet's.We have evaluated our results using ns-2.

KEYWORDS

Sinkhole attack, AODV, Mobile Adhoc Networks (MANET).

1. INTRODUCTION

Mobile adhoc networks are different from other networks. The mobile nodes are not having any predefined infrastructure. They share the communication medium. In MANET every node is acting as a router node and each node exhibits autonomous behaviour. Due to mobility, the nodes share dynamic topology and have limited energy of computer resources. There exist lot of differences between wired networks and MANET. For example, when the nodes interfere with neighbour nodes bandwidth decreases asymptotically with hop count in MANET.Manet's are widely applicable in areas such as terrain, disaster relief, earthquakes, tsunamis, hurricanes. Routing in MANET can be classified as three types. They are Flat, Hierarchial, and Geographic.Flat routing protocols are classified into three types. They are reactive, proactive and hybrid. In this paper we will discuss AODV protocol which is reactive that is on demand routing protocol.

Routing protocols for adhoc networks does not consider about security [1].Since the nodes are highly dynamic any eavesdropper can change the routing mechanism. Mobile adhoc networks have lack of security because of the nodes are mobile in nature. Any nodes [3][4] can join with any other nodes at any time. Hence eavesdropper can easily attack the communication. Eavesdropper can attack the nodes in various ways. One such type of attacking behaviour is known as sinking attack. Identifying this attack is one of the most critical tasks in MANET. We will study the attacking behaviour and analyze the impact of this attack using various network attributes. For this we have developed AAS architecture to efficiently study and analyze the attacks in MANET. We will study the attacking behaviour and analyze the impact of this attack using various network attributes. In most current security issues, the authors proposed various mitigation technologies to defend against various kinds of attacks in MANET. For example in [2] the authors compared various routing protocols such as DSDV, AODV, and DSR under various kinds of attacks. Some specific attacks and defending techniques are discussed in [5][6] [7].

DOI : 10.5121/ijasuc.2012.3307

The rest of the paper is organized as follows. Section 2 we discuss about the working of AODV routing protocol in detail. Section 3 we describe the characteristics of Sinkhole attack and its behaviour, Section 4 discusses about the architecture to analyze attacks in detail. Section 5 discusses simulation environment and results. Finally we conclude the section in 6.

2. AODV ROUTING PROTOCOL

Aodv routing protocols are known as reactive routing protocols. AODV [8] is source initiated routing protocol. AODV protocols are different from traditional proactive protocols since in proactive the routing mechanism is based on periodic updates this leads to high routing overhead. The key goal for designing this protocol is to reduce overhead. For example when number of traffic session is much lower than the number of nodes, overhead reduces obviously. In AODV no routing structure is created prior. The route discovery process of AODV consists of two key methods. First one it is source routing. Second one is backward learning. Since this protocol uses the concept of periodic updates it is adaptive to network dynamics.

Source initiated means source floods the network with a route request packet when a route is required to a destination. The flooding is propagated outwards from the source. The flooding transmits the request only once. On receiving the request from the source node the destination replies to the request if it has the valid path. Reply from destination uses reversed path of route request. Since route reply is forwarded via the reverse path which forms forward path. Thus it uses forward paths to route data packets. AODV protocol uses hop-by-hop routing. That is each node forwards the request only once. In the meanwhile unused paths expire based on timer. AODV uses the concept of optimization that is any intermediate nodes can reply to route request if it has valid path which makes the protocol to work faster. But the major problem with optimization causes loops in presence of link failure. Each node maintains sequence number. It acts as a timestamp. The most interesting feature of sequence number is, it signifies the freshness of the route. When a node maintains high sequence number makes it up to date in the routing. In AODV path maintenance is based on Route Error (RERR) message. Next we discuss about occurrence of sink Hole attack in MANET.

3. SinkHole Attack in AODV Protocol

Sink hole attacks are difficult to find because of following reasons. When the normal communication takes place in MANET, the sinking node tries to attract the neighbouring nodes in various ways. In AODV protocol it either alters the data packets or drops the packets silently. One can wonder how it happens; the malicious node increases its sequence number. As we discussed above, the sequence number in AODV is used to intimate about the freshness of the route. The malicious node overhears the communication channel as a part and observes the sequence number of all nodes. After that it assigns itself as having highest sequence number among all the nodes in the route and invades the channel abruptly and drops the packets. For example in the following figure node 1 is source node and node8 is the destination.

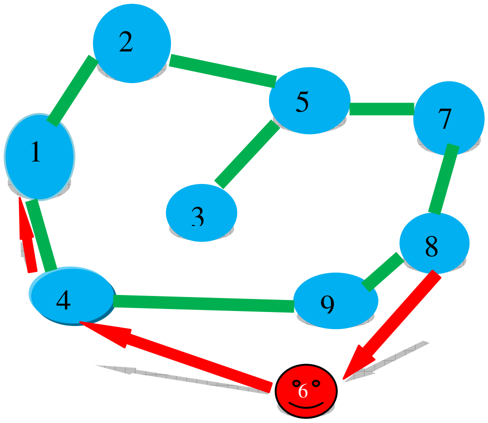

Figure 1. Example for Sinkhole attack inMANET.

Initially node 1 wants to send information to node8 by broadcasting the RREQ message. Node 2 checks whether if itself is the destination node. Since it is not the destination node it simply forwards the packet. Likewise the information propagates through the channel and finally reaches the destination; hence communication takes place among the nodes. But when the invader or malicious node invades the network, the communication breaks. For example node 6 is the malicious node in which it overhears the network and updates its sequence number and set its sequence number as the highest sequence number among all the nodes and broadcasts it to others. The other nodes in the communication path also update this value in their routing table. This is the way in which the malicious node 6 attracts other nodes. When other nodes believe this and start forwarding the packets through this. But the node 6 simply drops all the packets which come into it. This is the way the sinkhole attack takes place in this MANET.

4. Attack Analysis Architecture

In this section we discuss about attack analysis architecture in detail. We also discuss simple framework for sinkhole attack creation and discuss about pseudo code to simulate sinkhole attack. Figure 2 discusses about simple scenario to analyze attack.

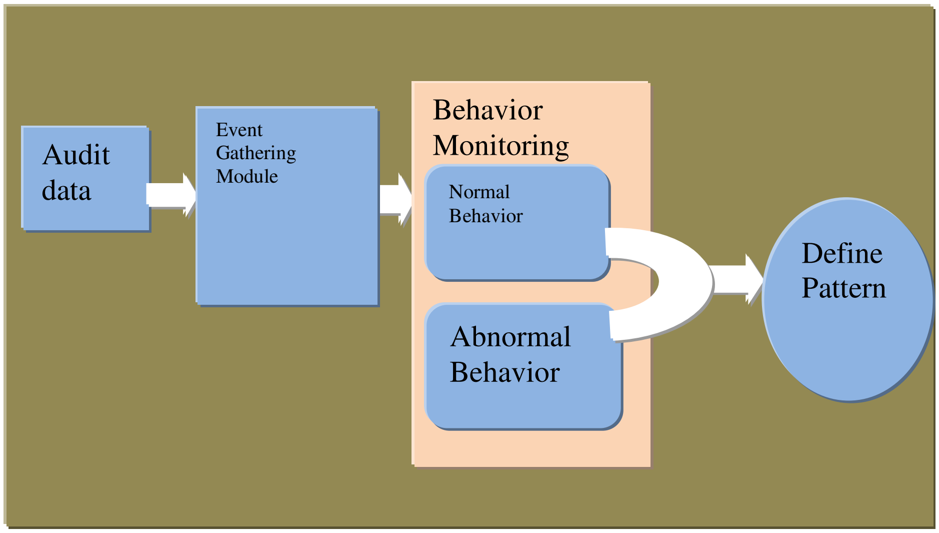

Figure 2. Attack Analysis Architecture (AAS) for Sinkhole Attack.

4.1Event Gathering Module

This module is responsible for independently collecting features from routing layer to aid in analyzing network intrusions. Event gathering module captures the data's from the audit data. at which the event occurred, sequence number, node at which the event occurred, packet type, transmit power,inter arrival time of packets.

Table 1. Parameters from Audit Data

S.No	Events
1	Number of Packets Send
2	Number of packets Dropped
3	Number of packets received
4	Time at which the event occurred
5	Sequence Number
6	Node at which the event occurred
7	Interarrival time of packets
8	Transmit Power

Table 1 discusses about the parameters used to analyze the attacks.We have considered the following events in which these parameters contribute in deciding the attacking scenario.

4.1.1 Packet delivery ratio

From audit data we have calculated the parameters related to packets are number of packets send, receive and drop. The number of packets sends is used to know how many packets are transferred from one node to other node. The received ratio is also used to know how many packets we have exactly received from that of sent packets. The dropped packets are used to calculate how many packets are dropped in order to know the vulnerability of the attack

4.1.2 Time

We are calculating time in order to know at what the event happened. For example at what time the packets send from node A to node B.

4.1.3 Sequence Number

In on demand routing protocols sequence numbers are used to calculate the freshness of the route. The nodes which have highest sequence number denote the freshness of the route. So it is also one of the important attribute

4.1.4 Transmit Power

Transmit power is the useful measure to know the energy level of a node. We measure the energy level of each node in order to understand the degradation of energy.

4.2Behavior Monitoring Module

In this module we have monitored the behaviour of MANET. For that we have implemented a protocol known as SAA-AODV.Now we discuss the pseudo code and simple framework for creating attack. We have created a simple framework in which we have created the sink hole behaviour in existing AODV protocol.

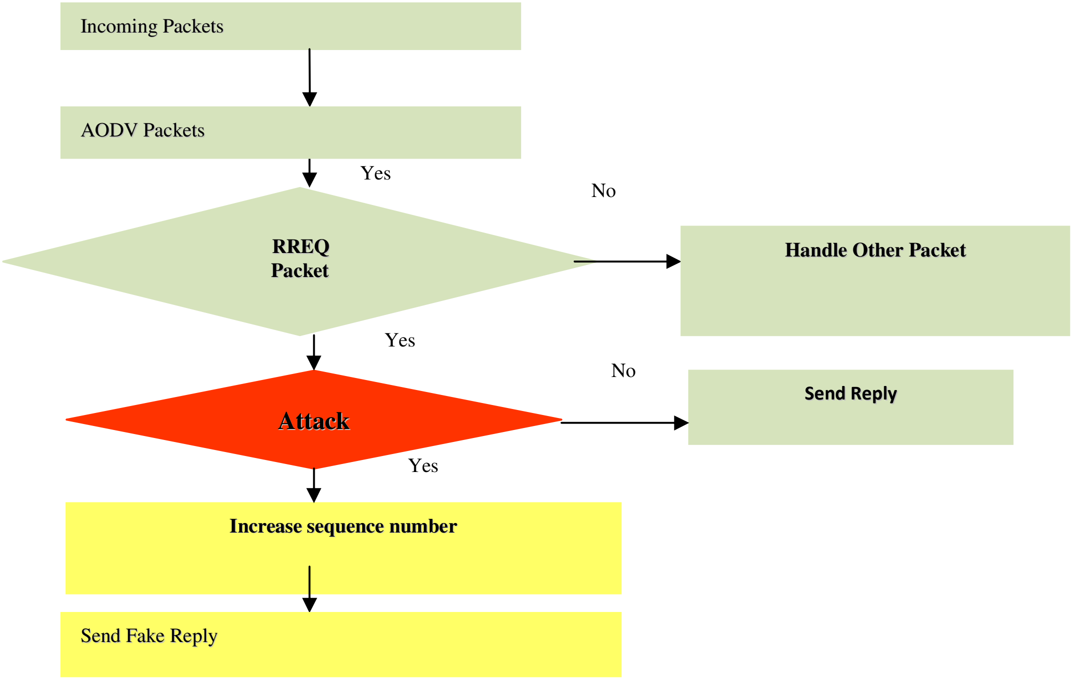

Figure 3.Simple framework for simulating Sinkhole attack

In figure 3 we have simulated simple framework for creating sinkhole attack. The incoming packets are being checked for RREQ packets. If the intruder wants to create attack he just increases the sequence number of its own by comparing the sequence number with other nodes. It then sends fake reply to nodes by thus increasing its sequence numbers. In figure 4 it shows the pseudo code to known as SAA-AODV (sink Hole AODV) to implement sinkhole attack in ns2 frame work.Thus shown in above the intruder node invades into the routing process and drops the packets maliciously. The following pseudo code explains about the algorithm we proposed for simulating sinkhole attack in NS-2.

```
If (AODV_Packet) {
    If (RREQ) {
        If (I am the source or previously seen it) {
            Drop the Packet
        } else {
if {No Attack} {
        Resolve the Route;
        SendRouteReply;
} else (SinkHoleAttack) {
//Maliciously sending wrong route
    Search the current seqno of source and destination
    Increase the sequence number of destination node
}
        SendRouteReply;
}
        }
} else {
Handle it in Normal way
}
}
else {
if(it is a packet which I am originating) {
Handle it in Normal way
} else {
//it is the packet I am forwarding
    if {No Attack} {
    Handle it in Normal way
} else (SinkHoleAttack) {
//Maliciously dropping the packet
    Drop the Packet
} //Maliciously dropping the packet
    Drop the Packet
}
}
}
```

Figure 4.Pseudocode of SAA-AODV to implement Sinkhole attack in MANET

5. Simulation Environment

We have implemented our simulation in ns-2(network simulator).NS2 [9][10] is an open source event driven simulator. In order to evaluate the sinkhole attack we have implemented a new protocol known as SAA-AODV.The implementation of Sink Attack AODV (SAA-AODV) has been discussed above. The modified AODV algorithm simulates the sinking behaviour by increasing the sequence number and compares it within the routing table of its neighbor. Thus we have implemented the attack in AODV. We conducted our experiments on an Intel Core 2 Duo PC with 4 GB RAM and simulated our environment using NS2.34 in cygwin environment.

5.1Random Simulation Environment

For simulation, we have set the parameter as shown in Table 2 and in Table 3.We have used Random Waypoint Model (RWP) which is used as the mobility model of each node. In this model, each node selects a random destination within the simulation area and a node moves to this destination with a random velocity. Table 2 and Table 3 we are discussing the parameters for simulation.

Table 2. Parameters from Audit Data

Parameters	Values
Traffic Agent	Constant Bit Rate
Transport Agent	UDP
Traffic Source	7
Traffic Sinks	7
CBR Rate	10 Kbytes/Sec

Table 3. Parameters for simulation

Parameters	Values
Simulator	Ns2-.34
Simulation time	100sec
Topology	600m x 600m
Routing Protocol	AODV
Antenna type	Omni Antenna
Max packet in Queue	50
Mobility Scenario	10 m/s
Pause Time	20 sec

Next we discuss about performance metrics in which we evaluated our results.

5.2Performance Metrics

In this section we analyze the parameters which are greatly useful in understanding the behaviour of sinkhole attacks.

5.2.1Packet Delivery Count

Packet delivery count is used to measure the number of packets delivered to the destination node to that of the packets delivered from the source node.

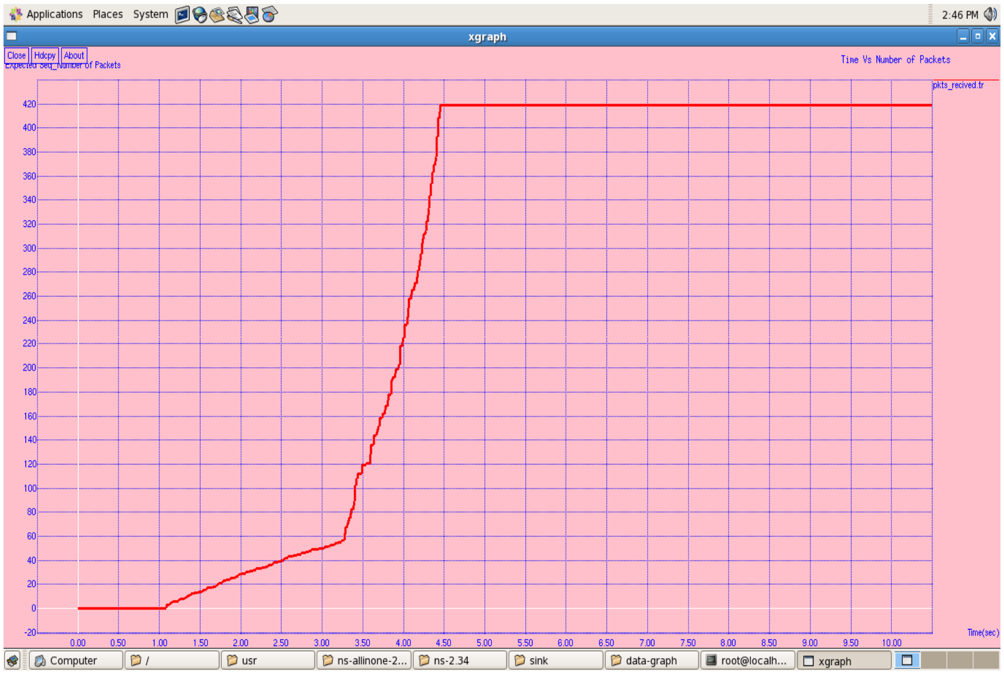

Figure 5. Time vs. Packet delivery count

The above graph explains about packet delivery count from source node to destination node. When the attack takes place the sinkhole attack randomly drops the packets.

5.2.2Delay Calculation

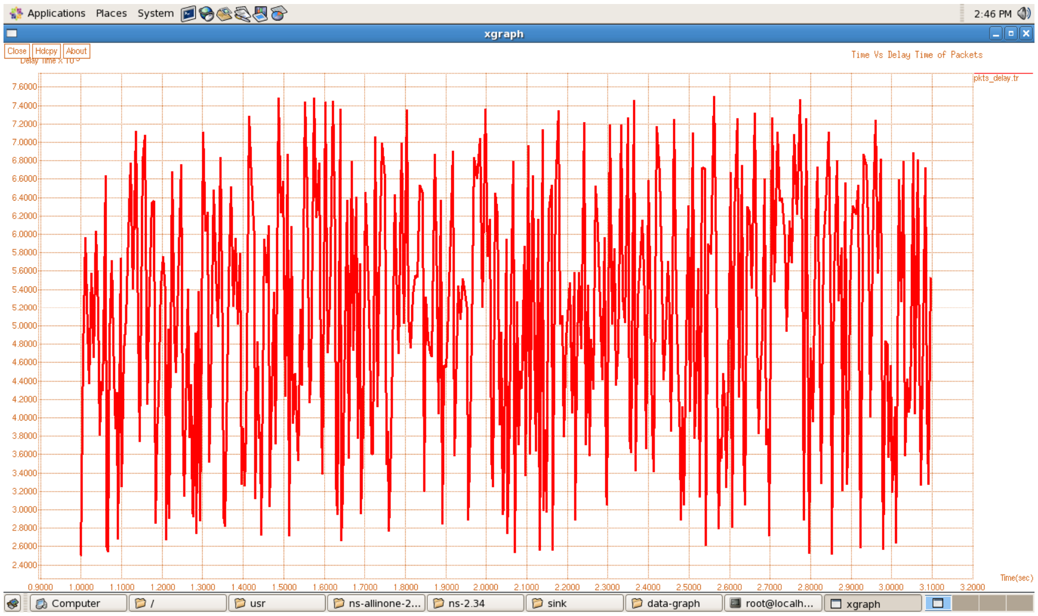

Figure 6. Time vs. Inter arrival time of packets

The above graph explains about the time vs. interarrival time for the packets. This metric is used to find the number of packets transmitted per second.

5.2.3Energy Level

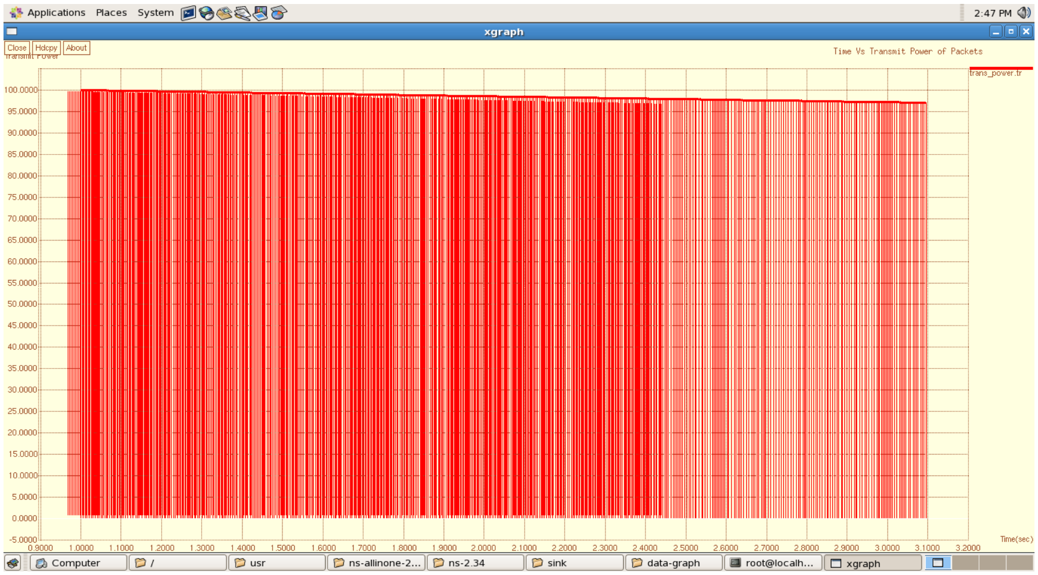

Figure 7. Time vs. Transmit power of packets

The above graph shows about time vs. Transmit power. Energy level is the important metric in adhoc networks in order to know the status of battery power. Initially the node has the energy of 100% at time t=1, when the time t=1.4 sec the energy level gets reduced to 99.4%, then at time t=3 sec the energy had reduced to 97.2% as shown in above figure. When the sinkhole attack takes place the energy level gradually decreases. This is calculated based on the energy of the transmitting node and the reception node capacity.

6. CONCLUSIONS

We have broadly studied about the behaviour of sinkhole attack in MANET. We have analyzed these attacks with various performance metrics such as transmission power, packet delivery ratio. Thus we have identified the impact of this attack in MANET. We have simulated this attack by implemented a new protocol known as SAA-AODV.From the results we can observe that when the attack took place the packet delivery count gradually decreases. Energy level in node is also reduced. Thus this attack is more vulnerable to mobile adhoc networks. The detection of sinking behaviour in MANET is still a challenging and research issue.

ACKNOWLEDGEMENTS

We would like to thank everyone who helped us.

REFERENCES

[1] Nikola Milanovic Miroslaw Malek, Anthony avidson, Veljko Milutinovic,"Routing and Security in Mobile Ad Hoc Networks"Pubished by IEEE Computer Society.Feb2004

[2] Su Mon Bo, Hannan Xiao, Aderemi Adereti, James A. Malcolm and Bruce Christianson, “A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack", IEEE proceedings of Multitopic Conference, INMIC 2004.

[3] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU,"An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" 24th IEEE International Conference on Advanced Information Networking and Applications.2010.

[4] XiaoYang Zhang, Yuji Sekiya and Yasushi Wakahara,"Proposal of a Method to Detect Black

Hole Attack in MANET", IEEE conference onISADS, Digital Object Identifier:10.11.09/ ISADS.2009.5207339, Publication Year: 2009, Page(s): 1 - 6.

[5] Chen Wei Long Xiang Bai Yuebin Gao Xiaopeng,"A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", IEEE conference on CHINACOM '07, Digital Object Identifier: 10.1109/CHINACOM.2007.4469403 Publication Year: 2007, Page(s): 366 – 370.

[6] Al Mazrouei.M.S, Narayanaswami.S,"Mobile adhoc networks: A simulation based security evaluation and intrusion prevention", IEEE conferecnce on Internet Technology and Secured Transactions, Page(s): 308- 313, 2011.

[7] Adaobi.Okoli, Igbesoko.Ejiro, Ghassemian.Mona,"Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-Organized Networks ", IEEE conference On New Technologies, Mobility and Security (NTMS), Page(s): 1- 5, 2012.

[8] P.Vigneswaran, Dr.R.Dhanasekaran,"A Dynamic Approach for Anomaly Detection in AODV", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.4, December 2011.

[9] Teerawat Issariyakul, Ekram Hossain,"Introduction to Network Simulator NS2", 2009 Springer.

[10] K. Fall; K. Varadhan, NS notes and documentation, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

Authors

Ms.G.Usha is currently doing Ph.D in Anna university,Chennai,Tamilnadu,India, She completed her M.E in Computer Science and Engineering and B. E in Computer Science and Engineering from Anna University. She is currently working as Teaching Fellow, Department of Computer Science and Engineering, Anna University, Chennai.Her area of interest includes Network Security, Adhoc Networks, Artificial Intelligence and Graph theory.

Dr.S.Bose received Ph.D in Anna University, Chennai, and Tamilnadu, India. He published several papers in National and International Journals and Conferences. Presently he is working as Assistant Professor in Anna University, Guindy, Chennai.His area of interest is Networks, Webtechnology, Security, Artificial Intelligence, Multimedia Streaming and Data mining.