Improvement of Black Hole Detection Technique Wireless Sensor Network

[1]Akshay Kansra, [2]Ankur Singhal
[1]Research scholar, [2]Assistant Professor,
[1]Department of Electronic Science Engineering
[1]Geeta Institute of Management and Technology , Kurukshetra, India

***Abstract* - In Infrastructure networks each node directly connected to the nearly base station. Every node gets the signals directly from the nearly base station. In this network we need the base stations at very small distance because a base station have limited coverage area .It is very costly network also because the cost of a base station is very higher. Some other problems in this network are we need a specific destination for the base station from where it covers the maximum area. These are the some problems comes in the infrastructure wireless networks. The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This organization is important because the attacker can develop the network either as internal, external or/ as well as active or passive attack against the network.**

***Index Terms* - WSN, MANET,AODV,OLSR,DSR.**

I. INTRODUCTION

1.1 Wireless Network

The term "wireless" should not be confused with the term "cordless", which is normally used to refer to powered electrical or electronic devices that are able to operate from a convenient power source (e.g., a battery pack) without any cable or cord to limit the mobility of the cordless device through a link to the mains power supply.

1.1.1 Wireless network can be classified two ways :-

- Infrastructure wireless networks
- Infrastructure less (Ad-hoc) wireless networks

In Infrastructure networks each node directly connected to the nearly base station. Every node gets the signals directly from the nearly base station. In this network we need the base stations at very small distance because a base station have limited coverage area .It is very costly network also because the cost of a base station is very higher. Some other problems in this network are we need a specific destination for the base station from where it covers the maximum area. These are the some problems comes in the infrastructure wireless networks.

1.2 Wireless Sensor Networks:- Wireless Sensor Networks (WSN) are used in variety of fields which includes military, healthcare, environmental, biological, home and other commercial applications. The vast advancement in the field of embedded computer and sensor technology, Wireless Sensor Networks (WSN)[14] is a self-assured of several thousands of sensor nodes which are capable of sensing, actuating, and relaying the collected information, have made significant impact everywhere. The Wireless Sensor Network are typically self-organizing and self-healing. Self-organizing networks allow a new node to involuntarily connect the network without the need for manual intervention. Self-healing networks allow nodes to reconfigure their link relations and find option pathways around failed or powered-down nodes..

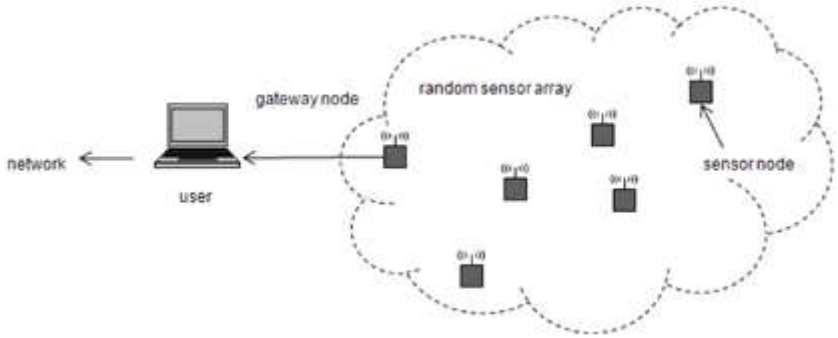

Fig 1.1: Wireless sensor/actuator network.

1.3 Ad Hoc Networks:-

An ad-hoc network is a self-configuring network of wireless links between mobile nodes. These nodes may be routers and/or hosts. The mobile nodes or mobile devices communicate directly with each other and without the aid of access points, and they have no fixed infrastructure. They form an topology, where the routers are free to move at random and assemble themselves as necessary.

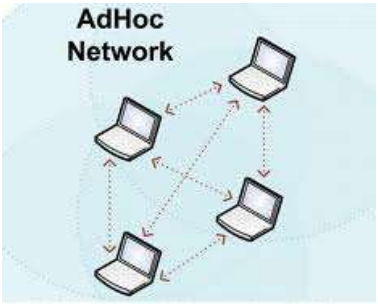

Fig. 1.2 Adhoc Network

Ad hoc networks date back to the Seventies. They were developed by the Defense Forces [16], to comply with a military framework. The main motive is to rapidly organize a robust, mobile and reactive network, under any conditions. These networks then prove useful in cost-effective and manufacturing fields, first aid operations and invention mission. Ad hoc networks, also called peer to-peer networks.

2. PRESENT WORK

2.1 Our Proposal:-

Previously the works done on MANETs mainly focused on comparing the routing protocols AODV and DSR, AODV and OLSR. This thesis compare the three routing protocols AODV, OLSR and TORA which are reactive, proactive and hybrid routing protocol respectively in nature. Previously the works done on MANETs focused mainly on different security threats and attacks such as DoS, DDoS, and Impersonation, Wormhole, Jellyfish, and Black Hole attack. Among these attacks Black Hole attack involved in MANET is evaluated based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using Reactive, Proactive and Hybrid Protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address for three protocols under the attack, as well as the impacts of the attacks on the MANETs. This thesis analyzes Black Hole attack in MANETs using AODV, OLSR and TORA which are reactive, proactive and hybrid routing protocol respectively in nature.

- To study the various protocol like AODV OLSR and TORA and its implementation in NS2 for larger ad hoc network.
- Implementation of Black hole attack and simulate these with three said protocols.
- Compare the results in NS2 using these protocols with and without Black hole attack.

2.2 MANET Model

A MANET of 50 nodes with a simulation time of 50 seconds was considered. The mobile nodes were placed on a 1000 X 1000 flat grid. AODV, OLSR and TORA were used as the routing protocols. Thus, 50 different nodes were involved in the communication. The mobility of the nodes is depending on the Random Way Point Model.

MANET Models are defined with help of two models:

1. Mobility Model
2. Traffic model

2.2.1 Mobility Model

An important factor in mobile ad-hoc network is mobility of nodes, which is defined by speed, direction and rate of change. Mobility in the physical world is unpredictable, often unpredictable and it has a dramatic effect on protocols developed to support node movement. Mobility model represents the movement of mobile users and how their location, velocity and acceleration change over time. Such models are frequently used for simulation purpose when new communication or navigation techniques are investigated. For the MANET, the topology configurations used is: 1000 m x 1000 m field with 50 nodes. At a specified time, each mobile node starts its journey from current location to a specified destination with a chosen speed (depending on the mobility scenario). Once the destination is reached, a new destination is targeted. There is no fixed pause time. If the node reaches the destination ahead of its next move, it pauses; else, it continues to move. Identical mobility model was used in simulations across protocols to yield fair result.Currently there are two types of mobility models used in simulation of networks:

- **Trace model:**
  Traces are those mobility patterns that are observed in real life systems. Traces provide accurate information, especially when they involve a large number of participants and an appropriately long observation period.
- **Synthesis models:**

However, new network environment i.e. ad-hoc networks are not easily modeled if traces have not yet been created. In this type of simulation it is necessary to use synthetic models. Synthetic means to realistically node movement, but without using network traces.

Seven different synthetic entity mobility models based on random directions and speed are being discussed:

1. Random Walk Mobility Model: A simple model based on random directions and speed.
2. Random Way point Mobility Model: A model based on random waypoints and random speeds that includes pause times between changes in destination and speed.
3. Random Direction Mobility Model: A model that forces mobile nodes to travel to the edge of simulation area before changing direction and speed.
4. A Boundless Simulation Area Mobility Model: A model that converts a 2D rectangular simulation area into torus-shaped simulation area.

5. Gauss- Markov Mobility Model: A model that uses one tuning parameter to vary the degree of randomness in mobility pattern.
6. A Probabilistic Version of Random Walk Mobility Model: A model that utilizes a set of probabilities to determine the next position of a mobile node.
7. City Section Mobility Model: A simulation area that represents streets within a city.

2.2.2 Traffic Model: Continuous bit rate (CBR) traffic source were used. The CBR traffic, once started, continued throughout the simulation. 50 sources –destination pairs are chosen in such a manner that they are spread across the network and the path between them changes often. The hop distance of some paths is less and some is more. The forwarding nodes that participate in data plane operation (i.e. routing) were chosen from nodes that handle multiple traffic at some point in time. At different pause time different traffic model were used like TCP, UDP etc. For Fair results these same traffic were used at that particular pause time in different scenarios.

Simulation Parameters:

The communication pattern randomly created by the set dest tool defined in ns2 simulator. The tool contains following arguments. The Simulation Parameters which are used in my thesis work are shown in Table 3.1

Table 2.1 Simulation Parameter

Parameter	Value
Simulation Time	50 Sec
No. of Nodes	50
No. of Receivers	50
Traffic Type	CBR
Pause Time	10 Sec
Maximum X-coordinate value	1000 M
Packet Size	512 byte
MAC Protocol	802.11
Mobility Model	Random Waypoint
Routing Protocols	AODV,OLSR,TORA
Observation Parameters	EED, Throughput, PDF

2.3 Simulation Environment:

The primary approach for this study was computer simulations. The network simulator ns-2 developed by the VINT research group in 1989 at University of California at Berkeley has been used for the simulations. The Monarch research group at Carnegie Mellon University extended the ns-2 simulator to include wireless scenarios with mobile nodes.

2.3.1 Comparison of Different type of Simulators:-

	Free	Open Source	Programming language
NS-2	Yes	Yes	C++,TCL
GloMosim	Limited	Yes	Parsec
Openet Modeler	No	No	C

Table:-2.2 Comparison of Three Simulators**.**

After Comparing the three simulators, we decided to choose NS-2 as network simulator for our thesis because:-

1. NS-2 is open source free software, It can be easily downloaded and installed.
2. Programming Language C++ is compatible.

2.4 Implementation:-

The implementation is based on Linux Fedora 8. After installation of fedora, Network Simulator ns-2 is installed to compare the routing protocols in the light of Performance metrics with and without Black hole effect.

Procedure:-

Step1.

Install Linux with 3 GB RAM (min) and install the Fedora 8 on a machine NS-2.

Steps to install ns-2 on Fedora 8:

Step 1.1:

Download ns-allinone-2.34.tar.gz from the following link
http://sourceforge.net/project/showfiles.php?group_id=149743&package_id=169689&release_id=684492

Step 1.2:

Execute the following commands to install ns2.34 from the terminal. And login as root.

$cp ns-allinone-2.34.tar /opt/
$cd /opt/
$tar -xzf ns-allinone-2.34.tar.gz
$cd ns-allinone-2.34
$./install

Step 1.3:

After a long wait and a whole lot of text, and see the installation finish up with text like the following: Please put /opt/ns-allinone-2.34/bin:/opt/ns-allinone-2.34/tcl8.4.18/unix:/opt/ns-allinone- 2.34/tk8.4.18/unix into your PATH environment; so that you'll be able to run itm/tclsh/wish/xgraph.

Step 2: Wireless network is build where the mobile nodes were moves on the bases of Routing Protocols which are defined in scripts.

Steps to make the wireless network:

Step2.1: Define the node configuration:

```
set val(chan)        Channel/WirelessChannel        ;#Channel Type
set val(prop)        Propagation                    ;# radio-propagation model
set val(netif)       Phy/WirelessPhy                ;# network interface type
set val(mac)         Mac/802_11                     ; # MAC type
set val(ifq)         Queue/PriQueue                 ;# interface queue type
set val(ll)          LL                             ;# link layer type
set val(ant)         Antenna/OmniAntenna            ;# antenna model
set val(ifqlen)      50                             ;# max packet in ifq
set opt(stop)        50.0                                ;# simulation time
set val(nn)           50                            ;#  number of mobile nodes
set val(rp)          AODV/OLSR/TORA
set  bandwidth       40000000
```

Step 2.2: Then Area will be defined i.e. 1000*1000 m

```
set val(x) 1000
set val(y) 1000
```

Step 2.3: Define the Trace and Nam files.

Trace files: Records all the network events that occurred during the simulation. Files have extension .tr . And these files are post analyzed with the help of AWK scripts.

Nam files: Records all the visual events that happened during the simulation.

```
$ns_ trace-all $tracefd
set namtrace [open  AodvSimulation.nam w]
```

Step 2.4: Define the Topography and create the flat grid area.

In this area movements of nodes will be shown.

```
set topo      [new Topography]
$topo load_flatgrid $val(x) $val(y)
```

Step 2.5: GOD will be created.
General Operation Director(GOD) is created to supervise each node movements.

```
set god_ [create-god $val(nn)]
```

here nn defines the no. of nodes.
Step 2.6: Start node creation.
Any no. of nodes can be created.

```
set node_(0) [$ns_ node]
set node_(1) [$ns_ node]
set node_(2) [$ns_ node]
and so on… up to 50 nodes are created.
```

Step 2.7: Then Initialize the node to initial position to them.

```
for {set i 0} {$i < $val(nn)} {incr i}
        {
            $ns_ initial_node_pos $node_($i) 50
                }
```

Step 2.8: Then define the random positions to nodes.

when the simulations are performed at different pause time nodes will move to different position. With the help of "at" function the position of node at particular time, when the simulation is running is defined.
Step 2.9: Define the traffic models:-

3. Result

This chapter focuses on result and its analysis based on the simulation performed in NS-2 Simulator. My simulated results are provided in Figure (3.1-3.3). To compare the performance of routing protocols AODV, OLSR and TORA with and without black hole attack, considering the performance metrics of packet End-To-End Delay, Throughput and network Packet Delivery Ratio.

Packet End-to-End Delay:-

Comparing the End-to-End Delay of routing protocol AODV, OLSR and TORA with effect of Black hole attack.

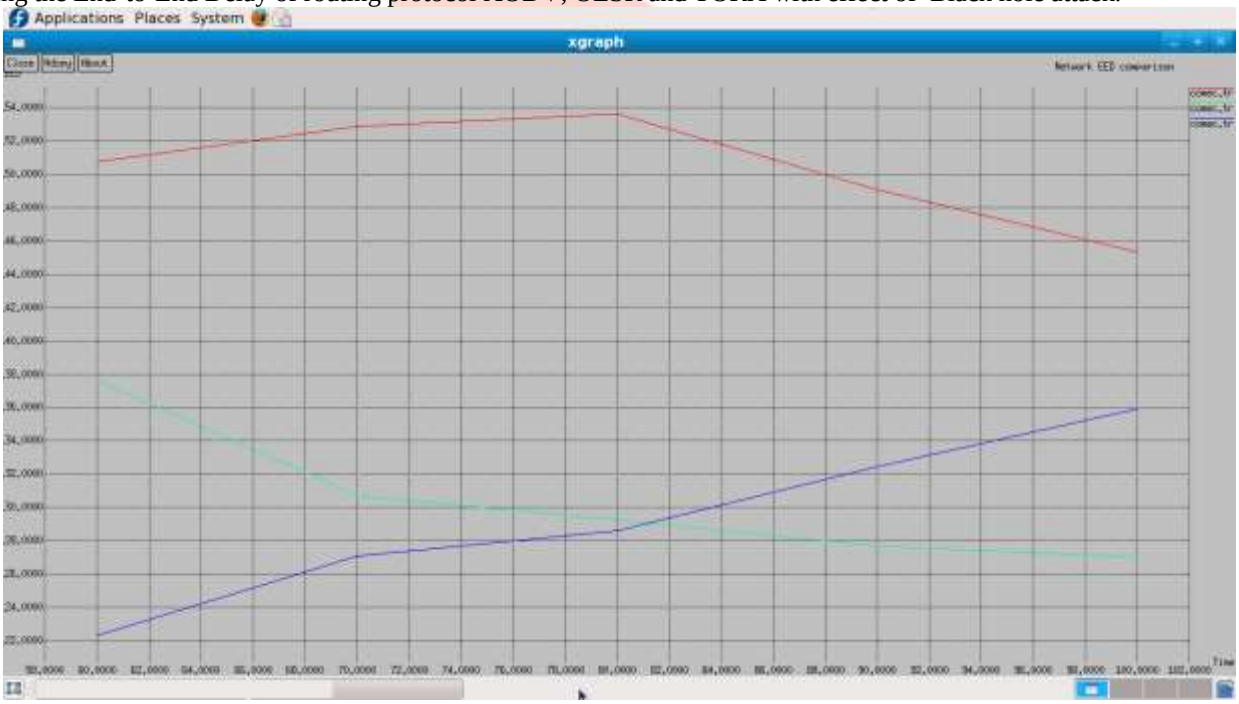

Figure 3.1 : End to End delay vs. Pause Time

4. Figure 3.1 compares the End-To-End packet delay of AODV, OLSR and TORA with Black hole attack. The behavior of attack (Black hole) depends on protocol, routing procedure and number of nodes occupied. Figure 3.1 shows the delay for AODV, OLSR and TORA. This result was passed out when black hole attack was introduced and the graph is compared with the normal working protocol so as to view the effect of attack on the whole network. The graph illustrates higher delay when there is a malicious node present in the network. Due to the present of malicious node, it consumes the packets transferred between source and destination, the end-to-end delay increases. The end-to-end packet delay included the delay for the route discovery if necessary. In this figure, TORA exhibited the lowest average end-to-end delay, while AODV had the highest delay in case of without attack. TORA had lowest average end-to-end delay because it did not need to rediscover the route for the same destination by maintaining the route entry in the routing table.

   Throughput:

   Comparing the throughput of routing protocol AODV, OLSR and TORA with and without the effect of Black hole attack:-

   Figure 3.2 shows the throughput for AODV, OLSR and TORA with black hole attack. OLSR in case of no attack (no malicious node present) is higher than the throughput of OLSR under attack (in the presence of malicious node). This is

because of the less routing forwarding and routing traffic. Here the malicious node rejects the data rather than forwarding it to the destination, thus effecting throughput.

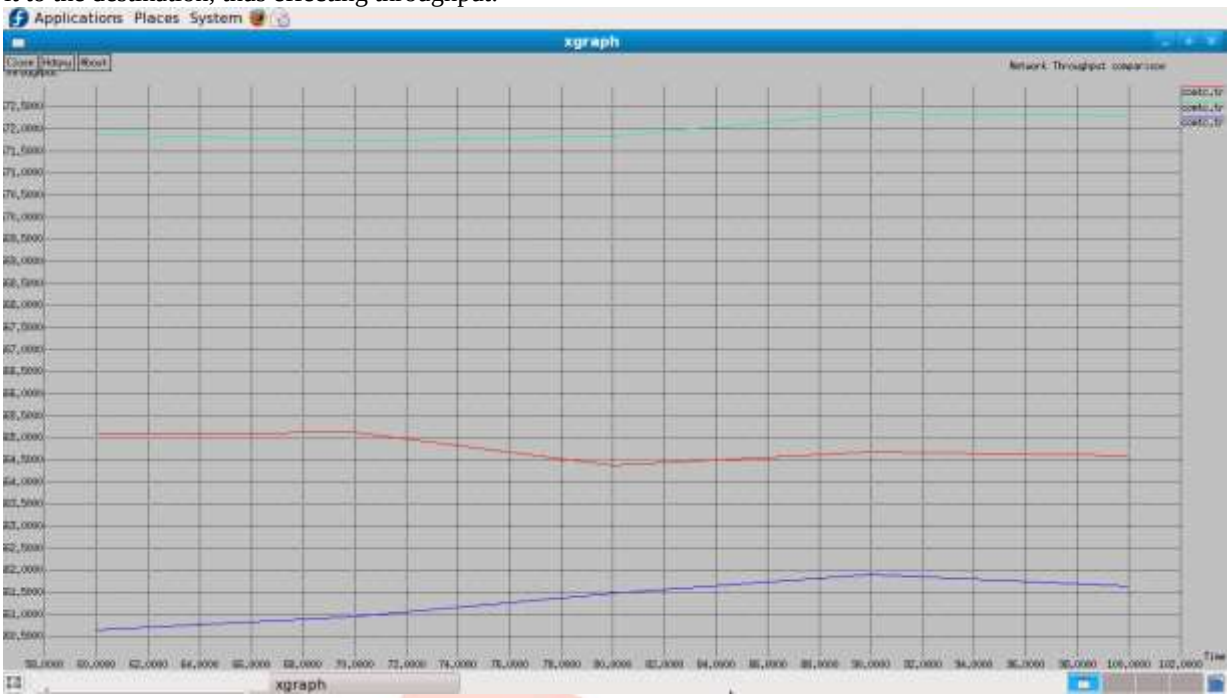

Figure 3.2: Throughput (kbps) vs. Pause Time

Packet Delivery Ratio:

Comparing the packet delivery ratio of routing protocol AODV, OLSR and TORA with the effect of Black hole attack: Figure 3.3 shows the PDR of the three protocols AODV, TORA and OLSR with attack. The PDR of AODV is greater than OLSR and TORA. With high mobility all three of protocols behave same but with less mobility AODV has maximum PDR, OLSR lies in between AODV and TORA. TORA has minimum PDR. Higher the PDR as good the routing protocol performed. In case of black hole attack PDR of these protocols decreases due to the present of malicious node present in the network

Figure 3.3 Packet Delivery Ratio vs. Pause Time

TABLE 3.1: Performance comparison of AODV, OLSR, and TORA with Black Hole Attack

Performance metrics		AODV	OLSR	TORA

Total throughput(in kbps)	Avg. Thp.	52.27	47.96	11.11
	Start Time	10.91	10.96	10.90
	Stop Time	49.97	49.99	40.58
Average end-to-end Delay(in sec)		52.596128	76.235037	30.902797
Packet Delivery Ratio	r/s	.7598	.7287	.5973

CONCLUSION & FUTURE SCOPE

Conclusion

Performance comparison of routing protocol in MANET is one of the important aspects. In this thesis, I have analyzed the performance and different act matrices for MANETs using different protocols (AODV, OLSR and TORA) and compared their performance matrices, like End to end delay, Packet delivery Fraction and Throughput with and without black hole attack. In Table 3.1 performance comparisons of routing protocols AODV, OLSR, TORA with and without black hole attack respectively are shown using ns2 simulator. For Throughput and PDF, AODV behaving the best and for End to End delay is concern TORA is taking less delay.

Having simulated the Black Hole Attack, results show that the packet loss is increased in the mobile ad-hoc network. Table's 3.1of simulation results show the difference between the degradation of performance of protocols due to the number of packets lost in the network with Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

Future Scope

Wireless Ad-Hoc networks are mainly used in networks due to their flexible nature i.e. easy to organize regardless of geographic constraints They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research.

REFERENCES

[1] C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks", Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[3] C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3561.html. [Accessed: April. 10, 2010]

[4] Y.F.Alem, Z.C.Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010.

[5] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[6] T.Clausen, P.Jacquet , "Optimized Link State Routing Protocol (OLSR)", RFC 3626 October, 2003

[7] Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.

[8] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.