International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Detection and Prevention of Blackhole Attack in Wireless Sensor Network Using Ns-2.35 Simulator

Abhinav Kaurav, Kakelli Anil Kumar
Department of Computer Science and Engineering, Indore Institute of Science & Technology, Indore, Madhya Pradesh, India

ABSTRACT

Wireless sensor network (WSN) is a network consists of tiny sensor nodes made of semiconductor device distributed over a large geographical area which is used to measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. These networks are easily prone to security attacks. Unattended implementation of sensor nodes in a geographical area causes many security threats in the wireless sensor networks. There are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Black Hole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. This can ultimately is drop of some important data packets and can disrupt the sensor networks completely. In this paper we have introduced prevention mechanism against the blackhole attack in WSN. We have used the popular AODV protocol mechanism to detect and prevent this attack in NS-2.35 simulator.

Keywords : Wireless Sensor Network, Blackhole Attack, Aodv Protocol, Ns-2.35 Simulator, Package Delivery Ratio, Throughput.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are a most challenging and emerging technology for the research due to their low processing power and associated low energy. The sensor network is a group of self-organized, low priced sensor nodes and creates network in spontaneous manner[1].The WSN combines sensing, computation and communication in a single small device, called Sensor Node. It mainly contains battery, radio, microcontroller and power devices. The sensors in a node provides the facility to get the data like temperature, pressure, light, motion, sound etc. and capable of doing data processing. All sensor nodes are connected to each other and forms a Sensor Node Network.

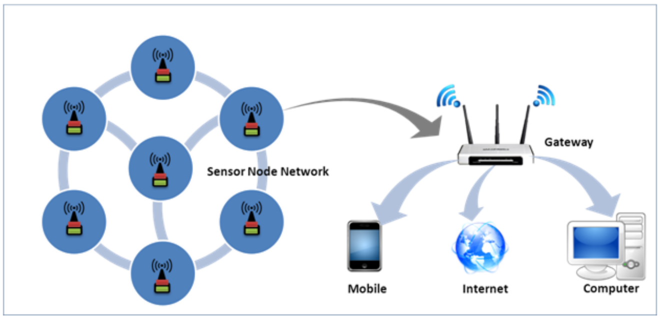


Figure 1: Architecture of WSN

A WSN system incorporates a gateway that provides wireless connectivity between the existing networks and sensor node network. Gateways may be considered as a proxy for the sensor network on the Internet. In this way the senor nodes gathers all the environmental information and transfer it to the internet through which the user can access it. Because of their static wireless network and less infrastructure environment of WSN, they are more vulnerable to many types of security attacks[2]. Generally, the attacks are of two types in WSN- active attacks and the passive attacks.

Black-hole attack is one of the harmful active attacks[3].

II. ATTACKS IN WSN

a) *Jamming*: Jamming attack is related with disrupting the radio frequencies used by sensor nodes. Attacker may get physical access to some nodes and creates jam in the network to disrupt the network[4]. Jamming attack come under physical layer attack.

b) *Tampering*: Refers to gaining physical access to a set of sensors by tampering with their hardware configuration and making nodes to act as adversary node. Tampering is possible at physical layer[9].

c) *Sybil Attack*: Sybil attack is defined as a malicious device illegitimately taking on multiple identities. An adversary can appear to be at the same time in multiple places in syblil attack. A single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of authenticated nodes[1]. It is a Network layer attack.

d) *Wormhole attack*: Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. This generates a false scenario that the original sender is in the neighborhood of the remote location. The tunneling procedure forms wormholes in a sensor network. The tunneling or retransmitting of bits could be done selectively[1].

e) *Hello Flood Attack*: Hello flood attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range (termed as a laptop-class attacker) and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN[5].

f) *Blackhole Attack*: In blackhole attack, a malicious node acts as a black hole to attract all the traffic in the sensor network through a compromised node or malicious node. A compromised node is placed at the center or any respective position, which looks attractive to neighboring nodes and attracts nearly all the traffic of surrounding nodes that was destined for a base station[1].

III. ROUTNG PROTOCOLS

PROACTIVE and REACTIVE Protocols are the two types of routing protocol.

a) *Proactive Protocol*: In this routing protocol, Routing tables are periodically distributed throughout the network to maintain fresh lists of destinations and their routes. The routing information is computed and shared and the path is set prior to the actual transfer of data packets between the source and destination. Example of Proactive routing protocol are- OLSR, DSDV, CGSR[6].

b) *Reactive Protocol*: In this routing protocol, routes are found on demand by flooding the network with route request packets. The source initiates the data transfer process by issuing a route request, the most relevant immediate neighbor issues a route reply to this request and takes forward the data transfer process. The process happens till the destination is reached and the data packet received .Examples of Reactive routing protocol are DSR, AODV, CBRP[6].

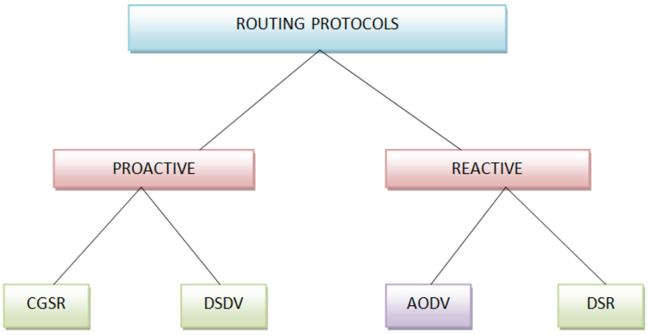


Figure 2: Routing Protocols

IV. AODV Routing Protocol

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is planned for use by mobile nodes in an ad hoc network. It offers quick adaptation to low processing and memory overhead, dynamic link conditions, low network utilization, and determines unicast routes to destinations within the ad hoc network[6]. AODV uses the destination sequence numbers to make sure loop freedom at all times, avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

AODV is a reactive routing protocol therefore it uses traditional routing tables, sequence numbers and one entry per destination are used to determine whether routing information is up-to-date and to prevent routing loops. It helps in both multicasting and unicasting. AODV makes use of route request (RREQ) and route reply (RREP) pair to find the route. The source node broadcast the RREQ i.e. Route Request message to its neighbors to find the route to destination. The RREQ message contains the source and destination address, lifespan of message, sequence numbers of source and destination and request ID as unique identification. The Destination Sequence Number is the very latest sequence number received in the previously by the source node for any route in the direction of the destination node. Source Sequence Number is the current sequence number to be used in the route entry pointing towards the source of the route request[6]. If any node from a list of neighbors is destination or knows the route to destination, it can send RREP message to source.

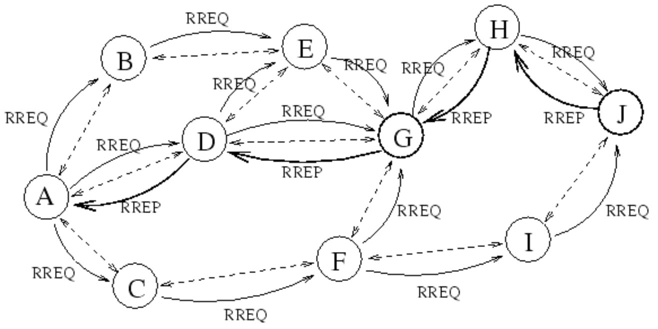


Figure 3: AODV Routing

V. BLACKHOLE ATTACK

Blackhole attacks are one of the attack in WSNs. It is an attack which is mounted by an external adversary on a subset of the sensor nodes (SNs) in the network. In the blackhole attack, a malicious node advertises the wrong paths as good paths to the source node during the path finding process as in reactive routing protocols or in the route updating messages as in proactive routing protocols. Good path means the shortest path from source node to the destination node or the most stable path through the sensor network[7].

Fig. 4 to illustrate these terms. In the figure, are black hole node is represented by red border and the black hole region is represented by dotted lines. When the source node selects the path which includes the attacker node, the traffic starts passing through the adversary node and this nodes starts dropping the packets selectively or in whole. Black hole region is the entry point to a large number of harmful attacks.

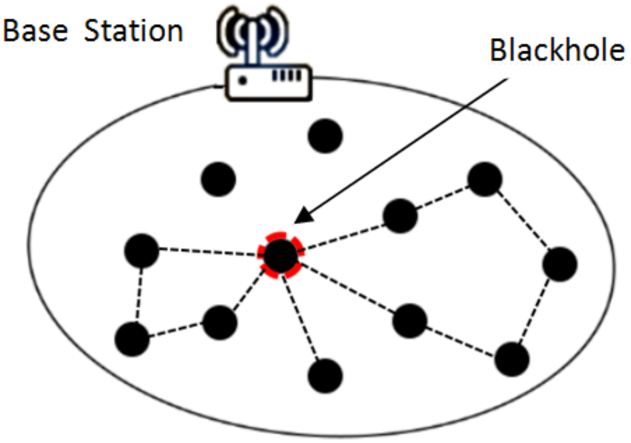


Figure 4: Blackhole Attack in WSN

VI. Mechanism of Blackhole Attack In AODV Protocol

In Blackhole attack a malicious node advertises about the shortest path to the node whose packets it wants to intercept.In figure 6, imagine node 3 is malicious node. When node 1 broadcasts a RREQ packet, nodes 2 and 3 receive it. Node 3, being a malicious node, this node does not check up with its routing table for the requested route to node 6. Thus, it immediately sends back a RREP packet, claiming that it has a route to the destination node[8]. Node 1 receives the RREP from node 3 before node 2 sends RREP.

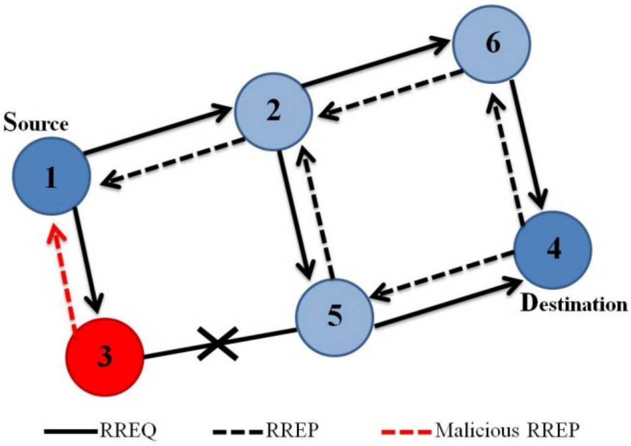


Figure 5: Blackhole attack in AODV

Node 1 assumes that the route through 3 is the shortest route and sends any packet to the destination through it. When the node 1 sends data to 3, it absorbs all the data and thus behaves like a Blackhole[10].

VII. NS-AllinOne-2.35 Simulator

It is developed by UC BERKELEY[6]. NS-Allinone-2.35 stands for Network Simulator version 2.35. It is called NS-Allinone-2.35 because it has a rich library of network and protocol objects. NS-2.35 is a discrete event simulator for networking research. It was developed as a part of VINT Project (Virtual Internet Testbed). It was a collaboration of many institutes like UC Berkeley, AT&T, XEROX PARC and ETH. Its first version was developed in 1995 and version 2.35 was released in 2011. Basically, NS-2.35 works at packet level. It provides substantial support to simulate bunch of protocols like TCP, UDP, FTP, HTTP and DSR. NS-2.35 simulates both the wired such as P2P links, LAN etc. and wireless networks like ad-hoc, cellular, GPRS, UMTS, WLAN, Bluetooth. It is UNIX based and use TCL as its scripting language as front end. NS-2.35 is a standard experiment environment in research community.

1.) *NS-2.35 Architecture*:

NS-2.35 simulator is based on an object oriented simulator, written in C++ and an object oriented extension of Tcl called OTcl interpreter which is used to execute user's command script. The interpreted OTcl one and the compiled C++ hierarchy are the two hierarchies classes with one-to-one correspondence between them[6].

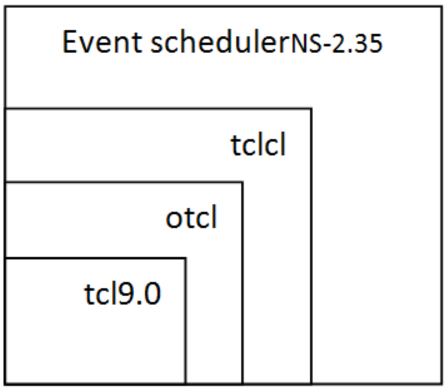


Figure 6 :NS-2.35 Architecture

Efficiency in the simulation and faster execution times is achieved due to the compiled C++ hierarchy. This is in particular useful for the detailed definition and operation of protocols. This provide us to reduce packet and also event processing time. Then in the OTcl script provided by the user, we can define a particular network topology, the specific protocols and applications that we wish to simulate and the form of the output that we wish to obtain from the simulator.

2.) *Simulation Setup*:

The various tools and the protocol to be used for this implementation and analysis have been selected by a thorough study of the reference papers and guidance provided by my mentor.To evaluate the behavior of simulated based black hole attack, to observe the network under the attack or not so, we considered the performance parameters of networks are Packet Delivery Ratio, Throughput and End to End Delivery Ratio.

A. Packet Delivery Ratio: Packet Delivery Ratio (PDR) is the ratio of number of delivered data packets to the total number of packets sent. The greater value of packet delivery ratio means the better performance[6].

B. Throughput:It is described as the total number of received packets at destination out of total transmitted packets[6].

C. End to End Delivery Ratio:It is described as time taken for a packet to be transmitted across a network from source to destination[6].

Parameter Type	**Parameter Value**
Protocol	AODV
Number of Nodes	7
PDR	r/s
Packet Type	TCP Packet
Simulation Time	100,000ms
Platform	Ubuntu
Simulator	NS-2.35
Malicious Node	1

Simulation is carried on by a display showing the working of the network with the protocols. This is done by using Network Animator (NAM). NAM is a TCL/TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation and various other data inspection tools.

VIII. Detection of Blackhole in AODV Protocol Using NS-2.35 Simulator

NS-Allinone-2.35 simulator generates a TCL (Tool Command Language) file. Three files are generated on running a TCL file, namely the first one is Terminal File which shows the status of the packet from which node the packet is delivered from the node the packet is forwarded. The second file is NAM (Network Animator) file which is a visual display showing all the nodes and how packets flow along the network. The third file is the Trace File which shows all the corresponding information regarding thenetwork and data flow In the figure 8, A network is created with multiple nodes which uses a AODV protocol. Then an attacker node (red) is implemented, where it generates the performance. The attacker node is attracting all the traffic towards itself by advertising it as a shortest path to the destination node (blue), it immediately sends back a RREP packet, claiming that it has a route to the destination.

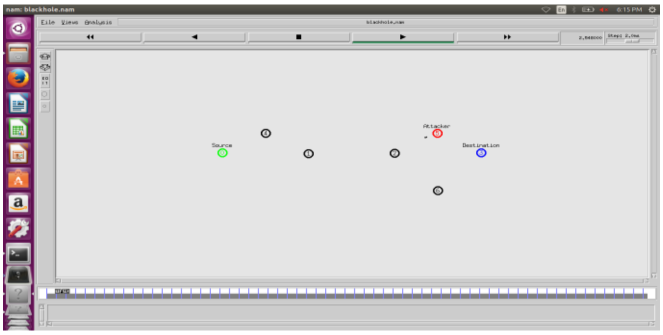


Figure 7: Packets are delivered to attacker node (red). It absorbs all the data and thus behaves like a Black hole and does not deliver to destination node. Hence, This results into 0 Packet Delivery Ratio (PDR) and therefore showing the network is attacked by blackhole attack.

IX. Prevention of Blackhole Attack in AODV Using NS-2.35 Simulator

To Prevent the blackhole attack we have used Intrusion Detection System (IDS) and provided a unique ID for each of the original sensor nodes.IDS monitor the traffic of the network and if it finds and irregular malicious activity by any node then sends an alert message to base station with the node information. The IDS is deployed on each node which can access the information of the node. When a packet is transmitted by the node, the IDS monitor the packet. IDS monitor each node and check is if all the nodes having the unique ID are transmitting packet in the network.

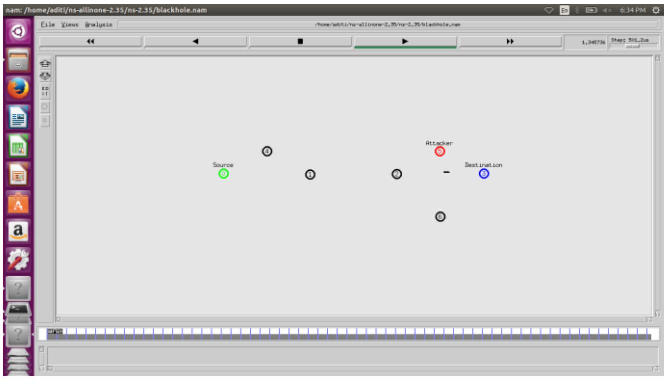
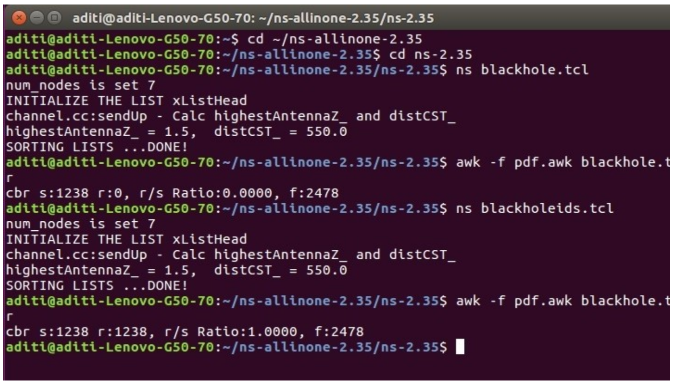


Figure 8: Packets are delivered to the destination node (blue) after successful prevention.

In figure 10, When the request packet (RREQ) is send by the source node (green), it identifies the unique ID of the destination node (blue) and the nodes through which the data packet is to be delivered. The IDS makes sure that the request data packets moves only through those nodes which posses unique identity.When the request packet received by the destination and they give the RREP to sender then the data packets are send by source node to the destination node. This results in to PDR ratio equals to 1, which means all the data packets are delivered successfully.

X. RESULTS

1.) *Package Delivery Ratio (PDR)*: The PDR (r/s) ratio observed during implementation of our proposed mechanism is shown in the figure 9 and the comparison of PDR between AODV with attack and AODV with IDS is shown in figure 10. The results show that during the attack in the WSN the PDR is 0, which shows none of the packet is delivered to the destination node. After the successful implementation of proposed security mechanism the increases drastically in AODV with IDS.



```
aditi@aditi-Lenovo-G50-70: ~/ns-allinone-2.35/ns-2.35
aditi@aditi-Lenovo-G50-70:~$ cd ~/ns-allinone-2.35
aditi@aditi-Lenovo-G50-70:~/ns-allinone-2.35$ cd ns-2.35
aditi@aditi-Lenovo-G50-70:~/ns-allinone-2.35/ns-2.35$ ns blackhole.tcl
num_nodes is set 7
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
aditi@aditi-Lenovo-G50-70:~/ns-allinone-2.35/ns-2.35$ awk -f pdf.awk blackhole.t
r
cbr s:1238 r:0, r/s Ratio:0.0000, f:2478
aditi@aditi-Lenovo-G50-70:~/ns-allinone-2.35/ns-2.35$ ns blackholeids.tcl
num_nodes is set 7
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
aditi@aditi-Lenovo-G50-70:~/ns-allinone-2.35/ns-2.35$ awk -f pdf.awk blackhole.t
r
cbr s:1238 r:1238, r/s Ratio:1.0000, f:2478
aditi@aditi-Lenovo-G50-70:~/ns-allinone-2.35/ns-2.35$ █
```

Figure 9: Packet Delivery Ratio (r/s) results display during proposed implementation.

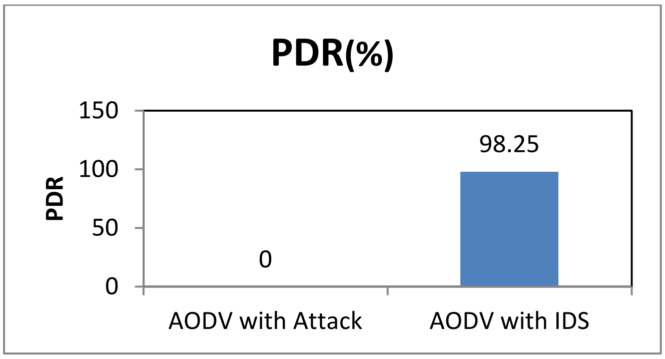


Figure 10: PDR comparison between AODV with attack and AODV with IDS

2.) *Throughput*: The comaparison throughput between AODV with attack and AODV with IDS is shown in the figure 11. The throughput during attack is very low as compared to throughput after the security mechanism applied through IDS.

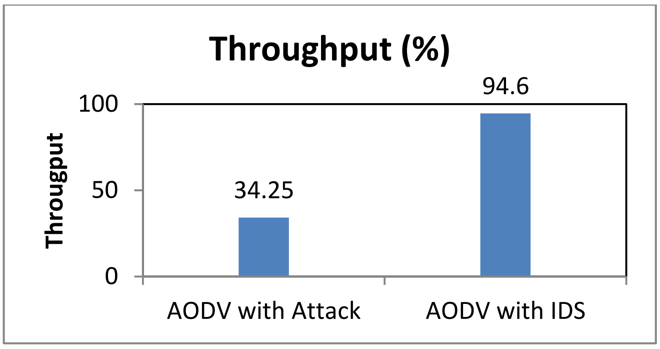


Figure 11: Comaprison of throughput between AODV with attack and AODV with IDS.

XI. CONCLUSION

In this paper we have introduced a security mechanism in Wireless Sensor Network.We have proposed Intrusion Detection System based on AODV protocol.The results clearly show that it is successful to detect the malicious nodes and prevent it by IDS. The packet delivery ratio of proposed IDS is 1 as compared with without any IDS system which is 0. Security of WSN is one the most demanding and prominent key feature in today's world. Therefore our future work will be focused on how to prevent the WSN in various other new protocols.

XII. REFERENCES

[1]. Dr. Banta Singh Jangra, VijetaKumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", IJEIT, Volume 2, Issue 3, September 2012.

[2]. Aditya Sharma, GarimaTripathi, MdSohail Khan, Kakelli Anil Kumar, "A Survey Paper on Security Protocols of Wireless Sensor Networks", IJEIT, Volume 3, Issue 8, Nov. 2015.

[3]. B.R.Baviskar, V.N.Patil, "Black Hole Attacks Mitigation And Prevention In Wireless Sensor Network", IJIRAE, Volume 1, Issue 4, May 2014.

[4]. Mohamed-LamineMessai, "Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application, University of A.MIRA Bejaia, Algeria, April 2014.

[5]. Dr. G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", IJCSIS,Vol. 4, No. 1 & 2, 2009.

[6]. Anu Arya, Jagtar Singh,"Comparative Study of AODV, DSDV and DSR Routing Protocols in Wireless Sensor Network Using NS-2 Simulator", IJCSIT, Vol. 5 (4 , 2014.

[7]. NiteshGondwal, ChanderDiwaker, "Detecting Blackhole Attack In WSN By Check Agent Using Multiple Base Station", AIJRSTEM, ISSN (Online): 2328-3580.

[8]. Sunny Chanday, Rajeev Kumar, Dilip Kumar, "An Intrusion Detection System Against Multiple Blackhole Attacks In Ad-Hoc Networks Using Wireless Antnet", IJRASE, Volume 3 Issue V, May 2015.

[9]. Vinay Soni, Pratik Modi, VishvashChaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network", IJAIEM, Volume 2, Issue 2, February 2013.

[10]. ChanchalAghi, ChanderDiwaker,"Black hole attack in AODV routing protocol: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.