International Journal For Technological Research In Engineering
Volume 5, Issue 12, August-2018 *ISSN (Online): 2347 - 4718*

DETECTION OF BLACKHOLE IN UNDER WATER ACOUSTIC SENSOR NETWORKS

Veena N[1], Dr. Akhila S[2]
[1]M.Tech Student [DCN, ECE], [2]Professor of ECE Department,
BMS College of Engineering, Bengaluru, Karnataka, India.

Abstract: ***The Sensor nodes are connected wirelessly to form a network called as the wireless sensor network (WSN). The nodes have confined battery power and the battery of the nodes cannot be replaced. These sensor nodes are used for collecting the sensor data and transmit them to the sink or base station. This data transmission from a node to the other node utilizes more energy if the data is broadcasted the from sensor nodes directly to the sink.***
In the black hole attack, the attacker node broadcasts good paths to the node falsely during the route-establishment process. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them. If the Black Hole Node is present in the network, it will reduce the network performance along with the depletion of the energy in the network. In this paper, the technique presented is for detection and isolation of black hole nodes from the sensor network. In this technique, the black hole node is identified by monitoring the fake reply packets that are transmitted by the nodes and it will be removed from the network.
For the implementation of our methodology NS2 tool is used. The overall results by the simulation increases the detection rate of malicious node and that leads to the increase in network performance by lowering the rate of packet drop ratio.
Key Words: UASN, Black Hole Node, Malicious node.

I. INTRODUCTION

A Underwater Acoustic sensor network (UASN) is a collection of sensor nodes spread over a particular area under water where the changes should be monitored. A Underwater Acoustic sensor network consists of sensing elements, storage unit, processing unit and these nodes can interact with the other nodes. All sensor nodes transmit through a wireless transmission. The sensor nodes are randomly distributed in the area. If the sensor node is not able to transmit to the other node through an explicit link, i.e. they are out of their broadcasting range; the packet can be sent to that node by using the intermediate nodes. The concept of using the intermediate nodes to transmit the data is called as multi-hopping. There is no requirement to provide an infrastructure to set up the network as the wireless sensor networks are not the centralized systems. The wireless sensor networks have the end-to-end communication between the nodes. Wireless sensor networks have self-healing and self-organizing capabilities. Self-healing allows the sensor nodes to reconfigure themselves and try to discover an alternate path for the nodes when the link fails or powered-down. The sensor node collects and forwards the data to the information sink using the multi-hop wireless network. A sensor network is self-organizing because it permits the network to join a new node without any transmission interference.
Sensors are the powerful accessories which are capable of gathering the data from different devices, stores them, sensing and transmitting the information to the sink or the base station. The sensor networks have the ability to withstand environmental conditions and it has the ability to cope with the node failure. In wireless sensor networks, the sensor nodes are cooperative in nature and are organized in a cooperative manner. In sensor network, nodes are not required to be installed, as they are easily deployed anywhere in the network. The data gathered from different devices can be retrieved from either the sink or the base station.
AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node [1]. Black hole leads to serious loss in the network by receiving the packet and dropping the received packets that has to receive by the destination.

1.1 AODV

As the name describes AODV forms the route from source to destination and between the intermediate nodes when there is demand for forwarding packets using MANETS. AODV (Ad-hoc On-demand Distance Vector) is a reactive routing protocol, yet it is fundamentally an improvement of DSDV routing protocol which is proactive protocol [2]. Route discovery process takes place onlywhen required.
AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings. However, it makes no provisions for security. In Route Discovery Process of AODV there are three types of messages: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages.
 RREQ- It is basically the broadcast request to find the route to a required destination node. Thus it helps to create a route discovery process by broadcasting Route Request message to its neighbouring nodes. The neighbouring nodes save the path where RREQ request is transmitted. After that it verifies the new or fresh route to the desired node in the routing table by the use of RREQ request [3].
 RREP- when the node finds a fresh path for destination then a route reply message is unicasted to the originator of the RREQ if the receiver is either the node using the requested address or is having a valid route to the requested address.
 RRER-it helps to keep eye on link status of the next hopin

the appropriate route. RERR message is broadcasted to whole nodes whenever the breakage in the link is found. This is also called route maintenance.

Advantages:

 Connection set up delay is less

 Destination sequence numbers are used to find the latest route to the destination.

 On-demand route establishment with small delay

 Link breakages in active routes can be efficiently handled

Disadvantages:

 Periodic beaconing leads to bandwidth consumption

 Intermediate routes can lead to inconsistent routes if the source sequence number is old.

 Multiple RERR packets in response to single RREQ packet may lead to heavy control overhead

1.2 INTRODUCTION TO BLACK HOLE ATTACK

A black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified destination and drops all the receiving packets [4]. A Black Hole node has two properties: (a) the node enters in AODV by represent itself as a valid route for destination.

Then it starts receiving the packet from the valid node (b) drops the packet containing valuable information.

 Single Black Hole Attack: In single black hole attack only one malicious node attack on the route [5]. When the source node broadcast RREQ message then the malicious node takes an advantage of vulnerabilities of AODV protocol. It responds with high sequence number to its preceding node in the path. Thus source node assumed malicious node as a destination node and start the process of data forwarding. The malicious node then drop all the packet received.

 Co-operative Black Hole Attack: The number of malicious notes is more than one in the network [6]. The overall result of cooperative is complete decrease in throughput and increase in packet drop ratio in the network. Thus for better security and better performance in UASN's it is very important to eradicate the Cooperative attack.

II. ASSUMPTIONS & METHODOLOGY

2.1 ASSUMPTIONS:

The whole methodology is based upon the following assumption to analyses the network performance with and without the effect of malicious node at distributed levels.

1. Malicious node does not acknowledge with data packet in the network.
2. Black hole node will receive the packet but instead of forwarding the packet it will drop all the received to lower the packet delivery ratio and network efficiency.

2.2 Model

The below model describes overall architecture of execution of blackhole in NS2 environment. It has both Otcl & C++ backend execution models. We write TCL Scripts which intern calls C++, Operation execution done by calling the particular .cc file which takes helps from header files (.h) and creates obj file (.obj).

The Execution is done based on layering concepts which works based on open system interconnection (OSI). These are typically consist of 7 Layers each layer has its own functionality. In ns2 we would like to take care of all the layers. Below diagram depicts layer wise functionality.

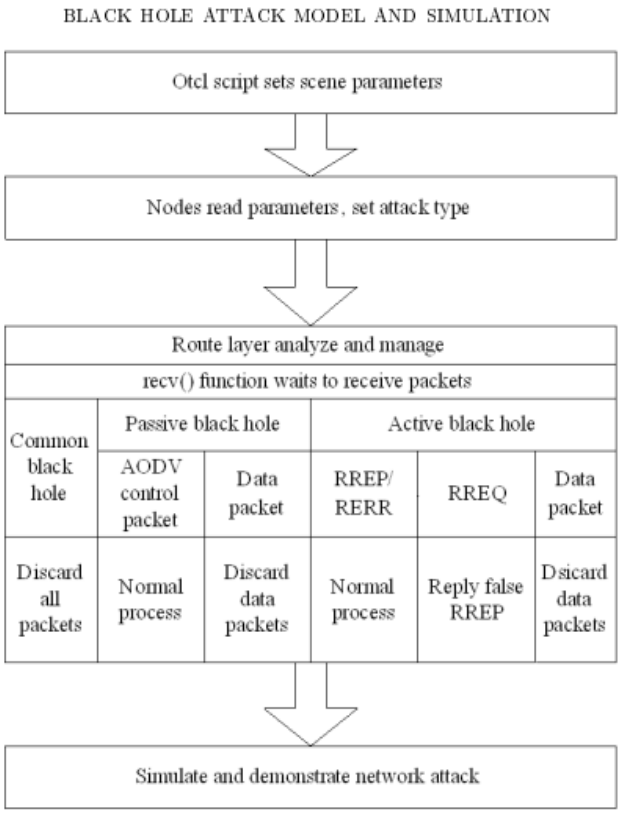

Fig 1.1 Overall Simulation Model of BlackHole Network

2.3 METHODOLOGY:

For the performance analyses of network with and without the entry of malicious nodes, distributed approach is proposed. For that firstly deploy the nodes in the networks. Introduce the cooperative black hole nodes in the network.

Detection of malicious nodes - The detection of cooperative black hole nodes within network are done with the help of nodes. Here, if any member of the network does not acknowledge with network then it is treated as a black hole.

Sequence Number Comparison: This method is similar to the Detection, Prevention and Reactive AODV method. In this method, it will check the sequence number of the source node and the sequence number of the intermediate node who will send the route reply message to the source node first. Here a system is developed for comparing the sequence number. The comparison is done in between the sequence number of the route request method and the sequence number of the route reply method. If there is a huge difference is detected or measured the method considered it as the route reply is coming from the malicious node. This method will just remove that node from the routing table and make it isolated from the network. In this presentation we are using this method to detect the Black-Hole attack. This method is very simple and most effective. This method is not only detecting the black-hole node but also preventing the network from the malicious node.

Parameter	Value
Simulator	NS-2
Version	NS 2.35
Number of Nodes	25
Channel	Wireless channel
Traffic Type	CBR
Routing Protocol	AODV
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
AntennaType	Omnidirectional

Table -1: Simulation Parameter Table

METRICS FOR SIMULATION

Throughput ratio: It is defined as a rate at which message is successfully delivered between a source and sink. It is measured as bits per second. More is the throughput ratio more will be the performance of the network.

Packet delivery ratio: It helps to predict the drop rate of packet. It is basically the ratio of the total number of data packets received by the sink to the total number of data packets sent by the source node. Similar to the throughput ratio, the value of packet delivery ratio must be high for better network performance. Its higher ratio leads to the decrease in drop rate of packet.

Attack Detection Rate: Rate that defines number of black hole node detected with the total number of black hole nodes taken.

Energy Consumption: It is defined as number of Energy consumed for data transfer between nodes in overall simulation time. It is measured as joules per second. Less is the energy consumed more will be the lifetime of the network.

E2E Delay: It is defined as time taken by the two nodes to deliver an data/message between them. The Average end to end delay is measured in secs.

III. SIMULATION SCENARIO USING NS2

3.1 Deployment of nodes in the network

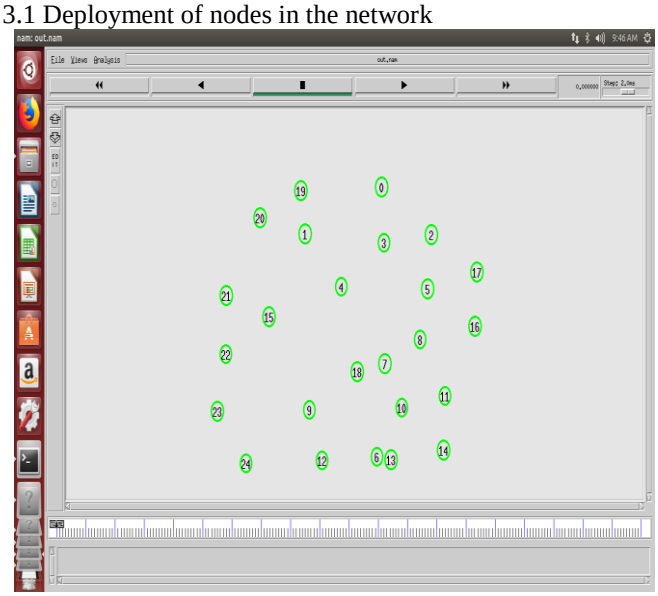

Fig 1.2 Deployment of Nodes

IV. RESULTS AND COMPARISON

The proposed methodology is compared with the existing approach of safe route method based upon the sequenced number of route reply message on the basis of throughput, packet delivery ratio and attack detection rate.

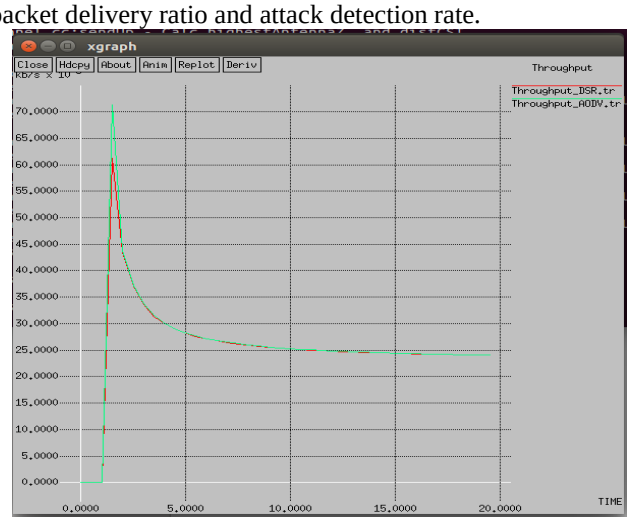

Fig 1.3 Throughput Analysis

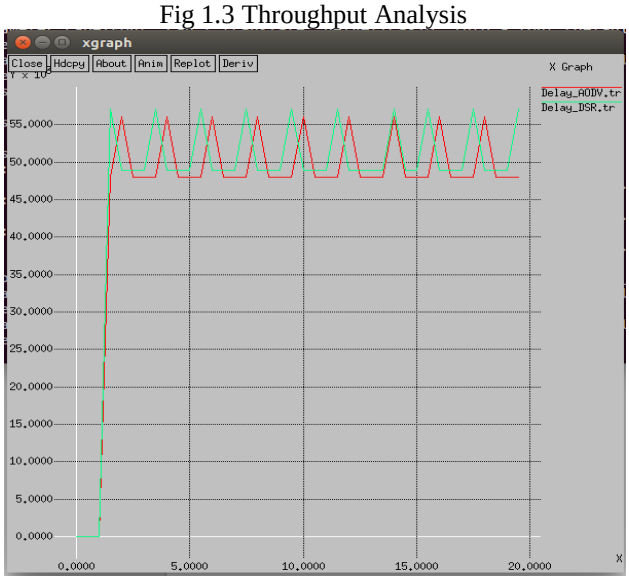

Fig 1.4 Delay Comparison b/w AODV & DSR

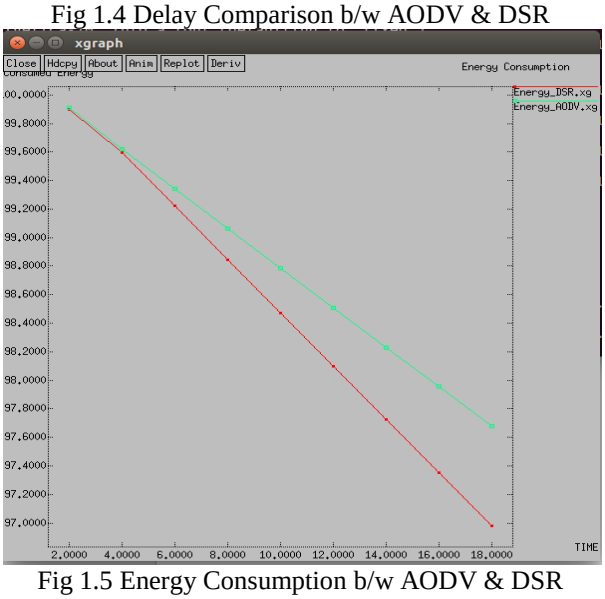

Fig 1.5 Energy Consumption b/w AODV & DSR

V. CONCLUSION AND FUTURE WORK

Black hole attack is hazard to AODV. In the existing approach of safe route method based upon the sequence number they are only able to detect the malicious node that occurs between the route of source and destination instead of detecting black hole nodes in the whole network. Our approach successfully detects the malicious nodes in the entire network and simulation results are predicted to be more efficient than the existing approach of safe route method with high packet delivery ratio as well as high detection rate of black hole nodes.

REFERENCES

[1] Gurung, Shashi, and Krishan Kumar Saluja. "Mitigating Impact of Blackhole Attack in MANET." Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC. 2014.

[2] Abusalah, Loay, AshfaqKhokhar, and Mohsen Guizani. "A survey of secure mobile ad hoc routing protocols."Communications Surveys & Tutorials, IEEE10.4 (2008): 78-93.

[3] Akhlaq, Monis, et al. "Addressing security concerns of data exchange in aodv protocol."World Academy of Science, Engineering and Technology16 (2006): 29-33.

[4] Sowmya, K. S., T. Rakesh, and P. HudedagaddiDeepthi. "Detection and Prevention of Blackhole Attack in MANET Using ACO."International Journal of Computer Science and Network Security12.5 (2012): 2124.

[5] Goyal, Priyanka, VintiParmar, and Rahul Rishi. "Manet: Vulnerabilities, challenges, attacks, application."IJCEM International Journal of Computational Engineering & Management11.2011 (2011): 32-37

[6] Khin, Ei andThandarPhyu. "Comparative Analysis of Black Hole Attack Solutions in AODV Protocol."IJCCER1.2 (2013): 21-25.

[7] Devassy, Antony, and K. Jayanthi. "Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting."

[8] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." Communications Magazine, IEEE 40.10 (2002): 70-75.

