Effect on Packet Delivery Ratio (PDR) & Throughput in Wireless Sensor Networks Due to Black Hole Attack

M.Khaeel Ullah Khan, K.S.Ramesh

Abstract— Wireless Sensor Networks are in rapid advance occupying every field of our lives. They are in great demand and are widely used in transmission of data like temperature, pressure, humidity, speed etc. As these networks are wireless and are easily prone to intrusion by the attackers. Hence the basic concern is security of data. The nodes in the network will be sending information between the nodes, and in between the nodes intrusion takes place with attack like wormhole attack, black hole attack, sybil attack, hello flood attack etc. which corrupts data. These attacks effect the efficiency of the network and the parameters like packet delivery ratio and throughput of the network is affected. Black hole is a severe attack in network which alters most of the data before it is received at the sink, hence has to be detected and prevented.

In this paper, Adhoc on demand distance vector (AODV) protocol is used to detect and prevent the black hole attack using Network Simulator (NS-2.3)

Keywords— Sensor Network, Black hole attack, AODV Protocol, Network Simulator-2.3 Simulator, Packet delivery ratio, packets transmitted from input to output (Throughput)..

I. INTRODUCTION

Sensor Networks are the widely used networks in today's world as it does not require highly configured and permanent network as well requires low power for transmission of data in the network. The basic blocks of the wireless sensor networks are motes which consist of sensors which sense the desired data, process it according to the function and transmit it. Motes will also consists of power source as battery, transmitting component as antennas, the computing and processing elements as microcontroller, storage components memory. Sensor networks do not have well defined permanent networks but creates its own adhoc network which is self designed as per the need [1]. The major issue in these networks is the power as the networks are runs with the power source as independent battery and also the concern in the network is security as it is more prone to the external attacks by intruders. There are many algorithms developed for the efficient utilization of the power like LEACH, MODLEACH etc. When intruder attacks the network the mostly it effects the transmission of packets by modifying the data or completely averting the data in reaching the destination node hence by dropping the throughput. Hence in this paper, a comparison is made on the important parameters of the network such as packet delivery ratio and throughput with and without black hole attack effect and shown that with black hole attack the quality of the network is considerably decreased.

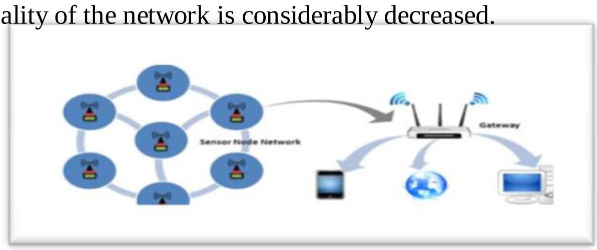

Figure 1: A wireless sensor network interfaced with other networks

Figure 1, shows structure of wireless network, which is interconnected with other networks like mobile network, internet and to the other computer node with a gateway which connects the already available networks with the sensor network. As it is well known that gateways works as the intermediate modules between the sensor network and the internet.

The nodes in the network collects information, process it out and sends it to destination, from which user can access the data [2].

As these networks are not having a standard infrastructure as wired networks have they are prone to the attacks.

II. ATTACKS IN WIRELESS SENSOR NETWORKS

- Jamming attacks
- Wormhole attacks
- Sink hole attacks
- Hello flood attacks
- Rushing attacks
- Greyhole attacks
- Black hole attacks

2.1: Jamming attack

Jammers are used to prevent the successful transmission of the data between sink and hole in Wireless Sensor Networks. A jammer node is pushed into the network which it stops data transmission among the nodes. Jammer nodes can be classified as internal jammer nodes and external jammer nodes [3&4].

Internal jammer nodes are defined and present within the cluster and are having a chance to become the nodes for transmission.

External Jammer nodes are outside the cluster.

There are four types of Jammers.

(a) Constant jammer

(b) Deceptive jammer

Revised Manuscript Received on September 14, 2019.

M.Khaeel Ullah Khan, Research Scholar, ECE department of K L University, Vaddeswaram, Guntur district, A.P, India.

K.S.Ramesh, Professor, ECE department, of K L University, Vaddeswaram, Guntur district, A.P, India.

Retrieval Number: L110710812S19/2019©BEIESP
DOI: 10.35940/ijitee.L1107.10812S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(c) Random jammer
(d) Reactive jammer

2.2: Wormhole attack

In these attack two intruders interrupt the flow of data in the network, which is termed as worm hole attack. An attacker tunnels in the network through weak link and from that point alters the data in receiving to the other node. The tunnel between two colluding intruders is called wormhole. Packet leash is used in avoiding the attack.[5]

2.3: Sinkhole attack

Sinkhole attack is considered as complex attacks in wireless sensor networks. If routing protocol characteristics are known, the attacker can easily attract the traffic through that point. It can divert the traffic through the attacked link rather than moving through the normal link. The nodes which get attacked by sinkhole attack will be under the attacker control and can lead to other attacks like grey and black hole attack as well.[6]

2.4: Hello flood attack

In hello flood attack the intruder sends 'HELLO' packets as convincing packets to sensor node in the network. Intruder uses high radio transmission range referred as Lap-top attack and sends HELLO packets for processing to the large number of nodes in WSN.

2.5: Rushing attack

In rushing attack, more than one intruder conspire and use a high link path for intrusion as is done in worm hole attack. The networks which require fast transmission of data between source and sink, the affected tunnelled data packets are transmitted faster than those of the normal rate using multi-hop route. As the propagation is fast, this attack is termed as rushing attack which is denial of service (DoS) attack.

2.6: Grey hole attack

In wireless sensor network, grey hole attack intercepts the normal flow of packets. The attack procedure has two steps. In initial step, a effected node interrupts the ad - hoc on demand distance vector protocol by advertising itself as valid node in the route from initial node (source) to final node(destination), for interrupting the normal flow the data and makes the normal route as malicious.

The node which is affected in the first stage drops the data packets in the second stage arbitrarily. Due to the misbehaving of the routing, it leads to packets selectively. For countering the grey hole attack the best method is employing signature algorithm which traces the affected nodes which are dropping the packets in network. This attack resembles the black hole attack. Due to greyhole attack the normal node suddenly starts acting as affected node and drops packets in network. Security for this attack is exigent [7].

2.7: Black hole attack

Black hole attack is one of the denials of service attacks where the node attacked by intruder transmits a fault message to the source which is having a very short propagation distance to the sink node. Then source node will form a different route and forward the packets to the effected node. In turn the malicious node stops sending these data packets to the destination node. Other flavour is co-operative attack in which many nodes are affected by it which adversely effects the network performance [8].

As to assure flow of packets between the transmitting and receiving nodes , protocol will designate one destination node such that it identifies the source of given data, also the source node is designated by the protocol in for verifying packets being sent to desired destination node. Hence, effected node which is attacked, is segregated from the nodes thereby routing process is secured. A safe wireless protocol with payment method that avoids node to be itself in networks after attack is evolved and studying metrics of network with and without attack is compared in this paper. Sending of data between source and sink can be done effectively and securely with the design of intermediate nodes. To have low packet drop ratio and throughput data has to be continuously monitored, verified and secured in the network by the designed algorithm to avoid intrusion.

III. ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

3.1: Proactive protocol:

In pro-active routing protocol, all the destinations as well routes of the network are formed as rows and columns which forms the routing tables and is well defined in the network to have periodical check. Before transmit of the packets information of the routing is processed initially and shared while the packet transmission takes place. That is the set of route from source to sink is defined beforehand itself. Some of the proactive routing protocols are optimized link state routing protocol (OLSR), destination sequenced distance vector protocol (DSDV), Cluster switch gateway routing protocol (CSGR)[6].

3.2: Reactive protocol:

Reactive routing protocol, a request is made by the source to destination for the transfer of the data packets with a command 'route request'. Then, the process of data transfer starts when a route request is initiated, immediately the neighbour nodes of the source node responds then source forwards the data. The process of transmit of data will continue till the all the data is transferred. Dynamic source routing(DSR), Ad hoc on demand distance vector (AODV) and Cluster based routing (CBR) are examples of reactive routing protocol schemes. [9].

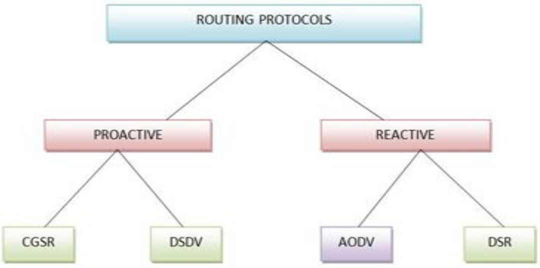

Figure 2: Different routing protocols in WSN

IV. THE AODV PROTOCOL

In many of the networks the widely implemented protocol is ad hoc on-demand distance vector (AODV) routing protocol. It is extensively used in mobile transmissions as it is easily adaptable. In a network where the processing rate is low, memory overhead is required, dynamic link is needed, low network utilization is required and a decision is to be made using unicast routes from source to destination within the ad hoc network[10]. A unique sequence called destination sequence ordered numbers are used in AODV protocol for verifying the availability of loop at any time, and hence reduce the cases such that count should not tend to infinity, which is encountered in other distance vector protocols. As discussed earlier the use of routing arrays, sequence identifiers and single allocation for end node is availed to find out the status of data and to avoid overlap of reroute loops of reactive protocol. This technique enhances the transmission in both multicasting and unicasting. The commands like route request (RREQ) and route reply (RREP) are used to check out the route path in AODV. The first node broadcasts the RREQ i.e. it sends message to its neighbouring nodes for checking the path to final node. Address of initial node and sink nodes are in RREQ message, also it contains time of alive nodes, sequence identifiers of first, last node and request identification as sole entity number. The designated destination identification entity is the most recent identification number which is taken for prior search by node which wants to transmit the data in the route of final node which is receiving the data. Source identification entity points to present identification number that is availed for path ingress directing in the direction of final node of the route request [6]. When a packet entity is nearer to the receiving node or falling in the route of destination from the list after which RREP message is send to source.

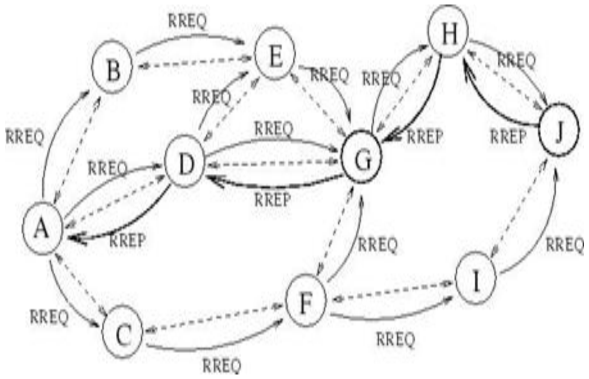

Figure 3: AODV Protocol

V. BLACK HOLE ATTACK

The major issue in wireless sensor networks is security of the data as they are easily accessible to attacks. Intruders attack the network by sending malicious data packets in the network. One among the wireless networks attacks is black hole attack, in which a subset of sensor nodes is formed and introduced in the network externally. Due to this attack new routing paths are introduced by the intruder with the help of malicious node as though they are a part of the designed algorithm and hence manipulated the routes. As the packets has to be transmitted in the shortest path from source to destination in the network, due to the black hole attack even the other paths are also shown as shortest paths and hence the sensor network becomes instable as the packets are dropped.[11 & 12].

Figure 4 shows the node attacked by black hole as red node border and the area which is attacked by black hole is shown as dotted lines. While transmission starts from source to destination, source node selects the shortest path but if malicious node attacked by the black hole attack is included in the path of selection, then the packets are dropped completely or partially by the attacked node and hence decreases the throughput of the network. If this attack is not detected and prevented at the early stages then it will have adverse effect at the further stages. [1,2].

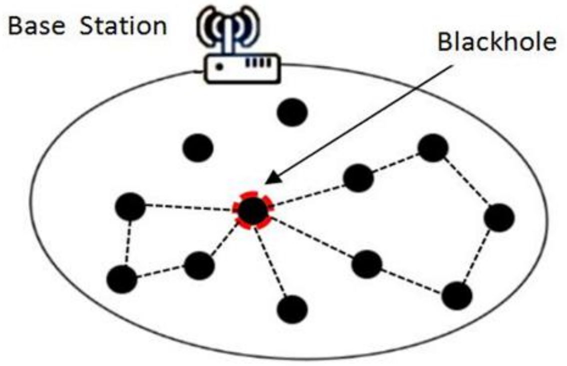

Figure 4: Black hole attacked node

The black hole attack intruder designates the attacked node or the malicious node in the shortest path to divert the packets in the other route rather than shortest path. In figure 5, let node 3colored red is black hole attacked node. As node numbered1 sends the message RREQ packet, nodes designated 2 and 3 accepts it. As node 3, is a affected node, it will not verify given routing table for the requested route to node 6. Hence, node 6 at that time responds again a routing request packet, claims as though route is having path towards final node [13]. Therefore first packet entity gets the routing request packet from red - node before second entity sending RREP.

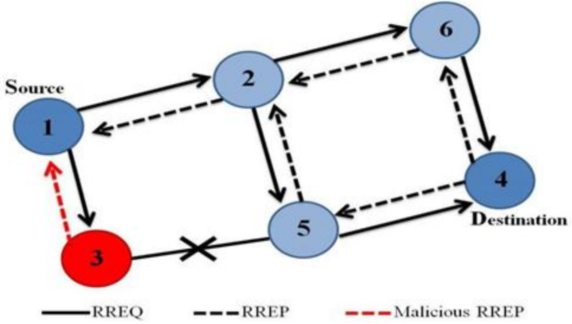

Figure5: Black hole attacked network

VI. PROCEDURE TO DETECT BLACK HOLE ATTACK

A number of sensor nodes are created in the network and AODV protocol is implemented. An attacked node is pushed in network (red node). Due to this malicious node the routing path is altered as it attracts the data as though the path crested by this node is shortest path. The intruder labels the node as it is in the shortest path from source to destination nodes (blue). As soon as any node sends the RREQ request the malicious node immediately responds with RREP and diverts the flow of packets from source to destination. Hence packets are delivered to red node instead taking the path to destination. Then it takes up all the data and will not any packet to the actual destination node, thereby decreasing the through put and packet delivery ration of the network. Packets are delivered to the attacker node (red node).It absorbs all the data and behaves as Black hole and does not deliver the data to the destination node [14].

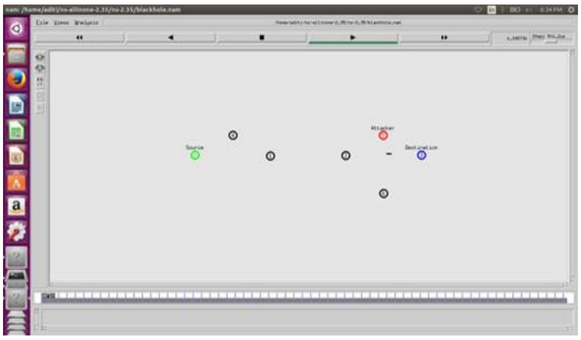

Figure 6: Packets transmitted successfully to the sink (blue nodes)

VII. PREVENTION OF BLACK HOLE ATTACK IN NETWORK

In this paper a method is proposed for prevention of black hole attack, in which each node is assigned by a unique identification number for every original node. This method intrusion detection system monitors the flow of packets from initial to final node and if any abnormalities in the data traffic or any malicious node is found then it immediately sends the message to the base station with that particular node details. This intrusion detection system developed in such a way that it monitors every node in the network.IDS monitors each node from Source to Sink node and the transmission of the packets. IDS always checks out for the unique ID designated to the nodes [14].

VIII. SIMULATION SETUP:

The tool used for simulation of the attacked network is Network Simulator 2.3. The protocol is AODV and number of nodes are 10. The key quantitative variables are packet delivery ratio, throughput and end to end delivery ratio of the network.

A Packet delivery ratio:

Packet delivery ratio (PDR) can be measured as the ratio of number of packets delivered in total to the total number of packets sent from source node to destination node in the network. It is desired that maximum number of data packets has to be reached to the destination. As the value of PDR increases the performance of the network also increases [15].

B Throughput:

In wireless sensor network throughput can be termed as number of successfully transmitted packets from source to destination per second. For good designed network the value should be high and if it is attacked by any attack the value of throughput considerably decrease. [16].

Parameter	**quantity**
Protocol	AODV
Simulator	NS-2.3
Number of nodes	10
Packet	TCP
Simulation time	100000ms
Operating platform	Ubuntu
Malicious node	1

Table: Simulation setup

IX. RESULTS

In the proposed paper, a node which is attacked by black hole is made available in network and simulated for measure the following parameters:

(a). Packet delivery ratio (PDR) : A comparison is made with and without black hole attack in network and PDR is calculated. It is found that during the attack PDR is very less compared to the ratio without attack, which illustrates fewer packets are reached to the sink node.

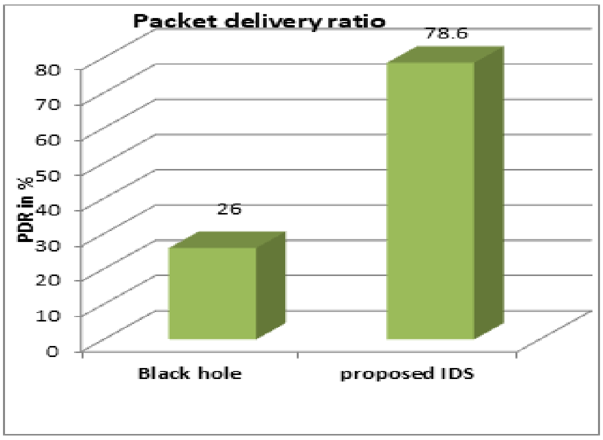

Figure 7: Comparison of packer delivery ration in network

After implementation of the proposed system PDR increases.

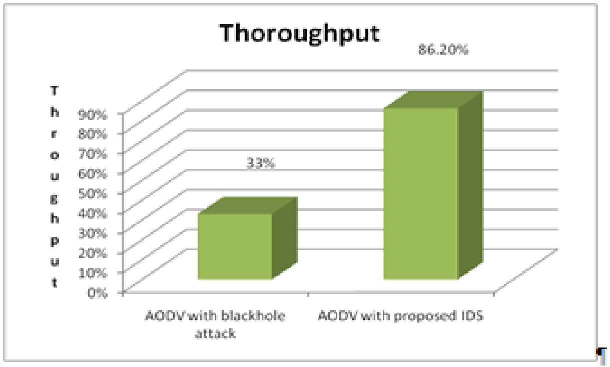

Figure 8: Comparison of throughput of the network

Retrieval Number: L110710812S19/2019©BEIESP
DOI: 10.35940/ijitee.L1107.10812S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

X. CONCLUSION:

After simulation it is clearly seen that the black hole attack is having a considerable effect on packet delivery ratio and throughput in wireless sensor networks. Hence as this attack is vulnerable, hence it has to be detected and prevented in wireless sensor networks for better efficiency of transmission..

REFERENCES

1. A study on Black hole attack in Wireless Sensor Networks by Umashankar Ghugar, Dr.Jayaram Pradhan in International Journal of advanced computing and applications, ISSN 2321-4546, Issue 1, June 2017.
2. Adwan Yasin, Mahmoud Abu Zant, “Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique” Wireless Communications and mobile computing, Volume 2018, Article ID 9812135, 10 pages, https://doi.org/10.1155/2018/9812135
3. Fan-Hsun Tseng, Li Der-Chou, Han-Chie Chou,”A survey of black hole attacks in wireless mobile and adhoc networks” Human-centric Computing and Information Sciences,22 Nov.2011.
4. Rashmi, Ameeta Seehra, “ Detection and prevention of black hole attacks in MANETS” International Journal of Computer Science Trends and Technology, Vol.2, Issue 4, Jul-Aug. 2014.
5. Khaled M. Elliethy, Drazen Blagovic, Wang Cheng, Paul Sideleau, “Denial of Service Attack Techniques: Analysis, Implementation and Comparison”, Systemic, cybernetics and Informatics, Vol. 3, No. 1, pp: 66-71
6. Brain Yarbrough,Neal Wagner, “Assessing security risk for wireless sensor networks under cyber attack ”, SpringSim-ANSS,Society for modelling and simulation international, April 2018.
7. Parli B.Hari, Shailendra Narayan Singh, “Security issues in Wireless Sensor Networks: Current research and challenges”, 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring): DOI: 10.1109/ICACCA.2016.7578876
8. Mohammed Tanveer Khan, “Review: Network security mechanisms and cryptography”, International Journal of Computer Science and mobile computing, Vol. 6, Issue 7, July 2017, pp: 138-146.
9. Chaudhari H.C. and Kadam L.U., “Wireless Sensor Networks: Security, Attacks and Challenges”, International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16.
10. Gurijender Kaur, V.K.Jain, Yogesh Chaba, “Detection and Prevention of Blackhole Attacks in Wireless Sensor Networks”, International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, 11 October 2017, pp 118-126.
11. Y.Pavan Kumar Gupta, M.Madhu, “Improving security and detecting black hole attack in wireless sensor networks” , International Journal of Professional Engineering Studies, Volume 8 /Issue 5 / Aug. 2017.pp: 260-265.
12. Different types of attacks in Mobile ADHOC Network: prevention and mitigation techniques. http://www.doc88.com/p-410724870368.html.
13. Wu B., Chen J., Wu J., Cardei M. Wireless/Mobile Network Security. Berlin, Germany: Springer; 2006. A survey on attacks and countermeasures in mobile ad hoc networks.
14. Qussai M Yaseen,Monther aldwairi, “An enhanced AODV protocol for avoiding black holes in mantes” , Procedia computer Science,Volume 134, 2018,pp:371-376.
15. Culler D., Estrin D., Srivastava M. Guest Editors’ introduction: overview of sensor networks. Computer. 2004;37(8):41–49. doi: 10.1109/mc.2004.93. [Cross Ref]
16. Bellavista P., Cardone G., Corradi A., Foschini L. Convergence of MANET and WSN in IoT urban scenarios. IEEE Sensors Journal. 2013;13(10):3558–3567. doi: 10.1109/JSEN.2013.2272099. [Cross Ref]
17. Udhayan J., Babu R. Lightweight vigilant procedure to implement security measures in highly roving military operations. Journal of Computer Science. 2013;9(10):1420–1426. doi: 10.3844/jcssp.2013.1420.1426. [Cross Ref].
18. S. Geetha, C.Karpagam,” Routing protocols in wireless ad-hoc network: An Overview”, International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-2, Issue-2, February 2016.
19. Renu Bala, Dr.Yashpal Singh,” Secure Routing in Wireless Sensor Network”, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, May 2015, pg.966 – 973.
20. Yugarshi Shashwat, Prashanth Pandey,K.V.Arya , Smit Kumar,” A modified AODV protocol for preventing blackhole attack in MANETs”, Information Security Journal : A global perspective,Vol:26, Issue 5,25 Sept. 2017, pp: 240-248.

AUTHORS PROFILE

M. Khaleel Ullah Khan is a research scholar in ECE department of K L University, Vaddeswaram, Guntur district, A.P, India. He has completed his M.Tech. (VLSI System Design) from JNTUH and M.Tech. (Computer Science Engineering) from JNTUK. His area of research interest is wireless sensor networks, Intrusion detection, Cyber security. He published a paper in international journal and 4 papers in national journal.

Dr. K. S. Ramesh, is a professor in ECE department, of K L University, Vaddeswaram, Guntur district, A.P, India. He has completed his Ph.D. in 1988 from Andhra University. He is expertise in earth quake studies using GPS. He has published 17 journal articles and 9 conference papers. His areas of research include Wireless networks, Satellite communication, GPS, GSM.