BLACKHOLE ATTACK DETECTION AND PREVENTION IN WIRELESS SENSOR NETWORKS: A STUDY

[1] **Bindu Rani** [2] **Harkesh Sehrawat**
[1]Deptt.of CSE, UIET MDU Rohtak
[2]Deptt.of CSE, UIET MDU Rohtak

Abstract- Wireless Sensor Network (WSN) [1] is a network which has several small sensor devices responsible for communicating and sensing data wirelessly with each other. WSN have a various field of applications such as military, healthcare monitoring, traffic monitoring, industrial monitoring, undersea monitoring, agriculture monitoring etc. These networks are implemented in unprotected environments, thus vulnerable to various kind of security threats results in breaching network security[2]. Blackhole attack is one of such kind of attack. Different techniques have been studied which detects and prevents blackhole attack. Various advantages and disadvantages of different techniques are also discussed which helps in finding best approach for blackhole attack. This paper focuses on analysis of various detection and prevention methods of blackhole attack in WSN.

Keywords WSN, Malicious node, Blackhole attack.

1. INTRODUCTION:- Wireless Sensor Network (WSN) is a network which has a huge number of small autonomous sensor devices which are responsible for sensing data to their environment and are able to communicate with each other wirelessly. The sensor on each node is able to detect phenomena such as light, pressure, heat, sound, temperature etc[3]. Each sensor node is sending their sensing data to a sink node (or center node). Sensor nodes execute different significant tasks such as computation, signal processing, and network self-configuration to expand network coverage and strengthen its expandability.

Wireless sensor networks have some capabilities such as self-healing and self-organizing .

Self-healing capability allows the sensor node to choose the different path or route in case if the link gets fails while on other hand Self-organizing allows joining new node in the network without any transmission interference[4]. In sensor network, there is no need to install nodes because nodes can be place anywhere in the network. The sensor is provided with a battery as a power supply, which means that the wireless sensor network performance is highly dependent on the rate of energy consumption.

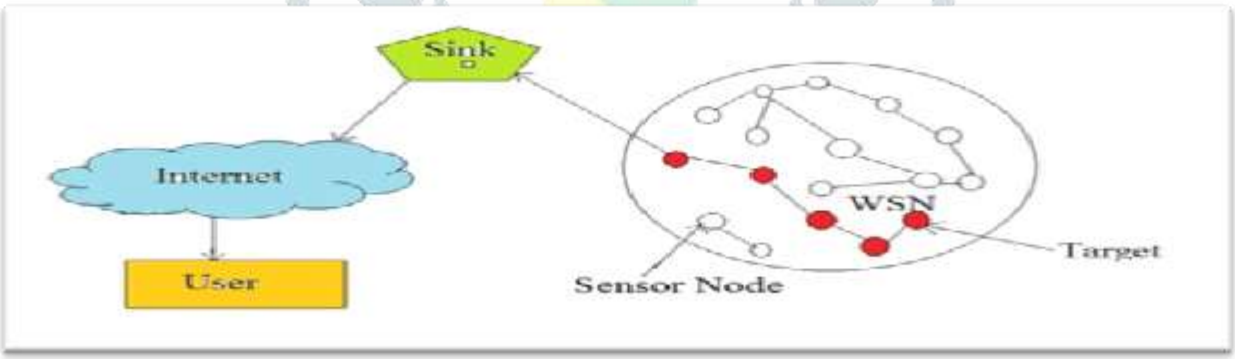

Figure 1: Wireless Sensor Network[5]

2. ATTACKS IN WIRELESS SENSOR NETWORK

There are different types of attacks that can be done by the malicious node in order to damage the network some of these attacks are as given below:-

a) DENIAL OF SERVICE

This attack makes use of additional unnecessary packets and sending them to the user thus preventing the user from accessing the services, networks or other resources.

b) JAMMING

In Jamming attack, jamming signal mix with the other signals thus damage the network and prevent the source to communicate with the destination.

c) SYBIL ATTACK

In Sybil Attack malicious node posses more than one identity in a network and these fake identities are called as sybil nodes which makes the network corrupted.

d) BLACKHOLE ATTACK

In blackhole attack, malicious node captures all the data and does not forward any packet thus prevent the source node to communicate with the destination node.

e) WORMHOLE ATTACK

In this type of attack, wormhole nodes make a fake route which is shorter than the other routes available in the network thus confuse the routing mechanism which is based on the knowledge about the distance between nodes. Thus disturb the entire network.

3 BLACKHOLE ATTACK IN WSN

Blackhole attack is a passive attack. It occurs when an attacker captures all the data of the network and does not forward them to the destination. The entire network get disturbed and malicious node absorbs all the packets as a result of it, all information that is forwarded to the black hole region is captured[6].

In this, a malicious node makes advertisement of itself shows that it contains the shortest path and thus try to attract all the other nodes available in the network. It then consumes all the data without sending it to the destination.

Types of Blackhole Attack:

1)Single blackhole attack

2)Collaborative blackhole attack

If there is single malicious node then it is called as single blackhole attack, while when more than two malicious node are present in the network then it is called collaborative blackhole attack.

In wireless network when a node wants to communicate with the other node then it try to search the shortest path. Routing is important part in the network, attackers take advantage of this and attack on routing protocol.

Blackhole Attack in AODV Routing Protocol

In blackhole attack the process of searching of route starts when source node broadcast packet to all its neighbor, this packet contains the Route Request (RREQ). After getting the (RREQ) the neighbor forwards it towards the destination by adding their own address to it. The malicious node sends Route Reply (RREP) packet with least hope count and highest sequence number to the source node and acts as a destination node, after that source node compare all the responses and select the path which contain largest sequence number and minimum hope count. The source node then sends all the data to the malicious node without knowing that it is not the correct destination. As a result of this, the source node will never able to communicate with the destination node.

Blackhole attack is similar to the universal blackhole which absorbs everything which comes to it.

Causes of blackhole attack in the network

- In a network when a router is in offline mode then it is undetected by the other routers, as a result any packet which sends to the offline router will drop and causes blackhole attack.
- If no host is appointed to a specific IP address then that address is considered as dead address. Attackers use this dead address to generate blackhole attack.
- When network firewall breach, it gives opportunities to the attackers to generate blackhole attack in the network.

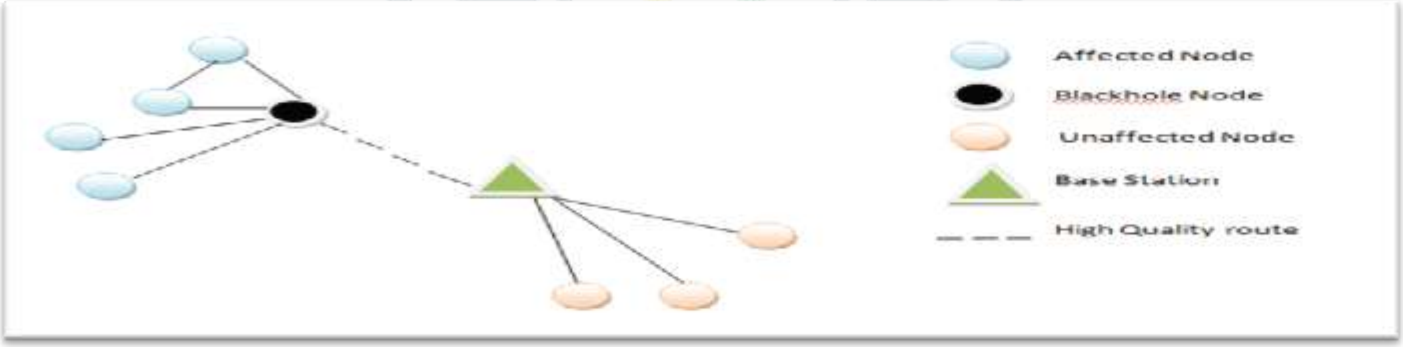

Figure 2 Blackhole Attack

4 DETECTION AND PREVENTION METHODS FOR BLACKHOLE ATTACK

Several techniques are encountered by different authors to detect and prevent blackhole attack . Each technique has some advantages and disadvantages. Related works presented by different authors are as given below:

Abdullah Aljumah and Tariq Ahamed Ahange[3] proposed a method using "Network basic parameters" to detects and prevent the blackhole node in the network. They suggested that both the parameters i.e throughput and end-to-end delay greatly affected when blackhole node is present in the network. Their study shows that network performance declined when there is an increase in delay time and the decline in throughput.

Abhinav Kaurav and Kakelli Anil Kumar [7]discussed that by using Intrusion Detection System(IDS) based on AODV, it is possible to detect and prevent malicious node in the network. Their results shows that packet delivery ratio of their proposed IDS is "1" while it is "0"whithout any IDS.

Nigahat and Dr. Dinesh Kumar [8] suggested that blackhole attack can be detected and prevented in a network based on AODV with shortest distance algorithm. Malicious node presents itself in such a way knowing that it has the shortest path, thus other node get into the trap causes formation of blackhole attack. Network Simulator2(NS2) is used for the implementation of their proposed system.

Dr. Shreenath K N and Manasa V M [9]proposed a method which is consist of zone creation phase. Equal size of small zones is created by dividing the sensor field. Each Zonal Head (ZH) is responsible to communicate with their respective sensor node. Mobile Agent(MA) then visits randomly to the nodes, zone head and their respective zones. If any ZH or node is not able to forward or receive packet then it is considered as a malicious node. That suspended node then removed from the network.

Mehndi Shamra and Naveen Kumar Gondhi [10]presented contingency table approach with the help of which it is possible to detect blackhole attack by making use of density curve. Their proposed work depict that if there is fall in density curve with respect to the time when the packet travel from the source node to sink node, then this fall in density curve illustrates that malicious node surely present in the network. Also if there is no fall in the curve with respect to time then there is no malicious node in the network.

A.Babu Karuppiah and J.Dalfiah [11]presented a work which is based upon Intrusion Detection System (IDS). The basic concept behind detecting the blackhole attack is the trade of packet between a sensor node and base station. Thus base station is responsible to take the part of monitor node in order to detect the malicious node.

Umashankar Ghugar et al. [12]discussed a trust based secure protocol. The protocol determines honest nodes during packets transmission. To determine which node is honest node, trust value is calculated periodically for each node present in the network. Nodes are monitored time to time which results in determining malicious node if exits in the network. Also after identifying the malicious node, it can be rejected from the routing table.

Vinod Bhupathi et al. [13]proposed a method which make use of SODV or (secure AODV) protocol. They compare AODV and SADOV to detect the malicious node. It is observed that it is possible to detect blackhole attack with the help of SAODV.

Anjali P.Rathod and Nekita A .Chavhan [14]presented that blackhole attack in mobile and ad hoc network by using the routing tables. The routing table entries consist of the following fields in the AODV protocol: (a)Destination sequence number (b) Destination IP address (c)Next-hop IP address (d)Hop count (e)Session expiry time. They suggested that if there is blackhole node in the network then in the routing table entry, the field "Next hope IP address" contains the address of that malicious node which absorbs all the data packets. Therefore by observing routing table, one can easily determine the blackhole node.

Kalaiselvan.K and Gurpreet Singh[4] suggested a method which consider the depletion of energy i.e battery power. according to them, there is a blackhole node in the network if overall performance is below the considered threshold. They make use of clustering concept in order to enhance the lifespan of the sensor node and to minimize the usage of battery power in the node.

Garima Gupta and Atul Mishra [15]suggested a cross-checking algorithm, implemented to check the throughput and delay value in an environment.(a)When there is no blackhole node in the network.(b)When single blackhole node is present in the network.(c)When multiple blackhole nodes are present in the network. There result shows increase in throughput and lower delay value.

Dr.Sharvani G.S and Rakesh R[16] discussed authentication mechanism and architecture of SENMA. The malicious node can be easily detected using SENMA because it provides the direct line of sight, on the other hand there will be a secure route from source to destination using authentication mechanism.

M.Rajesh Babu et al. [17] proposed an architectural level solution which support multiple applications run successfully over the network. Their proposed mechanism proactively detect the blackhole attack in the network and separate the malicious node from the network for secure communication.

Mehak Kaushal and Mr. Gunjan Gandhin [18]discussed HOOSC scheme, in this scheme by using multiple base station with encryption algorithm blackhole node can be determined in the network. They suggested that there is no direct connection b/w source and destination. Intermediate nodes are present in the network through which data is transmitted.

Jaspreet Kaur and Bhupinder Kaur [19] proposed a system called BHDP. The system is able to detect and prevent blackhole attack in the network. The main advantage of their proposed system is that there is no need to modify the packet and hence the same packet can be sent to multiple base station. They use different parameters which act as an indicator to determine the blackhole attack, such parameters are delivery ratio, total packet drop etc.

Vipul Sharma et al. [20] proposed a method which provides a mechanism based on Leach protocol in order to protect the system from blackhole attack. Their proposed mechanism is able to save power consumption.

Sheela.D et al. [21]proposed a system designed to prevent the blackhole attack using multiple base station available in the network. They suggest that if there are chances of blackhole node in the network then only routing through multiple base station is activated and to check the possibility of the blackhole node is determined by the mobile agents as mobile agents are responsible for detecting abnormal behavior. Also, simulations used to check the overall performance of the system.

Satoshi Kurosawa1 et al.[22] proposed an anomaly based detection system using dynamic training method. In this method at regular time training data is updated. Their result show that it possible to detect blackhole attack through effective simulation.

Advantages and Disadvantages of different techniques

S.no	**Approach**	**Advantages**	**Disadvantages**
1	Basic network parameters and novel approach. (Abdullah Aljumah et al)[3]	Influence of blackhole attack is measured.	It is not a powerful method, as if number of attackers increases , stability of system get affected.

2	Intrusion Detection System based approach (Abhinav Kaurav et al)[7]	Detect and prevent blackhole attack using NS-2.35 simulator is feasible.	Applicable only for AODV protocol.
3	Distance Vector Protocol based approach (Nigahat et al)[8]	Evaluation based on PDR and delay which provide better results.	Cost is high, thus not suitable for a MANET environment.
4	Concept of Mobile Agent approach(Dr. Shreenath K N et al)[9]	Applicable only in zone based wireless system	No prevention method is described.
5	Contingency approach (Mehndi Shamra et al)[10]	Density curve with respect to time can determine malicious node in the blackhole attack	No preventon method is described. Applicable only for AODV network.
6	Improvised hierarchal vitality efficient IDS based approach (A.Babu Karuppiah et al)[11]	Simple approach that can detect and prevent blackhole attack.	Not an efficient mechanism.
7	Watchdog Monitoring Technique (Umashankar Ghugar et al)[12]	Improves network performance by detecting and preventing blackhole attack.	Applicable only for AODV protocol.
8	Trust Based Mechanism(Vinod Bhupathi et al)[13]	It is possible to detect blackhole node using secure AODV .It provide secure data transmission.	NS2 simulator is used in which bugs are unreliable.
9	Routing Table base approach(Anjali P.Rathod et al)[14]	Reduces cryptographic operation for authentication.	No prevention method is described.
10	Monitoring fake packet replays based approach(Kalaiselvan.K et al)[4]	Using threshold performance blackhole attack can detected.	It is difficult to set threshold value.
11	Cross Checking Algorithm (Garima Gupta et al)[15]	Detailed information is provided for co-operative blackhole attack.	Not an efficient algorithm as delay value remain constant in each case. Moreover there is little rise in throughput.
12	Authentication Mechanism and q-out-of-m rule based apprach (Dr.Sharvani G.S et al)[16]	Using authentication mechanism, it is possible to make secure pat between source and destination.	No prevention method is given.
13	Alleviation Procedure (M.Rajesh Babu et al)[17]	Different protocols are used to check the vulnerability of blackhole as well as other attacks in WSN. SAR protocol shows best result of non-vulnerability for blackhole attack. Solution is cost effective.	Other then SAR protocol , there are several problems associated with them.
14	HOOSC Scheme based approach (Mehak Kaushal et al)[18]	Simple approach used which reduces the impact of blackhole attack. Also prevention method is described	It is not an efficient method for the security of data.
15	Fuzzy Logic Algorithm (Jaspreet Kaur et al) [19]	No modification of packet is required thus if there is presence of blackhole attack still all the base station receive the same packet. Detect and prevent the blackhole attack	Storing rule base might require significant amount of memory.
16	LEACH protocol based approach (Vipul Sharma et al)[20]	Detection method is energy efficient	All that need to be done by the attacker is to attack on the base station, therefore security is measure concern.
17	Routing through multiple base station algorithm based approach(Sheela.D et al)[21]	Provide secure routing algorithm. Avoid unnecessary packet transmission over multiple base stations.	Make use of several base station which increase system cost.
18	Anomaly Based Detection System approach(Satoshi Kurosawa1 et al)[22]	Simulation result clearly shows if there is blackhole attack present in the network or not.	No prevention method is provided.

CONCLUSION:- Wireless sensor network is unprotected from different kind of attacks. In this paper firstly we have studied what is blackhole attack and how it is implemented, what is the behavior of malicious node and then concluded that it is one of the major issues in the network. For this we have studied various techniques and their pros and cons in order to detect and prevent blackhole attack in the wireless sensor network.

REFERENCES:-

[1] I. J. C. Network, "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks," vol. 8, no. February, pp. 1–10, 2011.

[2] D. Virmani, A. Soni, S. Chandel, and M. Hemrajani, "Routing Attacks in Wireless Sensor Networks: A Survey," *arXiv Prepr. arXiv1407.3987*, 2014.

[3] A. Aljumah and T. A. Ahanger, "Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks," vol. 17, no. 2, pp. 194–201, 2017.

[4] K. Kalaiselvan and G. Singh, "Detection and Isolation of Black Hole Attack in Wireless Sensor Networks," vol. 4, no. 5, pp. 3516–3524, 2015.

[5] C. Science and S. Engineering, "International Journal of Advanced Research in Computer Science and Software Engineering A Review on Detection of Blackhole Attack Techniques in MANET," vol. 4, no. 4, pp. 364–368, 2014.

[6] C. Lal, "An Energy Preserving Detection Mechanism for Blackhole Attack in Wireless Sensor Networks," vol. 115, no. 16, pp. 32–37, 2015.

[7] A. Kaurav and K. A. Kumar, "Detection and Prevention of Blackhole Attack in Wireless Sensor Network Using Ns-2 . 35 Simulator," vol. 2, no. 3, pp. 717–722, 2017.

[8] "Nigahat*, Dr. Dinesh Kumar UCCA, Guru Kashi University, Talwandi Sabo UCCA, Guru Kashi University, Talwandi Sabo DOI : 10.5281/zenodo.546354," vol. 6, no. 4, pp. 314–319, 2017.

[9] K. N. Shreenath, "Black Hole Attack detection in Zone based Wireless Sensor Networks," vol. 5, no. 4, pp. 148–151, 2017.

[10] M. Samra and N. K. Gondhi, "Blackhole Attack Detection in Wireless Sensor Networks Using Support Vector Machine," vol. 3, no. 5, pp. 48–52, 2016.

[11] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, and S. Rajaram, "An improvised hierarchical black hole detection algorithm in Wireless Sensor Networks," *Int. Confernce Innov. Inf. Comput. Technol.*, no. Iceict, pp. 1–7, 2015.

[12] U. Ghugar, J. Pradhan, and M. Biswal, "A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol," *IJCSN Int. J. Comput. Sci. Netw. ISSN*, vol. 5, no. 4, pp. 2277–5420, 2016.

[13] V. Bhupathi, P. Priyanka, and G. S. Reddy, "DETECTION OF BLACK HOLE," vol. 5, no. 2, pp. 305–311, 2016.

[14] C. Engineering, A. P. Rathod, and N. A. Chavhan, "Detection Mechanism for Black hole attacks in," vol. 5, no. 4, pp. 98–100, 2016.

[15] G. Gupta and A. Mishra, "Simulation Based Study of Cooperative Black Hole Attack Resolution Using Cross- Checking Algorithm," *Int. J. AdHoc Netw. Syst. (IJANS)*, vol. 5, no. 2, pp. 17–28, 2015.

[16] G. S. Sharvani, "Detection of blackhole attack in distributed wireless sensor networks," pp. 172–175, 2015.

[17] M. R. Babu, S. M. Dian, S. Chelladurai, and M. Palaniappan, "Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version," *Sci. World J.*, vol. 2015, 2015.

[18] M. Kaushal and G. Gandhi, "Detection Prevention and Mitigation of Black Hole Attack for MANET," vol. 4, no. 4, pp. 1431–1437, 2015.

[19] bhupinder kaur Jaspreet kaur, "Network under Black Hole Attack," vol. 2, no. 9, pp. 142–151, 2014.

[20] V. Sharma, K. Patil, and A. Tiwari, "Detection and Suppression of Blackhole Attack in Leach based Sensor Network," vol. 5, no. 6, pp. 1873–1877, 2014.

[21] S. D, S. V R, A. Begam, and C. G. M, "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent," *Artif. Intell.*, pp. 15–16, 2012.

[22] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," vol. 5, no. 3, pp. 338–346, 2007.

[23] Harkesh Sehrawat,Yudhvir Singh. *"Wormhole detection in Wireless Senor Networks"* International Journal of Scientific Research in Science and Technology, ISSN 2395-6011, 2018.

[24] Harkesh Sehrawat,Yudhvir Singh. *"Detecting Sinkhole attack in Wireless sensor Networks"* International Journal of Engineering Sciences Paradigms and Researches, ISSN 2319-6564, 2018.

[25] Rajat Malik, Harkesh Sehrawat, Yudhvir Singh, "Comprehensive study of selective forwarding attack in Wireless Sensor Networks", *International Journal of Advanced Research in Computer Science*, ISSN 0976-5697, vol 8, no 5, May-June,
352.

[26] Manvi Bhatia, Harkesh Sehrawat, Yudhvir Singh, Rajat Malik, "Comprehensive study of Blackhole attack in Wireless Sensor Networks:", *International Journal of Computer & Mathematical Science*, ISSN 2347-8527, vol 6, no 7, July, 2017, pp 84-89.

[27] Neelam, Harkesh Sehrawat, Yudhvir Singh, Rajat Malik, "Routing Protocol in Wireless Sensor Networks: Comprehensive study", *International Journal of Engineering Technology Science and Research*, ISSN 2394-3386, vol 4, no 7, July, 2017, pp 1835-1838.