© 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939

A survey on defense mechanisms against Black hole and Gray hole attacks in Wireless Sensor Networks

[1]Archana M, [2]Dr.Binu G.S, [3]Prof.Vinod G.
[1]M.Tech Scholar, [2]Associate Professor, [3]Associate Professor
[1]Department of ECE,
[1]NSS College of Engineering, Palakkad, India

***Abstract* – Wireless Sensor Networks (WSNs) consist of large number of small sensor nodes that continuously observe environmental conditions. Energy consumption is a major challenge in WSNs due to its dynamic topology, highly decentralized infrastructure and resource constraint sensors. WSNs are easily compromised by various denial of service attacks due to these factors and that result in disastrous consequences. Gray hole and Black hole attack are attacks that reduce the performance of a WSN. So as to attain energy efficiency in WSNs, there is a need for efficient and secure protocols to defend against Gray hole and Black hole attacks. Many algorithms have been developed to protect against these attacks and each one claims them itself to be better than others. So in this paper, a survey of different detection mechanisms to protect against black hole and gray hole attacks in wireless sensor networks is discussed.**

***Index Terms* – Wireless Sensor Networks, Black hole attacks, Gray hole attacks, Ad-hoc On-demand Distance Vector Routing, Route Request, Route Reply**

I. INTRODUCTION

Wireless Sensor Network (WSN) is a distributed system that consist of a Base Station (BS) and large number of Sensor Nodes (SN) that incorporate sensing, computing and wireless communication capabilities, which can detect various events associated to its surrounding environment such as speed, temperature, pressure, light, etc. Sensor nodes carry out various tasks such as signal processing, embedded computing, and connectivity. They are also responsible for sensing environment and transmitting information. The sensors exchange information about the environment to build a global scenario of the environment. WSNs are used in various fields like environment, industry, military, healthcare, security and many others. Data flows from sensor nodes towards a few aggregation points which further forward the data to base stations. Also base stations could broadcast control information to sensor nodes. WSN follows different topologies like star network, wireless mesh network etc. according to the requirements of the network. WSN uses low cost embedded devices, which have small size, limited memory and works on wide range of applications. There is a centralized approach in WSNs in terms of network control. Data flows from sensor nodes towards a few aggregation points which further forward the data to base stations. Also base stations broadcast query or control information to sensor nodes. WSNs works in environment conditions particularly where wired connections are not possible. The challenges and limitations of wireless sensor networks are the following:

- Limited functional capabilities
- Power factors
- Node costs
- Environmental factors
- Transmission channel factors
- Topology management complexity and node distribution

To design security protocols for wireless sensor network is a difficult work because of following factors. Firstly, wireless communication medium used in wireless sensor networks are accessible by everyone who has a radio interface set at the same frequency. Because of this characteristic, monitoring and taking part in communication process is suitable in wireless channel and attackers can easily attack the network. Second factor is that sensor nodes have limited resources in the term of memory, computational capability. Due to this, effective security model is very critical to apply and execute because of complex nature of security model. Thirdly, wireless sensor networks are normally deployed in warlike region with ad-hoc architecture. Without any architecture it is very complex to continuously monitor the network after node deployment. Because of this, attackers can easily attack the network [1].

Security is one of the main challenges of any system and wireless sensor network may be influenced by different types of attacks. The security attack concern for WSN is because of physical accessibility of sensor and actuator devices and usage of minimal capacity in the network. These security holes causes attacks in WSN and it can be handled using various security architectures and security services like integrity, authenticity and confidentiality in the wireless domain.

II.SECURITY ISSUES IN WSNs

There are various scenarios like military etc. where the information needs to be maintained with some privacy level. Therefore, there are various issues in WSN to maintain security [2].

A. Availability

It means to ensure that the data should be accessible to the authorized user at any time. Some attacks make the authorized users not to use the data.

B. Data Confidentiality

It means to dissent or hide information to the unauthorized users. It is the most important feature of security. Cryptography and encryption are the techniques that provide confidentiality.

C. Integrity

It is to ensure that the data is secure and unaffected compared to the original information.

D. Data Authentication

Data authenticity is a guarantee of the identities of communicating nodes. Nodes must be capable of recognizing and rejecting the information from illegal nodes.

E. Data Freshness

Data freshness ensures that the data communicated is fresh and no previous messages have been replaced by an opponent.

III. SECURITY ATTACKS IN WSNs

A. Passive attack

A passive attack is one where the attacker compromises and intercepts an aggregator node in the network, inspects it, listens, and reads useful data in it, trying to learn which nodes have more value within the topology. Under the attacker's control, the new compromised node can be used to launch new malicious attacks. It doesn't involve modification of the data stream and do not cause direct harm to the network. It makes the attacker to see the future actions. Passive attacks result in the access of data information or data files to an intruder without the knowledge of the user.

Some of passive attacks are as follows:

- *Monitor and Eavesdropping:* It is defined as interception and interpretation of messages and conversations by unintended receivers. It attempts to gain the confidential information that should be kept secret during the communication.

- *Traffic Analysis*: The nature of communication is guessed by monitoring the frequency and length of messages transmitted even when it is encrypted. It causes malicious destruction to the sensor network.

B. External attack

External attacks are done by outsiders without taking support from the insider or authorized user. Anyone in skilled attacker, a malicious experienced user or a group of malicious organization can do such attacks .Scanning and gathering information are the most important ways in this technique of attacking networks.

C. Internal attack

An internal attack or insider attack involves someone from the inside attacking the network. Internal attacks can be malicious or non- malicious. Malicious insiders deliberately eavesdrop, steal, or damage the data information or data files, use information in a false manner or deny access to other legitimate users. The attacker employs a significant amount of resources, tools and skill to launch an attack and potentially remove any evidence of that attack.

D. Active attack

In this attack, an attacker intends to disrupt the network's functionality. It attempts to alter system resources or affect their operation. The active attacks jam communications by making changes to data already stored in the WSN in addition to modifying configuration parameters of the WSN's components. Active attack usually tries to break protection features to steal or change information. Active attacks cause direct harm to the network because they can control the data stream. There are various types of active attacks:

- Routing attacks
- Denial of Service attacks
- Node Malfunction

- Node Duplication
- False Node
- Information Gathering

A few of the active attacks on routing are as follows:

a. Black hole attack

In this attack, black hole immediately sends a false route reply messages when it receives an RREQ message, without checking its routing table. Also malicious node refuses to forward data packets to the destination. The false route reply messages are to inform other nodes in the network that the destination is on the next hop from this attacker node and the attacker node has the best route to that destination. All neighboring nodes update their routing tables and make the attacker node their next hop for the destination. Now when this attacker node receives the data packets, it drops all the packets and the packets do not reach the destination [3].
It is of two types:

- *Single black hole attack:*

If a single node is malevolent in the network, then it is called as single black hole attack. Detection of this attack is easy compared to the multiple black hole attacks in the network.

- *Cooperative black hole attack:*

In this type of attack, numerous black holes in a group are present in the network. Detection of this attack is hard and is difficult to prevent when compared to single black hole attack.

b. Sybil attack

Sybil Attack is named after the subject of the book *Sybil*, a case study of a woman diagnosed with multiple fake identities. These fake identities are known as Sybil nodes. The victim node is masqueraded as another node, which receives false data packets and compromises the trustworthiness of the information relayed. Usually, peer to peer systems are susceptible to Sybil attack.

c. Gray hole attack

Gray hole attack is an expansion of black hole attack in which a malicious node behavior is exceptionally unpredictable. It is a selective packet dropping attack. A malicious node exploits the AODV protocol to broadcast itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. Also the node drops the intercepted packets with a certain probability. Due to the uncertainty in nature of this attack, it is more difficult to detect when compared to black hole attack where the malicious node drops the received data packets with certainty. Malicious behavior is exhibited by gray hole node in different ways. It may drop packets coming from or destined to certain specific nodes in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult .This attack is also known as misbehaving attack[4].

d. Wormhole Attack

Wormhole attack is an attack on the routing protocol in which the packets or individual bits of the packets are captured at one location, tunneled to another location and then replayed at another location. In this attack the two colluding nodes create an illusion that the locations involved are directly connected though they are actually distant.

e. Hello Flood Attack

It is an attack in which HELLO PACKETS are transmitted by the nodes to show their presence to their neighbors and the receiving nodes assume that it is within the radio frequency range of the sender. This assumption may prove to be false when a laptop-class attacker transmit routing information or other information with an abnormally large transmission power to establish every other node in the network that the malicious node is its neighbor.

f. Jamming

Jamming is one of the serious attacks in which it uses to interfere with the radio frequencies of the sensor nodes. Jamming is of two types: constant jamming and intermittent jamming. Constant jamming involves the complete jamming of the entire network whereas in intermittent jamming nodes are not communicating continuously.

IV. DETECTION AND PREVENTION OF GRAY HOLE AND BLACK HOLE ATTACKS

A. Gray hole attack

1) Channel Aware Detection*:* A channel aware detection algorithm for detection of gray hole nodes is discussed in [5]. There are two phases in this algorithm. In the first phase, channel estimation is done in which the algorithm estimates normal loss rate in a network i.e., loss due to bad channel quality or medium access collision under infinite buffer assumption. The second phase is traffic monitoring in which the algorithm estimates actual loss rate in the network and in this phase it monitors the upstream and downstream behavior of each node. The estimated actual loss rate is then compared to threshold to see if any node is misbehaving. The algorithm adjusts the threshold dynamically according to the network condition. The algorithm also detects limited transmit power attack and bad mouthing attack. But there is a disadvantage that it fails to detect collusive gray hole attacks.

***2) AODV based Detection**:* A method to detect gray hole attack which is based on AODV protocol is proposed in [6].The protocol detects both single and cooperative gray hole attacks. There are 4 phases in this mechanism: Neighborhood data collection, Local anomaly detection, Cooperative anomaly detection and Global alarm raiser .In the first phase, neighborhood data about routing is collected in a data routing information table. Suspected nodes are pointed out from the table and then local anomaly detection is started. In the local anomaly detection phase, an initiator node (IN) starts the checking process with the help of cooperating node (CN).IN sends RREQ and when it gets a reply from the suspected node (SN),it sends a probe packet to the CN through SN. If it has received the probe packet, IN confirms with CN after a particular duration. If not, the SN is further tested through the co-operative anomaly detection technique. In cooperative anomaly detection, the IN takes help of all the neighbors of the SN. It asks all SNs neighbors to send packets to the IN through SN and keeps cross checking through notifications via another route that does not involve SN. In this way it is detected if a node is acting as a gray hole node for a particular node at a particular time. A global alarm is then raised against that node.

***3) Path based Detection**:* A path based scheme is discussed in [9]. In this method, a node does not observe every neighboring node, but only observes the next hop in recent route path. Each node should keep a packet digest buffer named as FwdPktBuffer. Whenever a packet is forwarded to, its digest is added into the FwdPktBuffer and the detecting node overhears. Once it is overheard that the next hop forwards the packet, the digest will be released from the FwdPktBuffer .The detecting node should calculate the overhear rate of its next hop in a fixed period of time, and compare it with a threshold. Overhear rate is defined as total overheard packet number divided by total forward packet number. In this method, every node only depends on itself to detect a gray hole. Routing packet overhead is not more in this process. Also this algorithm does not send out extra control packets. There is an extensive amount of calculation in this method.

B. Black hole attack

***1) Cross Checking Technique**:* Data routing information (DRI) table and cross checking technique in discussed in [9] .It identify the cooperative black hole nodes and modified Ad-hoc On-demand Distance Vector (AODV) routing protocol is used in this method. All nodes need to have an extra DRI table, in which 1 represents for true and 0 for false. The table has two entries, ‘From’ to have the information on routing data packet from the node and ‘Through’ to have the information on routing data packet through the node. The source node sends Route Request (RREQ) message to each node and wait for Route Reply (RREP) message. Then it sends packets to the node which replies the Route Request (RREP) packet. The intermediate node then sends next hop node (NHN) information and DRI table to the source node (SN). Now source node cross checks its own table and the DRI table received from the intermediate node to verify the INs honesty. Then source node sends the further request (FREQ) message to INs next-hop-node for gathering its routing information including the current NHN, the NHNs Data Routing Information (DRI) table and its own DRI table. Finally, the SN compares the above details by cross checking to find out the malicious nodes in the routing path.

***2) Exponential Trust Mechanism**:* An Exponential Trust based mechanism is proposed in [10] in which a table is maintained in the memory which stores the trust factor (TF) of each node. Trust factor is 100 for every node initially. A streak counter is maintained in memory. It keeps count of every consecutive packet dropped. Initially the value for each node of the counter is 0 and is incremented by 1 with every successive packet dropped. The black hole attack causes the node to drop all the packets that it has received. As soon as the node forwards a packet to its next node in the routing table the streak counter is set to 0 again. The trust factor of a node is calculated. The fault tolerance of the network is also considered. If fault tolerance is very high for the network then it should be kept closer to 1 when the network can tolerate packets being dropped. So the decrease in the TF with each consecutive packet dropped will be very less. If it is closer to 0 that means the fault tolerance of the network is very less. In this case, the trust factor of the node will fall considerably for every node. If the value of fault tolerance is too high it can lead to a large number of packets being dropped before being detected and a very low value will lead to the node being declared as malicious after dropping only a few consecutive packets.

***3) Hierarchical Intrusion Detection**:* An intrusion detection system is proposed in [11] to detect and prevent black hole attacks. In this, each sensor node sends a control packet to the base station at the end of transmission phase. Each control packet contains the node identifier (id), and the number of packets sent to cluster head. On getting control packet, base station compares this of each node with the amount of packets received from its cluster head (CH). That allows base station to detect an eventual black hole attack. In this case, base station will broadcast an alarm packet to all network nodes. The alarm packet contains identifier of black hole node (detected CH).All sensor nodes maintain a black hole table, which contains identifiers of detected black hole nodes .Then, each sensor node checks its black hole table before the selection of its next cluster head which prevents that attacker node will be selected one more time as cluster head. Sensor nodes can send their control packets directly to the base station but this can be energy inefficient and bring extra overhead to the network. Therefore, a second cluster head (SCH) is selected to transmit control packets to the base station. The choice of the SCH is simple and is based on node energy reserve. Therefore, node with the maximum energy reserve will be selected as a second CH.

4) Distributed and Cooperative mechanism: A distributed and cooperative mechanism (DCM) is suggested in [15] to resolve the black hole attacks. It has four phases: In the local data collection phase, each node in the network constructs and maintains an estimation table. Each node evaluates the information of overhearing packets to find out whether there is any malicious node. If there is one doubtful node, the detect node enters to the local detection phase to identify whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If it receives the positive inspection value, the doubtful node is regarded as a normal node. Otherwise the initial detection node runs the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making process. The network traffic is increased because the notify step utilizes broadcasting, so a constrained broadcasting algorithm is run to limit the notification range within a fixed hop count. A threshold value contains the maximum hop count range of cooperative detection message. At the end, the global reaction phase is executed that set up a notification system to send warning messages to the whole network. Global reaction phase contains some reaction modes. The first reaction mode notifies all nodes in the network. There is wastage of communication overhead in this mode. Each node maintains its own black hole list and arranges its data transmission route in other mode. But there is a chance to exploit this route by malicious nodes and requires more operation time.

C. Both gray hole and black hole attacks

***1) Optimal Path Routing**:* A solution for the prevention of black and gray hole attacks is proposed in [8] by leaving the first and selecting the second shortest path for data packets transmission. It prevents gray hole attacks by choosing the secure route for data packets transmission. Also it gives more security for data integrity and detection of malicious node on the safe route. When source node receives Route Reply (RREP) messages from other nodes connected with destination node, it rejects the first RREP message coming from any intermediate node connected with destination node. By this method, the source selects second shortest route to transmit data packets to destination node instead of choosing the first optimal route. So it is difficult for malicious node to check the entire network to know where to place itself in the network and mislead the source node by claiming that it has the second shortest route to the destination. There is a chance of multiple malicious nodes working in the network so is possible for a malicious node to be a part of second optimal route. To identify that malicious node in the second optimal route, a hash function is used on the message that has to be sent. Source node sends the data packets to destination and sends the hash value of message in the first data packets to the destination. When destination node receives all the data packets in the dedicated time, destination node appends hash function on the data packet and calculates the hash value. If the computed hash and received hash value of the message that has been sent by the source node become equal, it means that all the packets have been received successfully and there is no such black or gray hole.

***2) Cluster based detection**:* An energy efficient algorithm for wireless sensor networks is discussed in [12]. In its first round, a node with the highest energy is chosen as the cluster head. The source node (SN) broadcasts Route Request(RREQ) packet .Data packets keep on transferring to the next hop by first checking if the node is compromised or not and then transferring packets to it or searching for another cluster head if the node is compromised. The complete steps are repeated till next hop node cluster head NHN_CH is not the destination node. Algorithm for selection of CH at each round of CH selection is based on detecting compromised node first and preventing such node to become CH in the next round of CH selection mechanism. Thus compromised node is being prevented from being CH to increase the lifetime of network.

***3) Opinion Trust based technique**:* An opinion based technique is discussed in [13] which consist of two conditions to decide whether the node is trustworthy or not. The neighbor's reply for any destination including sample time is taken first and the node stores the sequence number along with destination number and neighbor's IP. Packet delivery ratio of neighbor's node is calculated. Initially the trust value of all the nodes is set as 0.0 i.e. same trust values for all the nodes. For first condition, it will compare the packet delivery ratio of neighbor nodes and on the basis of packet delivery ratio it will increase or decrease the trust value of the node i.e. If the packet delivery ratio is greater than certain threshold value then it will increase the trust value and if the packet delivery ratio is less than threshold then it will decrease the trust value. For second condition, along with trust value it also checks sequence number i.e. if the current node receiving the reply with same sequence number but the destination is not same than it may be malicious reply. Therefore, it will reduce the trust value of the node. If sender node finds that trust value is satisfactory then it will forward the packet and if trust value is unsatisfactory then that node will be assumed as malicious node.

V. CONCLUSION

In this paper a brief review on wireless sensor network, security issues in sensor networks, security attacks in wireless sensor networks and techniques used for detecting and prevention of black hole and gray hole attacks on wireless sensor networks is discussed. Security is an important requirement in WSNs so as to protect the sensitive data involved. Black and Gray hole attack reduce the performance of the network and also affects the end to end packet delivery ratio. To achieve energy efficiency, it is necessary to defend against these attacks. An overview of the techniques used for detection and prevention of black hole and gray hole attacks is presented.

REFERENCES

[1] John Paul Walters, Zhenjiang Liang, Weisong Shi, and Vipin Chaudhary, , “Wireless Sensor Network Security: A Survey”, Department of Computer Science, Wayne State University, Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) Auerbach Publications, CRC Press,2006.

[2] Kahina Chelli, “Security Issues in Wireless Sensor Networks: Attacks and Countermeasures”, Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1-3, 2015, London, U.K.

[3] Binod Kumar Mishra, Mohan C. Nikam, Prashant Lakkadwala, “Security Against Black Hole Attack In Wireless Sensor Network”, Fourth International Conference on Communication Systems and Network Technologies,2014.

[4] Dharmendra Mishra, “A Review on Gray Hole Attack in Wireless Sensor Network”, International Journal of Computer Applications ,Volume 122,No.2, July 2015.

[5] Devu Manikantan Shila, Yu Cheng, Tricha Anjali, “Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs”, IEEE Transactions on Wireless Communications, Vol. 9, No. 5, May 2010.

[6] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, “A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks”, IEEE ICICS,2007.

[7] Weerasinghe H, Fu H, “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.

[8] Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin, “Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash”,2013 IEEE.

[9] Jiwen Cai, Jialin Chen, Zhiang Wang, Ning Liu, “An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network”, 24th IEEE International Conference on Advanced Networking and Applications,2010.

[10] Dr.Deepali Virmani, Manas Hemrajani, Shringarica Chandel, “Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network”, IJRASET, Vol. 2 Issue III, March 2014.

[11] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami , “Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs”, Computer Sciences Department, M’Sila University, IEEE 2013.

[12] Snehal P. Dongare, Ram S. Mangrulkar, “Implementing Energy Efficient Technique for Defense against Gray-Hole and Black-Hole Attacks in Wireless Sensor Networks”, IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015.

[13] Mitali Khandelwal, Sachin Upadhya, “An Opinion Trust Based Detection and Prevention Method for Defending Black-hole and Gray-hole Attacks in Wireless Sensor Networks”, International Journal Of Scientific and Engineering Research, Volume 7, Issue 7, July-2016.

[14] Deng H., Li W. and Agrawal, D.P, “Routing security in wireless ad hoc networks”, Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[15] Yu CW, Wu T-K, Cheng RH, Chang SC, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network”, PAKDD Workshops,Nanjing, China, 22-25 May 2007.

[16] Bo Sun, Yong Guan, Jian Chen, Udo W.Pooch, “Detecting Black-hole Attack in Mobile Ad Hoc Network”, 5th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 495.

IJEDR