A Review on Gray Hole Attack in Wireless Sensor Network

Dharmendra Mishra
PG Scholar
Oriental University, Indore

Deepak Sukheja, Ph.D
H.O.D
Computer Science Department
Oriental University, Indore

Sunil Patel
Assistant Professor
Oriental University, Indore

ABSTRACT
Sensor networks are currently used in wide spread deployment, so security issues are also a large concern in Sensor Networks, or Sensor Node Networks. Gray Hole attack is very much deleterious attack against the sensor node networks, and makes the whole networks malfunctioning, and also affects the whole sensor networks communication.

In this paper I have described different defense intrigue according to my knowledge, and also as per different research papers studied. As per my knowledge, I have described drawbacks of Gray Hole Attack, or Selective Forwarding Attack, thus providing better way to understand the Gray Hole Attack in better way and the proposed solution. In the proposed solutions, I have tried to give better solutions in the sense of detection and prevention of Gray Hole Attack or Selective Forwarding attack.

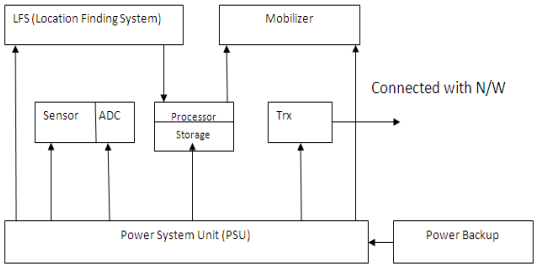
Keywords
Sensor Networks, Security, and Gray Hole Attack/Selective Forwarding Attack

1. INTRODUCTION
Sensor Network came into existence in 1990's, when there is invention of Motes devices [1, 2] and the tiny OS [3] came into existence.

Wireless Sensor Networks [4], comprised of large number of Sensor Nodes, in any physical environment. These Nodes having the capability of Sensing, Computation, Monitoring, Storage and wireless Communication.

Sensor Nodes can be spread in Remote areas, by means of spreading them manually, or by other means (Helicopters, Airplanes Etc.), to collect data from environment, and in last these collected data are processed and show desired results.

Wireless Sensor Node can be understood by below diagram, which shows main components of Wireless Sensor node:



TRx= Tran receiver Unit,

LFS= Location Finding System

ADC= Analog To Digital Convertor

Fig.1 Elements of Sensor Node

As earlier stated that Sensor Nodes are spread onto remote areas, or we say that in any sensing field, from where to be collected or processed. This can be understood from below diagram in Fig.2 in which nodes are spread in sensing field and can be connected via wireless sensor network.

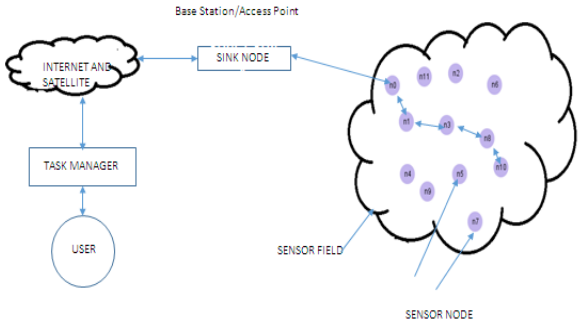


Fig.2 Sensor Node in Sensor Field

In the studied paper, we have investigated that Gray Hole attack or Selective forwarding attack is easy to implement, but very difficult to detect. In the Gray Hole attack normal node works nasty nodes shows itself normal and takes place in the reception of the packets transmitted from the source node, on reception of packets these nasty nodes drops the selected packets and only transmits the left packets to the neighbor node.

So, Selective forwarding attack or Gray Hole attack is very harmful, if the wireless Sensor Networks, is implemented from certain mission, critical applications, so due to the Gray hole attack network seems to be useless.

In this paper, I have tried to explain systematic analysis of Gray hole or Selective Forwarding attack, and its all defense mechanism which is used by researchers.

The main objectives of this paper are to give the outlines of dictation and prevention techniques done by developers and researchers.

Now I am explaining Grey Hole or Selective forwarding attack in brief and its different types.

2. GRAY HOLE ATTACK AND ITS DIFFERENT TYPES
Gray Hole attack is first described by Chris Karlof and David Wagner [2] in 1990s.

In the Gray Hole attack nasty or malicious node is acting as normal node and drops the message or packets which is passing through them, hence hiding the important information to forward to the next node or destiny node.

Gray Hole can be understood by below Fig.3

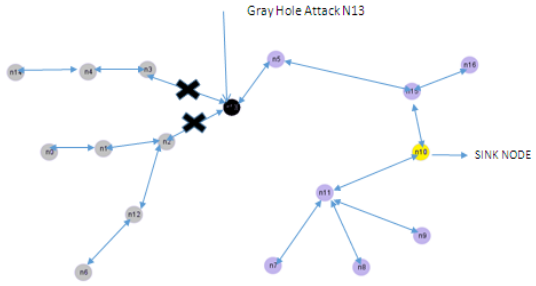


Fig.3 Gray Hole Attack at Node No.13

3. GRAY HOLE CAN BE CLASSIFIED ACCORDING TO NODE COUNT IN WSN [5]

3.1 Single Nasty Node

In the Single Nasty Node, Selective Forwarding attack, as per Fig.4. Node No.4 is acting as nasty node and dropping selective packets.

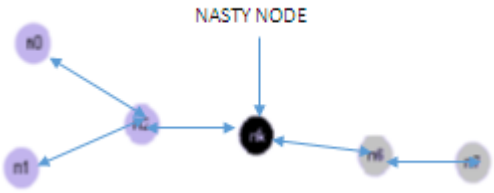


Fig.4 Single Nasty Node Gray Hole Attack

3.2 Two Consecutive Nasty Node

In Fig.5 Two consecutive Nodes N4 and N5 node acting as nasty nodes, dropping packets and forwarding selective packets only.

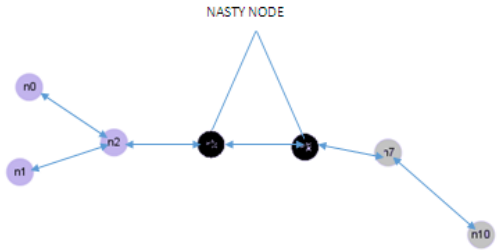


Fig.5 Two Consecutive Nasty Node Gray Hole attack

3.3 Non-Consecutive Nasty Node

In Fig.6 N3 and N7 and are the non consecutive nodes and they are acting as nasty node of the attackers, which forward or drops the selective packets on Network.

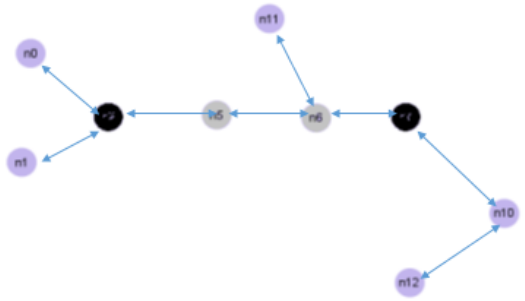


Fig.6 Two Non Consecutive Nasty Node Attack

3.4 Surrounding Nasty Node:

In Surrounding Nasty Nodes attack, Sometimes attackers affect the forwarding of the Selective packets in influence of the surrounding Nodes N6, N8 and N9.

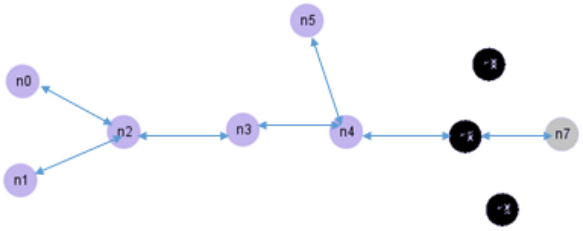


Fig.7 Surrounding Nasty Node Attack

4. GRAY HOLE CAN BE FURTHER DIVIDED ACCORDING TO DROPPING OF PACKETS

1. Drops Packets of some specified node.
2. Drops Packets of some specified types.

5. DIFFERENT LAYER ATTACKS [6]

Before we explain the attacks on TCP/IP layers, the attacks can be also classified as:

5.1 Active Attacks

In the Active attacks, attackers influence the normal operation of the WSN, by altering modifying or fabricating the packets or message text.

5.2 Passive Attacks

In the case of Passive Attacks, the attacks only interfaces in the exchange of data between the two Nodes, but in the passive attacks does not alter the information of the packets transmitted.

5.3 External Attacks

In the case of External attacks, the attacks is to be carried out by the node which does not belongs to the network, in which the attackers have placed nasty node for the attacks.

5.4 Internal Attacks

In the case of Internal attacks, the attacks is performed by the node, which belongs the network which is taken park in the transmission and receiving of the packets.

Now, we will summarize the attacks on different layer in below Table.1

Table 1. Attacks on Different Layer

LAYRES	ILLUSTRATION
PHYSICAL	Jamming,Alteration,Eavesdropping (hearing someone by hiding itself)
DATA LINK	Unfairness, Selfish MAC,Flodding
NETWORK	Flooding, Wormhole Attack, Sybil Attack, Gray Hole Attack, Black Hole Attack Routing Table Overflow Attack, False Routing Control Message
TRANSPORT	Syn-Flooding, De-Synchronization
APPLICATION	Logic Overflow, Buffer Overflow

In our research paper we will only focus on Attacks on **Network Layer [7].**

1. Black Hole Attack (BH)

In Black Hole Attack, the Nasty Node exploits Routing Protocol to advertise himself as valid and secure Route for exchange of packets between two nodes, and then it drops all the packets which is transferred or routed from this nasty node. As shown in below Fig.8

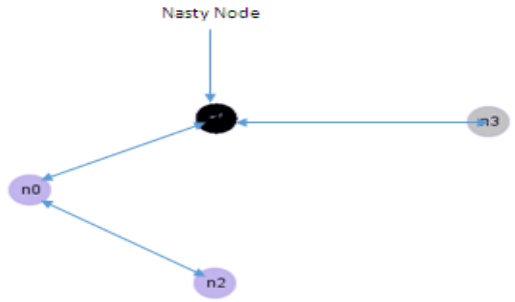


Fig.8 Black Hole Attack

2. Worm Hole Attack

In Worm Hole Attack, the attacker captures packets at one location and tunnels them to another location, by the help of attacker nasty node.

In Worm Hole attack, nasty node shows itself attractive node and shows the shortest route to the network to route the packets from the source node, hence drop all the packets which is transmitted from this node. In the below Fig.9, Worm Hole took place in N1-N10-N6 (shortest path to route Packets)

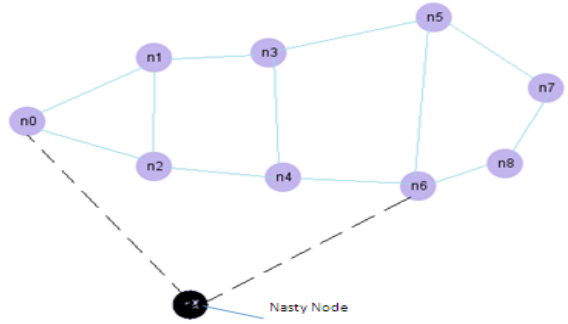


Fig.9 Worm Hole Attack

3. Sybil Attack

In the Sybil Attack, the attacker or Nasty Node shows its multi Identity, hence affect the Routing table and exploit the transmission and reception of the packets between the nodes.

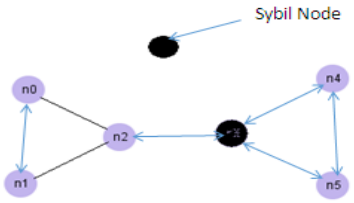


Fig.10 Sybil Node use Identity of node n4 and n5

4. Flooding

In the Flooding, the nasty node simultaneously broadcast or transmits large number of packets, so due to this it is not possible to receive the packets from the neighbor node or source node, hence flooding affect the reception of packets in the network.

6. RELATED WORK

6.1 G.Padmavathi and Mrs. Shanmugpriya [8] have discussed wide range of security attacks, in the Network and also discussed challenges faces by the user to collect information from the network.

In the Research paper, Author described the Selective Forwarding or Gray Hole attack and took this attack in the category of Active attack.

6.2 B.Yu [9] proposes a method based on check points and acknowledgement based for detection of Gary Hole attack. Here in the proposal of B.Yu, he selected certain nodes and the path for communication among these nodes is random, and these nodes are transmitting acknowledgement to the source node, If the acknowledgement is not transmitted by the certain nodes to the source node, attack is detected but there is some limitation of this proposed method.

1. As the method is based on acknowledgement based, cost of the network is increases.
2. Sometimes false detection is also done; as if the acknowledgement is not transmitted due to congestion then also Gray hole is detected.

6.3 Jiang [10] proposes a method of trust and packets loss for the detection of Gray Hole attack or Selective Forwarding attack. In the Proposal of Jiang, on Network Topology, when Data is transmitted on the path to the different nodes from the source node, total packets which is received at particular node is counted, if there is any packet loss the loss is informed to the source node, after this Source Node will transmit the packets again taking the another path for transmission, here with the total count of the packet it is also counted that, if the specified type of packets are dropped by nasty node, if this happens this is due to Active gray hole Attack.

6.4 Sophia Kaplantzis [11] uses centralized intrusion detection system based technique on SVM (Support Vector Machines), and sliding windows. Here Sophia uses the intrusion detection at the Sink Node, so the energy of nodes is also saved. She proposed that this is the best method for detecting the Gray Hole attack without utilizing the energy of the sensing node.

6.5 Brown and Xiaojiang [12] uses heterogeneous sensor network (HSN) for detection of selective forwarding attack. In the HSN model consist of high end large Sensor Node (H-Sensors) and Low end (L-Sensors). After deployment of all Sensor nodes, a cluster formation takes place with H-Sensors as Cluster Head.

6.6 Xin with his colleagues [13] uses light weight defense schemes for the detection of Gray Hole attack. He uses the neighbor node as monitoring nodes and resends the dropped packets again to the nodes associated with that node.

6.7 Guori Li [14] with his colleagues uses sequential mesh test based scheme. The Cluster head node detects the nasty node based on the sequential mesh test method after receiving the report from the nodes. In the scheme it extracts small samples from the networking nodes instead of doing test on whole network in advance. In the sequential mesh test method, the test decides whether to continue the test or to hold after final conclusion.

The advantage of this scheme is that it requires less power, less computational method less communication and shorter detection time.

6.8 Din-Yin Zhang [15] with his colleagues proposes the techniques based on the digital watermarking technique for detection of Gray Hole attack.

In the digital watermark technique, digital watermark is fixing with the source data packets and these digital watermarks are extracted at the sink node. By the help of received packets at the sink node lost packets is calculated and it also detect the tampered node which creates the Gray Hole attack.

In brief by the help of below **Table.2** we can see the analysis of different proposed techniques:

Table.2. Quantative Analysis of Different Techniques

Detection Techniques	Counter Other Attacks	Scheme Nature	Consider Other Means of Packet dropping	Acknowledgement Based	Neighbor Monitoring Based	Multipath based	Reliable Data Delivery
Sophia SVM Technique	Yes	Centralized	No	No	Yes	No	No
Brown et. Al Technique	No	Centralized	Yes	No	Yes	No	No
YU and Xiao's Technique	No	Distributed	Yes	Yes	No	No	No
Watermark Technique	No	Distributed	Yes	No	No	No	No
Wangxing Sheng et. Al Schemes	No	Distributed	No	No	Yes	No	Yes
A Sequential Based Mesh Technique	No	Centralized	No	No	Yes	No	No

7. PROPOSED TECHNIQUES

In Our proposed technique we are using method of Mod technique and sequence method for the detection of Gray Hole Attack in Network and analyze the result in the form packet delivery ratio, end to end delay, bandwidth utilization etc.

8. CONCLUSION

Security, Confidentially, authentication and timely transmission and reception of packets is need of any wireless sensor networks. The attack which affect the WSN and not easy to detect is Gray Hole attack, in which nasty node drops some part of packets which is transmitted from source node.

As we seen and study different methods are proposed from different researchers, but all having drawbacks. Also sometimes happens that due to congestion of the network false attacks came into existence.

In the proposed technique, I have tried to give the better utilization of bandwidth, good packet delivery ration and less end to end delay, which help us and also to new researchers to design networks which counter this type of attacks.

9. ACKNOWLEDGEMENT

The authors wish to acknowledge oriental university for their support & motivation during this research. The

Author would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. Author also like to give thanks to Dr. Deepak Sukheja and Asst. Prof. Sunil Patel for discussions in specific domain.

10. REFERENCES

[1] Anthony Wood, John A.Stankovie,"Deniel of Service In Sensor Network" IEEE Computer,pg: 54-62, October 2002.

[2] C.Karlof and D. Wagner "Secure Routing in wireless Sensor Networks and Countermeasures" in Adhoc Network, Vol. 1 pg 293-315.

[3] B.YU and B.Xiao"Detecting Selective Forwarding Attack in Wireless Sensor Network" in pg 1-8.

[4] Ian F.Akyildiz, weilian Su, Yogesh Subramanian and Erdas Cayirei" A Survey on Sensor Networks".

[5] Leela Krishna Byrani and Ashok KumarTuruk" A survey on Selective Forwarding attack in Wireless Sensor Network".

[6] Kanu Geete, Piyush Kumar Shukla, and Anjana Jayant Deen" A Survey on Gray Hole Attack in Wireless Mesh Network".

[7] Vikas Solomon Abel" Survey of Attacks on Mobile Adhoc Wireless Network". Vol.3 No.2.

[8] G. Padmavathi, D. Shanumugapriya"A Survey on Attacks, Security mechanism and challenges in Wireless Sensor network". Vol. 4 pg 117-125, 2009.

[9] B Yu, B Xiao " Detecting Selective Forwarding attack in Wireless Sensor Network".

[10] Jiang Changyone, Zhang Jianming" The Selective Forwarding attack Detection in WSN".pg 140-143, 2009.

[11] Sophia Kaplantzis, Alistair Shilton, Nallasamy mani, Y.Ahmad, Ekesnio Glu"Detecting Selective Forwarding attack By using SVM. Intelligent Sensor Networks and Informations, 3rd Internation Conference, pg 333-340.

[12] Jeremy Brown and Xiaojiang Du." Detection of Selective Forwarding Attack in Heterogeneous Network", In ICC pg 1583-1587, 2008.

[13] Wang Xin-Sheng, Zhan Yong-Zhao, Xiang Shu-ming and Wang Liangmin,"Lightweight defense scheme against selective forwarding attack in Wireless Sensor Networks" pg 226-232. Oct 2009.

[14] Gouri Li, Xiangdong Liu and Wang" A Sequential Mesh Based Test based Selective Forwarding attack, detection schemes in wireless Sensor Nrtworks".

[15] Ding Yin Zhanga,Chao Xub, Lin Siynan"Detecting Selective Forwarding Attack in WSN".

[16] Preeti Sharma. Monika Saluja and Krishna Kumar Saluja" A review of Selective Forwarding Attack in Wireless Sensor Networks.