ISSN:0975-9646

An Effectual Defense Method against Gray Hole Attack in Wireless Sensor Networks

Jaspreet Kaur, Vinod Kumar
Department of computer science
Lovely Professional University Phagwara (PB), India

***Abstract*-Wireless Sensor Network (WSN) is usually consisting of huge number of limited sensor devices which are communicated over the wireless media. There are a lot of its applications in military, health and industry. Many of WSN applications such as military and healthcare are critical and required certain level of security. Therefore it is necessary to provide wireless sensor network not only with the acceptable reliability of services but also adequate level of security. As sensor devices are restricted, security in WSNs is a challenging task and the networks exposed to various kinds of attacks and conventional defences against these attacks are not suitable. Wireless sensor network is a growing technology which is offering solution to variety of application areas such as health care, military and industry. These kinds of networks usually apply number of devices known as sensor devices. These sensors which are limited are distributed over the environment and communicate through the wireless media. In this paper I am working on a multi level secure routing scheme against Gray Hole atac in WSN. I hereby propose the use of local monitoring technique to defend the Gray Hole attack in WSN. The tool that I will use to defend is NS2 that is compatible with fedora Linux operating system.**

I. INTRODUCTION

In WSN, sensor nodes use wireless communication to send packets. Due to limited transmission range, a sensor node uses multi-hop transmission to deliver the packet to a base station. Hence a packet is forwarded through so many hops/nodes to reach the destination. As, we discussed sensor networks are usually deployed in hostile environments, an adversary can launch attacks. Attacks can be classified into two types, inside attacks and outside attacks. The latter one can be easily detected and security solutions are provided. In former one, adversary compromises some internal nodes and Launches attacks which will be difficult to detect. One kind of such attack is Selective Forwarding. In Selective Forwarding, the compromised internal node selectively drops/forwards. Wireless sensor networks (WSN) have seen increased attention due to their wide application in living life. The most essential applications are monitor systems, such as military monitor system or security service system. These applications can allow some normal packets lost in a short period but cannot tolerate the loss of critical event packets. For example, in military monitor systems, when a sensor node detects enemy tank movements, it will send this sensitive information back to the base station. If the base station does not receive this information, it cannot react immediately. Therefore it is necessary to provide wireless sensor network not only with the acceptable reliability of Services but also adequate level of security. As sensor devices are restricted, security in WSNs is a challenging task and the networks exposed to various kinds of attacks and conventional defenses against these attacks are not suitable. One of the most severe attacks to detect and defend in wireless sensor network is wormhole attack which, a malicious attacker receives packets from one location of network, forwards them through the tunnel (wormhole) and releases them into another location.[1-5]. In this paper, we have discussed about selective forwarding attack, its types and some countermeasure schemes. The rest of the paper is organized as follows. In section 3, we discussed some of the attacks in sensor networks. In section 4, we discussed about selective forwarding attack and classified it.

II. SENSOR DEVICE ARCHITECTURE

The sensor node device as the simplest tool in the wireless sensor networks and considers the five elements for sensor device. According to their works, sensor node device has the Microcontroller which manages all tasks. It also equipped with the memory which is used to store environmental sensed data. The radio transceiver is used to transmit data. Additionally it has the sensor to sense environment. And finally the power source, the battery, which is used to provide required power for the other elements. As sensor device consist of limited components, it could note used for complex tasks and processes. Mechanisms including security approaches, should meet these restrictions in order to be viable in sensor networks.

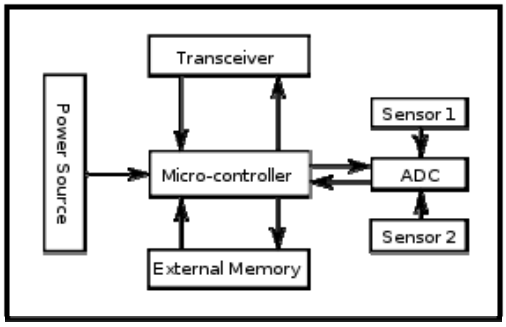

Figure 1 Sensor Node Architecture

III. ATTACKS AND THEIR CLASSIFICATION

To secure wireless sensor network, it has to satisfy all the security properties like integrity, confidentiality, availability and authenticity. Before discussing selective forwarding attack, we discuss some of the security attacks [6]

A. Selective Forwarding

In a selective forwarding attack [7], [8], malicious nodes Behaves like black hole and may refuse to forward certain

messages and simply drop them. However, such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets. Originating from a few selected nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing. After receiving a packet, the attackers selectively forward or not to forward the packet, or just send the packet containing the routing information to prevent it from reaching the destination. In that case, the packet needs to be re-transmitted and the network traffic and power consumption will increase, and thus the lifetime of the entire network is reduced.

B. Wormhole

In the wormhole attack [9], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

C. Sybil

The concept of Sybil (or multiple-identity) attacks was first proposed by Douceur in P2P networks [13], and it is defined as a single node has multiple identities to disrupt the accordance between entities and physical devices in the networks. A method was proposed using the trusted certification center to verify the physical identity for preventing multiple-identity attacks. The multiple-identity attacks usually use a single malicious node to confuse neighbor nodes, causing chaos among them, and finally the entire network is interfered and thus cannot function properly.

D. Acknowledgement Spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements [10]. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for"overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

E. Impersonation

Node Replication Also called Multiple Identity, Impersonation. An attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. Node replication attacks can occur if an adversary can copy the node identification of a network node. In this manner packets could be corrupted, misrouted or deleted, and if this adversary could perform this replication it is possible that cryptographic keys could be disclosed.

F. Eavesdropping

The attacker collects data by eavesdropping to obtain secret data or useful information. For the proposed mechanism, the public key and base point *G* are points on an elliptic curve. The attacker cannot derive the secret key even with the public key and base point *G* since it doesn't have the private keys to solve the DLP. Besides, the secret information can also be transmitted with encryption and signatures to prevent from eavesdropping.

G. Traffic Analysis

Traffic analysis attacks are forged where the base station is determinable by observation that the majority of packets are being routed to one particular node. If an adversary can compromise the base station then it can render the network useless.

H .Gray Hole Attack and its classification

Gray Hole Attack is one of the network layer attack described in [12]. In multi-hop WSN, the nodes send packets to the neighboring nodes thinking that they forward messages to destination faithfully. In Gray Hole attack, a malicious or compromised node legitimately refuses some packets and drops them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing through it. However in such an attack, the nodes can easily detect the attack and can exclude attacker from routing. But, here in selective forwarding attack, malicious nodes selectively drop/forward packet which makes detection of the attack more complicated.

IV. ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORK

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's

source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery. Multicast routes are set up in a similar manner. A node wishing to join a multicast group broadcasts a RREQ with the destination IP address set to that of the multicast group and with the 'J'(join) flag set to indicate that it would like to join the group. Any node receiving this RREQ that is a member of the multicast tree that has a fresh enough sequence number for the multicast group may send a RREP. As the RREPs propagate back to the source, the nodes forwarding the message set up pointers in their multicast route tables. As the source node receives the RREPs, it keeps track of the route with the freshest sequence number, and beyond that the smallest hop count to the next multicast group member. After the specified discovery period, the source node wills unicast a Multicast Activation (MACT) message to its selected next hop. This message serves the purpose of activating the route. A node that does not receive this message that had set up a multicast route pointer will timeout and delete the pointer. If the node receiving the MACT was not already a part of the multicast tree, it will also have been keeping track of the best route from the RREPs it received. Hence it must also unicast a MACT to its next hop, and so on until a node that was previously a member of the multicast tree is reached. AODV maintains routes for as long as the route is active. This includes maintaining a multicast tree for the life of the multicast group. Because the network nodes are mobile, it is likely that many link breakages along a route will occur during the lifetime of that route.

1) The basic message set consists of:

RREQ – Route request
RREP – Route reply
RERR – Route error

2) AODV Operation – Message Types

RREQ Messages

1) While communication routes between nodes are valid, AODV does not play any role.
2) A RREQ message is broadcasted when a node needs to discover a route to a destination.
3) As a RREQ propagates through the network, intermediate nodes use it to update their routing tables (in the direction of the source node).
4) The RREQ also contains the most recent sequence number for the destination.
5) A valid destination route must have a sequence number at least as great as that contained in the RREQ.

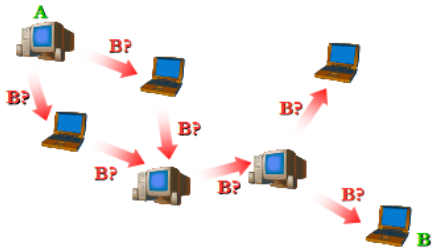

Figure 2RREQ Message

RREP Messages

1) When a RREQ reaches a destination node, the destination route is made available by uni casting a RREP back to the source route.
2) A node generates a RREP if: It is itself the destination. It has an active route to the destination. Ex: an intermediate node may also respond with an RREP if it has a “fresh enough” route to the destination.
3) As the RREP propagates back to the source node, intermediate nodes update their routing tables (in the direction of the destination node).

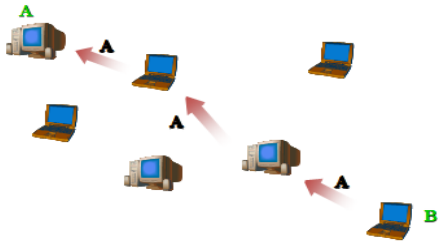

Figure 3 RREP Message

RERR Messages

1) This message is broadcast for broken links
2) Generated directly by a node or passed on when received from another node

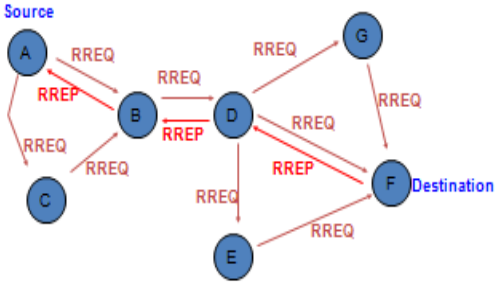

Figure 4 Message Routing

V. SELECTIVE FORWARDING AND ITS CLASSIFICATION

Selective Forwarding Attack is one of the network layer attack described in [10]. In multi-hop WSN, the nodes send packets to the neighboring nodes thinking that they forward messages to destination faithfully. In Selective Forwarding attack, malicious nodes legitimately refuses some packets and drops them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing.

VI. NS-2 SIMULATOR

NS is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior. At the simulation layer NS uses OTcl (Object oriented Tool Command Language) programming language to interpret user simulation scripts. OTcl language is in fact an object oriented extension of the Tcl Language. The Tcl language is fully compatible with the C++ programming language. At the top layer, NS is an interpreter of Tcl scripts of the users; they work together with C++ codes. An OTcl script written by a user is interpreted by NS. While OTcl script is being interpreted, NS creates two main analysis reports. Simultaneously. One of them is NAM (Network Animator) object that shows the visual animation of the simulation. The other is the trace object that consists of the behavior of all objects in the simulation. Both of them are created as a file by NS. Former is .nam file used by NAM software that comes along with NS. Latter is a ".tr" file that includes all simulation traces in the text format. NS project is normally distributed along with various packages (ns, nam, tcl, otcl etc.) named as "all-in-one package", but they can also be found and downloaded separately.

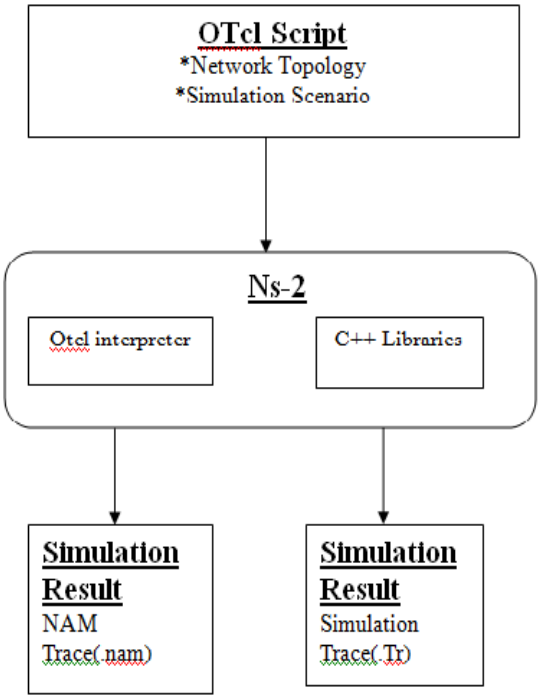

Figure 5 NS-2 Simulators

VII. SIMULATION PARAMETERS

1) *Implementing the new routing protocol in ns-2 which show Gray Hole behavior*

Implementation of the Gray Hole attack is done in AODV protocol and simulated in NS-2.34. To show the Gray Hole behavior, one node is selected as attack node and it will drop packets randomly. The attack node should be able to participate in

```
# grayholeaodv patch
Simulator instproc create-grayholeaodv-agent { node }
        set ragent [new Agent/ [$node node-addr]]
        $self at 0.0 "$ragent start"
        $node set ragent_ $ragent
        return $ragent
}
```

Figure 6 ns –lib.tcl Gray Hole modification

The AODV messaging. For this the new protocol which exhibits Gray Hole attack should be able to participate in AODV messaging. Implementation of the new routing protocol which performs Gray Hole attack is explained below. All routing protocols in NS2 are installed in the ns-2.34 directory. We start by duplicating the AODV protocol in this directory and named the directory as " GrayHoleaodv "(all the header files and classes of AODV directory are modified). All the files in the AODV directory are modified with GrayHoleaodv such as GrayHoleaodv .cc, GrayHoleaodv .h, GrayHoleaodv rqueue.cc, gaodv rqueu.h etc except for "aodv packet.h. The new protocol use the same AODV packets and thus its possible for the new GrayHoleaodv protocol to send the same AODV packets. So we have changed all the names of classes, structures, functions in all the files except for the struct names that belong to the AODV packet.h code. By creating all this we have designed aodv and GrayHoleaodv protocols to send packets with each other. To integrate the GAODV protocol to the NS2, two common files has to be modified. Since we are using the same packets used in AODV, we don't have to modify the common files related to packet. Thus had to modify two files [18]. The first modified file is the ns - lib.tcl. It's in this file the protocol agents are coded in a procedure. So here we have to add the protocol agent for the newly created GrayHoleaodv protocol. When a node is using GrayHoleaodv protocol this agent is scheduled at the beginning of the simulation and is assigned to the nodes which use the protocol. The next file to be modified is the ns-agent.tcl. In this we have to set the port numbers for the new routing protocol. **Sport** is the source port and **dport** is the destination port.

```
Agent/grayholeaodv instproc init args {

        $self next $args
}

Agent/grayholeaodvset sport_    0
Agent/grayholeaodvset dport_    0
```

Figure 6 ns- agent.tcl GrayHoleaodv modification

```
grayholeaodv/grayholeaodv_logs.o grayholeaodv/grayholeaodv.o \
grayholeaodv/grayholeaodv_rtable.o grayholeaodv/grayholeaodv_rqueue.o \
common/ns-process.o \
```

Figure 7 makefile.in GrayHoleaodv modification

The third file modified is the makefile.in in the root directory of ns-2.34. This file is modified for creating the object files for the cpp coded files. After all the implementations are ready, we have to recompile NS-2 again to create the object files. Till now we have implemented a new routing protocol in NS-2 which is labeled as GrayHoleaodv. But we still didn't implement the Gray Hole attack in this protocol. As of now this protocol act similar to the AODV protocol. To add Gray Hole behavior in to the new protocol to make some changes in the GrayHoleaodv .cc C++ file. By explaining the working mechanism of AODV and GrayHoleaodv protocol we will describe the changes made to the GrayHoleaodv:cc. In aodv.cc code when a packet is received it is received by a function called the recv and the received packets are processed based on the type of the packet. In this code the different control packets in AODV like RREQ, RREP and RERR packets are processed by different functions. The recv function checks whether the received packet belongs to any of these control packets. If it so then it will call the recv AODV function. If the received packet is a data packet, usually

```
//If destination address is itsself
if ( (u_int32_t)ih->saddr() == index)
   forward((gaodv_rt_entry*) 0, p, NO_DELAY);
else if ((rand()%6)==3 || (rand()%6)==4 || (rand()%6)==1)
// For grayhole attack in the wireless adhoc network, after giving a true route to demanding
// node, misbehaving node drops some packets according to the random function.
   drop(p, DROP_RTR_ROUTE_LOOP);
```

Figure 8 GrayHoleaodv.c modification

The AODV protocol will forward the packet to the destination address. But in GrayHoleaodv protocol the code is modified such that it will drop random packets without forwarding it. This attack is implemented in the recv function of GrayHoleaodv. First the conditions checks whether the packet is destined to itself if it so it will accept the packet, otherwise a condition is checked which is made of random numbers and if the condition becomes true the packet is dropped otherwise it will forward the packet.

2) Implementation

In this chapter, we discuss the simulation. We simulated the proposed method using NS-2 simulator which runs in Linux Fedora.

3) Simulation environment

For simulation, we have selected NS-2.34 simulator. The numbers of nodes is fixed between 6 and are randomly deployed in an area of 300x300 square meters. Simulation time is 300 seconds. Simulation parameters are shown in the Table 1. The metrics we considered for comparison are the packet delivery ratio and packet drop ratio in presence and absence of malicious node and compared with and without the proposed scheme.

Simulation Area	300x300
No. Of Nodes	6
Simulation Duration	300 Seconds
Data Rate	10kb
Packet size	512

Table 1 Simulation Parameters

4) Network Simulation Model

The NS-2 network simulator is use to create a simulation environment. The visual simulation network model is shows in NAM (Network Animator) programmed. The source-destination pairs are spread randomly over the network. The number of sources is varied in the simulations, the nodes act as source, node 19, 10 and node 3, meanwhile the nodes act as destination, node 6, 4 and node 2. The network model consists of 25 nodes. This diagram shows the create nodes in the NAM.

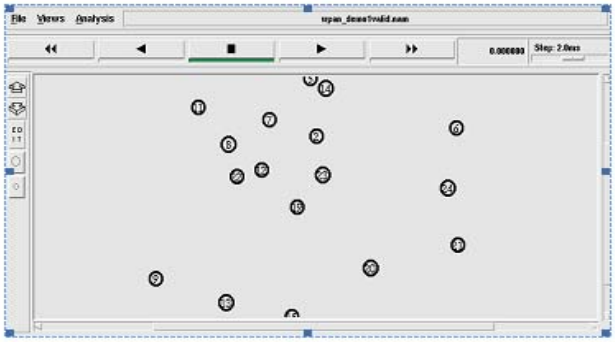

Figure 9 Network model.

5) Simulation of AODV vs. Gray Hole AODV

The simulation of AODV and Gray Hole AODV was carried out within the same simulation time but with different agent, which AODV used agent AODV meanwhile Gray Hole AODV used agent Routing agent.

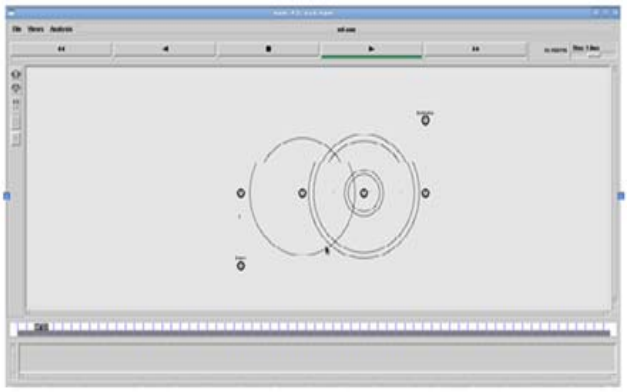

Figure 10 Data Forward from Source to destination Node

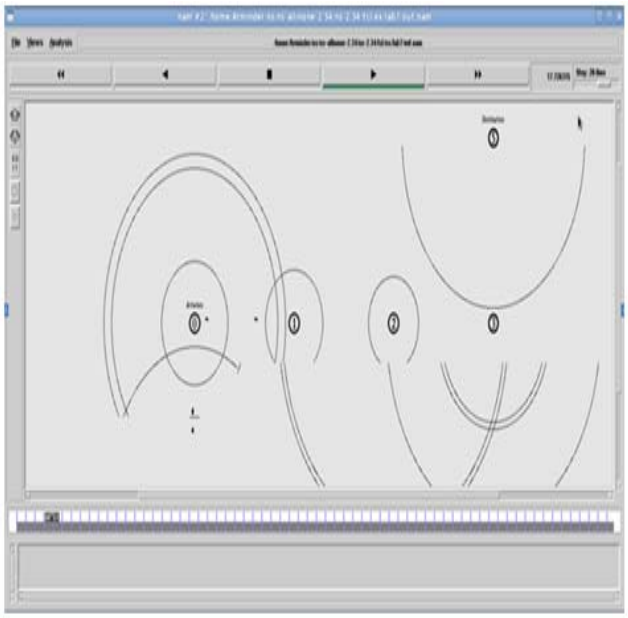

Figure 11 Data Forward from Source to destination Node Using Attacker node

In the Fig. 7.3 There are 6 nodes Data is send from source node 4 to destination node 5 via 0,1,2,3 0 node is attacker node .Attacker Node drop selective packets and some packets are forward to its neighbor node.

VIII. CONCLUSION

In WSN, sensor nodes use wireless communication to send packets. Due to limited transmission range, a sensor node uses multi hop transmission to deliver the packet to a base station. Hence a packet is forwarded through so many nodes to reach the destination. Sensor networks are usually deployed in hostile environment where an adversary can compromise some internal nodes which may launch various inside attacks. One kind of attack caused by malicious nodes is Selective Forwarding. In Selective Forwarding attack, the compromised internal nodes intentionally drop some packets passing through them. If node drops all the packets then it becomes black hole attack. The selective forwarding is difficult to detect since the wireless communications are not reliable where normally there is a loss of data packets. Due to noise. In some cases sensor nodes goes into sleep state to save power, in that period of time node cannot send and receive data. So we have to be careful whether the packet drop is due to selective forwarding or any other reason.

REFERENCES

[1] Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis. Zhao, Zhibin, et al. s.l. : IEEE, 2010. WASE International

[2] Conference on Information Engineering. pp. 251 - 254.An Approach towards Detection of Wormhole Attack in Sensor Networks. Prasannajit B, Venkatesh, et al. 2010. WASE International Conference on Information Engineering. pp. 283 - 389.

[3] Secure Routing in Wireless Sensor Network: Attacks and Countermeasures. Karlof, Chris and Wanger, David. 2003, IEEE, pp. 113-127.

[4] Security of Wireless Sensor Networks. Rehana, Jinat. 2009. Seminar on Internetworking.

[5] Sensor Network Security: A Survey. Chen, Xiangqian, et al. 2009, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, pp. 52-73.

[6] Hemanta Kumar Kalita and Avijit Kar. Wireless sensor network security analysis. In *International Journal of Next-Generation Networks*, 2009

[7] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009.

[8] S. Kaplantzis, A. Shilton, N. Mani, and Y.A. Sekercioglu. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 335 –340, 2007.

[9] Y.C.Hu, A.Perrig, and D.B.Johnson. Packet leashes: a defense against wormhole attacks in wireless networks In *In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications.IEEE Societies*, 2003.

[10] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293– 315, 2003.

[11]Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liang-min. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. Pages 226–232, oct. 2009.

[12] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. Un-mask: Utilizing neighbor monitoring for attack mitigation in mul-tihop wireless sensor networks. Volume 8, pages 148–164, 2010.

[13] Chris Karlof and David Wagner. "Secure routing in wireless sensor networks": attacks counter measures. *Ad Hoc Networks*, 1(2-3): 293–315, 2003

[14] Brown, J.; Xiaojiang Du "Detection of Selective Forwarding Attacks in Heterogeneous Sensor Networks" ,. *"IEEE International Conference on"* 2008 , Page(s): 1583 - 1587

[15] Hung-Cuong Le, Herve Guyennet, Noureddine Zerhouni "Over-hearing for Energy Efficient in Event-Driven Wireless Sensor Network" "*International Conference on IEEE* 2006" Page(s): 633 - 638

[16] Young Ki Kim, Hwaseong Lee, Kwantae Cho, and Dong Hoon Lee "CADE: Cumulative Acknowledgement Based Detection of Selective Forwarding Attacks in Wireless Sensor Networks" "*convergence and Hybrid Information Technology, ICCIT '08. Third International Conference on* 2008." Page(s): 416 - 422

[17] Modirkhazeni, A.; Aghamahmoodi, S.; Modirkhazeni, A.; Niknejad, N. "Distributed approach to mitigate wormhole attack in wireless sensor networks" "*Networked Computing (INC), The 7th International Conference on*2011" Page(s): 122 - 128

[18]Yenumula Reddy!, Jan Durand#, and Sanjeev Kafle "Detection of Packet Dropping in Wireless Sensor Networks" *"Seventh International Conference on Information Technology* 2011"

[19]Zang Li et al, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks", "*Proceedings of the 4th international symposium on Information processing in sensor networks2005"*.