Survey on different attacks in Wireless Sensor Networks and their prevention system

Ruchita Dhulkar, Ajit Pokharkar, Mrs. Rohini Pise

[1] *BE IT, Department of Information Technology, PCCOE, Maharashtra, India*

[2] *BE IT, Department of Information Technology, PCCOE, Maharashtra, India*

[3] *Assistant Professor, Department of Information Technology, PCCOE, Maharashtra, India*

---***---

Abstract – ***Wireless Sensor Network (WSN) is a large network of sensor nodes. Wireless Sensor Networks are very popular and have their special characteristics such as limited battery, limited power and limited storage that makes the energy consumption. Although there are some limitations but there are many advantages of Wireless Sensor Networks. Some advantages are robustness, scalability, flexibility. WSN also reduces the cabling cost. Now a days WSN is mostly used in modern technologies to gain the output in most efficient way. Some applications of WSN are area monitoring, health care monitoring, Earth sensing, Landslide detection etc. In this paper we are detecting and preventing black hole attack, gray hole attack, misdirection attack and DOS attack. For prevention of all these attacks we are using one protocol which is LEACH protocol. LEACH protocol means Low Energy Adaptive Clustering Hierarchy. This protocol uses limited energy which increases the network lifetime.***

Keywords - *Wireless Sensor Network, Black Hole attack, gray hole attack, misdirection attack, DOS attack, LEACH*

Introduction:

Wireless sensor network is a network composed with a number of small sensor devices that communicate with each other wirelessly. wireless sensor network provides a bridge between the real, physical and virtual words. WSN have a wide range of potential applications to industry, science, transportation, civil infrastructure and security. WSN has an important application such as remote environment, the applications design objectives, cost, hardware and system constraints.

1. Attacks in Wireless Sensor Networks:

1.1 Black Hole Attack :

Black hole attack occurs when an attacker captures and attacker reprograms a set of nodes in the network to block the packets which they receive instead of forwarding towards base station. Important Event information do not reach the base stations. In presence of black hole attack throughput becomes very less and end-to-end delay increases.

1.2 Gray Hole Attack :

In gray hole attack normal nodes works very unpleasant way which shows itself as a normal node and takes part in the transmission of packet from packets. These unpleasant nodes drops the selected packets and only transmits the left packets to the neighbor node.

1.3 Misdirection attack :

In misdirection attack malicious nodes misdirect packets to other destination. Here while sending packets some packets change its direction during transmission.

1.4 DoS attack :

DoS attack is an attempt to make a machine or network resource unavailable to its intended users. A denial of service attack is characterized by an explicit attempt by attacker to prevent legitimate user of a service from using that service.

Literature Survey :

Wireless Sensor Networks (WSNs) are prone to various attacks in which Black hole a kind of Denial of Service (DoS) attack is very difficult to detect and defend. In black hole attack, an intruder captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result any information that enters the blackhole region is captured and not able to reach and low throughput. Previously little amount of work is done for detection and prevention of the Blackhole attack in the WSN making its detection and prevention very crucial as per network performance is concerned. In this paper initially the affect of Blackhole attack is measured on the network parameters followed by the proposal of a novel technique for the detection and prevention of Blackhole attack in WSN.

Wireless Sensor Network (WSN) is a large network of sensor nodes, which operates in low power and capable of transmitting to a shorter distance with low bandwidth. It comprises of sensing unit, processing unit, memory unit, power supply and transceiver. As these sensor nodes are battery operated, the lifetime of the sensor node depends on the life of the battery. The sensor nodes in the network communicate in a mesh and multi-hop fashion, redundant data may exist in the network. In order to enhance the robustness and accuracy of the information obtained by the network, redundancy has to be reduced. One such protocol which works on the basis of data fusion to reduce redundant data is LEACH (Low Energy Adaptive Clustering Hierarchy). The LEACH protocol uses limited energy thus increases the network lifetime. The security of information transfer via wireless network is a challenging issue. In order to check the reliable operation of LEACH routing protocol, we implemented gray hole attack and evaluated the performance of the LEACH protocol in terms of metrics like packet drop ratio, throughput and Average End-to-End delay. The evaluation of LEACH with Gray hole attack has been done with the help of Ns2 simulator. Constrained resources, the ad-hoc nature of deployment and the vulnerability of wireless media are some of the most challenging characteristics of Wireless Sensor Network (WSN) which pose a need for unique security solutions. WSNs are susceptible to various attacks, in which Misdirection a kind of Denial of Service (DoS) attack is very difficult to detect and defend. In Misdirection Attack, the intruder misdirects the incoming packets to a node other than the intended node which introduces high end-to- end delay (sometimes infinite) in the network. The performance of the network (i.e. throughput) is also degraded. Thus the detection and prevention of this attack becomes very crucial. In this paper we have proposed a novel Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack. The network parameters calculated by the use of this technique shows considerable amount of improvement in throughput while introducing small amount of delay.

With the facility of deployment, Wireless Sensor Networks becomes very popular but have special characteristics such as limited battery, limited processing power, and limited storage that makes the energy consumption saving a real challenge. Add to this and due to their distributed

deployment, these networks are exposed to denial of service attacks such
as jamming and greedy attacks. In all cases these attacks tackle the energy consumption in order to degrade the overall Quality of Service (QoS).

In this paper, we propose an energy-preserving solution to detect compromised nodes in WSNs.

NODE	ID
R1	IDR1
R2	IDR2
R3	IDR3
---	----
R6	IDR6

The proposed method is based on hierarchical clustering technique which elect Controlled nodes (Cnode) that analyze the traffic inside a cluster and to send warnings to the cluster-head (CH) whenever an abnormal behavior is detected. The proposed method is dynamic as the Cnodes are periodically elected among ordinary nodes on each atomic cluster. Such a solution results in a better energy balance while maintaining good detection coverage as it is based on the distance between nodes, the output throughput and delay between packets transmission. destination causing high end- to- end delay

Existing Method :

In this scenario we have 6 sensor nodes (SN1, SN2, ----- SN6) , And two router nodes (R1, R2) and a coordinator.
The sensor nodes sense any physical phenomenon, convert this into information and send this sensed and processed information to router node R1 and R2. Sensor nodes SN1, SN2 and SN3 are reporting to router R1 and SN4, SN5 and SN6 are reporting to router R2. The router R1 sends data to coordinator node. But router R2 is a Black hole attacker and absorbs all the traffic coming to it without sending it further to coordinator. Router R2, the black hole node is represented by a black background here. When cluster is formed, cluster coordinator is elected and it becomes the responsibility of the cluster coordinator to detect the intruder node in that cluster. All the sensor nodes are in the supervision of coordinator node. Coordinator maintains a table via assigning IDs to all intermediate nodes as shown in Table.

Co is the coordinator node of the cluster . R1, R2 and R3 are the intermediate router nodes reporting to the cluster coordinator. SN1, SN2 ,…., SN9 are sensor nodes which are sensing the physical phenomenon, converting it to information and sending information to the routers. The authentication Phase I process in which cluster coordinator in the network sends the authentication packet to each of the sensor nodes in the network. This authentication message contains two fields; one is the ID of the intermediate node and a bit is set to make it possible to recognize that it is an authentication packet. All intermediate nodes respond to the authentication packet being sent by the coordinator node in Phase I with Response Packet .ACK field having a particular bit is set, used for authentication. The purpose was to prove that the response is coming from the legitimate node.

Sensor nodes (SN1, SN2, -----, SN9) sense physical phenomenon, converts this into information and pass that information to the router nodes in the form of Sensed Data Packet (SDP). Router nodes further process this information and pass it to the cluster coordinator node in the form of Data Packet (DP). The detection of Black hole node by coordinator as ID of router R1 is detected because it is sending the Response Packets (RP) but not the Data Packets (DP). After the detection of the black hole node (here R1), the cluster is reformed by removing node R1. Sensor nodes SN1, SN2 and SN3 which were initially reporting to router R1 now are sending SDPs to R2.

A. Blackhole Attack Detection and Prevention Algorithm

//A node can be coordinator for some period of time defined by tm_lmt (threshold)

// battery_pow (threshold) is the battery power of a coordinator node which decides whether the node is going to act as coordinator or not

// wait-tm is the threshold value of time for which the coordinator node is supposed to be waiting for the incoming packet

// w_tm is the period of time for which a intermediate node makes the coordinator node wait for the incoming packet

// IDj is the ID of detected blackhole node

// ARRV_RESP_DATA: response packet and data packet both arrive

// NOT_ARRV_RESP_DATA: response packet and data packet both not arrived

// ARRV_RESP_NOT_ARRV_DATA: response packet arrived but data packet not arrived

1. Maintains a cluster of sensor nodes as C= {S1, S2, S3, S4………… Sn}

2. Assigns ID to all nodes as ID= {ID1, ID2, ID3, --------------IDn}

3. Selects a coordinator (Si) from the set C as per criteria for some time, all remaining nodes are in the supervision of this node

3a. criteria_ fairness node can be the coordinator upto certain time limit<= tm_lmt

3b. criteria_ efficiency node can be the coordinator if it has battery power>= battery _pow

4. Coordinator maintains a table for ID of all nodes
5. Si periodically checks the ID of each node from the set C'={S1,S2,S3……..Si-1, Si+1,……..Sn} via beacon signal

if (ARRV_RESP_DATA) then no intrusion threat otherwise

if (NOT_ARRV_RESP_DATA)

if (w_tm>= wait-tm) then node failure otherwise w_tm++;

Otherwise

if (ARRV_RESP_NOT_ARRV_DATA) then if (w_tm>= wait-tm)

then

the node can be a malicious node (blackhole) detects its ID (IDj) otherwise

w_tm++;

6. Remove that node from the cluster C''={S1,S2,S3…..Sj-1,Sj+1,…..Sn}
7. Inform its previous nodes via beacon signal for the node with which now they have to communicate

8. Reform the cluster with node set as C''={S1,S2,S3…..Sj-1,Sj+1,…..Sn}

9. Continue detection process

B. Gray Hole Attack :

It is a special type of black hole attack [5] in which the malicious node selectively drops some of the packet it receives.

Algorithm of the attack:

Let GN be the gray hole node

Let Ni,…Nn be the number of source nodes Let SN be the sink node Ni broadcasts and receives HELLO messages

Set round, r=0 ClusterHead()

{ If (SNi threshold > SNi-1 threshold) Set SNi is CH Else SNi-1 is CH }

r=r+1; For every Ni to Nn in the transmission range CH advertises GN joins to the CH Set threshold for GN For every time period T ClusterHead();

If CH=GN Drops packet for an interval Ta Else Go to idle mode

C. Misdirection Attacking Scenario:-

Elect a cluster head using any election algorithm. RETURN: Discover an optimum route from source to destination. Set timer (t) at CH. Start packet transmission from source to destination on the selected route Source maintains a buffer corresponding to each packet

// t is the time when packet was sent by source for iÅ1 to n do assign number to each packet , pack[t][i];

Source shares this buffer to CH Maintains a receiving buffer at each intermediate node at time= t'

// suppose packet takes t1 units of time from in reaching from one node to other node. t'=t + t1;

for iÅ 1 to n do assign number to each packet , recvbuffpack[t'][i];

Cluster Head periodically compares its buffer to receiving buffer at each intermediate node. for each node[x] do for iÅ 1 to n do for jÅ 1 to i do compare pack[t][i] and recvbuffpack[t'][j];

//two possibilities are there all the packets are misdirected to some other node then in that case the receiving buffer of node [x] is empty or some packets are misdirected then it has some entries like packet 1, 2, 3 are misdirected but packet 4 is directed towards intended recipient. if (pack[t][i] ≠recvbuffpack [t'][j] or recvbuffpack[t'][]) then do

Complexity Analysis:

$$=\sum_{i=1}^{n} \Sigma_{j=1}^{i}\ \mathrm{i}$$

$$=\Sigma_{i=1}^{n}\ \mathrm{i}$$

= 1+2 +3 + -----------+ n= n (n+1)/2 If the value of the timer is t = t (n (n+1)/2) If the number of nodes are x = x t (n (n+1)/2) x and t are constant values. Therefore the complexity is Ɵ(n2).

Proposed Method :

We are detecting and preventing black hole ,
Gray hole, misdirection and DOS attack by using one protocol i.e. LEACH protocol.
LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. In LEACH, the cluster head (CH) nodes compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station.

The operation of LEACH is separated into two phases:

i. The setup phase

ii. The steady state phase

In the setup phase, the clusters are organized and CHs are selected and in the steady state phase, the actual data transfer to the base station takes place. During the setup phase, a predetermined fraction of nodes, p, elect themselves as CHs as follows. A sensor node chooses a random number, r, between 0 and 1. If this random number is less than a threshold value, T(n), the node becomes a cluster-head for the current round. The threshold value is calculated based on an equation that incorporates the desired percentage to become a cluster-head (p), the current round (r), and the set of nodes that have not been selected as a cluster-head in the last (1/P) rounds, denoted by G. It is given by:

$T(n) = p/(1-p(r \bmod(1/p)))$

if n €G Where G is the set of nodes that are involved in the CH election.

Wireless sensors are susceptible to many types attacks like capture node, node replication alter data, or cut off the nodes from neighbor. This attacks can comes from several sources like malicious nodes which use the technique of flooding network by sending a large number of message for its neighbors or for the base station. To secure vulnerable WSN from these attacks, several solutions have been proposed in the literature. We regard the solution based on the election of the control nodes to beastly cover the entire network to identify the maximum number of compromise nodes to block their activities. In the beginning, we will present the principle operating of leach algorithm then we will develop the proposed method to elect the Cnode using Leach algorithm. LEACH is probably one of the easiest algorithm to apply to partition the network. It is a dynamical clustering and routing algorithm. It splits a set of nodes into several subsets, each containing a cluster head. This CH is the only node to assume the cost-expensive transmissions to the BS. The self-designed CH inform the other nodes by broadcasting a message with the same transmitting power, using carrier sense multiple access (CSMA) MAC. The other nodes choose to join the cluster associated to the CH whose signal they receive with most power. They message back the CH to inform it (with the CSMA MAC protocol again). CHs compile a “transmission order” (time division multiple access, TDMA) for the nodes which joined their clusters. They inform each node at what time it is expected to send data to its CH.

CHs keeps listening for the results. Normal sensors get measures from their environment and send their data. When it is not their turn to send, they stay in sleep mode to save energy. Collisions between the transmissions of the nodes from different clusters are limited thanks to the use of code division multiple access (CDMA) protocol. CHs aggregate, and possibly compress the gathered data and send it to the BS in a single transmission. This transmission may be direct, or multi-hopped if relayed by other CHs.

Conclusion :

We have studied different attacks like black hole attack , gray hole attack , misdirection attack and DOS attack in WSN. We have proposed a common protocol for prevention of these attacks in WSN.

Refrences :

[1] Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network
Mohammad Wazid,Student Member, IEEE,Avita Katal, Student Member, IEEE,Roshan Singh Sachan, Student Member, IEEE,R H Goudar and D P Singh

[2] Performance Analysis of LEACH with Gray Hole Attack in Wireless Sensor Networks A.Pravin Renold, R.Poongothai, R.Parthasarathy TIFAC-CORE in Pervasive Computing Technologies Velammal Engineering College, Chennai, India

[3]Yi-ying ZHANG, Xiang-zhen LI, Yuan-an LIU, "The detection and defence of DOS attack for wireless sensor network" , Elsevier Journal of China Universities of Posts and Telecommunications, Volume 19, Supplement 2,October 2012,Pages 52-56.

[4] Shashikala , C. Kavitha, "A Survey on Secured Routing Protocols for Wireless Sensor Network", IEEE ICCCNT'12, Coimbatore, India,26-28th July 2012.

[5] Detecting DOS attacks in WSN based on Clustering Technique

D. Mansouri Laboratoire LSI USTHB, Algeria mansouri.dj@gmail.com

L. Mokdad Laboratoire LACL University of Paris-Est lynda.mokdad@u-pec.fr

[6] Jiwen Cai, Ping Yi, Jialin Chen, Zhiyang Wang, Ning Liu, "An Adaptive approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," aina,pp.775-780, 2010 24th IEEE International Conference on Advanced Information networking and Applications, 2010