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

pravinrenold.tifac@velammal.edu.in, poongothairajendran@gmail.com, partha_vimal@yahoo.com

***Abstract*— 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.**

***Keywords*— Gray hole attack, LEACH, Ns2, Wireless Sensor Networks.**

I. INTRODUCTION

The function of sensor network is gathering and sending back the information of the monitoring area which the relevant sensor nodes are set in. But the sensor network node resources are very limited, which mainly embodies in battery capacity, processing ability, storage capacity, communication bandwidth and so on. Because of the limited monitoring range and reliability of each sensor, we have to make the monitoring area of the sensor nodes overlapped when they are placed in order to enhance the robustness and accuracy of the information gathered by the entire network. In this case, certain redundancy in the gathered data will be inevitable. On the way of sending monitoring data by multi-hop relay to the sink nodes (or base stations) which are responsible to gather the data. It is necessary to reduce the redundant information by data fusion [1]. The application of Wireless Sensor Network includes habitat monitoring, surveillance, military applications, monitoring environmental conditions etc. The nodes deployed in sensor networks are classified as source and sink nodes. The source node monitors the physical environment and if any event happens it generates data packet and forwards to sink node. The sink nodes process the collected data from source nodes and forward it to the base station for further analysis and decision making. The communication among source and sink nodes are achieved with the help of transceivers by IEEE 802.15.4 protocol [2] which is designed specifically for short range communications and is supported by most academic and commercial sensor nodes.

A. Threats to sensor network

The WSN deployed in hostile environment where human monitoring of the network is not always possible can be easily compromised. Node compromise is the most detrimental attacks in WSN [3].

The attacks can be classified as active, passive, external and internal.

Active: The attacker exploits the weak link in the security protocol to launch attacks like packet modification, replaying etc.

Passive: The attacker obtains access to information without being detected. It is a kind of attack which is difficult to detect.

External: The attacker is external and has no rights to access the network.

Internal: The attacker gets authorization to access the network, the attacker deploys malicious node to compromise the sensor nodes and takes control of the network.

II. THE ROUTING PROTOCOL LEACH

The routing protocol plays a main role in transmitting the data from source by forming a route to the destination via intermediate nodes and also helps for the effective usage of the power of the nodes when not in the mode of transmission. The LEACH [4] (Low Energy Adaptive Clustering Hierarchy) protocol is a type of hierarchical routing protocol.

Working Methodology:

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

978-1-4577-1583-9/ 12/ $26.00 © 2012 IEEE

reduce the amount of information that must be transmitted to the base station.

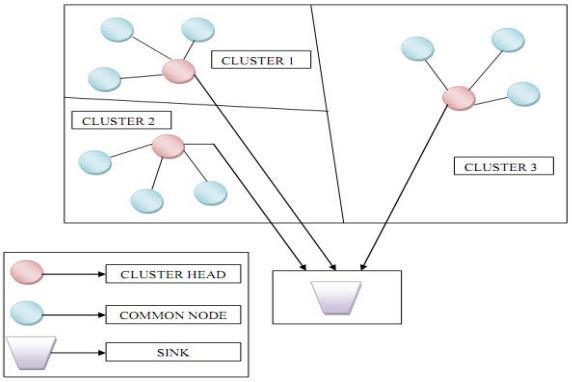

Fig 1. LEACH's work mode for data transfer

LEACH uses a TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. After a given interval of time, a randomized rotation of the role of the CH is conducted so that uniform energy dissipation in the sensor network is obtained.

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:

$$T(n)=\frac{p}{(1-p(r \bmod(1/p))} \quad \text{if } n \in G$$

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

Each elected CH broadcast an advertisement message to the rest of the nodes in the network that they are the new cluster-heads. All the non-cluster head nodes, after receiving this advertisement, decide on the cluster to which they want to belong to. This decision is based on the signal strength of the advertisement. The non cluster-head nodes inform the appropriate cluster-heads that they will be a member of the cluster. After receiving all the messages from the nodes that would like to be included in the cluster and based on the number of nodes in the cluster, the cluster-head node creates a TDMA schedule and assigns each node a time slot when it can transmit. This schedule is broadcast to all the nodes in the cluster

The cluster-head node, after receiving all the data, aggregates it before sending it to the base-station. After a certain time, which is determined a priori, the network goes back into the setup phase again and enters another round of selecting new CH. Each cluster communicates using different CDMA codes to reduce interference from nodes belonging to other clusters.

III. 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 (SN_i threshold > SN_{i-1} threshold)
Set SN_i is CH
Else
SN_{i-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 T_a
Else
Go to idle mode

IV. SIMULATION RESULTS

In this section the work made on comparing the performance of LEACH routing protocol with and without gray hole attack been discussed.

The number of sensor nodes Mica2 [6], chosen is 20 in a network of size 100m X 100m and the sensor nodes were deployed in a random fashion. Initially the simulation was done without gray hole attack. After that we made two nodes to be compromised, in our scenario the nodes named 6 and 7 were made to behave as gray hole attacked malicious node.

The compromised nodes take part in the communication at the initial stage, after some time it starts to drop the received packets purposely.

The Fig 2 shows the nodes are communicating among themselves and the Fig 3, shows data transfer between nodes.

TABLE I
SIMULATION PARAMETERS

Terrain	100m X 100m
Simulation time	100 seconds
No of common nodes	20
Application layer traffic	CBR
Item to send	500
Item size	70 bytes
Start time	1 sec
End time	0 sec
Routing Protocol	LEACH
MAC	IEEE 802.15.4
Energy model	Mica2
Antenna	OmniAntenna
Radio Propagation	Two Ray Ground

Fig 2. Nodes in the network are in communication

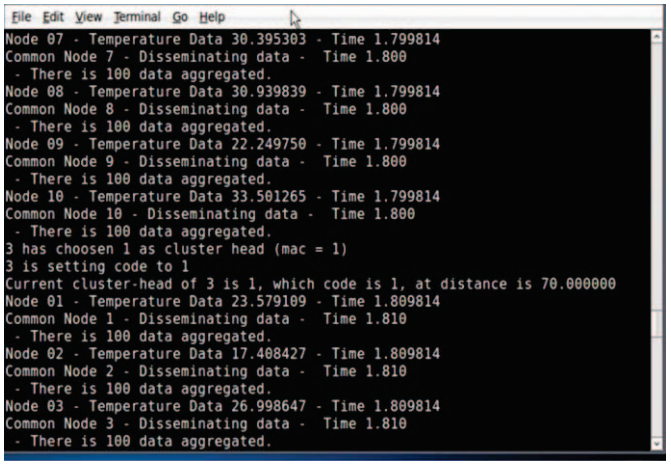

Fig 3. Data transfer between nodes

A. *Performance Analysis*

The metrics, packet delivery ratio, throughput and average end-to-end delay are used to determine the performance of LEACH with and without gray hole attack.

B. *Packet Delivery Ratio*

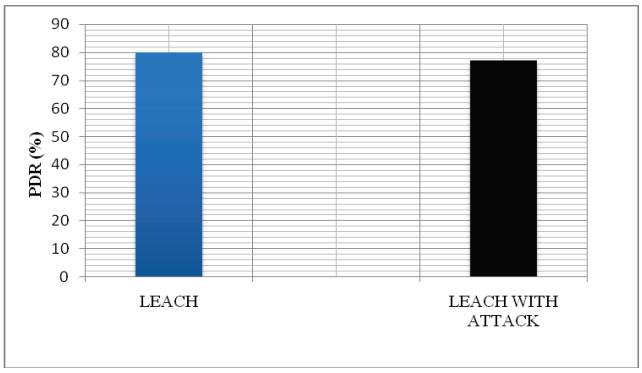

Fig 4. Packet Delivery Ratio analysis

The packet delivery ratio is defined as the ratio of number of packets received by the destination to that of the generated packets. The Fig. 4 shows the results obtained in comparing the working of LEACH in a network with and without gray hole attack. It shows that the inclusion of attack results in PDR drop which shows a reduction from 80% to 77%.

C. *Throughput*

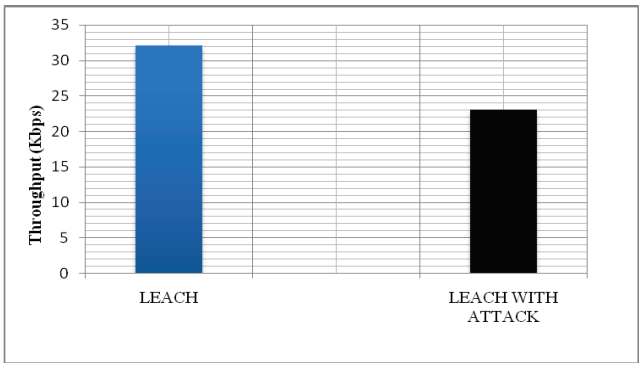

Fig 5. Throughput analysis

Throughput is defined as the number of bits transmitted per unit second over a communication channel. The Fig. 5 shows the results obtained in comparing LEACH with and without gray hole attack. While comparing the results with respect to throughput the LEACH protocol without attack gives 32.06 kbps and the value dropped to 23.11 kbps with gray hole attack.

D. *Average End-to-End Delay*

End-to-End delay is calculated by considering the time taken by a packet to be transmitted from source to destination in the network. The Fig. 6 shows the result obtained in the case of LEACH with and without gray hole attack. Due to presence of gray hole attack the delay had been increased from 4.69ms to 5.17ms.

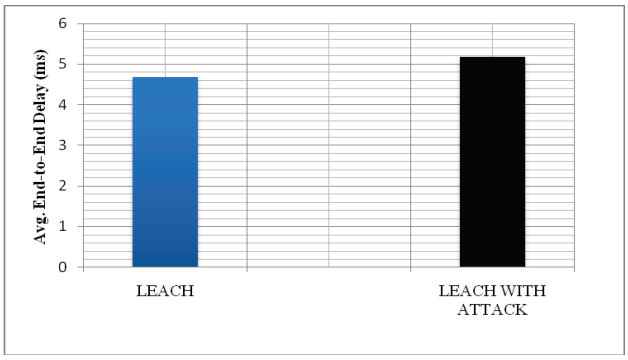

Fig 6. Average End-to-End Delay analysis

V. CONCLUSION

In this paper the performance evaluation of LEACH routing protocol for WSN with and without gray hole attack has been performed. Apart from the case of throughput the impact of the attack is not that huge in PDR and average end-to-end delay, it is due to the fact that the cluster head plays a major role in compressing and forwarding data to the sink. Also the cluster head changes dynamically for every specific period of time, results in low change.

As part of future work, we planned to evaluate the performance of LEACH routing protocol against various active and passive type of attacks.

REFERENCES

[1] Junguo Zhang; Wenbin Li; Xueliang Zhao; Xiaodong Bai; Chen Chen; , "Simulation and Research on Data Fusion Algorithm of the Wireless Sensor Network Based on NS2," *Computer Science and Information Engineering, 2009 WRI World Congress on* , vol.7, no., pp.66-70, March 31 2009-April 2 2009

[2] Gutierrez, J.A., Naeve,M., Callaway, E., Bourgeois, M., Mitter, V., and Heile, B," IEEE 802.15.4: A developing standard for low-power low-cost wireless personal area networks," in etwork,IEEE,2001,p.12.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Applications (SNPA'03), May 2003.

[4] Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H.;, "Energy-efficient communication protocol for wireless microsensor networks," System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on , vol., no., pp. 10 pp. vol.2, 4-7 Jan. 2000

[5] 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

[6] http://blog.memsic.com/mica2_mote/(URL)