COMPARISON OF DIFFERENT ATTACKS ON LEACH PROTOCOL IN WSN

[1]SIDDIQ IQBAL, [2]ARAVIND SRINIVAS S P, [3]SUDARSHAN G, [4]SAGAR S KASHYAP

[1]Assistant professor, Dept. of Telecommunication, B.M.S. Institute of Technology, Bangalore
[2,3,4]Dept. of Telecommunication, B.M.S. Institute of Technology, Bangalore
E-mail: [1]siddiq@bmsit.in, [2]arvind.srinivas92@gmail.com, [3]Sudz2s@gmail.com, [4]sagarismers@gmail.com

Abstract- Wireless sensor networks consists of large number of small, low cost and energy dependent sensors which are deployed to monitor many physical parameters such as temperature, pressure, vibration, motion etc. Several protocols are employed in WSN in order to reduce the amount of energy consumed. One such protocol is the hierarchical protocol called LEACH. The nature of LEACH protocol is prone to attacks. In this paper comparison of two such attacks namely Blackhole and Sinkhole on the LEACH protocol is performed and the simulated results are shown.

Keywords- WSN, LEACH, Sinkhole attack, Blackhole attack, Residual energy.

I. INTRODUCTION

Wireless sensor networks are a rapidly growing technology where the deployed sensors form a network by connecting to each other. These sensors are normally grouped into clusters to reduce the energy consumed, the control overhead and increase sharing of resources. One such popular protocol is Low Energy Adaptive Clustering Hierarchy (LEACH). This is a hierarchical protocol which reduces the amount of energy consumed by formation of clusters where aggregation or fusion of data takes place at the clusters and data is finally transmitted to the base station. A distributed algorithm is used to form the clusters since the nodes make decision without any centralized algorithm or control. A node chooses a random value between 0 and 1 if it wants to be the cluster head and the threshold value is given by

$$T(n) = \begin{cases} p/1-p(r \bmod 1/p) & n \in G \\ 0 & \text{otherwise} \end{cases}$$

If the random value chosen is less than the threshold value it then becomes a cluster head for the current round and advertises by sending a broadcast message to the rest of the nodes to join its cluster. Depending on either the distance or the signal strength the nodes join the clusters.

II. LEACH PROTOCOL

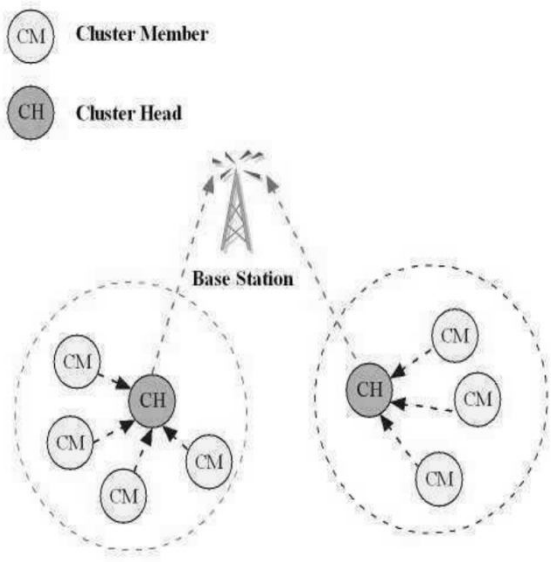

Figure 1: Illustration of LEACH protocol

LEACH has mainly 2 Phases:

1) Setup phase
2) Steady phase

Setup phase is divided into:

- Advertisement phase
- Cluster Set up phase

In the advertisement phase the cluster heads send an advertisement packet to the non-cluster heads. In the cluster setup phase non cluster heads choose the cluster head whose packet has the highest signal strength [4]. In this phase the cluster head selection is random and dynamically new clusters are formed. Each node here independently decides which cluster it should belong to. For a node to become the cluster head the decision is taken based on when the node was last a cluster head.

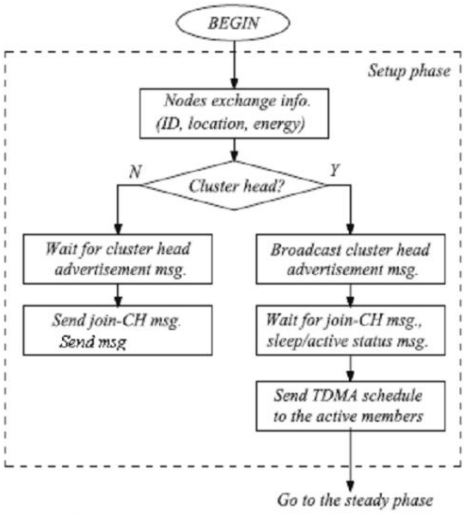

Figure 2: *Flowchart for setup phase in LEACH protocol*

Steady phase is divided into

- Schedule creation
- Data transmission

In schedule creation sensor nodes are allocated the time slots and frames are created. The sensor nodes transmit their data in each round to their respective cluster heads during their TDMA slot. These cluster heads aggregate the data and transmit it to the base station.

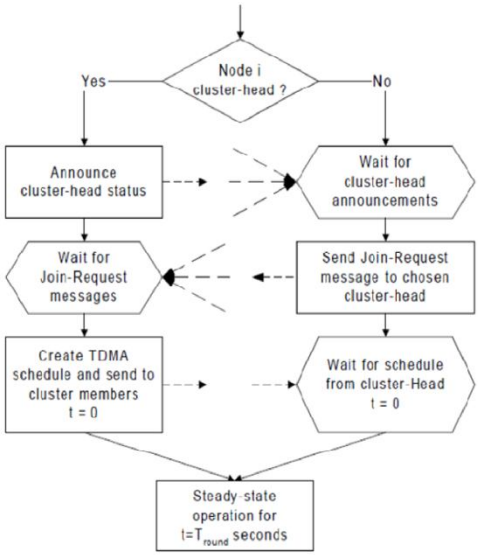

Figure 3: *Flowchart of steady phase in LEACH protocol*

LEACH protocol has many drawbacks:

1) The setup phase is non deterministic and there maybe collisions in this phase.
2) Large energy consumption if the distance between the cluster heads and the base station is large [6].
3) LEACH protocol is applicable only to small regions.
4) LEACH uses dynamic clustering and does not provide good cluster head distribution.

Due to these drawbacks LEACH protocol is susceptible to many attacks and the simulation results of two of such attacks are considered.

III. ATTACKS ON LEACH PROTOCOL

A. Blackhole attack:

In this type of attack the attacking node is having more initial energy than the other nodes and hence it becomes one of the cluster heads in the first round and even in later rounds, as it is not consuming any energy for data transmission. Hence it becomes cluster head in almost all the rounds [1]. After becoming cluster head it receives data from all of its cluster members, aggregate it and later does not forward the data to the base station and thereby reducing the amount of total data transmitted.

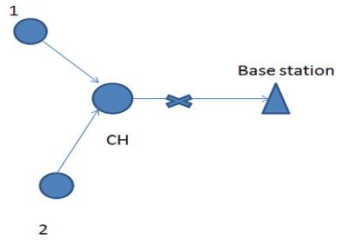

Figure 4: *Blackhole attack*

B. Sinkhole attack:

In Sinkhole attack the attacker attracts all the traffic in the area with the help of a compromised node. This compromised node broadcasts high amount of energy in order to attract the nodes [2]. This node collects all the data and in turn might lead to either dropping of packets, modifying the data or partial transmission. This attack can result in cluster failure [3].

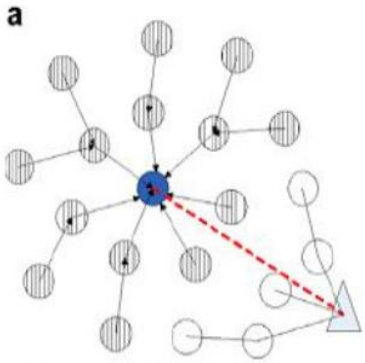

Figure 5: *Sinkhole attack*

To perform simulation of attacks on the protocol the algorithm is as follows:

Step 1: Initialize the malicious node and its parameters.
Step 2: The clusters are formed as in the basic LEACH protocol.
Step 3: Check if any of the nodes are malicious nodes If yes, then perform the attack.
Step 4: Update the energy values accordingly.

IV. SIMULATION

The simulation results shown were generated using MATLAB software. The parameter settings are as shown below in table 1.

Table 1: Simulation parameters

Parameter	Value
Network area	100m X 100m
Number of rounds	3000
Number of nodes	100
Packet size	4000
Initial energy	0.5 J
Data aggregation energy	5 X 10^-9 J
Transmission/reception energy	50 X 10^-9 J
Amplification energy	0.0013 X 10^-12 J
Energy of free space signal	10 X 10^-12 J
Sink position	(50m,50m)

To simulate the Blackhole attack, the parameters shown in table 1 are considered. Here, 10 of the 100 nodes are assumed to be compromised. These nodes do not transmit the data that they receive and hence affects the throughput of the network. To simulate the sinkhole environment a single node is assumed to be compromised at the (25m, 25m) position in the network. This node broadcasts larger amount of energy than the other nodes so that it can become the cluster head. This increases its probability to attract more number of nodes. The data received by this node is not transmitted further and hence results in poor performance of the network.

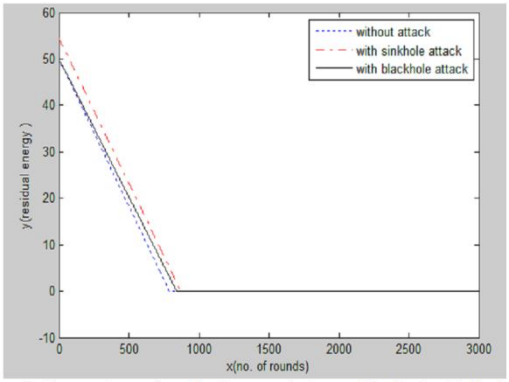

Figure 6: *Comparison of residual energy between Blackhole, Sinkhole and LEACH without attack*

Figure 6 shows the comparison of the residual energy in the networks with attacks and network without attack. As seen in the graph, the network with sinkhole attack will be left with more residual energy compared to the other two mentioned. In sinkhole attack, the compromised node broadcasts higher energy and hence the residual energy of the network is more. In blackhole attack, the compromised nodes do not transmit the received data packets and hence will be left with more energy. The network without any attack will be left with the least residual energy.

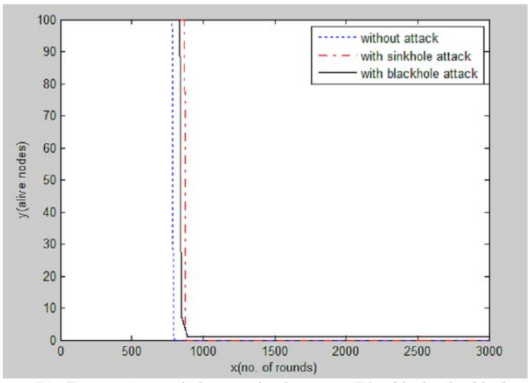

Figure 7: *Comparison of alive nodes between Blackhole, Sinkhole and LEACH without attack*

Figure 7 shows the comparison of alive nodes. This parameter is dependent on the residual energy factor. At any given point of time, more the residual energy, more the number of alive nodes. As explained earlier in figure 6, the residual energy in network with sinkhole attack is more than the one with blackhole attack and without any attack. Due to this, the network with sinkhole attack will have more number of alive nodes compared to the one with blackhole attack and the one without any attacks.

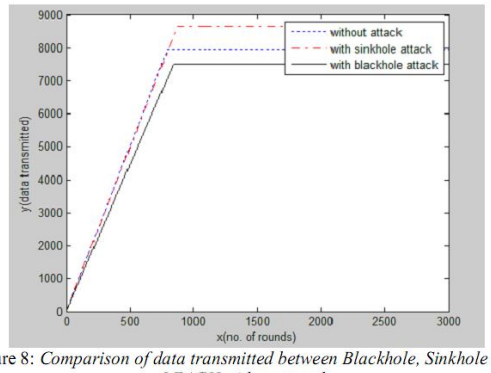

Figure 8: *Comparison of data transmitted between Blackhole, Sinkhole and LEACH without attack*

Figure 8 shows the comparison of data transmitted in the networks. In an uncompromised network, the data transmitted is higher compared to the compromised networks. The data transmitted during the sinkhole attack is lesser than in the network without attack i.e. during the active period of the network and this is shown in figure 9 which is the enlarged version of figure 8. As the number of rounds progresses the

network without the attack dies due to lack of energy and the network with the attack continues to operate for a longer duration and hence transmits data for a longer period of time. In blackhole attack, since the compromised nodes do not transmit data, the overall data transmitted to the base station is less.

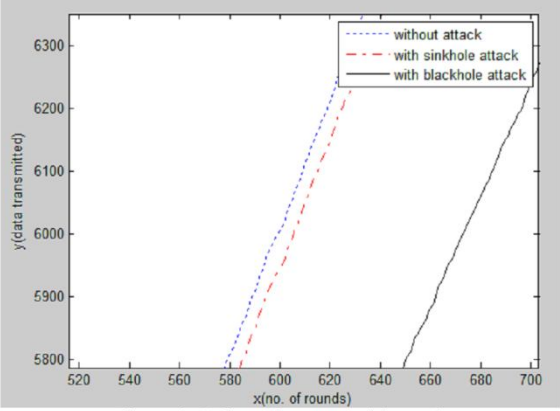

Figure 9: *Enlarged version of figure 8*

CONCLUSION

The goal of sinkhole attack is to attract all the data in a particular area with the help of the compromised node and the goal of the blackhole attack is to collect as much data possible by the malicious nodes and later drop them. Hence in this paper we are providing the simulation results for the effect of sinkhole attack and blackhole attack in the network. There is a reduction in the data transmitted in the network with the blackhole and sinkhole attack than in the network without attacks. Also, the residual energy left is higher in the attacked network due to less data being transmitted which is an effect of malicious nodes. Due to this more energy the total number of nodes which are alive will be more in the network with these attacks than in the ones without attacks. Hence with the help of simulation it is shown that both sinkhole and blackhole attacks will result in huge packet drops and the malicious nodes can affect the data. It can also be seen that a sinkhole attack is more deleterious than blackhole attack.

FUTURE WORK

For simulation purpose 10 nodes are considered as malicious for blackhole attack and one node is considered as the sinkhole node. For further simulation purposes the number of malicious nodes can be increased.

REFERENCES

[1] Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN by Meenakshi Tripathi,M.S.Gaur,V.Laxmi Malaviya National Institute of Technology, Jaipur, India 2013 published by Elsevier B.V.

[2] A Recent Technique to Detect Sinkhole Attacks in WSN D. Sheela, Nirmala. S, Sangita Nath and Dr. G Mahadevan 2013

[3] Dealing with Sinkhole Attacks in Wireless Sensor Networks Junaid Ahsenali Chaudhry, Usman Tariq, Mohammed Arif Amin, Robert G. Rittenhouse Advanced Science and Technology Letters Vol.29 (SecTech 2013), pp.7-12

[4] Leach and Its Descendant Protocols: A SurveyJ.Gnanambigai, Dr.N.Rengarajan, K.Anbukkarasi International Journal of Communication and Computer Technologies Volume 01 – No.3, Issue: 02 September 2012 ISSN NUMBER: 2278-9723

[5] Prevention of Cooperative Black Hole Attackin Wireless Ad Hoc Networks Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard 2012, Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105

[6] An Energy Balanced Clustering Algorithm Based on LEACH Protocol Qian Liao, Hao Zhu 2nd International Conference 2012 on Systems Engineering and Modeling

[7] A Review of Routing Protocols in Wireless Sensor Network Prabhat Kumar, M.P.Singh and U.S.Triar National Institute of Technology Patna, Bihar, India International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 4, June - 2012 ISSN: 2278-0181

★★★