RESEARCH ARTICLE OPEN ACCESS

Effect of Blackhole Attack on Single Hop and Multihop Leach Protocol

Siddiq Iqbal, Aravind Srinivas S P, Sudarshan G, Sagar S Kashyap
IEEE student member Assistant professor, Dept. of Telecommunication, B.M.S. Institute of Technology, Bangalore
Dept. of Telecommunication B.M.S. Institute of Technology, Bangalore
Dept. of Telecommunication B.M.S. Institute of Technology, Bangalore
Dept. of Telecommunication B.M.S. Institute of Technology, Bangalore

Abstract
Wireless micro sensor networks provide reliable monitoring of remote areas for data-gathering. Due to the limited battery capacity of sensor nodes, energy consumption plays an important role in the operation of WSN. This can be improved by using a protocol called Low energy adaptive clustering hierarchy (LEACH).Malicious attacks are generated in the network due to power supply, processing abilities and capacity for high power radio transmission. In this paper one such attack namely BlackHole attack and its effect on single hop LEACH and multihop LEACH has been compared, simulated and analyzed.

Index terms-WSN, LEACH, Blackhole, Multi hop, Residual Energy.

I. INTRODUCTION

Wireless sensor networks consists of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants at different locations. It combines sensing computation and communication into a single tiny device [7].

LEACH is an application specific hierarchical protocol formed to reduce power consumption which involves data aggregation or fusion and subsequent transmission to base station[3]. All non-cluster-head nodes must transmit their data to the cluster-head, while the cluster- head node must receive data from all the cluster members, perform signal processing functions on the data (e.g., data aggregation), and transmit data to the remote base station.

II. LEACH PROTOCOL

LEACH has two phases 1) Setup phase
2) Steady phase

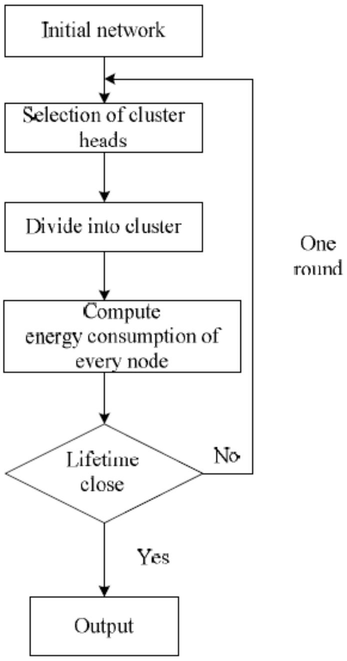

Figure 1: Flowchart of LEACH

Set-Up Phase: Cluster is constructed by Cluster Head election. Each node decides independent of other nodes if it will become a Cluster Head or not[6]. This decision takes into account when the node served as a Cluster Head for the last time. Its main functions are

- organizing the network into clusters
- Advertisements of the cluster heads
- Transmission schedule creation

Steady phase: Steady phase is further divided into 2 parts:

- Schedule Creation
- Data Transmission

In the steady working stage, each member node of the cluster send data to the corresponding cluster head during the allotted communication slot. After receiving all the data, the cluster head aggregate it and sends to the sink. In order to minimize the power consumption, the steady phase duration is kept far greater than the cluster constructing phase duration.

Due to dynamic topology, limited resources and open nature of wireless medium it makes it easier for the outsiders to attack and interfere with the network[5]. Hence LEACH protocol is prone to several attacks. One of such attack is blackhole attack.

III. BLACKHOLE ATTACK ON MULTI-HOP LEACH PROTOCOL

A. *Multi hop LEACH*

When the network diameter is increased, the distance between the base station and the cluster head increases. Hence the leach routing protocol is not helpful. Thus, in order to increase the energy efficiency multi-hop communication within the cluster is done. The communication between the cluster head and the sink is done via multiple hops by choosing an optimal path

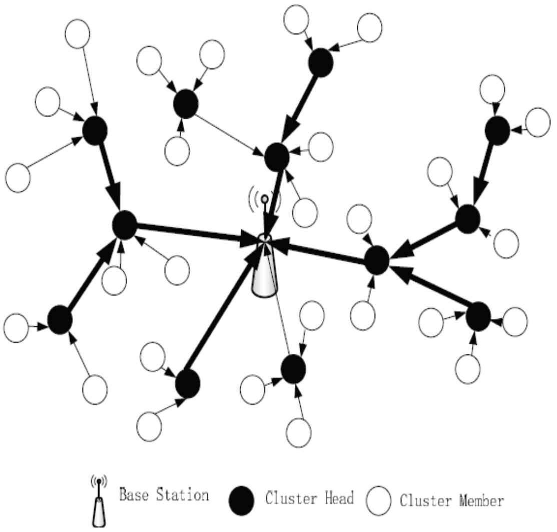

Figure 2: Multi hop LEACH

B. *Multihop Algorithm*

In the multihop LEACH network, each node does 2 types of transmission [2]. One is to send the data collected by it to its local cluster head. The other is to forward the data to other nodes as part of the multihop transmission if it is part of the routing path of any other node. The multihop routing path used here is a static route calculated based on the least distance factor. The routing path for any node can be determined by using the following algorithm:

Step 1: the node whose route needs to be determined is considered to be the source node.
Step 2: The nodes which fall in the transmission range of this source node are shortlisted.
Step 3: Among these nodes, the node which has the shortest distance from the base station is considered as the next hop of the source node.
Step 4: This next hop node is then considered as the source node and steps 2 and 3 are repeated to find out the subsequent next-hops.
Step 5: The above step is repeated until the base station node is part of the shortlisted nodes i.e. it falls in the transmission range of a next-hop node.
Step 6: All the next-hop nodes are stored in an array for later use.

C. *Blackhole attack:*

This is a type of DOS attack where the attacker collects the data and then later drops it. Since attacker is having higher initial energy than the other nodes 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 [1].Hence it becomes cluster head in almost all the rounds. 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 [4].

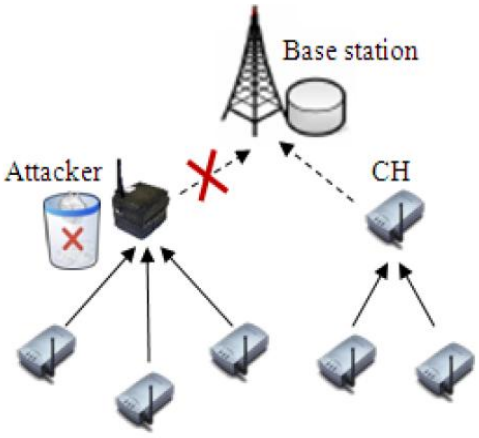

Figure 3: blackhole attack

IV. SIMULATION

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

To simulate the Blackhole attack, the parameters shown in table 1 are considered. Here, 5 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.

Table 1: Simulation parameters

Parameter	**Value**
Network area	200m X 200m
Number of rounds	2500
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	(100m,100m)

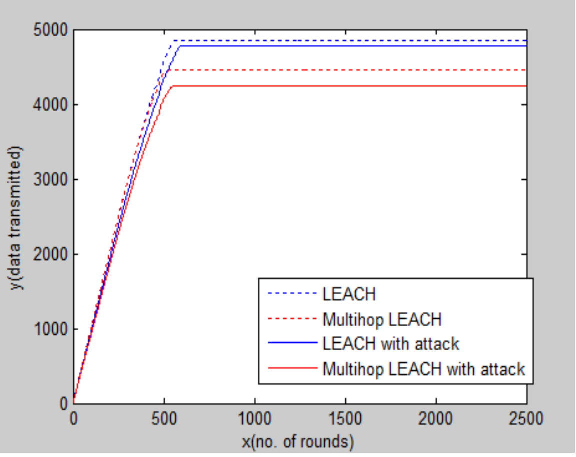

Figure4: Graph of data transmitted in single hop and multi hop LEACH during the event of Blackhole attack.

As seen from the figure 4 above the data transmitted during the single hop LEACH without attack is maximum. In multihop LEACH without attack the data transmitted is significantly less due to the higher energy consumption during multiple hops from the cluster head to the base station. In the event of a Blackhole attack, the effect of the attack on multi-hop LEACH is maximum resulting in least data being transmitted to the base station. In case of Blackhole attack on single hop LEACH the data transmitted is lesser than the basic LEACH but still higher than multi-hop LEACH without attack. In the operation of LEACH the data before being transmitted to the base station is aggregated at the cluster head and then transmitted as a single packet. Due to this the difference in data transmitted in all the above cases in the figure is minute.

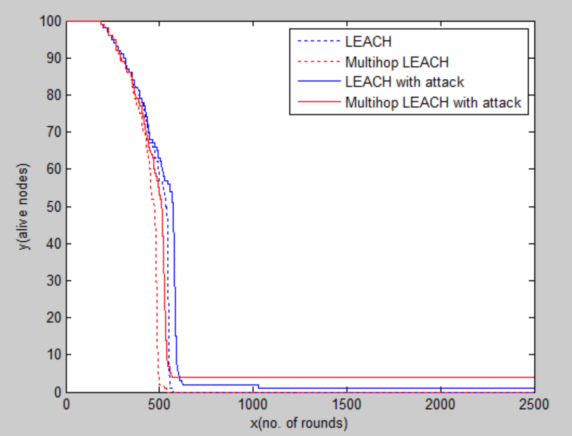

Figure 5: Graph of alive nodes in single hop and multi hop LEACH in the event of Blackhole attack.

In case of Blackhole attack the energy consumption is less since the packets are not transmitted to the base station. This, results in the nodes staying alive for a longer duration. From the figure 5 it is evident that the single hop LEACH with the attack has nodes which are alive for a longer duration than the single hop LEACH without attack. In case of multi-hop LEACH with attack the nodes stay alive for a longer duration than multi-hop LEACH without attack but lesser than the single hop without attack. This is because the energy consumption during multiple hops in the network is more. In single hop LEACH the compromised node affects itself and its cluster members. In multi hop LEACH since the compromised node can be a part of the multi hop path it can affect other clusters as well. Hence energy consumption is more in multi hop LEACH

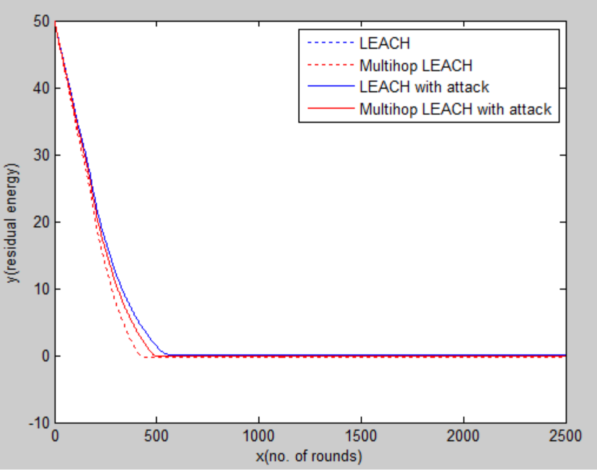

Figure 6: Graph of residual energy in single hop and multi hop LEACH during the event of Blackhole attack.

It is evident from the figure 6 that the residual energy of the single hop LEACH with attack is maximum since the energy consumption is less and the packets are not transmitted to the base station. The multi-hop LEACH with Blackhole attack has more residual energy than the LEACH protocols without attack and lesser than single hop LEACH with attack due to multiple hops. The residual energy of the LEACH protocols without attack is similar.

V. CONCLUSION

The goal of the blackhole attack is to collect as much data possible by the malicious nodes and later drop them. In this paper we are providing simulation results for data transmitted, number of alive nodes and residual energy by comparing single hop LEACH, multi hop LEACH and the effect of Blackhole attack on them. The data transmitted is least in the multi hop LEACH network affected by Blackhole attack and maximum in the network of single hop LEACH without attack. The nodes are alive for a longest duration in single hop LEACH with attack. The residual energy is highest in the single hop LEACH with attack. Hence, the impact of Blackhole attack is more on multi hop LEACH network than a single hop LEACH network.

REFERENCES

[1] Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami, 978-1-4799-0462-4/13/$31.00 ©2013 IEEE.

[2] Improvement on LEACH Protocol of Wireless Sensor Network, Fan Xiangning, Song Yulin, 0-7695-2988-7/07 $25.00 © 2007 IEEE.

[3] Performance Evaluation of LEACH Protocol in Wireless Network, M. Shankar, Dr .M. Sridar, Dr. M. Rajani, International Journal of Scientific & Engineering Research, Volume 3, Issue 1, January-2012 1 ISSN 2229-5518.

[4] 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.

[5] Leach and Its Descendant Protocols: A Survey J. 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.

[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 Networks 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