Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN

Padmalaya Nayak
Department of IT,
GRIET, Hyderabad

V. Bhavani
Department of IT,
GRIET, Hyderabad

B. Lavanya
Department of IT,
GRIET, Hyderabad

ABSTRACT
With the drastic growth of Internet and VLSI design, applications of WSNs are increasing tremendously that ranges from environmental monitoring, habitat monitoring, traffic surveillance to battle fields. In WSN a number of tiny sensor nodes managed by small batteries are deployed in a hostile environment to monitor the physical parameters. During transmission, the sensor nodes consume considerable amount of energy. There are many constraints on these sensor nodes such as limited memory, limited battery power, and limited processing capability. Moreover, these factors impose a restricted lifetime for the entire network. When sensor nodes send the information to the base station (BS), routing protocol plays the key role to deliver the information at the destination. Low Energy Adaptive Clustering Hierarchy (LEACH) and LEACH-C is the well-known distributed and centralized clustering routing protocol respectively. In LEACH, the cluster head (CH) is elected on a probabilistic threshold value on a rotation basis and only CHs are allowed to send the information to the BS. LEACH-C is the modified version of LEACH and works on the centralized principle. Further, WSNs are vulnerable to many types of attacks, as WSNs are normally deployed in a harsh environment. So, security is one of the major challenging issues that need to be focused. Many researchers have addressed these issues on LEACH protocol as LEACH is the first ever cluster based routing protocol. As far as our knowledge is concerned, there is a lack of research in the current literature by considering both LEACH and LEACH-C protocol under some attacks. So, we have made an attempt to analyze the performance of both the protocols under some well-known attacks like black hole and sink hole attacks. Again, we plan to propose a detection mechanism which is in progress.

Keywords
LEACH, LEACH-C, Black hole, Sink hole, NetSim Simulator

1. INTRODUCTION
Wireless sensor network (WSN) consists of hundreds or thousands of sensor nodes deployed in a particular geographical area for monitoring the environment. Each sensor node is equipped with transducer, microcomputer, transceiver, and battery power. The main function of transducer is to generate the electrical signal and it is processed by the microcomputer and is stored in the output of the sensor node. The monitored parameters ranges from humidity, temperature, pressure, wind direction, power line voltage etc. Even if the tiny sensor node is capable of sensing, processing and computing, it is limited with battery power. Further WSN are deployed in a hazardous environment where replacement of battery is nearly impossible. So there are many different issues like routing, fusion and localization are to be focused.

Routing is the main challenging issue in WSN. A number of routing protocols have been proposed [7] [8] for WSN to address these issues. The routing protocols are divided into flat and hierarchical based on the network structure. As huge numbers of sensor nodes are used, it is difficult to assign the identity to each node in flat routing. Therefore there is a need of data centric routing protocol, where BS gets data from a group of nodes. Clustering comes under hierarchical routing protocol where nodes are organized into clusters based on some metrics. For each cluster a leader is elected known as cluster head. The CH collects all the data from nodes, aggregates the data and sends the compressed date to the BS. This helps to avoid data redundancy, contention for accessing the channel, and increased network lifetime.

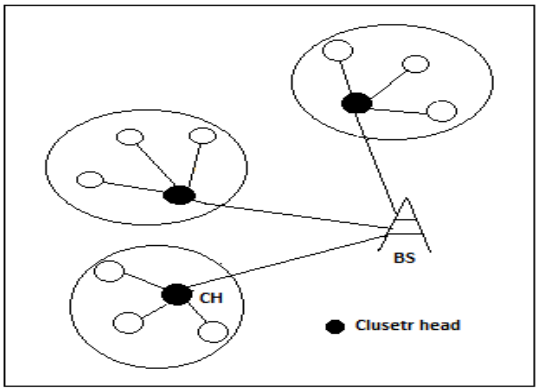

Fig. 1: General system model for clustered WSN.

Clustering has taken its own place to analyze the performance of WSN. Low Energy Adaptive Clustering Hierarchy (LEACH) [1] [2] is first ever distributed clustering protocol. In LEACH, the energy is evenly distributed among all the sensor nodes. The CH is elected based on pre-defined threshold value. At starting of each round, nodes having residual energy higher than the threshold value are elected as CHs. LEACH maximizes the network life time and reduces the energy dissipation by compressing the data forwarded to BS. The main disadvantage of LEACH is, as CH is elected randomly among the number of nodes, a node with less residual energy may be elected as a CH in several rounds. Therefore the node with less residual energy may die first.

LEACH-C [2] is an improved version of LEACH protocol that uses a centralized algorithm at BS for electing the CH. All nodes send their residual energy and distance information to BS prior to CH election. The BS elects the node with high residual energy as CH. Even if LEACH and LEACH-C work well in normal condition, these protocols perform poorly under some malicious nodes as WSNs are always vulnerable to attacks. These attacks might be inside the network or outside the network. In this paper, we have focused on two

network layer attacks such as black hole and sink hole attack on LEACH and LEACH-C protocols.

The rest of the paper is organized as follows. Section 2 describes the related work. Section 3 provides an overview of black hole and sink hole attacks. Section 4 speaks about our experimental set-up and simulation results have been given in Section 5 followed by a concluding remark in Section 6.

2. RELATED WORK

WSN is always vulnerable to many types of attacks because normally WSNs are deployed in an unattended environment [9] [10]. Lot of research is going on to analyze the effects of attacks on different routing algorithms/protocols. In one hand, many studies show the impact of attack and on the other hand some studies show the detection and prevention mechanisms for it. In [3], the author mentioned various possible attacks like Sybil attack, HELLO FLOOD attack, Black Hole and Gray Hole attack in LEACH. The author has analyzed the effect of black hole and grey hole attacks on LEACH protocol in [4]. Our aim is to analyze the effect of black hole and sink hole attacks on both LEACH and LEACH-C protocols and analyze the performance using Netsim Simulator.

3. OVERVIEW OF BLACK HOLE AND SINK HOLE ATTACKS

WSNs are considered as a special category of ad hoc networks and infrastructure less, and run without human attendance. Therefore they are prone to many type attacks such as jamming, worm hole, sink hole, black hole and Sybil attack. But, here we have focused only on black hole and sink hole attack. So, other attacks are not discussed in this paper.

3.1 Black Hole Attack

In black hole attack [5], compromised node tries to attract all the traffic from its surrounding nodes. The compromised node generates false routing information to neighboring nodes. This diverts all the traffic to the malicious node. Here, the malicious node advertises that it has high residual energy. By advertising this, malicious node becomes CH at each round. All the nodes send packets to the malicious node as it acts as a CH. The malicious node drops all packets and does not forward to BS. In summary, Black hole attack consists of two steps, attracting step and invading step. In attracting step the nodes attract other nodes by sending false information and in invading step the node invades the communication process and drops the packet.

Fig. 2 shows the example of WSN, where malicious node captures all the packets and instead of forwarding the packets, it drops the packets.

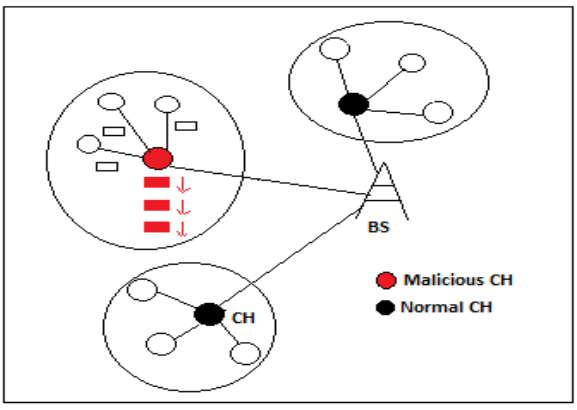

Fig. 2: Black hole attack

3.2 Sink Hole Attack

Sink hole attack [6] uses the same principle with little deviation, where malicious node advertises that it has high residual energy to increase its chances to be CH. Once malicious node becomes CH, it collects the packets and drops the packets selectively instead of dropping all the packets. Fig. 3 shows the example of WSNs under sink hole attack. In our simulations, either at every 1ms or after every fourth packet transfer, the malicious node drops the packets.

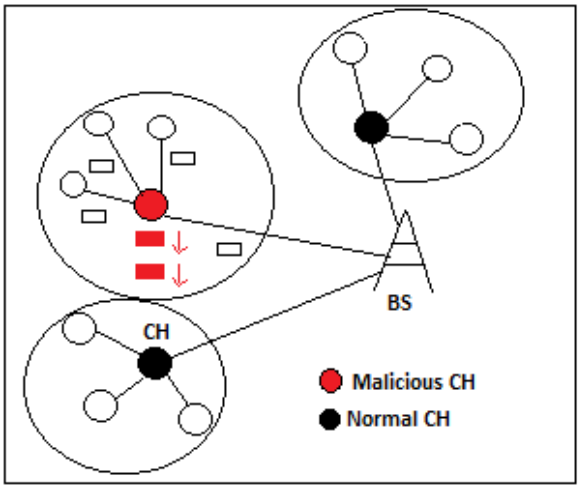

Fig. 3: Sink hole attack

4. EXPERIMENTAL SETUP

To analyze the performance of LEACH and LEACH-C protocol under black hole and sink hole attack, we have used NetSim Simulator Version 7. We have considered 100 nodes in a sensor field that are uniformly distributed between (x=0, y=0) and (x=50, y=50). The proposed WSN field is shown in Fig. 4. The BS is located at (x=22, y=23) in a 50m*50m field. The bandwidth of the channel is set to 1Mbs and message length is considered as 52 bytes long with the header length 8 bytes. For easy simulations, the parameters of interest have been provided in Table 1. In our simulations, we have considered 20 nodes in each cluster and we have taken maximum 5 clusters. Two malicious nodes have been considered to perform the black hole and sink hole attacks.

Table 1: Simulation Parameters

Simulation area	50*50
No. of Nodes	100
Channel Type	Wireless channel
Simulation time	100 seconds
Initial energy of node	1J
Nodes distribution	Uniformly distributed
Energy model	Battery
Communication channel	Bi-directional
Antenna Model	Omni directional antenna
Radio Propagation Model	Two way ground

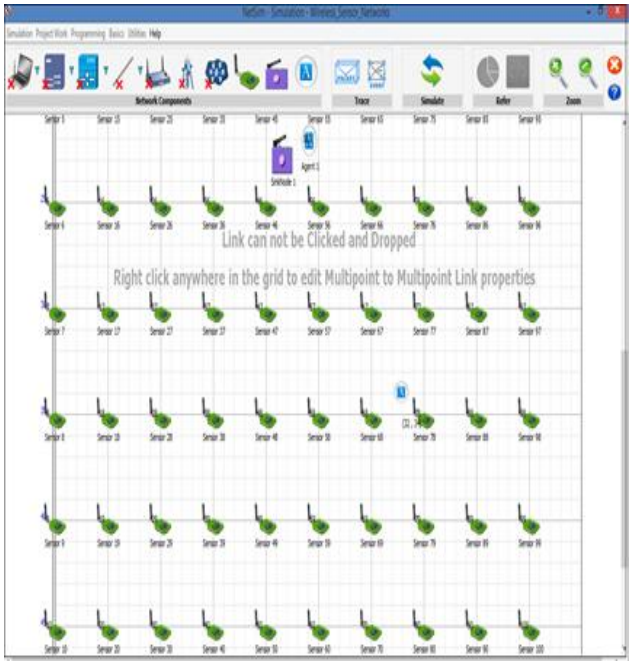

Fig. 4: WSN field consisting of 100 nodes

5. SIMULATION RESULTS AND ANALYSIS

In order to clearly analyze and understand the effect of black hole and sink hole attacks on LEACH and LEACH-C protocols, some parameters have been considered as the performance metrics that have been measured by NetSim Simulator. In case of sink hole attack, we have considered that packets are dropped either at every 1ms or every fourth packet transmitted from the source. Results obtained from the simulations based on our parameters of interest are plotted from Fig. 5 to Fig. 11 successively.

Performance Metrics

5.1 Number of Data Signals received at BS

We have compared number of data signals received at the BS as it is one of the major performance metrics to evaluate any routing protocol for WSN. It is clearly seen from the Fig. 5 that number of data signals received at BS is more in LEACH and LEACH-C without any attack. With sink hole attack, some packet drop will be there and even it is more in case of black hole attack.

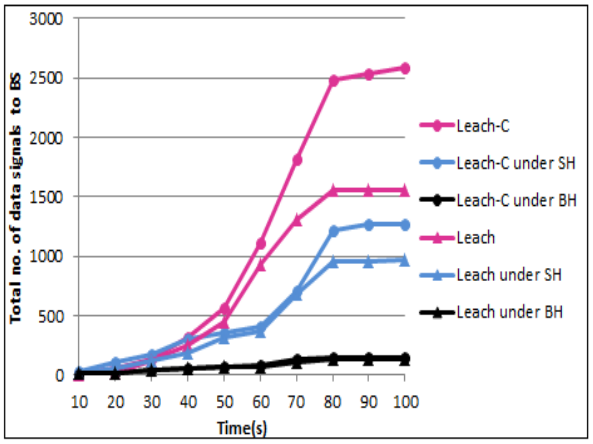

Fig. 5: No. of Data Signals v/s Time

5.2 Total Energy Consumption

It is seen from the Fig. 6 that total energy consumption is more in LEACH and LEACH-C without any attack. It decreases in case of sink hole attack and even decreases more in case of black hole attack. The reason is that each sensor node consumes some energy while transmitting the packets. As the packets processed are more, the energy consumption increases.

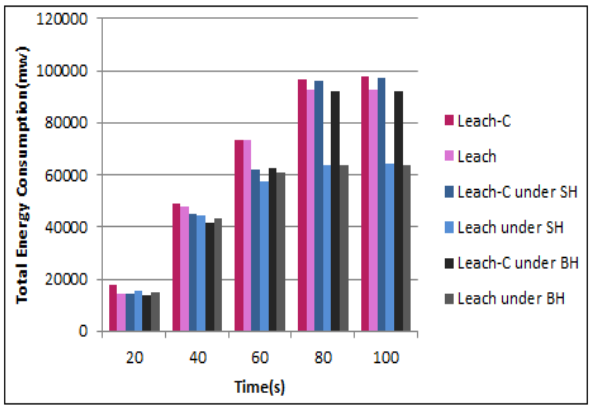

Fig. 6: Total Energy Consumed v/s Time

5.3 First Node Dies

From the simulation results it is concluded that first node dies first in case of black hole attack as the malicious node consumes more energy by dropping all the packets. Then, first node dies with the sink hole and it survives for longer period of time in LEACH without any attack. Similar in case of LEACH-C. It is seen from Fig. 7

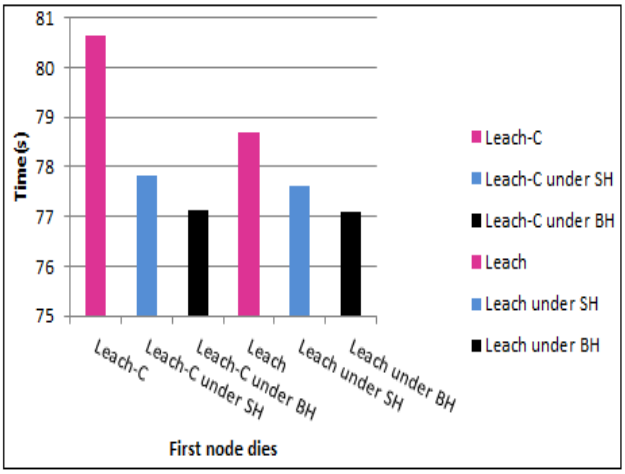

Fig. 7: First Node Dies v/s Time

5.4 Number of Packets Transmitted

From Fig. 8 it is seen that the number of packets transmitted in LEACH and LEACH-C is normal without any attack. Some packet loss occurs only due to the nature of wireless communication. When the malicious node acts as a black hole, it drops all the packets. When the malicious nodes act as the sink hole, it drops the packets selectively. So naturally, number of packets transmitted is more without attack, then it will come down in case of sink hole attack and finally, it will be less in case of black hole attack. It can be verified from Fig. 8.

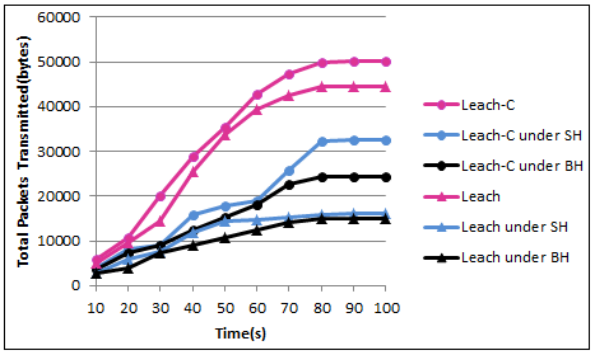

Fig. 8: Total Packets Transmitted v/s Time

5.5 Total Number of Nodes Alive

Fig. 9 shows that no. of alive nodes are less in case of black hole attacks and grows slowly with sink hole attack and even it is more under normal operating condition in LEACH and LEACH-C, because CHs acting as malicious nodes consume more energy than others by dropping the packets.

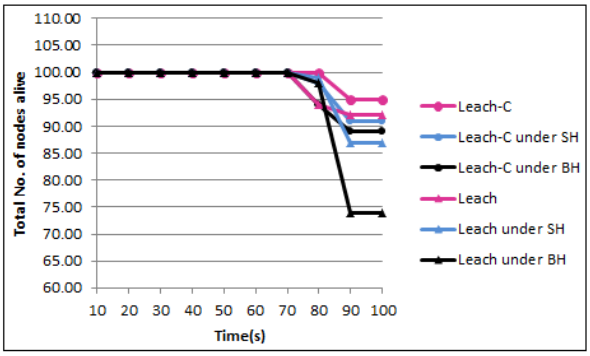

Fig. 9: Total no. of Alive Nodes v/s Time

5.6 Throughput

In LEACH and LEACH-C, the throughput is better in normal condition. Anyway, under attack packet loss is more resulting in decreased throughput. It can be verified from Fig 10, how the throughput getting effected by attack.

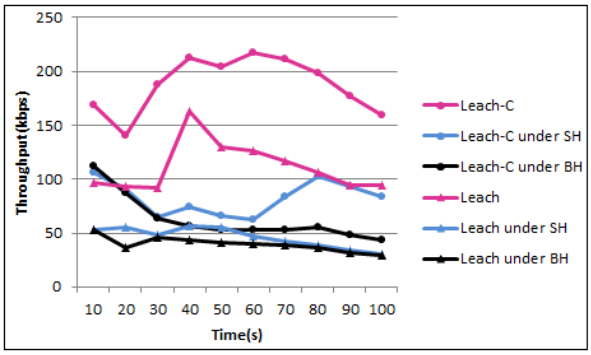

Fig. 10: Throughput v/s Time

5.7 Transmission Overhead

As seen in Fig. 8, the number of packets transmitted is more in LEACH and LEACH-C before attack. The more the number of packets will be transmitted, the more the transmission overhead will be there. When the number of packets transmitted reduces under sink hole and black hole attacks, the transmission overhead also will reduce simultaneously. It is seen from Fig. 11

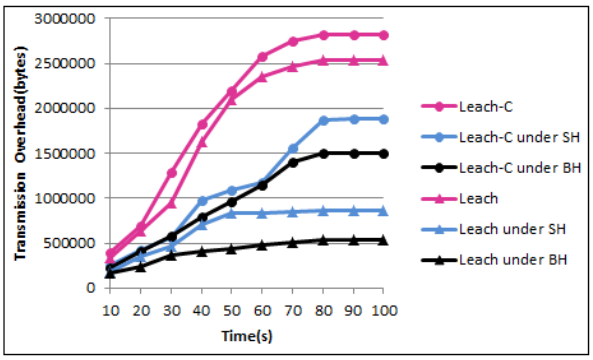

Fig. 11: Transmission Overhead v/s Time

6. CONCLUSION

In this paper, the performance of LEACH and LEACH-C protocols has been measured in presence of some malicious nodes. Particularly, we have measured the performance of WSN under black hole and sink hole attacks. In black hole attack, the malicious node acts like a cluster head and receives all the packets. But instead of forwarding the packets to the BS, it drops all the packets. The scenario is different in case of sink hole attack. The malicious node acts like a CH and receives all the packets from the neighbor nodes. What it does, instead of dropping all the packets, it creates its own tricks to forward or drop the packets. In our simulation, we have considered that the malicious node drops the packet either at each 1ms time interval or each fourth packet transmitting from the source node. Many parameters such as no. of data signals received at the BS, total energy consumption, routing overhead, throughput etc. to check the performance of LEACH-C and LEACH protocols. It has been concluded from the simulation results that LEACH and LEACH-C perform poorly in presence of black hole and sink hole attacks. Our future research will provide the information how to detect and prevent this type of attacks in Wireless Sensor Network.

7. REFERENCES

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy- Efficient communication Protocol for Wireless Sensor Networks,” Proceedings of the 33th Hawaii International Conference on System Sciences (HICSS), 2000.

[2] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan,“An application-specific protocol architecture for wireless microsensor networks,” in IEEE Transactions on Wireless Communications, Oct. 2002, pp. 660 – 670.

[3] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2-3, pp. 1293–1303, 2003.

[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] J. Luo, M. Fan, D. Ye, "Black hole attack prevention based on authentication mechanism," 11th IEEE Singapore International Conference on Communication Systems, 2008.ICCS 2008. pp. 173-177,Guangzhou, 19-21 Nov. 2008.

[6] Gagandeep, Aashim , "Study of sinkhole attacks in wireless Ad hoc networks", International journal on computer science and engineering, vol. 4, June 2011.

[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.

[8] S.K. Singh, M.P. Singh, and D.K. Singh, "A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[9] A.S.K. Pathan, H.W. Lee, C.S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Communications, IEEE Transaction, Feb 2006.

[10] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, vol. 4, 2009.