In WSN, Comparing the Effects of a Black Hole versus a Gray Hole Attack on LEACH

Kundan Kumar Pramanik, Assistant Professor

Department of Engineering & IT, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id- kundan.parmanik@arkajainuniversity.ac.in

ABSTRACT: The implementation of Wireless Sensor Networks (WSNs) in an unsupervised environment has resulted in a slew of security issues. This paper examines LEACH, the most widely used clustered routing protocol in WSNs, and how it may be hacked by Black Hole and Gray Hole attackers. To mimic these assaults on NS-2, the "high energy threshold" idea is utilized. The performance of a WSN under assault is extensively examined by putting it through its paces using a variety of network settings and node densities. It has been discovered that the Black Hole attack has a greater impact on network performance than the Gray Hole assault. WSNs are gaining popularity in a variety of fields, including military applications, environmental applications, smart homes, health monitoring, and so on. Any physical, mechanical, or chemical change in the environment is detected by the nodes of a WSN and sent to the base station, where the user may evaluate the findings. WSNs have a number of resource constraints, including memory, computing power, and battery life. Sensor nodes conduct substantial signal processing, calculation, and aggregation locally before sending the data to the base station, which reduces transmission and therefore energy costs. One of the most common routing protocols is cluster-based Low-Energy Adaptive Clustering Hierarchy (LEACH) , which equally distributes the energy burden across the different sensor nodes. All cluster members must submit data to the cluster head, which will aggregate and compress the data before sending it to the base station. All communication between nodes in WSNs is done wirelessly, and the nodes are so resource constrained that using security methods from other ad hoc networks is impossible. As a result, malicious nodes are more inclined to attack them. If the attacker becomes the cluster leader, the assault has a greater impact.

KEYWORDS: WSN, cluster, LEACH, Black Hole attack, Gray Hole attack, NS2

1. INTRODUCTION:

If the attacker becomes the cluster leader, the assault has a greater impact. In such situation, it may have an impact on the data of the whole cluster. Black Hole assault, Gray Hole attack, Sybil attack, Flooding attack, Wormhole attack, and other dangers have been proposed in theory for WSN. Existing cluster-based routing protocols such as LEACH, PEGASIS, and HEED lacked a security mechanism. In this article, we look at how a malicious node takes advantage of vulnerability[1].

Black Hole and Gray Hole attacks are possible using the LEACH protocol. We need to understand the behavior of these attacks in order to protect WSN against them. To do so, we thoroughly investigated and contrasted the behavior of these two assaults. We used Network Simulator 2 (NS-2) to do all of the simulations[2].

The first to describe the different vulnerabilities in WSN. In LEACH, they discuss several potential assaults such as the Sybil attack, the HELLO FLOOD attack, as well as the Black Hole and Gray Hole attacks. Many other studies have noted that the poor processing power of sensors, as well as their limited energy, is impediments to the implementation of security methods in WSNs, and that a rogue node may easily interrupt the regular routing process. Richa et al. proposed that intermediary nodes use routing packets to not only identify but also remove adversaries. To our knowledge, no prior study has investigated the impact of Black Hole and Gray Hole assaults on LEACH networks of various sizes.

LEACH Modification

We assume that the malicious node has more energy than the regular nodes in order to have the longest possible lifespan during network operation. We utilized Distributed Energy Efficient Clustering to ensure that nodes with high initial and residual energy had a higher probability of becoming cluster heads than nodes with low energy. As a result, the attacker has a better chance of becoming a cluster head, receiving more data, and having a greater impact on the network. There are two kinds of nodes in our network: attacker nodes and regular nodes. If E0 is the starting energy of normal nodes, then E0*(1+x) is the beginning energy of malevolent nodes. In this instance, the total energy of the network will be E = (N 1) E0 + E0 (1 + x). (1)

Choosing a Cluster-Head (Based On Residual Energy)

If in is the number of rounds in which node I may be a cluster head, then Pi=1/ni is the average chance of node I being a cluster head for in rounds. If Po pt is the best chance for a normal node to become a cluster head, then the attacker node's chance is: - Popt (1 + x) = Pmal (2) If Ei(r) is the energy of the ith node and Eavg(r) is the average energy in the network's round r, then Pi may be calculated as: - Pi = PoptEi(r) (1+a)Eavg Pi = PoptEi(r) (1+a)Eavg Pi = PoptEi(r) (1+a)Eavg Pi = PoptEi(r If I am a regular node,

Popt∗Ei(r)

If Eavg I f I is a malicious node, then Eavg I f I is a harmful node (3)

Eavg(r) = 1 n n 0 Ei Eavg(r) = 1 n n 0 Ei Eavg(r) = 1 n n 0 Ei Eavg(r) = 1 n n 0 Ei Eavg(r) = 1 (r) (4)

The values from Eq. (4) must be substituted into the following formula to determine the threshold:

- If in G 0 T(n) = Pi 1Pi(r mod 1 Pi) Otherwise \s(5)

It is apparent from this calculation that threshold is linked to each node's initial and residual energy[3].

As a result, the attacker with a high starting energy node will have a greater chance of becoming the cluster leader.

Attack on the Black Hole

In a Black Hole attack, the attacker attempts to gather the majority of the network's data before dropping it. We examined the situation when the intruder has a high starting energy relative to other regular nodes in our simulation. Cluster heads are chosen in LEACH depending on the residual energy of different nodes. Because the attacker has a greater starting energy, it becomes one of the cluster heads in the first round and even subsequent rounds, as data transmission consumes no energy. As a result, it becomes cluster head in nearly every round. It gets data from all of its cluster members after becoming cluster head, aggregates it, and then does not transmit the data to the base station[4].

Gray Hole Attack

In the Gray Hole attack, a malicious node first uses the LEACH protocol to promote itself as having a high chance of becoming a cluster head, with the goal of capturing packets. The node then drops the intercepted packets with a specific probability. A Gray Hole's malevolent activity may manifest itself in a variety of ways. It simply rejects packets from a particular node or nodes in the network while forwarding all packets to other nodes. Another kind of Gray Hole attack is when a node acts maliciously for a period of time by discarding packets, but then returns to normal behavior or only forwards packets with a certain packet ID. A Gray Hole may also show unpredictable behavior, dropping some packets while forwarding others, making identification even more challenging.

Modeling of Attacks

The Black Hole node discards all incoming packets, while the Gray Hole attack discards packets on a case-by-case basis. Algorithm 1 models the Black Hole and Gray Hole attacks on LEACH.

Require: V-Total nodes, Malicious ID of Malicious Node, BS Base Station CM stands for Cluster Member.

Ensure: PAHSE LURE

If ni == Mal, then Einit = E0 (1 + a) end if I V Mal, then Einit = E0 (1 + a) Calculate Pi and T (ni); if T (ni) T(ni1), CH = ni; else

if CH Broadcasts the Advertisement Messages, CH = ni1

The Cluster TRASH PHASE will be joined by the entire CM.

If CH == mal, then perform the attack; otherwise, CH generates a TDAM schedule and CM sends data to CH in a TDMA slot.

Model for Simulation

In order to simulate both attacks, we modified the LEACH protocol in NS-2 . We used an Intel Core 2 Duo PC with 2 GB RAM for all simulations and analyses. While simulating, we made the following assumptions: -

- BS has the most energy (theoretically infinite power).
- Malicious nodes have x times the amount of energy as normal nodes.
- The sensor nodes are all stationary.
- In every time frame, every node has data to transfer.

Our findings are based on a simulation of 200 sensor nodes forming a Wireless Sensor Network over a rectangular (100 100m) surface. As a MAC layer protocol, we utilized MAC-sensor. Malicious nodes are chosen at random from 0 to 1. The network densities were changed between 20, 50, 100, and 200. With a variable number of nodes in the initial topology, simulations were run in both attack and non-attack scenarios. The trace files were saved after each run, and then the performance was measured by analyzing the trace data. Figure 1 discloses Snapshot of Network Topology for Simulation[5].

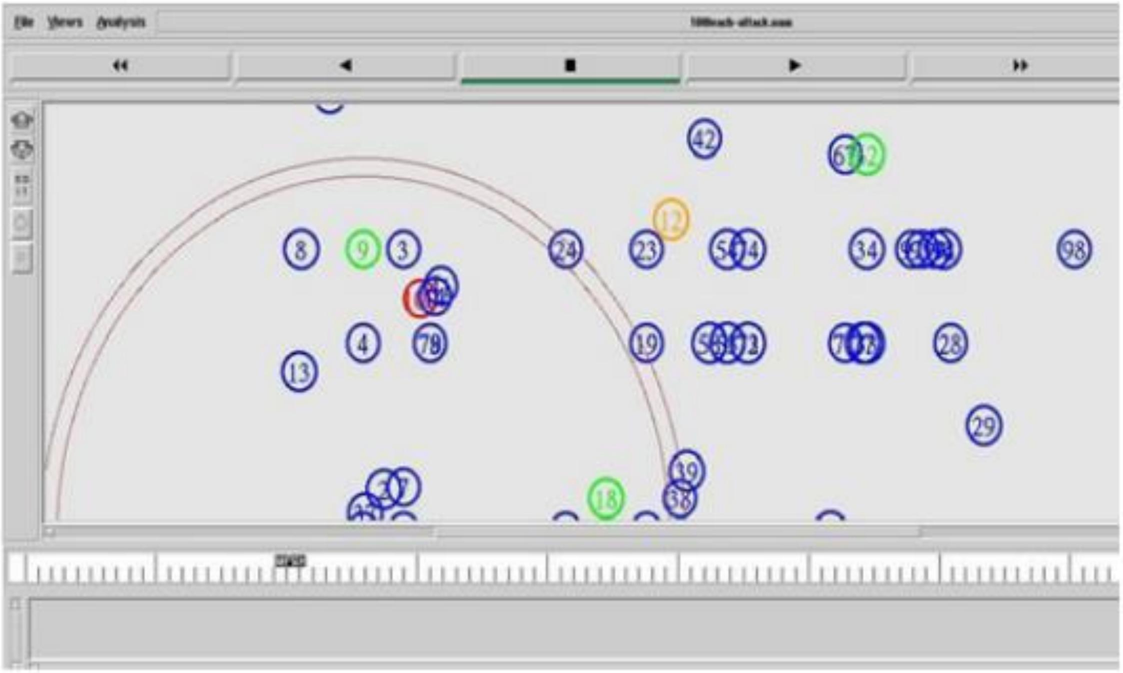

Figure 1: Snapshot of Network Topology for Simulation

2. DISCUSSION:

To get a clear knowledge and analysis of the assaults, we used the following techniques:

- Analyze typical LEACH using the given network settings.
- Use the same network settings to analyze LEACH using a Black Hole attack.
- Use the same network settings to analyze LEACH with a Gray Hole attack.
- Examining the effect on LEACH of Black Hole and Gray Hole assaults

The percentage of nodes that have not terminated their residual energy falls below a specific threshold, which is set according to the type of application, and the network lifetime begins with the first transmission in the wireless network and ends when the percentage of nodes that have not terminated their residual energy falls below a specific threshold, which is set according to the type of application (it can be either 100 percent or less)[6].

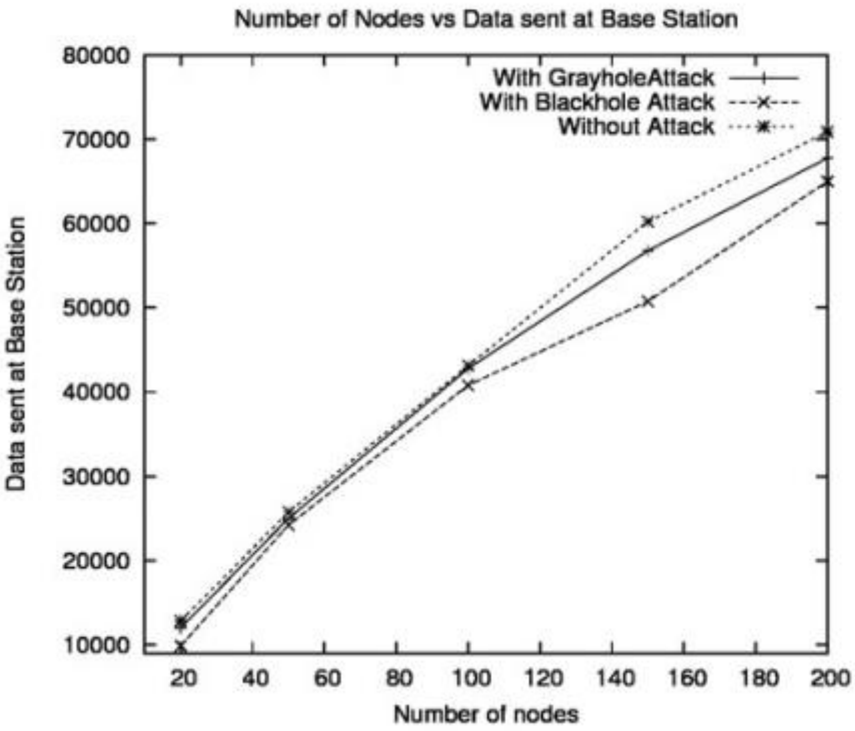

Figure 2: Simulation result in presence of Black Hole and Gray Hole attack

Extended Energy

The total amount of energy used by all nodes to send data to the base station. It is the total amount of energy used in creating clusters, transmitting data to cluster members, and finally delivering data to the base station.

LEACH in a Normal Scenario Performance Analysis

To begin, we ran simulations without any attacking nodes and with different node densities. We simulated LEACH in the second phase using Black Hole and Gray Hole nodes with different node densities.

Black Hole LEACH Performance Analysis

Normal nodes are represented by blue circles, cluster heads by green circles, and malevolent nodes by red circles. When there is no malicious node in the network, the base station gets a good quantity of packets, as shown in Figure 2 for LEACH in the absence of malicious node and in the presence of malicious node, subject to prediction accuracy restrictions. It has been found that when a malicious node is present in the network, the amount of data packets reaching the base station decreases because the malicious node drops all packets in its cluster. The effect of the Black Hole assault on the network lifespan is shown in Figure 3. As a result of the Black Hole effect, the network lifespan rises as compared to when there is no Black Hole attack. We change the number of nodes and see what happens. Figure 4 shows that the attack has a little effect on overall network energy consumption. This is due to the fact that, although the attacker is not transmitting data to the base station, it is still engaging in all other network activity, which uses energy[7].

Gray Hole Performance Analysis LEACH

In the absence of Gray Hole, the base station gets a good quantity of packets, and the results are LEACH in the absence of malicious nodes and in the presence of malicious nodes. It has been found that when a malicious node is present in the network, the amount of data packets reaching the base station decreases because the malicious node drops all packets in its cluster. The effect of the Gray Hole attack on the network lifespan. As a result of the Gray Hole effect, the network lifespan rises as compared to when the Gray Hole attack is not there. We change the number of nodes and see what happens show that the attack has a little effect on overall network energy consumption. This is due to the fact that, although the attacker is not transmitting data to the base station, it is still engaging in all other network activity, which uses energy[8]

The packets received at the base station in the presence of these two assaults are significantly impacted. When the impact of a Black Hole attack is compared to that of a Gray Hole attack, the packets received at the base station decreases more than the Gray Hole attack. From the preceding As can be seen, network lifetime increases in the presence of Black Hole nodes compared to Gray Hole attacks. In addition, the Gray Holes attack in LEACH resulted in an excessive number of packet drops. However, when the impact of a Black Hole attack is compared to the impact of a Gray Hole attack, the Black Hole attack causes significantly more packet drops than the Gray Hole attack. In a Gray Hole attack, the attacker spends some time transmitting packets to the base station, consuming energy. In a Black Hole attack, the attacker spends less time transmitting packets to the base station, consuming energy[9].

3. CONCLUSION:

BS is considered to be a trustworthy entity in WSN. It is capable of keeping track of the numerous CHs in multiple rounds. If a node appears in the CH set by the BS repeatedly, it may indicate nefarious behavior. BS may maintain track of nodes in the CH set as well as data transmitted by them for an observed time as part of detection. The BS blacklists a CH node for a certain amount of time if it appears frequently and does not transmit data for a set length of time. We demonstrated via simulation that both attacks result in massive packet losses. Experiments were also carried out on networks of various sizes. We find that the attack's impact grows in proportion to the size of the network. The number of nodes in a cluster grows as the network grows. The malicious node has the ability to influence the data of other nodes. We discovered that the Gray Hole assault has a lower impact than the Black Hole attack. We've also discussed a method for detecting these assaults. We want to develop and simulate the detection method on these lines in the future. Figure 2 discloses the Simulation result in presence of Black Hole and Gray Hole attack[10].

REFERENCE:

[1] D. Bak, M. Gutperle, and R. A. Janik, "Janus black holes," *J. High Energy Phys.*, 2011.

[2] I. D. Soares, "A boosted Kerr black hole solution and the structure of a general astrophysical black hole," *Gen. Relativ. Gravit.*, 2017.

[3] G. Ruppeiner, "Thermodynamic black holes," *Entropy*, 2018.

[4] Z. Xu, X. Hou, and J. Wang, "Possibility of identifying matter around rotating black hole with black hole shadow," *J. Cosmol. Astropart. Phys.*, 2018.

[5] N. Dadhich, J. M. Pons, and K. Prabhu, "On the static Lovelock black holes," *Gen. Relativ. Gravit.*, 2013.

[6] J. van Dongen and S. de Haro, "On black hole complementarity," *Stud. Hist. Philos. Sci. Part B - Stud. Hist. Philos. Mod. Phys.*, 2004.

[7] R. Emparan, P. Figueras, and M. Martínez, "Bumpy black holes," *J. High Energy Phys.*, 2014.

[8] H. C. Kim, J. W. Lee, and J. Lee, "Black hole as an information eraser," *Mod. Phys. Lett. A*, 2010.

[9] A. B. Nielsen, "Black holes and black hole thermodynamics without event horizons," *Gen. Relativ. Gravit.*, 2009.

[10] Y. F. Yuan, "Black hole binaries in the universe," *Scientia Sinica: Physica, Mechanica et Astronomica*. 2017.