Available online at www.sciencedirect.com

SciVerse ScienceDirect

ELSEVIER

Procedia Computer Science 19 (2013) 1101 – 1107

Procedia
Computer Science

The 8th International Symposium on Intelligent Systems Techniques for
Ad Hoc and Wireless Sensor Networks (IST-AWSN)

Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN

Meenakshi Tripathi,M.S.Gaur,V.Laxmi

Malaviya National Institute of Technology, Jaipur, India

Abstract

The deployment of Wireless Sensor Networks (WSN) in unattended environment has led to various security threats. This paper provides an overview of LEACH, the most popular clustered routing protocol of WSN and how LEACH can be compromised by Black hole and Gray Hole attacker. ”High energy threshold” concept is used to simulate these attacks on NS-2. The performance of WSN under attack is thoroughly investigated, by applying it on various network parameters with various node densities. It is observed that the effect of the Black Hole attack is more on the network performance as compared to the Gray Hole attack.

Selection and peer-review under responsibility of Elhadi M. Shakshuki

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

1. Introduction

Wireless Sensor Networks (WSN) are becoming popular these days in various areas like [1, 2] military applications, environmental application, smart homes, health monitoring etc. The nodes of a WSN sense any physical, mechanical or chemical change in the environment and send it to the base station where the user can analyze the results. WSNs have various limitations on resources like memory,processing power and battery power. One way to reduce the communication and consequently energy costs is that sensor nodes perform significant signal processing, computation and aggregation [2, 3] locally before forwarding the data to the base station.

Cluster based Low-Energy Adaptive Clustering Hierarchy (LEACH) [4] is one of the most popular routing protocol which disperses the energy load evenly among the various sensor nodes. All the members of the clusters have to transmit the data to cluster head only, which aggregate and compress the data and send it to the base station. In WSNs all the communication between the nodes is happening wirelessly and the nodes are so much resource constraint that it is difficult to employ any security solutions of other ad hoc networks. So they are likely to be attacked by malicious nodes. The effect of attack is more if the attacker becomes the cluster head. In that case it can affect the data of the whole cluster attached to it. Various threats [3] have been described in theory for WSN like Black Hole attack, Gray Hole attack, Sybil attack, Flooding attack,wormhole attack [5] etc. Existing cluster based routing protocols LEACH [4], PEGASIS [6], HEED [7] failed to provide any security mechanism. In this paper, we discuss how a malicious node exploits

1877-0509 © 2013 The Authors. Published by Elsevier B.V.
Selection and peer-review under responsibility of Elhadi M. Shakshuki
doi:10.1016/j.procs.2013.06.155

LEACH protocol and yields Black Hole and Gray Hole attacks. To secure WSN against these kinds of attack, we must have to understand the behavior of these attacks. In order to achieve this, we explored and compared the behavior of these two attacks in detail. We have done all the simulations using Network Simulator 2(NS-2) [8, 9].

2. Related Work

Karlof et al [3] was the first one to describe the various the vulnerabilities in WSN. They mention various possible attacks like Sybil attack, HELLO FLOOD attack along with Black Hole and Gray Hole attack in LEACH. Many Other researchers [10, 11] have also stated that the low computing power of sensors and especially their limited energy are obstacles to the deployment of security techniques in WSN and hence malicious node can easily disrupt the normal routing process. Richa et. al. [12] have not only suggested the detection but also the removal of adverseries by intermediate node through routing packets. To the best of our knowledge, none of the previous works have studied the effect of Black Hole and Gray Hole attacks in network of different sizes in LEACH.

3. Modification in LEACH

We consider that the malicious node is having higher energy as compared to the normal nodes to have maximum lifetime during network operation. We have used the Distributed Energy Efficient Clustering [13], so that nodes with high initial and residual energy will have more chances to be a cluster head than the nodes with low energy nodes. This way the attacker will have more chances to become a cluster head, gets more data and can affect the network more. In our network two types of nodes are there: attacker nodes and normal nodes. Suppose E_0 is the initial energy of the normal nodes than the energy of malicious node is considered as E_0*(1+x). Thus the total energy of the network in this case will be :-

$$E = (N - 1) * E_0 + E_0 * (1 + x) \tag{1}$$

3.1. Cluster-head selection (Based on residual energy)

Let n_i denote the number of rounds to be a cluster head for node i then P_i= 1/ n_i will be average probability for node i to be a cluster head during ni rounds. If P_opt be the optimal probability for a normal node to become a cluster head than probability for attacker node would be:-

$$P_{mal} = \frac{P_{opt}}{(1 + x)} \tag{2}$$

If $E_i(r)$ denotes the energy of ith node and $E_{avg}(r)$ denotes the average energy in the round r of the network, than P_i can be obtained as:-

$$P_i = \begin{cases} \frac{P_{opt}*E_i(r)}{(1+a)*E_{avg}} & If\ I\ is\ normal\ node \\ \frac{P_{opt}*E_i(r)}{E_{avg}} & If\ I\ is\ malicious\ node \end{cases} \tag{3}$$

And $E_{avg}(r)$ can be calculated as :-

$$E_{avg}(r) = \frac{1}{n} * \sum_{0}^{n} E_i(r) \tag{4}$$

To calculate the threshold we have to substitute the values from Eq. (4) to the following formula :-

$$T(n) = \begin{cases} \frac{P_i}{1-P_i*(r\ mod \frac{1}{P_i})} & if\ n_i \epsilon G \\ 0 & Otherwise \end{cases} \tag{5}$$

From this formula it is clear that threshold is correlated with the initial and residual energy of each node. Hence the attacker which is a high initial energy node will have higher probability to become a cluster head.

3.2. Black Hole Attack

In Black Hole attack [3, 14] the attacker tries to collect most of the data of the network and later drops it. In our simulation we considered the case in which the intruder has high initial energy as compared to other normal nodes. In LEACH cluster heads are being selected based on the residual energy of various nodes. Since attacker is having higher initial energy so 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. After becoming cluster head it receives data from all of its cluster members, aggregate it and later on do not forward the data to the base station.

3.3. Gray Hole Attack

In Gray Hole attack [3, 15],initially, a malicious node exploits the LEACH protocol to advertise itself as having a high probability to become a cluster head, with the intention of intercepting packets, next, the node drops the intercepted packets with a certain probability. A Gray Hole may exhibit its malicious behavior in multiple ways. It simply drops packets coming from certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later or it may packets of certain packet ID and forward the other packets. A Gray Hole may also exhibit a random behavior also in which it drops some of the packets randomly while forwarding other packets, thereby making its detection even more difficult.

4. Attack Modeling

Black Hole node drops all the received packets coming to it, while Gray Hole attack drops packets selectively. Our algorithm for Black Hole and Gray Hole attack on LEACH is described in Algorithm 1.

Algorithm 1 Model Black Hole and Gray Hole Attack

```
Require: $Mal - ID\ of\ Malicious\ Node, BS - Base\ Station,$
V-Total nodes CM- Cluster Memeber
Ensure: LURE PAHSE
  $E_{init} = E_0, \forall i \in V - Mal$
  if $n_i == Mal$ then
      $E_{init} = E_0 * (1 + a)$
  end if
  $\forall i \in V$ Compute $P_i\ and\ T(n_i)$
  if $T(n_i) \geq T(n_{i-1})$ then
      $CH = n_i$
  else
      $CH = n_{i-1}$
  end if
  CH Broadcast the Advertisement Messages
  All the CM will Join the Cluster
  TRASH PHASE
  CH generates TDAM schedule
  CM sends data to CH in TDMA slot
  if $CH == mal$ then
      Perform the Attack
  else
      Sends aggregated data to BS
  end if
```

5. Simulation Model

We have modified the LEACH protocol in NS-2 [10, 11] in order to simulate both the attacks. For all the simulation and analysis we have used Intel Core 2 Duo PC with 2 GB RAM. These are our assumptions while simulation:-

- BS is having highest energy (theoretically infinite power).
- Malicious node is having x times more energy than the normal nodes.
- All the sensor nodes are static.
- Every node has data to transfer in every time frame.

Our results are based on the simulation of 200 sensor nodes that forms Wireless Sensor Network over a rectangular ($100 * 100m$). We have used MAC-sensor as MAC layer protocol. We randomly select 0 to 1 nodes as malicious nodes. We have varied the network densities from 20, 50,100 and 200. While having different number of nodes in initial topology the simulation was done in both the cases i.e. with attack and without attack. After each run the trace files were saved and finally, the analysis of trace file was done to measure the performance.

6. Simulation results

We have implemented the following techniques to get a clear understanding and analysis of the attacks:

- Analyze normal LEACH under various network parameters as above
- Analyze LEACH with Black Hole attack under same network parameters
- Analyze LEACH with Gray Hole attack under same network parameters
- Comparing the impact of Black Hole and Gray Hole attacks on LEACH

6.1. Performance Metrics

6.2. Network Lifetime

Network lifetime can be defined as the interval of time, started with the first transmission in the wireless network, ending 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% or less).

6.3. Data sent at Base Station

Total amount of data received at the base station during the network lifetime.

6.4. Extended Energy

Amount of energy consumed by all the nodes in transmitting the data to the base station. It is the sum of energy consumed in setting clusters, sending data to respective cluster members and then in sending data to base station.

6.5. Performance Analysis for LEACH in Normal Scenario

Firstly, we have done our simulations without any attacking nodes with varying node densities. In second step, we have simulated LEACH with Black Hole and Gray Hole nodes with varying node densities.

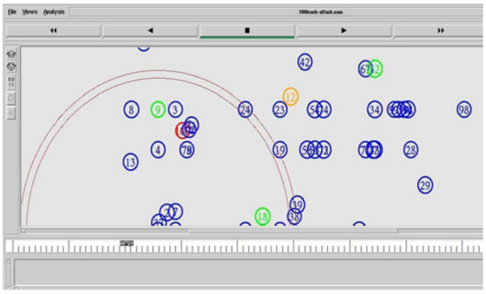

Fig. 1. Snapshot of Network Topology for simulation

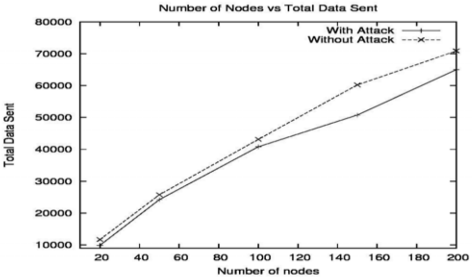

Fig. 2. Effect of Blackhole on Data sent to BS

6.6. *Performance Analysis for Black Hole LEACH*

Figure 1 shows one snapshot of network topology used for the simulation. Blue circle is representing normal nodes, green is for cluster heads and red circle represents the malicious node. When no malicious node is there in the network, base station receives good amount of packets and the results are presented in Figure 2 for LEACH, in the absence of malicious node and in the presence of malicious node, subject to the constraints of prediction accuracy. It is observed that in case of malicious node in the network number of data packets reached to base station reduces since the malicious node is dropping all the packets of its cluster. Figure 3 shows the impact of the Black Hole attack to the networks lifetime. The network lifetime also increases due to Black Hole effect as compared to that without the effect of Black Hole attack. We vary the number of the nodes and take the results. From Figure 4 it is observed that impact of the attack is not huge in case of total energy consumed in the network, it is due to the fact that although the attacker is not sending the data to the base station but still it is participating in all other activities in the network, which consumes energy.

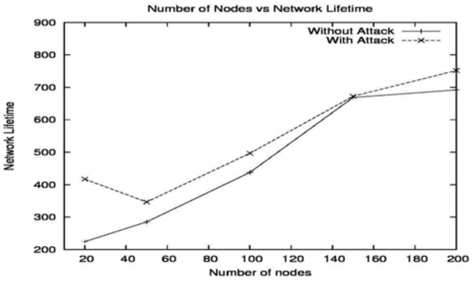

Fig. 3. Number of nodes Vs network lifetime (Black Hole attack)

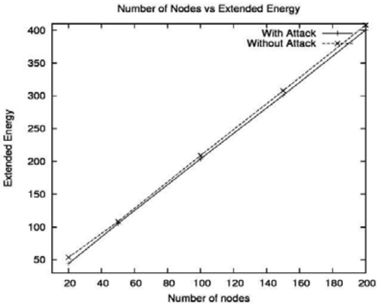

Fig. 4. Number of nodes Vs extended energy (Black Hole attack)

6.7. *Performance Analysis for Gray Hole LEACH*

In the absence of Gray Hole base station receives good amount of packets and the results are presented for LEACH in the absence of malicious node and in the presence of malicious nodes are shown in Fig. 5. It is observed that in case of malicious node in the network number of data packets reached to base station reduces since the malicious node is dropping all the packets of its cluster. Figure 6 shows the impact of the Gray Hole attack to the networks lifetime. The network lifetime also increases due to Gray Hole effect as compared to that without the effect of Gray Hole attack. We vary the number of the nodes and take the results. From Figure 7 it is observed that impact of the attack is not huge in case of total energy consumed in the network, it is due to the fact that although the attacker is not sending the data to the base station but still it is participating in all other activities in the network, which consumes energy.

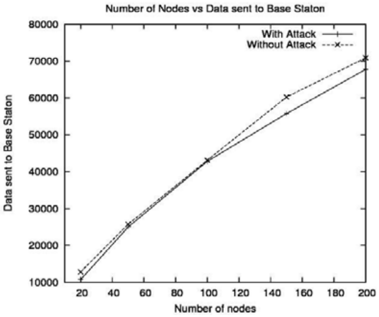

Fig. 5. Number of nodes Vs Total data sent to the base station (Gray Hole attack)

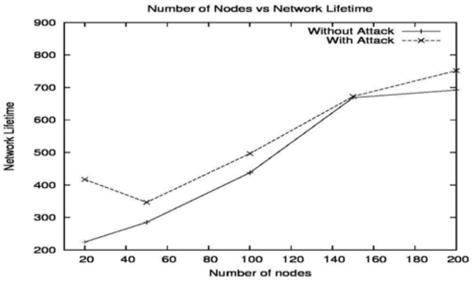

Fig. 6. Number of nodes Vs network lifetime (Gray Hole attack)

6.8. Comparison on the Impact of Black Hole and Gray Hole on LEACH

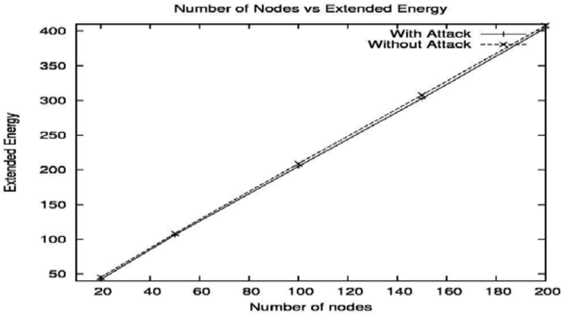

Fig. 7. Number of nodes Vs Total data sent to the base station (Gray Hole attack)

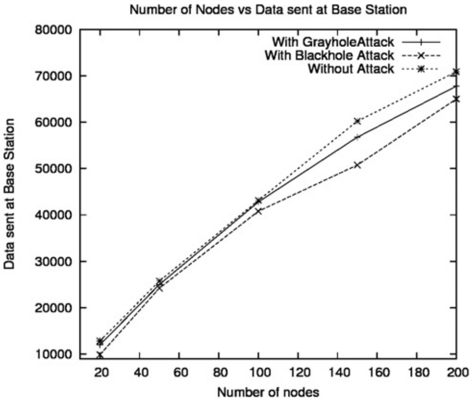

Fig. 8. Simulation result in presence of Black Hole and Gray Hole attack

As shown in the following Figure 8, the packets received at the base station in the presence of these two attacks are greatly affected. But if, we compare the impact of Black Hole attack with Gray Hole attack, then the packet received at the base station decreases more than that of Gray Hole attack. From the previous figures it is also clear that network lifetime increases in the presence of Black Hole node compared to that of Gray Hole attack. And Gray Holes attack in LEACH caused too much packet drops. But if we compare the impact of Black Hole attack with Gray Hole attack, then the Black Hole caused much packet drops than the Gray Hole attack. Energy consumed in all the process is less in case of Black Hole attack as compared to that of Gray Hole attack as in case of Gray Hole attack the attacker is some time transmitting the packets to the base station, hence, consuming the energy.

7. Proposed Detection Technique

In WSN, BS is assumed to be a trusted entity. it can keep track of the various CHs in different rounds. If a node occurs reapeatedly in the CH set by the BS, it may indicate malicious activity. Detection may incorporate BS keeping track of nodes in CH set as well as data sent by them for an observed period. If an CH node occurs repeatedly and not sending data for a threshold period of time, the BS blacklists that node for certain duration.

8. Conclusion

We have shown by simulation that the both the attack results in huge packet drops. We have also conducted our experiments on network of different sizes. We conclude that effect of the attack increases with increase in network size. Number of nodes in a cluster increase with increase in network size. The malicious node can affect the data of more nodes. We observed that the effect of the Gray Hole attack is less as comapred to the Black Hole attack. We have also floated an idea for detection of these attacks. In future, we plan to develop and simulate the detection technique on these lines.

References

[1] S. K. Sohraby, D. Minoli, T. Znati, Wireless Sensor Networks: Technology, Protocols, and Applications, John Wiley and Sons, 2007.

[2] Y. Zou, K. Chakrabarty, Sensor deployment and target localization based on virtual forces, in: Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 2, IEEE Computer Society, 2003, pp. 1293–1303.

[3] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, Special Issue on Sensor Network Applications and Protocols 1 (2-3) (2003) 1293 –1303.

[4] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energyefficient communication protocol for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.

[5] R.H.Jhaveri, S.J.Patel, D. Jinwala, A novel approach for grayhole and blackhole attacks in mobile ad hoc networks, in: Second International Conference on Advanced Computing and Communication Technologies, IEEE Computer Society, 2012, pp. 556–560.

[6] S. Lindsey, C. Raghavenda, Pegasis: power efficient gathering in sensor information systems, in: IEEE Aerospace Conference, IEEE Computer Society, 2002.

[7] O. Younis, S. Fahmy, Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks, IEEE Transactions on Mobile Computing 3 (4) (2004) 660–669.

[8] T. Issariyakul, Introduction to Network Simulator NS2, Springer, 2008.

[9] The network simulator ns2, `www.isi.edu/nsnam/ns`, visited July 2010 (1998).

[10] D. Martins, H. Guyennet, Wireless sensor network attacks and security mechanisms a short survey, in: 13th International Conference on Network-Based Information Systems, IEEE Computer Society, 2010.

[11] Y. Law, P. J. Havinga, ow to secure sensor network, in: International Conference on Sensor Networks and Information Processing,, IEEE Computer Society, 2010, pp. 89–95.

[12] R. Agrawal, R. Tripathi, S. Tiwari, Performance evaluation and comparison of aodv and dsr under adversarial environment, in: International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society, 2011, pp. 596–600.

[13] R. Verdone, D. Dardari, Wireless Sensor and Actuator Networks Technologies, Analysis and Design, 1st Edition, Academic Press, 2008.

[14] T. Roosta, S. W. Shieh, S. S. Sastry, Taxonomy of security attacks in sensor networks, in: First IEEE International Conference on System Integration and Reliability Improvements, IEEE Computer Society, 2006.

[15] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, An adaptive approach to detecting black and gray hole attacks in ad hoc network, in: 4th IEEE International Conference on Advanced Information networking and Applications, IEEE Computer Society, 2010, pp. 775–780.