SIMULATION OF SNOOZE ATTACK IN LEACH

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

Malviya National Institute of Technology, Jaipur-302017
{mtripathi,gaurms,vlaxmi}@mnit.ac.in

ABSTRACT

Wireless Sensor Network (WSN) consists of large number of sensor nodes capable of forming instantaneous network with dynamic topology. Each node simultaneously as both router and host. Number of nodes in a WSN can vary either due to the mobility or death of nodes due to drained conditions. Low Energy Aware Cluster Hierarchy (LEACH) is a most popular dynamic clustering protocol for WSN. Deployment in unattended environment, limited memory, limited power and low computational power of a sensor node make these networks susceptible to attacks launched by malicious nodes. This paper provides an overview of LEACH protocol and how LEACH can be compromised by malicious nodes. We propose a attack on LEACH – Snooze attack. This paper we present a way to simulate this attack on NS-2 which is demonstrative on throughput. We observe that during simulation throughput drops as an effect of attack. It is observed that the effect of the attack gets aggregated as we increase the number of attackers.

1. INTRODUCTION

Wireless Sensor Network (WSN) is slowly becoming the integral part of our daily life. Applications like smart home, smart offices, smart networking, smart security applications etc. rely on wireless communications among sensor nodes. WSNs are characterized by their flexibility and dynamism. In a WSN, one sensor node can communicate with other which is not even in the range of each other. Sensor nodes within communication range act as routers and pass information via a series of local hops to ensure connectivity to the Base station which may be situated at a far location. In WSNs, routing protocols help to enable communication between sensor nodes. Routing protocols can be either Flat or Hierarchical. In Flat protocols all the nodes perform the same task and have the same functionalities in the network. Data is being transmitted on the hop by hop by the means of flooding. Flooding and Gossiping [1], Sensor Protocols for Information via Negotiation (SPIN) [2], Directed Diffusion (DD) [3], Rumor [4] etc. are some of the examples of flat routing protocols in WSN. While in case of Hierarchical routing protocol sensor nodes are organized in the form of clusters based on some specific criteria and various nodes have different functionalities. Generally each cluster comprises a cluster head (CH) and some cluster member (CM) nodes. Cluster heads may from some more level of hierarchy. Low-energy Adaptive Clustering Hierarchy (LEACH) [5], Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [6] , Hybrid Energy-Efficient Distributed clustering (HEED) [7], Threshold sensitive Energy Efficient sensor Network protocol (TEEN) [8], The Adaptive

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA, SCAI - 2013
pp. 393–399, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3541

Threshold sensitive Energy Efficient sensor Network protocol (APTEEN) [9] etc. are some of the popular hierarchical routing protocols in WSN. Hierarchy in WSN provides loads of advantages [] like more scalability, less load, less energy consumption, more robustness, latency reduction, fault tolerance, maximizes the lifetime of the network etc.

LEACH is one of the pioneering hierarchical routing protocols used in WSN. It is simple and efficient. It has been any inspiration for many subsequent hierarchical routing protocols of WSN. Security is a key issue in any routing protocols. Attacks are launched to disrupt the routing operation. So to minimize the impact of attack on routing protocol it is essential to study the impact of attacks in routing protocols. In this paper, we propose a novel attack model on LEACH named Snooze attack. We implement and analyze effects of number of attackers executing Snooze attack on the network. Snooze attack mainly affects the hierarchical protocols because in a WSN we have large number of nodes which causes lots of redundant messages. In this case if only one node is affected by the attacker the impact will not be as effective as the attacker launches its attack on group of nodes. We have successfully simulated Snooze attack and to the best of our knowledge this has not been done before. We show through simulations the effect of Snooze attack on throughput and energy consumption. The rest of the paper is organized as follows. Section II introduces LEACH. Section III highlights the Snooze attack model in LEACH. Section IV presents related work. Simulation of attacks and their effect is described in Section V. Section VI concludes our work.

2. LEACH ROUTING PROTOCOL

The main idea behind LEACH [5] is to choose the cluster heads dynamically so that high energy communication with base station can be spread across all the nodes in the network.

LEACH works in rounds and each round consist of two phase set-up phase and steady-state phase. In set-up phase clusters are formed while in steady state phase data is being transferred to the Base Station. In set-up phase, initially all the nodes will have same probability to become a cluster head. Now every node chooses a random number between 0 and 1. A node becomes a cluster head if the number is less than the threshold T. Threshold is being calculated by the formula given below, which is based on the suggested number of CHs in every round (P) and the number of times a node became a cluster head so far.

$$T(n) = \begin{cases} \dfrac{P}{1 - P*(r \bmod \frac{1}{P})} & \text{if n} \in \text{G} \\ 0 & \text{otherwise} \end{cases}$$

Where r is the current round and G is the total number of nodes which has not been cluster head in the last (1/P) rounds.

When a node elects itself as a CH, it broadcast an advertisement message to all the nodes. Based upon the received signal strength of the advertisement, every node selects its CH for the current round and sends a join request to it. Now CH prepares a TDMA schedule for its members and broadcast it to its cluster members. In steady state phase various nodes send their sensed data to their respective CHs. After performing aggregation to reduce the communication cost, CH further sends the data to the BS. CDMA codes are used to avoid intra-cluster interference. CH rotation is done after every round to evenly distribute the load among the various nodes. So when the round time ends again the network enters into set-up phase for the selection of new CHs.

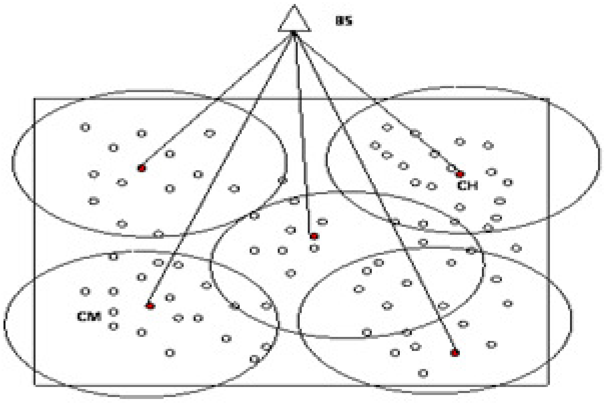

Fig. 1. Hierarchical Wireless Sensor Network

3. ATTACK MODEL IN LEACH

Snooze Attack

This is a DoS attack wherein, a malicious node targets group of nodes by becoming cluster head of that group. Once it becomes a cluster head and received data from its cluster members it goes into sleep mode. Target nodes will never come to know about his behavior. Consider the topology in Figure 1. Malicious node M sends the cluster head advertisement with high power. So it becomes cluster head in most of the rounds and does not forward the data to the BS. Cluster members like A, B never come to know about this behavior of M.

4. RELATED WORK

Karlof *et al* [11] discusses the following threat to the cluster based protocols in WSN.

- An adversary after becoming a cluster head can forward the data to the BS selectively.
- An adversary can generate multiple sybil nodes to disrupt the normal clustering process.

They suggested link-layer encryption and authentication, multipath routing, identity verification, bidirectional link verification, and authenticated broadcast to secure information exchange among various sensors and BS.

Ajay *et al* [14] has proposed sLEACH algorithm to detect the Sybil attack. The detection of sybil attack was done with the help of RSSI (an indicator of signal strength). The detection of intrusion was done when the number of cluster heads exceeded the threshold value.

SecLEACH proposed by Leonardo *et al* [15] uses random key predistribution to secure communication in LEACH. They provide efficient security to pairwise node to CH communication.

But none of these solutions have considered the case of sleep state of a node. Our attack model uses sleep mode of a CH to launch the attack which can severely hampers the network performance.

Simulation set up for Implementation of attack

To model the attack in WSN, NS-2 [13] simulator is used. LEACH module is modified to simulate snooze attack. Simulations parameters are set as shown in Table I. Nodes are initially placed in a grid of 100×100. Node id's are represented as N_i. All nodes are static. Throughput is used to measure network performance. This is defined as the amount of data transferred from sensor node to BS in a specified amount of time.

Table 1. Simulation Parameters.

Parameter	Value
Terrain Area	**100 X 100**
Number of Nodes	**20, 50,100,150 and 200**
Simulation Time	**7000 seconds**
Application Layer traffic	**CBR**
MAC	**SensorMAC**
Radio Propagation	**Two ray Ground**
Item to send	**500**
Item size	**70 Bytes**
No of Attackers	**0,1,2,3,4**

Implementation of Snooze attack

We are assuming that all the nodes are static. The attacker carries out the attack in two steps: First it declares himself as CH and broadcast the cluster head advertisement with high signal strength so that most of the nodes can join this cluster. Next, it accepts the data from all its cluster members, and go into sleep mode i.e. it will not transmit the data to the BS. None of the cluster member will come to know about this misbehavior of their CH and they keep sending the data to it.

In LEACH routing protocol after every round the cluster head has to change. To sustain this attack, we modified the LEACH code such that the attacker declares itself as cluster head in all the rounds and send a powerful advertisement to the nodes in the network.

1) Observations: In our experiment, number of nodes is varied from 20 to 200 in the network as well as number of attacker also increases from 0 to 4. Favorable metrics are transmitted from the start of simulation to allow the attacker to become cluster head for the most of the nodes in the network. After collecting the data from all the cluster members, the attacker goes into sleep mode. Attacker to BS there is no transmission. Figure 2 shows the effect of the attack on throughput. The graph shows that throughput drops in case of snooze attack. Throughput never falls to zero as

other cluster heads are still sending the data to the BS. To sustain the attack, attacker routinely updates powerful advertisement during cluster formation phase of every round.

2) Analysis: it is difficult to sustain the snooze attack in NS-2s implementation of LEACH. Because once the round time ends again the clustering process starts and all the clusters are formed again with different set of nodes eligible for becoming a cluster head. Objective of any attacker is to increase the duration of the attack. So we experimented with different ways to see the overall effect of snooze attack on different scenarios. Figure 2 shows throughput in three scenarios. Number of attackers is varied from 0 to 2. It is evident from the graph that throughput in case of more number of attackers is less compared to throughput in the absence of the attacker. This is true even if increase the number of nodes from 20 to 200. It is because the instead of sending data to the base station the attacker goes into sleep mode.

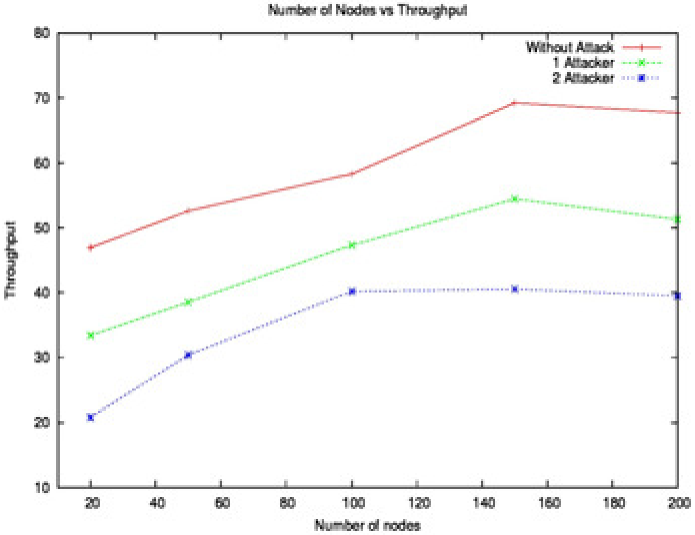

Fig 2: Effect of attack on Throughput

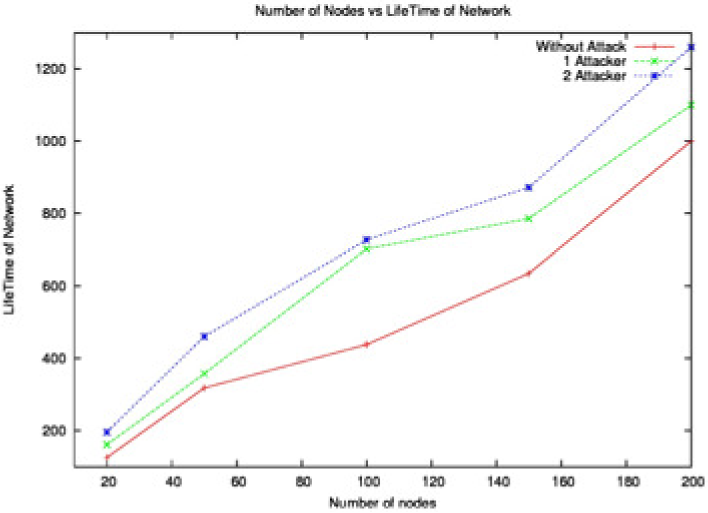

Fig 3 : Effect of attack on Network Lifetime

As the attacker is preserving its energy by going into sleep mode during the steady state phase the overall energy of the network increases and hence we observed an increment in overall network lifetime also. Figure 3 shows that network still continue to work for more time in case of 2 attackers as compared to no attacker was there.

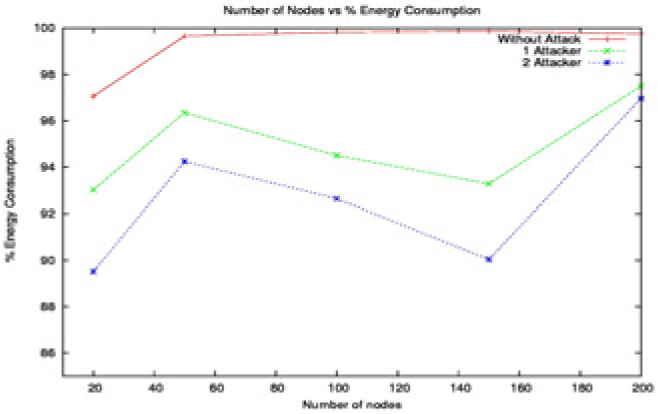

Fig 4: Snooze attack vs Energy consumption

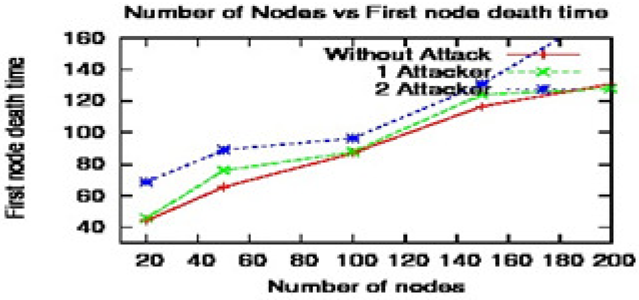

Fig 5: Attacker vs Time of FND

Figure 5 shows the effect of overall percentage energy consumption by all the nodes in the network and Figure 6 shows the death time of the first node (FND i.e. the time when the first node dies in the network). As again due to the effect of attack the death time of the first node is increased.

5. Conclusion And Future Work

LEACH routing protocol in its primitive form remains vulnerable to a variety of attacks that can influence the clustering process and launch denial-of-service attack. In this paper, we have proposed a novel attack model, snooze attack that acts as a denial of service (DoS) attack. We have observed that throughput drops when the attack is launched. From simulation we observed that due to dynamic clustering LEACH has natural methodology to alleviate the effect of snooze attack and we demonstrated a methodology to tear down the network. We also investigated the effect of snooze attack on various topologies. We observe that throughput at BS is low if there are less number of nodes in the network. If we increase the number of attackers this effect becomes more pronounced. As part of the future work, we plan to propose a countermeasure based on certification provided by BS to detect the snooze attack.

REFERENCES

[1] Li, C.; Zhang, H.X.; Hao, B.B.; Li, J.D. A survey on routing protocols for large-scale wireless sensor networks. Sensors 2011, 11, 3498–3526.

[2] Kulik, J.; Heinzelman, W.R.; Balakrishnan, H. Negotiation based protocols for dissemi-nating information in wireless sensor networks. Wirel. Netw. 2002, 8, 169–185.

[3] Intanagonwiwat, C.; Govindan, R.; Estrin, D.; Heidemann, J. Directed diffusion for wireless sensor networking. IEEE/ACM Trans. Netw. 2003, 11, 2–16.

[4] Braginsky, D.; Estrin, D. Rumor Routing Algorithm for Sensor Networks. In Proceed-ings of the First ACM International Workshop on Wireless Sensor Networks and Applica-tions (WSNA), Atlanta, GA, USA, 28 September 2002; pp. 22–31.

[5] W.R. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, An application- specific pro-tocol architecture for wireless microsensor networks, IEEE Transactions on Wireless Communications 1 (4) (2002) 660–670.

[6] S. Lindsey, C.S. Raghavenda, PEGASIS: power efficient gathering in sensor information systems, in: Proceeding of the IEEE Aerospace Conference, Big Sky, Montana, March 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] Manjeshwar, E.; Agrawal, D.P. TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. In Proceedings of the 15th International Parallel and Distributed Processing Symposium (IPDPS), San Francisco, CA, USA, 23–27 April 2001,pp. 2009–2015.

[9] 28. Manjeshwar, A.; Agrawal, D. P. APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. In Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Lauderdale, FL, USA, 15–19 April 2002, pp. 195–202.

[10] Xuxun Liu, A Survey on Clustering Routing Protocols in Wireless Sensor Networks. Sensors 2012, 12, pp. 11113-11153. doi:10.3390/s120811113

[11] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September, 2003.

[12] S. Bandyopadhyay, E.J. Coyle, An energy efficient hierarchical clustering algorithm for wireless sensor networks, in: Proceeding of INFOCOM 2003, April 2003.

[13] The Network Simulator NS-2 (1997). Available at www.isi.edu/nsnam/ns (Accessed: 25 June 2012).

[14] Ajay Jangra1, Swati and Priyanka, Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS), in : Proceeding of International Conference on Advances in ICT for Emerging Regions 2011, September 2011,Colombo,Sri Lanka.

[15] Leonardo B. Oliveira and Adrian Carlos Ferreira and Marcos Aurélio, SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks, Signal Processing,87(12),pp. 2882-2895,2007.