Impact of HELLO flood attack on Hierarchical Routing Protocols in WSN

[1] Shikha Magotra, [2] Naveen Kumar Gondhi
[1]Research Scholar, [2]Assistant Professor
[1]SoCSE, SMVDU, Katra,
[2]SoCSE, SMVDU, Katra,
[1] shikhabhimanyu.bali@gmail.com, [2] Naveen.gondhi@smvdu.ac.in

ABSTRACT

Wireless Sensor networks encompasses large number of micro sized sensors which are highly constrained in power thus, clustering is done in sensor networks in order to decrease delay, save power and increase throughput of the network. Such sensor networks make use of hierarchical routing protocols like LEACH, etc which suffers from serious security threats for HELLO flood attack. This paper studies this attack and analyses the influence of it on hierarchical protocols. The empirical simulation results in Matlab shows high performance metric- percentage packet delivery ratio.
Keywords: Wireless sensor networks, laptop-class attacker, Packet Delivery Ratio (PDR)

INTRODUCTION

Wireless Sensor Network (WSN) is defined as network of very large number of tiny sensors, highly constrained in terms of power, memory & cost, densely deployed in an area and are equipped with self-organizing protocols [1]. These tiny sensors sense data and transmit it to the sink node using various routing protocols developed for WSNs. Depending on the application for deployment of nodes in WSN, different hierarchical routing protocols are developed which uses clustering of nodes and used in applications where constant monitoring and minimum delay are required like urban environments.

Various hierarchical routing protocols used in WSN are – LEACH, PEGASIS, TEEN, APTEEN etc. LEACH is the first and fundamental protocol among all [7]. So we have considered LEACH as our baseline protocol for study. For clustering purpose, LEACH relies on Received Signal Strength of incoming HELLO packets thus making it defenseless to different kinds of attacks like HELLO flood, Sybil. Further, HELLO flood attack is the most easy to launch as only one laptop class attacker can threaten the whole network. We explored a lot of research papers describing methods for dealing with the attack [10] [13]. For best results of detection and isolation of attack, it is explored that its influence on routing mechanisms needs to be studied and analyzed. Till date, no work has been done to show the impact of this attack and thus, it motivates to our research in this direction.

The remaining paper is described as follows. Section II deals with the functioning of the LEACH hierarchical routing protocol. Section III describes the security issues encountered in hierarchical

routing protocols in WSN with emphasis on HELLO flood attack. Section IV describes the HELLO flood attack on hierarchical routing protocols. Section V describes the simulation scenario used & results for studying the impact of HELLO flood attack on hierarchical routing protocol (LEACH in our case). Finally, section VI gives the conclusion of the paper.

LEACH OVERVIEW

Heinzelman et.al [5] developed a hierarchical routing protocol for routing data in WSNs, namely Low Energy Adaptive Clustering Hierarchy commonly called LEACH. It divides the sensor nodes deployed in the network into clusters, each having its own cluster head. Each node in the network choose to become a cluster head by itself on the basis of certain threshold. After this, nodes becoming cluster heads send HELLO packets to the other nodes advertising themselves as cluster heads. The nodes receiving HELLO packets choose to join a CH on the basis of RSS of incoming HELLO packets.

After formation of clusters, each node in the cluster senses data and sends it to its CH using TDMA MAC. These CHs then, aggregates the data received from the various non CH nodes in the cluster and send it to the sink node using CDMA MAC protocol. Also, CHs drain more energy than other nodes as sending data to sink which maybe far located, requires more energy than sending data to own CH. So, in LEACH, nodes are randomly rotated to be CHs so that the distribution of energy consumed in the network is regular. According to the simulation done by the author, only 5% of the total nodes deployed in the network are sufficient to act as the CHs in each round for proper functioning of protocol. TDMA/CDMA MAC is also used to reduce further data packets collisions within the clusters as well as outside clusters. Thus, working of LEACH can be broadly divided into two phases:-

1. Setup phase / Cluster formation phase

2. Steady phase / Data Transmission phase

In setup phase, clusters are created and a cluster-head (CH) is selected for each cluster. While in the steady phase, data are sensed by each non CH node and transmitted to the sink node. Furthermore, the steady phase is kept longer than the setup phase so as to minimize the cost incurred.

Moreover, the threshold value (T(n)) used by the nodes to be CH in setup phase is given by the predetermined formula -

$$T(n) = \frac{p}{1 - p \times (r \times \mathrm{mod}\frac{1}{p})} \forall n \in G$$

Where p denotes the optimal probability to be cluster-head, r current round, and G set of nodes that have not become the cluster-head in the last 1/p rounds. Every node, for being cluster-head, chooses a random value lying between 0 & 1. If this number comes less than the threshold T(n), then the node is selected as cluster head for that particular round.

SECURITY ISSUES

In general, hierarchical routing protocols are hard to attack in comparison to other multi-hop routing protocols as due to clustering; only CH nodes can communicate with the sink node directly and these CHs can be located anywhere in the network. So, finding location of these CH nodes and then, launching attack on them further, is difficult. Moreover, in LEACH, random rotation of CHs is done which means that the CHs are periodically and randomly changed in each round. However, still as it uses cluster formation to transmit data to the sink; it relies completely on the CH nodes for data transmission. Thus, making CH nodes single point of failure. If any attacking node manages to becomes CH, it can launch further attacks namely Sybil, HELLO flood, selective forwarding [11].

In this scenario, laptop class attacker can easily become CH by sending bogus HELLO packets with high RSS to the whole network. Thus, every node will definitely choose attacker as CH thus causing attack.

Further, the traditional security methods used like standard key distribution schemes are less suited for WSN as it requires a lot of processing and huge memory [9]. Since WSNs are highly constrained in terms of energy and memory these methods are unable to provide sufficient security.

HELLO FLOOD ATTACK ON LEACH

Routing protocols which use HELLO packets assumes that receiving a HELLO packet from some node means that the sending node is in its radio range and thus, can be considered a neighbor. A laptop class attacker can easily use a transmitter with high transmission energy to transmit HELLO packets to a large area of nodes and thus, these nodes receiving HELLO packets will eventually consider attacker to be in their range which is actually not true. [10].

LEACH is the first and most used hierarchical routing protocols in WSN. In this protocol, non CH Nodes decide to join a CH on the basis of RSS of incoming Hello packets from CHs. So, HELLO Flood attack can be easily launched on such networks by broadcasting Hello packets to the whole network using a higher class attacking node like laptop. The attacking node will broadcasts with higher signal strength, all sensor nodes will select it as CH and send join packet to it, thinking that the sending node is in their range which is not true in reality.

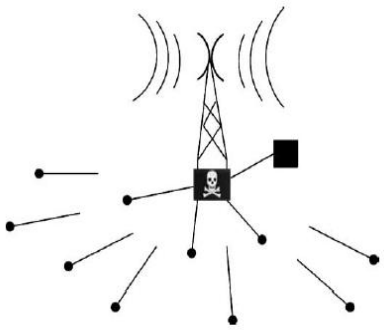

Figure – 1. Hello Flood Attack On Heirarchical Routing [4][13]

Thus, in hierarchical routing protocols, if CHs are attacked, the entire network will be compromised.

EXPERIMENTATION & EVALUATION

For simulation of LEACH protocol, received signal strength is calculated on Two Ray Ground propagation model. The following network model assumptions are made:

- Base Station is stationary and is located at the centre of the network
- All nodes are all the same and energy constrained
- Sensors will transmit data only if some event occurs
- Each node has location coordinates (x,y)

A. Simulation scenario

Parameter Used	**Value**
Network size(in meters)	100m x 100m
Sink Coordinates (x and y)	x=0.5*maxfield length y=0.5*max field width
Number of Nodes in the network (n)	100 + 1Base station
Probability of a node to be cluster head (p)	0.1
Tx & Rx Energy (ETX=ERX in Joules)	50*0.000000001
Tx & Rx Antenna gain (Gt=Gr)	1
Tx & Rx Antenna heights (Ht=Hr in meters)	1.5
Number of attacking nodes	1 to 5
Range of nodes(PThresh)	Diameter of field*sqrt(log(n)/n)
Total number of rounds (r)	100

Table (1) - Parameters Used & Their Values

We have used Matlab simulator for experiment purpose. An area of 100m × 100m is considered for simulating WSN having 100 sensor nodes with no mobility. Initially, the nodes are placed at random. 1-5 nodes out of total number of nodes have higher transmission, reception and carrier sensing capability which can be used for attacking purpose & one node is base station. Different parameters used for simulation and their values are given in table 1. The sink node/base station is placed at the center of the network located at (50, 50).

B. Result analysis

HELLO flood attack on hierarchical routing protocol (LEACH, in our case) is simulated and analyzed through performance metric - percentage packet delivery ratio. Percentage Packet

delivery ratio refers to the ratio of total no. of packets transmitted by all nodes to the total no. of packets received by sink node.

$$\%\text{age PDR} = \frac{\text{total no. of packets transmitted}}{\text{total no. of packets received}}$$

The results are shown graphically as:

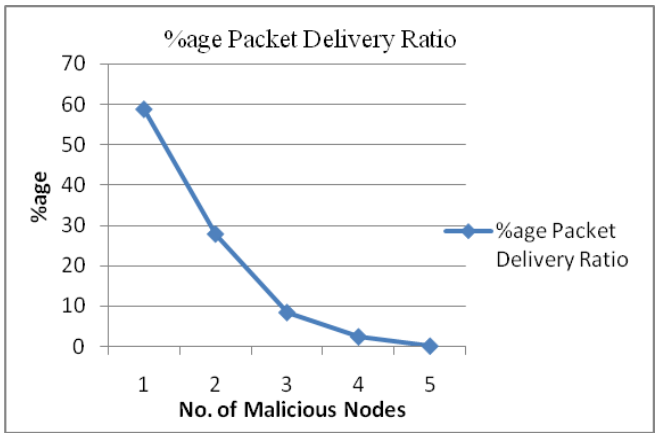

Figure – 2. Percentage Packet delivery ratio V/s malicious nodes

Here, in Fig.2 the percentage of PDR gets decreased in case of networks compromised by HELLO flood attackers. As seen from the graph, with the increase in no. of malicious nodes in network, percentage PDR keeps on decreasing as it declines to 60% with one attacking node and goes on decreasing to 10% with 3 attacking nodes.

CONCLUSION

Wireless sensor networks, like other networks, are prone to serious network threats and intrusion like spoofing, wormhole, Sybil, HELLO flood, selective forwarding. Among all, HELLO flood attack is an important attack which affects networks with hierarchical protocols like LEACH as it is the easiest to launch. Moreover, HELLO flood attack brings the whole network into a state of confusion and completely dysfunctions the steady phase of the LEACH protocol in that network. So, we considered this attack for our study. We analyzed this attack in simulated environment and compared the working of LEACH with HELLO flood attack with differing number of attacking nodes from 1 to 5. The analysis done is shown graphically using percentage packet delivery ratio, based on number of attacking nodes in the network. It shows exponential decline in PDR with the increasing number of attacking nodes upto 5.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, *Wireless sensor networks: a survey*, Computer Networks 38 (4) (2002) 393–422.

[2] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong; , "*Security in wireless sensor networks: issues and challenges*," Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference , vol.2, no., pp.6 pp.-1048, 20-22 Feb. 2006

[3] Chee-Yee Chong; Kumar, S.P.; , "*Sensor networks: evolution, opportunities, and challenges*," Proceedings of the IEEE , vol.91, no.8, pp. 1247- 1256, Aug. 2003

[4] C. Karlof and D. Wagner, "*Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*", Ad Hoc Networks, vol. 1, 2003, pp. 293-315.

[5] Wendi RabinerHeinzelman, AnanthaChandrakasan, and HariBalakrishnan, "*Energyefficient communication protocols for wireless microsensornetworks*," in Proceedings of the Hawaii International Conference on Systems Sciences, Jan. 2000

[6] Dr. Moh. Osama K., "*HELLO Flood Counter Measure for Wireless Sensor Network*," International Journal of Computer Science and Security, vol. 2 issue 3, 2007, pp-57-64.

[7] Suraj Sharma and S. K. Sena, "A Survey on Secure Heirarchical Routing Protocols in Wireless Sensor Networks," ICCCS'11, February 2011

[8] Patil, M.; Biradar, R.C., "A survey on routing protocols in Wireless Sensor Networks," *Networks (ICON), 2012 18th IEEE International Conference on* , vol., no., pp.86,91, 12-14 Dec. 2012

[9] Yong Wang; Attebury, G.; Ramamurthy, B., "A survey of security issues in wireless sensor networks," *Communications Surveys & Tutorials, IEEE* , vol.8, no.2, pp.2,23, Second Quarter 2006

[10] Virendra Pal Aishwarya S. Sweta Jain, "Signal Strength based HELLO Flood Attack Detection and Prevention in Wireless Sensor Networks," *International Journal of Computer Applications (0975 – 8887)* Volume 62– No.15, January 2013

[11] Aslam, M.; Javaid, N.; Rahim, A.; Nazir, U.; Bibi, A.; Khan, Z. A., "Survey of Extended LEACH-Based Clustering Routing Protocols for Wireless Sensor Networks," *High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on* , vol., no., pp.1232,1238, 25-27 June 2012

[12] Milan Simek, Patrik Moravek and Jorge sa Silva, *Wireless Sensor Networking in Matlab: Step-by-Step*, January 2010

[13] Magotra S; Kumar K, "Detection of HELLO flood attack on LEACH protocol", *2014 IEEE International Advance Computing Conference (IACC)*, 2014