ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MITIGATING HELLO FLOOD ATTACK ON WSN BY LEACH PROTOCOL USING ENERGY LEVEL

Dilpreet Kaur*, Rupinderpal Singh
* M.Tech, Department of Computer Science & Engineering, G.I.M.E.T, Amritsar, India
Asst. prof., Department of Computer Science & Engineering, G.I.M.E.T, Amritsar, India

ABSTRACT

Various Wireless sensor network applications use hierarchical routing protocol for routing sensed data to sink. LEACH (Low energy adaptive clustering Hierarchical) is one of the broadly used hierarchical, distributed clustering protocol in WSN. In LEACH, Non-Cluster head Nodes decide to join a cluster head based on Distance between Cluster head and nodes and Received Signal Strength (RSS) of receiving HELLO packets from Cluster head's making it vulnerable to HELLO Flood attack. In hello flood attack, Adversary node misleadingly claims superior route to the base station (BS) thereby inviting all the data traffic towards it. HELLO flood attack on LEACH protocol where the cluster head (CH) sends HELLO messages to the non-Cluster Head nodes claiming superior route to base station. The non-Cluster head nodes send the traffic towards the adversary causing data loss. Hello Flood attack detected the adversarial node in the network by comparing the received signal strength and the distance between with non-CH nodes and cluster head with the threshold values. However, in cases where the non-CH nodes are located closely to the adversary node then the method of threshold RSS and threshold distance will not work properly.

The research problem is to discover a new method will work in case where non CH nodes are located closely to the adversary node.

KEYWORDS: WSN, Adversary node, Cluster Head (CH), HELLO Flood attack, LEACH, Received Signal Strength (RSS).

INTRODUCTION

Hello flood attack is an attack on the network layer [5][9].Many routing protocols require nodes to broadcast Hello packets to announce themselves to their neighbors nodes and node receiving such a packet may assume that it is within normal radio range. This assumption may sometimes false; a laptop-class attacker broadcasting routing information with large enough transmission power could convince every node in network that the adversary is it neighbors node. An adversary advertising a very high quality route to the base station to every node in the network cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion. Then network is left in a state of confusion (as shown in figure1)

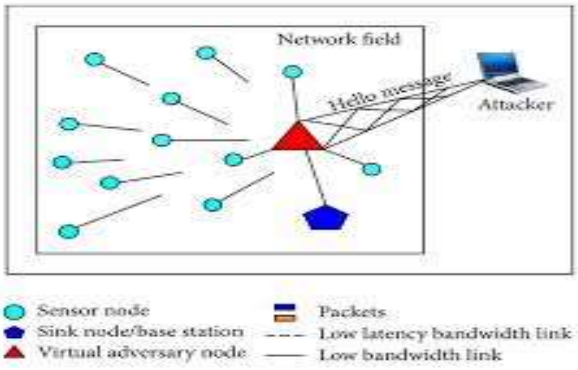

Figure 1: Hello flood attack

Protocols which depend on local information interchange between neighboring nodes for topology maintenance or flow control are also subject to this attack [9]. An adversary does not necessarily need to able to construct legitimate traffic in order to use the HELLO attack. It can simply re-broadcast packets with enough power to be received by all the node in the network. HELLO floods attack can also be thought of as one-way or simplex, broadcast wormholes.

Type of Attacks
There are basically two types of attacks:-

1) EXTERNAL ATTACKS
2) INTERNAL ATTACKS

external attacks
External attacks, in which the attackers aim to cause congestion, propagate fake routing information or disturb nodes from providing service in the network.

internal attacks
Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node.

LITERATURE REVIEW

General study of work done in the field of detection of HELLO flood attack on LEACH protocol in Wireless Sensor network is done and is categorized into two groups: Non-Cryptography-based approaches & Cryptography based approaches. This described as follows in sequential order:

Group A: Cryptography-based approaches
F-LEACH L. B. Oliveria et al. [9] FLEACH, protocol for securing node to node communication in LEACH-based network. FLEACH used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. FLEACH provides authenticity, integrity, confidentiality and freshness to node-to-node communication. But it is vulnerable to node capturing attack.

SLEACH this is modified secure version of LEACH called SLEACH [8], which is investigated the problem of adding security to cluster-based communication protocol for homogeneous WSN's consisting of sensor nodes with severely limited properties. SLEACH provides security in LEACH by using the building block of Security Protocol for Sensor Network(SPINS), symmetric-key methods and MAC (Message Authentication Code). SLEACH protects against selective forwarding, sinkhole and HELLO flooding attacks. It prevents intruder to send bogus sensor data to the CH and CH to forward bogus message. But SLEACH cannot prevent to crowd the time slot schedule of a cluster, results in DoS attack or simply lowering the output of the CH and does not guarantee data secrecy. It meant to protect only outsider attack.

R. Srinath et al. The protocol is based on LEACH protocol that Authentication Confidentiality cluster based secure routing protocol [7]. It uses both private key (in digital signature) and public key cryptography. This protocol deals with interior adversary node. Because of the high computational requirement it use of public key cryptography, it is not efficient for the Wireless sensor networks.

RLEACH Secure solution for LEACH has been introduced called RLEACH in which cluster are formed periodically and dynamically. In RLEACH the orphan node problem is raised due to random pair-wise key scheme so they have used improved random pair-wise key scheme to overcome. RLEACH has been used the one way hash chain, symmetric and asymmetric cryptography to provide security in the LEACH Hierarchical routing protocol. RLEACH resists many attack like spoofed, alter and replayed information, sinkhole, worm- hole, selective forwarding, HELLO flooding and Sybil attack.

Group B: Non-cryptography based Approaches
Signal strength based detection approach Virendra Pal Singh et al. [13] proposed a technique in the paper Signal Strength based HELLO Flood Attack Detection and Prevention in Wireless Sensor Networks using AODV protocol. They have used a threshold for RSS i.e. fixed signal strength for sensor nodes, and the RSS of the each received

HELLO packet is compared to this threshold. Signal strength = Fixed signal strength in radio, node = 'friend' Signal strength > Fixed signal strength in radio, node = 'stranger' Nodes which are significantly far from adversary will wrongly categorize the adversary as 'Friend'. As RSS is inversely proportional to the distance. The HELLO message receiving node sends simple test packet to HELLO sending node, if the reply comes in allotted time threshold then HELLO sending node is considered as a friend, if not then it is classified as a stranger.

Paper by Shikha Magotra, Krishan kumar used leach protocol that work to measure RSS (Received signal strength) and distance between nodes and cluster head to find malicious node. But it fails when actual node place at some distance.In cases where the non-CH nodes are located closely to the adversary node then the method of threshold RSS and threshold distance will not work properly. Comparison of different technique is in given table 1:-

S.NO	NAME OF AUTHOR	WORK DONE	DRAWBACKS
1	Shikha Magotra Krishan kumar	They work to measure RSS and distance between nodes and cluster head to find malicious node.	Where the non-CH nodes are located closely to the adversary node.
2	Virendra Pal Singh	They have used a threshold for RSS i.e. fixed signal strength for sensor nodes, and the RSS of the each received HELLO packet is compared to this threshold.	Nodes which are significantly far from adversary will wrongly categorize the adversary as 'Friend'.
3	R. Srinath	It uses both public key (in digital signature) and private key cryptography.	It is not efficient for the WSNs.
4	L.B. Oliveria	It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH.	But it is vulnerable to node capturing attack.
5	C.Wang K. Zhang and C.Wang	SLEACH provides security in LEACH by using the building block of SPINS (Security Protocol for Sensor Network), symmetric-key methods and MAC. SLEACH protects against selective forwarding, sinkhole and HELLO flooding attacks.	But SLEACH cannot prevent to crowd the time slot schedule of a cluster, causing DoS attack or simply lowering the throughput of the CH and does not guarantee data confidentiality. It protects only outsider attack.

Table 1:-Comparison table

IV. Leach protocol

Low Energy Adaptive Clustering Hierarchy (LEACH) is a hierarchical-based routing protocol which uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network [5]. LEACH works in two phases- Setup phase & Steady phase. In setup phase, each node decides to become Cluster head based on its residual energy and probability. Afterwards, it broadcasts "HELLO" packets to other nodes in its range. The nodes receiving "HELLO" packets then decide to join a CH based on Received Signal Strength (RSS) of a node. Though the use of clustering improves performance of routing protocol in terms of throughput, delay etc. It makes LEACH susceptible to various attacks like HELLO Flood attack, selective forwarding attack etc. As LEACH relies completely on Cluster heads for data transmission to the sink, if Cluster heads are compromised then whole network can be attacked by adversary node. Wireless sensor networks are mostly deployed in such areas where physical tampering of nodes is easy. So, it makes these networks more vulnerable to like HELLO Flood Attack and laptop class attacks.

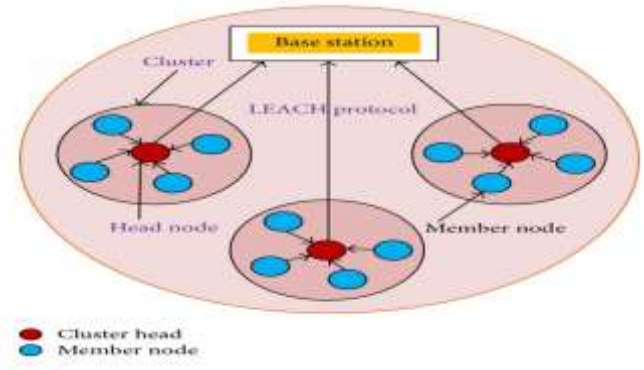

Figure 2:- LEACH protocol

Non-Cluster head nodes along with comparing of the Received signal strength of receiving HELLO packet also compare the distance between the non-CH node and Cluster Head node with the Distance threshold. So, only those nodes whose Received Signal Strength as well as distance is within threshold limits are considered for joining Cluster Head. Some adversary node sends wrong information in HELLO packet; it can be detected by sending test packet. We assume that every node has its location information and during Setup phase of LEACH protocol, when advertisement of "HELLO" packets is done by Cluster Head, it sends its location coordinates along with HELLO packets. Now, the nodes receiving HELLO packets from Cluster Head calculates the distance between as shown:-

$$Dist = sqrt\ [sq(x2-x1) + sq\ (y2-y1)]$$

Here, (x1,y1) are location coordinates of node receiving packet and (x2,y2) are location coordinates of Cluster Head sent through advertising HELLO packet. Receiving Node also calculates threshold value for RSS(Threshold received signal strength) (ThRSS) which corresponds to the radio range of each node in the network and threshold value for distance (ThDist) which corresponds to the distance covered through radio range of signal. Afterwards this, each node decides to join a Cluster Head based on distance calculated and RSS of receiving packet. For each non-Cluster Head node, If RSS < ThRSS and Dist < ThDist and then CH Node = 'Friend' otherwise test packet is sent. The algorithm used by each node for joining Cluster Head.

1. A< = C : id (CH) , join Adv, (xc, yc)
2. A: Dist= sqrt[sq(xc-x1) + sq(yc-y1)]
3. If RSS < ThRSS, then A(i) ! CH(j) : id(A(i)) , id(CH(j)) , join req
4. Elseif Dist < ThDist, then Send Test Packet
5. If reply packet comes within time threshold, then A(i) ! CH(j) : id(A(i)) , id(CH(j)) , join req
6. Else goto step1

The symbols are used here: ! – unicast, A - normal node, Join Adv - advertisement to join the cluster, Join req - request to join the cluster, id - identification number, (x1,y1) - location coordinates of node receiving packets, (xc,yc) - location coordinates of CH sent through advertising packet**,** Dist - Distance between node 'i' and CH 'c' in range of 'i' calculated in (1).

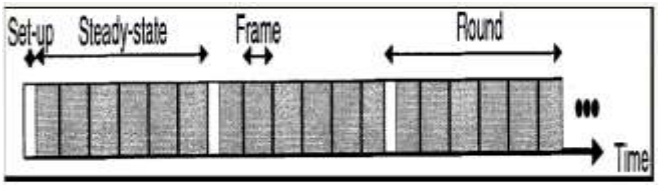

Fig 3 :- Phases of LEACH protocol

1) Setup phase:- At the beginning of each round, each node advertises it probability, (depending upon its current energy level) to be the Cluster Head, to all other nodes of network. Nodes (k for each round) with higher probabilities are chosen as the Cluster Heads. Cluster Heads broadcasts an advertisement message (ADV) using CSMA MAC protocol. Based on the received signal strength, each non-Cluster Head node determines its Cluster Head for this round (random selection with obstacle).Each non-Cluster Head transmits a join-request message (Join-REQ) back to its chosen Cluster Head using a CSMA MAC protocol. Cluster Head node sets up a TDMA schedule for data transmission coordination within the cluster.
2) Startup phase:- At the beginning of each round, each node advertises it probability, (depending upon its current energy level) to be the Cluster Head, to all other nodes. Nodes (k for each round) with higher probabilities are chosen as the Cluster Heads. Cluster Heads broadcasts an advertisement message (ADV) using CSMA MAC protocol. Based on the received signal strength, each non-Cluster Head node determines its Cluster Head for this round (random selection with obstacle).Each non-Cluster Head transmits a join-request message (Join-REQ) back to its chosen Cluster Head using a CSMA MAC protocol. Cluster Head node sets up a TDMA schedule for data transmission coordination within the cluster.

CONCLUSION

The nodes in wireless sensor networks are susceptible to various attacks. One such attack is the hello flood attack. In hello flood attack, the adversary node falsely claims the superior route to the base station thereby attracting all the data traffic towards it. In study done by Shikha Magotra, authors have studied the HELLO flood attack on the LEACH protocol where the cluster head sends the HELLO messages to the non-CH nodes claiming superior route to the base station. The nodes send the traffic towards the adversary resulting in the data loss. The authors have detected the adversarial node in the network by comparing the received signal strength and the distance between with non-CH nodes and cluster head with the threshold values. However, in cases where the non-CH nodes are located closely to the adversary node then the method of threshold RSS and threshold distance will not work properly. The research problem is to discover a new method will work in case where non CH nodes are located closely to the adversary node.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol.38, 2002, pp.393– 422.
[2] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong; , "Security in wireless sensor networks: issues and challenges," Advanced Communication Technology, ICACT 2006, 8th International Conference , vol.2, 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, 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. 293315.
[5] Shikha Magotra, Krishan kumar "Detection of HELLO flood Attack on LEACH Protocol," IEEE International Symposium on Network Computing and Applications, pp.145-154, Washington, DC, USA, 2014.
[6] M. Bern R. Dahab L. B. Oliveira, H. C. Wong and A. A. F. Loureiro "SecLEACH -a random key distribution solution for securing clustered sensor networks," Fifth 36 IEEE International Symposium on Network Computing and Applications, pp.145-154, Washington, DC, USA, 2006.

[7] A. V. Reddy R. Srinath and R. Srinivasan "Cluster based secure routing protocol for wsn," Third International Conference on Networking and Services, pp.45, Washington, DC, USA, 2007.
[8] C.Wang K. Zhang and C.Wang "A secure routing protocol for cluster based wireless sensor networks,"
[9] M. A. Vilaa H. C. Wong M. Bern R. Dahab L. B. Oliveira, A. Ferreira and A. A. F. Loureiro "SecLEACH-on the security of clustered sensor networks," vol.87, pp.2882-2895, December 2007.
[10] G. Hu D. Wu and G. Ni. "Research and improve on secure routing protocols in wireless sensor networks," 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), 2008.
[11] Dr. Moh. Osama K., "HELLO Flood Counter Measure for Wireless Sensor Network," International Journal of Computer Science and Security, vol. 2, 2007, pp-57-64.