International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Review study of detection and prevention methods of various possible attacks in Leach protocol

[1]Er. Jyoti, [2]Er. Ashu Bansal

[1]Student M.Tech. CSE, BFCET
[2]Assistant Professor, CSE, BFCET
bansal.ashu07@gmail.com

Abstract: *The aim of this review paper is to study the security of Leach protocol used in wireless sensor network. It includes various attacks possible on Leach protocol and methods to prevent it from attacks. Leach is low energy adaptive clustering (CH) hierarchical protocol which is a highly secure protocol still there are attacks possible on Leach. The wireless sensor network is more prone to attacks than wired network. Also there are energy issues and security issues arise in wireless sensor network. To resolve that issues various routing protocols have been proposed. Leach is one of the hierarchical routing protocols. For security of WSN various security mechanisms are also studied in this paper.*

Keywords: *WSN, CH, Leach, adversary.*

I. Introduction

Wireless sensor network is composed of thousands of sensor nodes deployed in sensing region. Nodes collect the data and send it to the base station. Main issues in WSN are limited memory and power resources. Security is another important issue considered in WSN. Various routing protocols are available till now to resolve these issues. Leach is widely used protocol in order to enhance the energy of sensor nodes.

I. LEACH

Leach stands for low energy adaptive clustering hierarchy. It is one of the first hierarchical protocols. Leach is clustering based protocol that randomly rotates cluster head to distribute energy load among sensor nodes in network [1]. It works in rounds. In each round there are two phases: set up phase and steady phase.

1) Set up phase:
a) Advertisement phase
b) Cluster set up phase

In set up phase each node decides whether or not to become cluster head for current round. It depends upon decision made by node choosing a random number between 0 and 1. The node whose number is bigger than threshold will become cluster head.

$$T(n) = \frac{p}{1 - p * \left(rmod \frac{1}{p} \right)} : \text{if n E G}$$

$$T(n) = 0 \quad : \text{Otherwise}$$

- P is probability of node being selected as cluster head node.
- r is number of rounds passed.
- G is set of nodes that have not been selected as cluster head in last 1/p rounds.
- Mod denotes modulo operator.

Nodes that are cluster head in round r shall not be selected in next 1/p rounds [3]. Then CH will broadcast an advertisement message to inform all other nodes that it is new cluster head. Then nodes send join request message containing their ID's by using CSMA to join a cluster [2]. The nodes join cluster according to signal received by them. After that each CH knows its own cluster member information. Based on message, CH creates TDMA schedule table and broadcast to cluster members. So all the member nodes know their idle slots, and then steady phase begins.

***2) Steady state phase*:** During steady phase when nodes need to sense the necessary data they turn on their radio. According to their allotted TDMA schedule, nodes start sending their data to CH. When CH receives all data sent by their members, it aggregates them and sends it to base station. Aggregation of data saves energy and hence reduces consumption of energy in Leach protocol [3].

II. NEED FOR SECURITY

***1) Data confidentiality*:** confidentiality means to conceal the data from passive attackers. So that data remains confidential within the sensor networks [4].
***2) Data authentication*:** It verifies the identity of sender and receiver.
3) *Data integrity*: Data integrity ensures that data has not been altered by attackers.
4) *Data Availability*: It ensures that all resources are available for use by nodes.

III. ATTACKS POSSIBLE ON LEACH PROTOCOL

1) Selective forwarding attack:

During communication nodes forward data from one node to next. During transmission some packets can be dropped by attacker nodes. Attacker nodes only forward the few packets instead of forwarding all packets. This kind of attack is known as selective forwarding attack [5].

2) Sinkhole attack:

In this attack goal of adversary is to attract all the traffic from particular area through compromised node, creating a sink hole with adversary at center. Compromised node becomes attractive to surrounding nodes and attracts all traffic from its neighbors by telling its neighbors that it has shortest route to reach to the base station. This route is artificial high quality route [6].

3) Black hole attack:

In this attack, the attacking node has more initial energy than other nodes and becomes one of the cluster head in first round and in other rounds. After receiving all data from cluster members aggregate it and do not forward data to base station and reducing the total amount of data to be transmitted.

4) Wormhole attack:

In this attack wormhole tunnel is created by any two malicious nodes which conspire together to create an illusion that they are just one hope away and there by routing the packets to as neighbor nodes. As soon as wormhole entities create the tunnel successfully, they can drop the packets, replay, tempers the packets or selectively forward them [8].

5) Sybil attack:

In this attack, attackers use multiple identities. Its multiple identities misleads to all other nodes. Malicious nodes forward the incorrect message to sensor node in network which decreases the normal performance of fault tolerant such as distribute storage and paths. Incorrect message may be anything, which may include the position of sensor nodes, strength; generation of nodes which is actually not exists [9].

6) Hello flood attack:

In this attack, hello packets will have high radio transmission range and these are used as weapons in WSN. Nodes with high transmission range send hello packets to sensor nodes with in a cluster. More powerful nodes pretend to other nodes as it is cluster head node and members of cluster starts send their data to these attacker nodes [10].

IV. SOME CRYPTOGRAHIC APPROCHES USED TO SECURE LEACH

SLEACH:It is first secure version of Leach protocol [11], which prevents sinkhole, selective forwarding and hello flooding attacks by using protocol SPINS (security protocol for sensor networks) and MAC for authentication. It prevent malicious node to send false data. It does not guarantee confidentiality and availability of data.

***RLEACH*:** It was proposed to solve the problem of secure Leach [12]. It is secure routing protocol for cluster based WSN, that uses the group key management. Here clusters are formed dynamically and it uses improve random pair wise key (RPK) management scheme, which use one way hash chain, symmetric and asymmetric cryptography to ensure security in Leach. RLEACH resists to different attacks such as selective forwarding, sinkhole attack, Sybil attacks and hello flood attacks. It is also energy efficient. When node transmits data to CH, member

nodes among a cluster can close their wireless devices during transmission phase to save energy. RLEACH balance the network security and energy consumption in cluster head WSN.

***SS-LEACH*:** It is another secure routing protocol based on Leach protocol [13]. Its main aim is to offer security as well as becomes energy efficient. It defines multiple path cluster heads chain to communicate with the base station, which increase lifetime of network. For security it uses key pre-distribution and self localization techniques. It prevents from selective forwarding, hello forwarding and Sybil attacks, but it controls neither data integrity nor freshness.

***SEC-LEACH*:**It provides an efficient solution for securing communication in Leach [14]. Random key pre-distribution is used in it securing hierarchical cluster heads and dynamic cluster formation. Random key distribution is applied in SEC-LEACH and symmetric key and one way hash chain is introduced to provide confidentiality and freshness. It provides authenticity, integrity, confidentiality and freshness to communication.

***ESMR*:** It is efficient security model of routing protocol to provide security solution for Leach; only public key cryptography technique is used in it [15]. The performance of ESMR by simulation results show that it is not good as Leach when there is no attacker in network, but as number of attacker increases it becomes better and better. Outside attacks are only prevented in this protocol but it has high computation burden due to use of public key cryptography.

***F-LEACH*:** It is the protocol proposed for securing node to node communication in Leach based network. For enhancing security in Leach, random key pre-distribution scheme with symmetric key cryptography. It provides authentication, integrity, confidentiality and freshness from node to node communication. But it can't protect from node capturing attack [16].

V. SOME NON CRYPTOGRAHIC APPROCHES

Signal strength based approach using AODV protocol: Virendra Pal Singh et al. [17] proposed a technique in which detection and prevention of hello flood attack is proposed based on signal strength of received hello message. Nodes have been classified as friend or stranger. They AODV protocol for this technique. A threshold value is used by them to compare it with RSS of each received hello packet.

Signal strength= Fixed signal strength in radio, node = 'friend'
Signal strength > Fixed signal strength in radio, node = 'stranger'

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 friend otherwise stranger.

Signal strength based approach using LEACH protocol:

ShikhaMagotra and Krishankumar proposed Detection of hello flood attack on LEACH protocol. In LEACH Non-Cluster head nodes decide to join the cluster head based on RSS (received signal strength) of receiving hello packets from CHs making it vulnerable to HELLO flood attack. To overcome the test packet overhead occurs in [18], a new methodology is proposed based on distance. In this methodology non-CH nodes compare the RSS of receiving hello packets as well as compare the distance between the non-CH nodes and elected-CH nodes with distance threshold. Thus only those nodes whose RSS and distance are within threshold limit are considered for joining CH. If adversary node sends wrong coordinate information in HELLO packet , it can be detected by sending test packet. Distance can be calculated by using formula as shown below:

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

This technique is effective in improving Performance of network.

RSS and Guide node based approach: SatwinderKaurSaini and Mansigupta Proposed approach [18] based on the Received Signal Strength (RSS) and the geographical information of the motesdeployed in the sensing region of interest. In their approach random GUIDE nodes are chosen, as these arerandomly chosen their distribution cannot be guaranteed to be uniform over the sensing region. These GUIDE nodes arechosen randomly in each round as the Cluster Heads depending upon the desired Guide node percentage. The GUIDEnodes are responsible for the work of detection of malicious Cluster Head and malicious node information disseminationas well. Larger is the Guide node percentage, more are the chances of early detection; However higher Guide node percentage will also result in more energy consumption.

S.no	Paper title	Year	Author	Approach	Protocol	Advantages
1.	Signal Strengthbased HELLOFlood Attack Detection andPrevention inWireless SensorNetworks	2013	Virendra Pal Singh,AishwaryaS. AnandUkeyand Sweta Jain	Signal strengthbased approach. COmparison of RSS withpre-calculated Threshold	AODV	Simple Approach withless computation overhead
2.	Detection of hello flood attack on LEACH protocol	2014	SikhaMagotra and Krishan Kumar	Geographical Info. basedapproach. Coordinate approach with distance.	LEACH	Simple approach with lesser detection time
3.	Detection of Malicious Cluster Head causingHello Flood Attack in LEACH Protocol in Wireless Sensor Networks	2014	SatwinderKaurSaini and Mansi Gupta	Signal Strength and geographical information based and detection depends upon no. of GUIDE nodes choosen.	LEACH	Simple approach with lesser detection time.

CONCLUSION: Leach protocol is highly secure protocol used in wireless sensor network. Still various attacks are possible on Leach protocol. The various methods are given to secure it. For security of WSN various security mechanisms are also studied in this paper. Various attacks possible on Leach are hello flood attack, sinkhole attack, Wormhole attack etc.

REFERENCES:

[1]. P. Vasan and M. Behniwal, "Secure and Reliable Data Transmission Using Homomorphic Encryption in WSN", in international journal of Advanced research in computer science and software engg, May 2014.

[2]. K. V. Shukla, "Research On Energy Efficient Routing Protocol LEACH For Wireless Sensor Networks" in International Journal of Engineering Research & Technology, March, 2013.

[3]. A. Gupta and V. Sharma, "A Confidentiality Scheme for Energy Efficient LEACH Protocol Using Homomorphic Encryption" in International Journal of Advanced Research in Computer Science and Software Engineering, may 2013.

[4]. S. Ghildiyal, A. Gupta, M. Vaqur, A.Semwal, "Analysis of wireless sensor networks: Security, Attacks and Challenges" in International Journal of Research in Engineering and Technology , march 2014.

[5]. H. Sun, C. Chen and Y. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in Proc. Of IEEE TENCON 2007, Oct. 2007, pp. 1-4.

[6]. V. Soni, P. Modi, V. Chaudhri , "Detecting Sinkhole Attack in Wireless Sensor Network" in International Journal of Application or Innovation in Engineering & Management ,feb 2013.

[7]. S. Iqbal, A.Srinivas S P, S.S Kashyap, "Comparison of different attacks on Leachprotocolin WSN" in Proceedings of ASAR International Conference, 14th May-2014, Mysore, India.

[8] K. Zhang, C. Wang and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in Proc. 4th IEEE International conference on Wireless communications, Networking and Mobile Computing, 2008, pp. 1-5.

[9] D.Wu, G. Hu, and G. Ni, "Research and improve onsecure routing protocols in wireless sensor networks",Fourth IEEE International Conference on Circuits andSystems for Communications (ICCSC), pp. 853–856,Shanghai, May 2008.

[10]. P. Maidamwar& N.Chavan, "Impact of warmhole attack on performance of Leach in wireless sensor networks " in International Journal of Computer networking, Aug 2013.

[11]. J. R. Douceur, "The Sybil Attack,"in 1st international workshop on peer to peer systems, 2002.

[12]. C. karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE, 2003.

[13]. K. Zhang and C. Wang, "A Secure routing protocol for cluster-based wireless sensor networks using group key management," in Proc. 4th IEEE.

[14] L. B. Oliveira, A. Ferreira, M. A. Vilaca, H.C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro,

"Secleach-on the security of clustered sensor networks", Signal Processing, 87(12):2882-2895, December 2007.

[15] J. Chen, H. Zhang, and J. Hu, "An efficiency security model of routing protocol in wireless sensor networks", In Proceedings of the 2nd Asia International Conference on Modeling and Simulation, 2008, pages 59-64, Washington, DC, USA, 2008, IEEE Computer Society.

[16] L. B. Olivera, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "Secleach- a random key distribution solution for securing clustered sensor networks", In Proceeding of the 5th IEEE International Symposium on Network Computing and Applications, pages 145-154, Washington, DC, USA, 2006, IEEE Computer Society.

[17] V. Pal Singh, A. S. AnandUkey, S. Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks" in International Journal of Computer Applications, Jan 2013.

[18]S.KaurSaini and M. Gupta, "Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks" in International Journal of Application or Innovation in Engineering & Management, May 2014.

[19] S. Magotra, K Kumar , "Detection of HELLO flood attack on LEACH protocol," *Advance Computing Conference(IACC), 2014 IEEE International* , vol., no., pp.193,198, 21-22 Feb. 2014.