iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3190

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Detection and Prevention of Hello Flood Attack on Leach Protocol

Vinod Kumar Sharma[1], Tushar Bhatia[2]
[1, 2]*Department of Computer Science, Faculty of Engineering and Technology, Tantia University*

Abstract: ***In wireless sensor networks various protocols are introduce to resolve the energy constraints. Leach (Low energy adaptive clustering hierarchical) is one of the oldest protocols which is based on concept of low energy. Security is considered an important issue in wireless sensor networks. As the various attacks are possible on Leach protocol such hello flood attack, selective forwarding attack and sinkhole attack etc. so many approaches are proposed to prevent it from those attacks which include cryptographic and non-cryptographic approaches. Cryptographic approaches used are found not to be very suitable as the complexity found in handling the keys.***
So non cryptographic approaches are introduces which are based on RSS (received signal strength), finding distance between nodes. These approaches are suitable up to some extent. In this paper we present the new non cryptographic approach i.e. by checking energy of cluster head. As we know when attacker starts dropping the packets its energy starts decreasing and it becomes the low energy node when compare with other nodes.
Keywords: LDK, WSN, LEACH, RSS.

I. INTRODUCTION

Leach (Low energy adaptive clustering hierarchical protocol) is already a highly secure protocol because the only node on which attacker can attack is cluster head node [1].
Various attacks are possible on leach protocol. Hello flood attack is found to be more dangerous as the attacker node sends the hello message to all nodes with powerful signals and nodes considers it as a cluster head and start sending packets to attacker [2]. In this paper firstly there is description of leach protocol and in second phase hello flood attack is described on leach protocol. In third phase the various non-cryptographic approaches for detection of hello flood attack is explained. In last section the proposed scheme i.e. energy of cluster head calculation is described.

II. LEACH (LOW ENERGY ADAPTIVE CLUSTERING HIERARCHICAL PROTOCOL)

LEACH is a cluster-based protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as cluster-heads and rotates this role to evenly distribute the energy load among the sensors in the network. In LEACH, the cluster-heads compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the BS in order to reduce the amount of information that must be transmitted to the BS [3]. Various attacks possible on LEACH In selective forwarding attack amid communication, nodes exchange information from one node to next. Amid transmission a few packets can be lost because of dropping by attacker node.
This sort of attack is known as selective forwarding attack [5]. In Sinkhole through traded off node, enemy draws in all the traffic from specific zone and makes a sink hole with foe at focus.
Traded off node draws in all traffic from its neighbours by revealing to them that it has most brief course to reach to the base station. This course is manufactured great course [6]. In black hole attack, the attacking node has more starting vitality than different nodes and it acts the cluster head in first round and in different rounds [12].
In the wake of getting all information from cluster individuals it don't send information to base station and decrease the aggregate sum of information to be transmitted.
In wormhole attack two attacker nodes make burrow which is utilized to make a dream that they are only one trust away and there by routing the packets to as neighbour nodes. At the point when passage is made effectively, they can drop the packets, replay, tempers the packets or selectively forward them [8]. In Sybil attack, various characters are utilized by attacker [11].
Its various characters are utilized to delude every other node. Malignant nodes send the false message to sensor node in system which debases the convey stockpiling and ways [9] [13].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

III. LITERATURE REVIEW

Various non-cryptographic methods are proposed to detect the hello flood attack.

A. RSS (Received Signal Strength) Based Approach

In this approach the identification is finished with the received signal strength. The nodes which are in scope of received signal are called as companion nodes and nodes which are not in scope of received signal strength are called as more unusual nodes. This approach works with AODV convention and finds the attacker node on the premise of received signal strength [14].

B. Distance Based Approach

In this approach the separation between the two nodes are discover by utilizing separation formulae. Before doing this base separation is settled and if computed separation is not as per evaluated settled separation then that node is considered as an attacker node [15].

C. Test Packet Based Approach

In this approach the guide nodes are presented. Test packets are utilized to recognize the attacker nodes. Amid cluster arrangement direct node is choosen along the cluster head. Manage nodes are randomoly choosen in each round amid cluster arrangement. Manage node has data about cluster head and if whatever other node tries to end up cluster head then guide dissiminate it to different nodes that it is attacker node [16].

D. LDK (Location Subordinate Key) Plot

In this plan there are three stages. One is pre-sending stage , second is initilization stage and third is communication stage. It expect that there is just requirement on their capacity of foes that it won't have the capacity to trade off a node for a little interim at first after the node is conveyed. This interim might be little. After this underlying interim an enemy may have the capacity to bargain any node.

IV. PROPOSED METHODOLOGY

Calculation of cluster head energy: Different techniques which are utilized to distinguish the hello flood attack on Leach convention have a few limitations.

As in RSS and distance based approach there is settled range and separation is considered, which is effective for most remote nodes. There are a few nodes that are closest to base station.

All things considered these approaches neglected to identify the attacker node. Our plan is productive to spare the information of node that lies close to base station.

In this approach recognition is completed on the premise of vitality of nodes. We expect that attacker node begins flooding as it enters in system. So its energy level will be low as contrast with different nodes.

A. Algorithm

1) Locate the nodes.
2) Flooding of hello message.
3) Calculate the RSS and distance .
4) Check if dist >THD and rssi> THR then nodes will not accept the hello message.
5) Else every node send test packet to get the energy level of cluster head.
6) Attacker node sends its energy level.
7) If average energy of cluster is more than energy of this node then not accept hello message and Alarm message is generated to alert other nodes note to join this attacker node.
8) Else nodes join cluster head.

We have implemented base scheme and compare it with our proposed scheme and found that our results are better than previous techniques. The previous approaches failed in that case where some nodes are nearest to base station.

B. Terminology

1) CH: Cluster Head

2) BS: Base Station

According to existing approaches nodes which are at distance more than threshold distance and whose RSS value is greater threshold RSS value then it is attacker node. But attacker can be present in distance less than threshold distance. As shown below attacker is present with in distance which is less than threshold distance value. Attacker node acts as cluster head for more than one cluster in its range. Here two clusters are in range of attacker for which attacker acts a cluster head.

TABLE I Simulation scenario using ns2

Parameter	Value
Channel Type	Wireless Channel
Max packet	500
Number of mobile nodes	50
X axis distance	1100
Y axis distance	1100
Initial Energy	50

C. Performance Parameters

1) Throughput: It is amount of information got at the objective node. On the off chance that throughput is all the more than its execution will be better.

2) Packet Delivery Ratio: It is characterized as ratio between number of information packets got to the quantity of information packets sent in the system. In the event that the attacker nodes are there in the system, then discovering PDR gets to be distinctly critical to break down as it chooses how much information is dropped in the system. Progressively the PDR, lesser the packet dropping and better the execution of the system.

3) Energy Consumption: if vitality utilized is less then execution is said to be better. The proposed scheme identifies the attacker nodes in the system and likewise utilized less vitality.

4) Routing Overhead: - It is ratio of number of routing packets sent in the system to the quantity of information packets got. On the off chance that the directing overhead is less then less routing is required to got the information in the system and execution of the system is better.

V. RESULTS

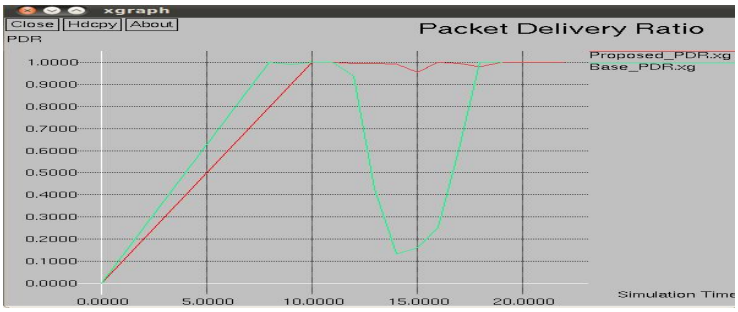


Fig. 1 PDR v/s Time

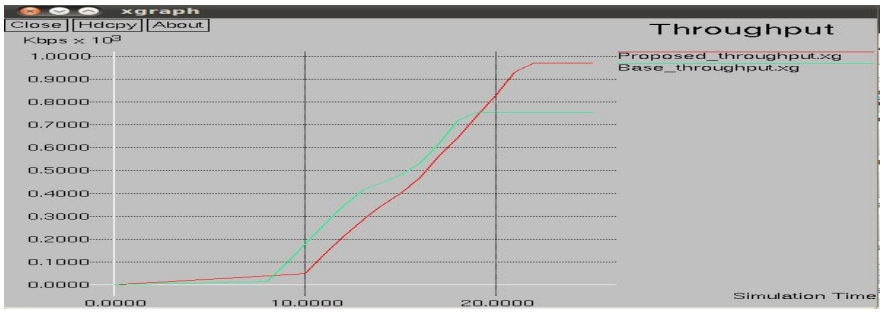


Fig. 2 Throughput v/s Time

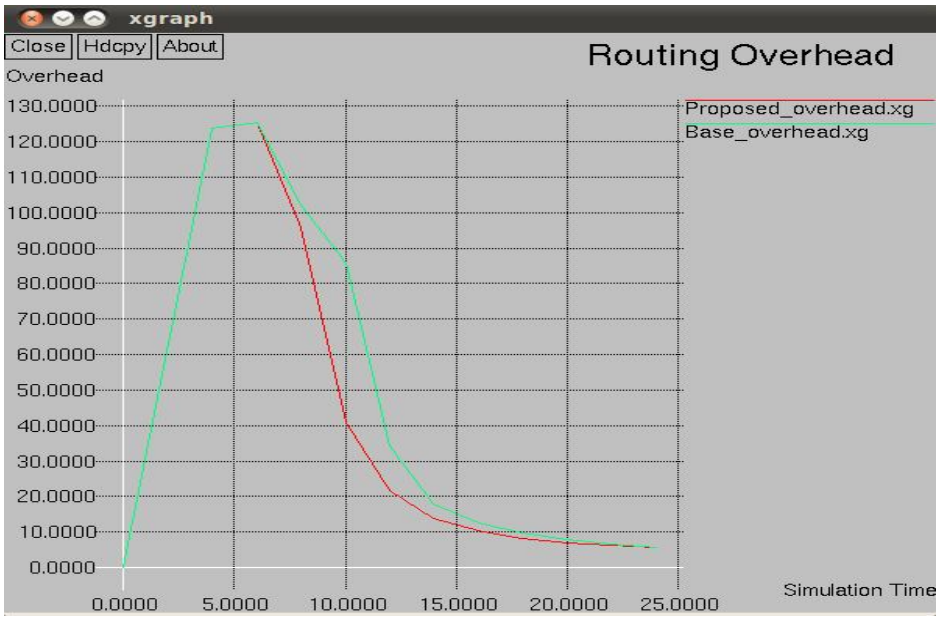


Fig. 3 Routing Overhead v/s Time

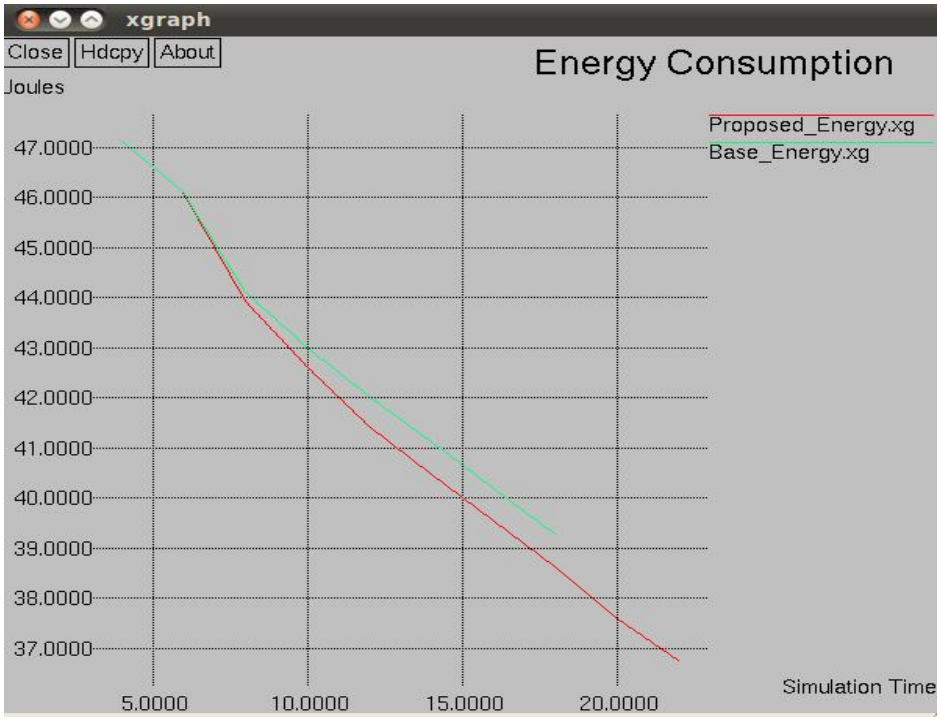


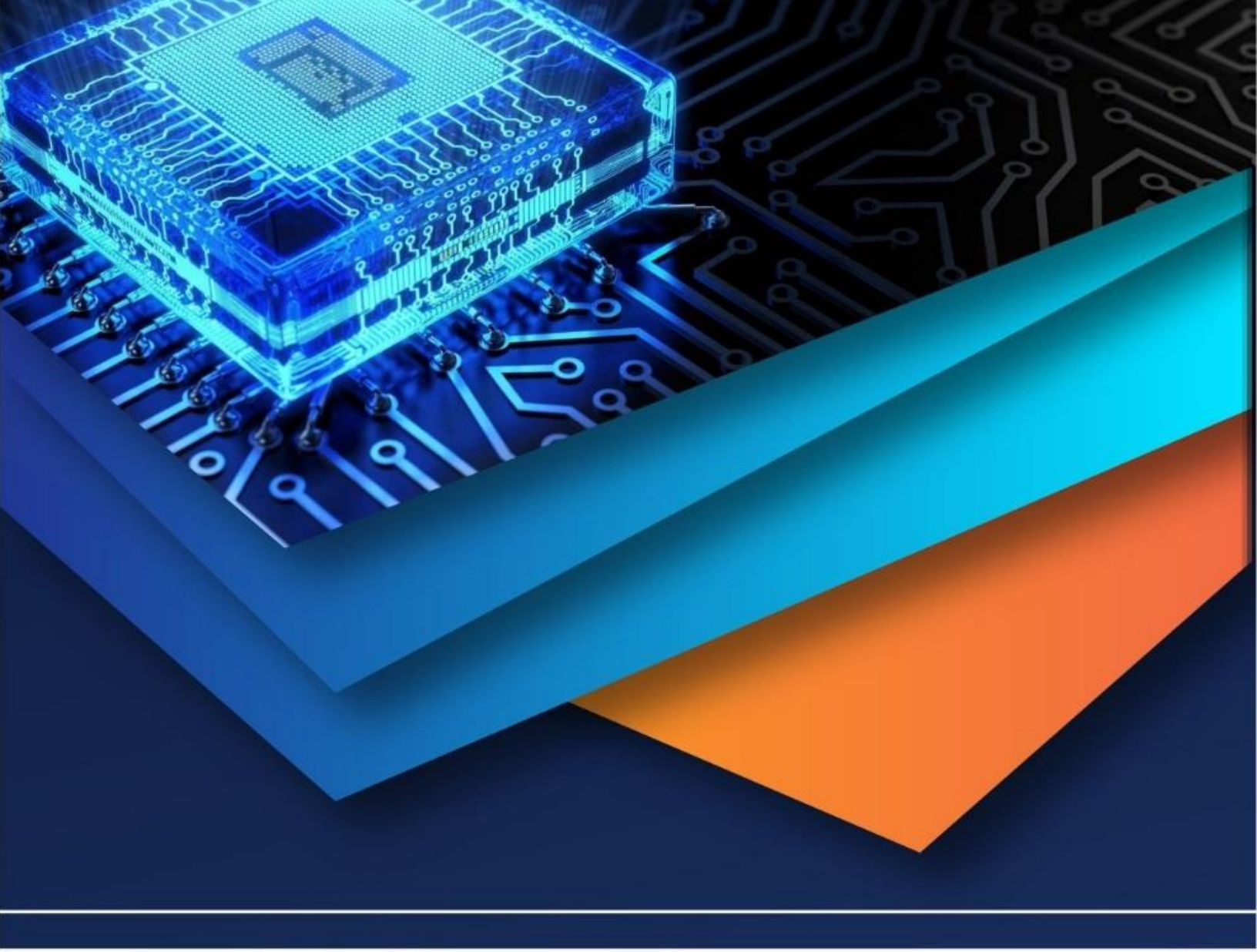
Fig. 4 Energy Consumption v/s Time

VI. CONCLUSIONS

Our new approach is more proficient in discovering attacker node and keep LEACH convention from hello attack. The past approach i.e. distance based recognition is neglected to provide information of that nodes which lies close to attacker node since it considers a settle separate. In the event that node sending hello flood message is found at more than limit separate then it is considered as attacker node. In any case, there is issue happens that if attacker node exists in limit remove then we can't discover attacker. Our approach is more appropriate all things considered. We have effectively executed this plan and our outcomes demonstrated that execution parameter is enhanced by utilizing our plan. We have additionally dispensed with the attacker from system. Future work should be possible to enhance some different parameters. In future acknowledgment of this idea should likewise be possible.

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.
[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 Leach protocol in 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.
[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] 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, pages 59-64, Washington, DC, USAIEEE Computer Society, 2008.
[14] 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.
[15] 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.
[16] 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.
[17] Mayur S and Ranjith H.D “Security enhancement on LEACH protocol from HELLO flood attack in WSN using LDK scheme” in International Journal of Innovative Research in science Engineering and technology, March 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY