ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Security Enhancment on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme

Mayur S[1], Ranjith H.D[2]

P.G. Student, Dept.of ECE, MITE College (Affiliated to VTU, Belagavi), Moodbidri, Karnataka, India[1]

Assistant Professor, Dept.of ECE, MITE College (Affiliated to VTU, Belagavi), Moodbidri, Karnataka, India[2]

ABSTRACT*:*In many wireless sensor network (WSN) applications uses hierarchical routing protocol for routing sensed data to the sink, among them LEACH is the first and most widely used hierarchical distributed clustering protocol in WSN. Security is important in wireless sensor networks as they are prone to various network threats and intrusion. In LEACH, Nodes decides to join a cluster head based on Received Signal Strength (RSS) of receiving HELLO packets from CHs making it vulnerable to HELLO Flood attack. Detection of HELLO Flood attack can be done either cryptographic approach which are less suitable in terms of memory and battery power or non-cryptographic which involves sending the test packet for detection which increases communication overhead as the energy required for transmission of the packet is far more than the energy required for processing/calculation. Based on these facts a non-cryptographic and cryptographic solution for detection HELLO Flood attack is proposed in this paper in which by considering RSS and distance calculation and by comparing both test packet approach is done hence the number of times the test packet is transmitted is greatly reduced and providing security by using location dependent key(LDK) management scheme where it involves loading random set of keys to the nodes prior to deployment, and also LDK doesn't require any knowledge of node deployment, eventually provides better connectivity and containment of node compromise.

KEYWORDS*:* wireless sensor network (WSN), LEACH, HELLO flood attack, Received Signal Strength(RSS), Cluster Head(CH), Security, Location Depended Key(LDK).

I. INTRODUCTION

Like living organisms a variety of modern devices and equipment's relies on the sensory data from the real world around it. These sensory data comes is provided by Wireless Sensor Networks (WSN) which consists of several tiny sensor nodes distributed over a large area to monitor physical or environmental conditions such as temperature, vibration, pressure, sound or motion and then collectively send these information to with one or more powerful central computing system called the base station or sink. All sensor nodes have limited power supply and have the capabilities of information sensing, data processing and wireless communication. Different routing protocols govern the movement of this information. Broadly the routing protocols can be classified as flat-based routing, hierarchical-based routing and location-based routing. LEACH (Low Energy Adaptive Clustering Hierarchy) 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. Sensor network protocols are quite simple and hence are very susceptible to attacks like Sinkhole attack, Selective forwarding, Sybil attack, Wormholes, HELLO flood attack, Acknowledgement spoofing, altering, replaying routing information. For example, Selective forwarding and HELLO flood attack affects networks with clustering based protocols like LEACH. In order to protect against various attacks which can be launched by adversaries therefore secure communication channels is crucial for these networks. Securing communication is possible through the use of encrypted keys.

DOI: 10.15680/IJIRSET.2015.0403040

II. RELATED WORK

Heinzelman, et.al [5] introduced a dynamic, hierarchical clustering protocol for sensor networks, called LEACH (LowEnergy Adaptive Clustering Hierarchy) which minimizes energy dissipation in sensor networks. It is very famous hierarchical routing algorithms for sensor networks which make clusters of the sensor nodes based on the received signal strength. Detection of HELLO flood attack can be cryptography based or non-cryptography based approach here non cryptographic approach way of detecting is RSS (received signal strength) Signal Strength based HELLO Flood Attack Detection and Prevention in Wireless Sensor Networks using AODV protocol.[8]. Geographical information based approach. Coordinate approach with distance calculation. Simple approach with lesser detection time TEST packet Communication overhead[1]. Cryptographical approach where sharing a secret key between any two nodes. Key generated during communication and only reachable node can decrypt [3]. Random key pre-distribution and pair wise key distribution approach for symmetric key cryptography and dynamic cluster formation for different types of attacks[4][10]. A widely used approach for key management is based on the use of symmetric algorithmswhich assume that nodes share prior context before the network operation begins. This prior context is generally in the form of an offline secret key pre-distribution before network deployment. Thus the symmetric keys are loaded on the sensors before deployment. These keys are then used by the nodes after the nodes are deployed in order to set up a secure communication infrastructure for use during the operation of the network. And also based on nodes being deployed with a random set of keys have been disclosed in references [12], [13], [14] and [15]. Several solutions based on pre-deployed keying have been proposed, including approaches based on the use of a global key shared by all nodes [16], approaches in which every node shares a unique key with the base station [17]. Another approach based on idea of leveraging the spatial diversity of sensor nodes in addition to the diversity due to randomly loaded keys depending on their location of sensor node which is done without knowing the knowledge about the deployment or location of sensors[11] .

III. LEACH

Low Energy Adaptive Clustering Hierarchy (LEACH) is a self-organizing, adaptive clustering protocol that utilizes randomization to balance the energy load among the deployed nodes in the network. LEACH assumes that all nodes start with uniform energy distribution and all nodes can communicate directly with the base station. It works in two rounds the set-up and the steady-state. The set-up round is responsible for forming clusters and cluster heads. During this round sensors vote for themselves to be cluster heads at any given time with certain probability based on their energy. Next the cluster head advertises their status to other sensors in the network. Accordingly each sensor node decides the cluster that it wants to belong to by selecting the cluster head that needs the least amount of communication energy. Finally all the nodes are arranged into clusters each cluster head creates a schedule for the nodes in its cluster to avoid collision. This results in the network structure that consists of a base station or sink cluster heads that communicate with the sink and sensor nodes each is recognized by a cluster and communicated with its cluster head that is a single hop to the sink. The steady-state phase is concerned with transferring the data from the sensors in the network to the base station or sink node. During this phase the cluster head collects the data from the sensors in its cluster. Once the data is collected from all nodes in the cluster than the cluster head locally aggregates the data in some way based on the application to remove the unreliable data. Later the cluster head transmits the collected data to the base station. LEACH uses the local processing to reduce global communication and also randomizes the rotation of cluster heads. Therefore it prolongs the network’s life time. On the other hand it is not applicable to large networks and time-critical applications. In addition to this the idea of dynamic clustering brings extra overhead. Furthermore the cluster heads send data to the sink through high power link which make these clusters consume their energy faster.

IV. ATTACKS ON LEACH

LEACH is very energy efficient routing protocol in WSN, because of its efficiency its network is vulnerable to some types of attacks. Some of the Attacks are as follows.

DOI: 10.15680/IJIRSET.2015.0403040

a. Selective forwarding attack

A node would always faithfully forward the received messages to its destination. However a malicious node would refuse to forward certain messages and simply drop them ensuring that the message doesn't reach the intended destination. This is called selective forwarding attack. A simple form of this attack is that the malicious node would act as a black-hole i.e. drops every message packet that arrives to it. But such nodes have the risk that the neighbouring nodes would consider them as dead nodes and would seek another route.Selective forwarding attacks are more effective when the attacker explicitly includes itself in the routing path of the data. Other ways of implementing selective forwarding is by jamming or causing collision on the transmitting information.

b. Sybil attack

In a Sybil Attack, the malicious node illegitimately can presents multiple identities to other nodes in the sensor networks. This is done either by creating new false identities or stealing identities of other nodes in the network. Sybil stack pose significant threats to location-based routing protocol. Therefore a single node may be used many times. This may cause many affects in the network such as increasing traffic, consuming energy, reducing network life time, packet dropping etc.

c. Hello flood attack

Many protocols require broadcasting HELLO packets by the sensor nodes to announce it to the neighboursthereby alerting them that it's within their transmission range. But an adversary could flood false HELLO packets. Hence the nodes would consider it to be within the range while the adversary may be situated far from it. In such scenarios nodes would be unnecessarily transmitting message and hence draining its energy. Protocols which depend upon exchange of location information between the nodes are likely to be targets of such attack.

V. LOCATION DEPENDENT KEY (LDK)

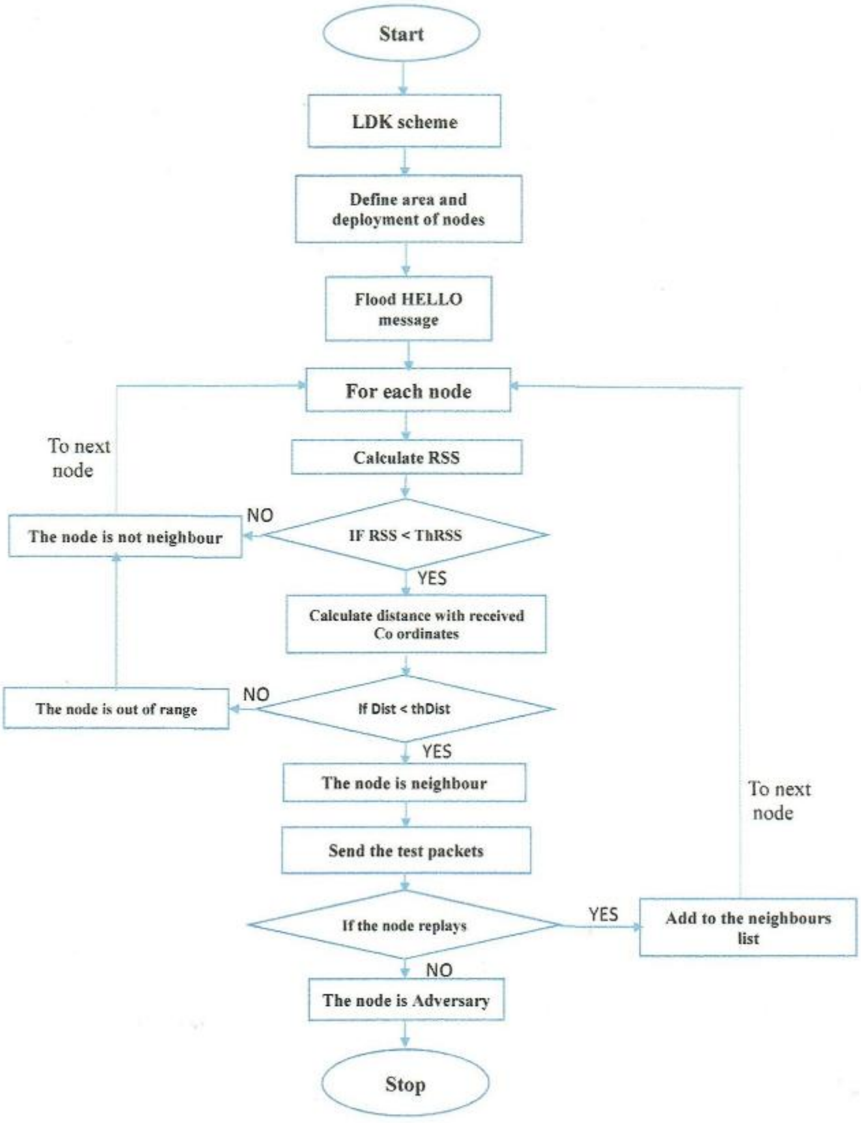
The network scenario that we consider consists of resource constrained sensor nodes. Nodes can be added to this network at any point in time. The threat model that we consider assumes that the adversaries have very strong capabilities. The only constraint on their capability is that the adversaries will not be able to compromise a node for a small interval initially after the node is deployed. This interval can be of the order of milliseconds and not more than a couple of seconds. After this initial interval an adversary might be able to compromise any node. Once the node is compromised, the adversary has access to all the keying material on the node. Following such node compromise the adversary is able to eavesdrop on all the links that have been secured using the compromised keying material. Here we assume two types of nodes namely the regular sensor nodes as well as special nodes called anchor nodes. The only extra capability that an anchor node needs to have is the ability to transmit at different power levels. In the LDK Scheme, Sn is the number of sensor nodes and Sp is the number of special nodes and the following three phases are executed in their lifetime. These are

- Pre-deployment phase
- Initialization phase
- Communication phase

During the Pre-deployment Phase, one trusted Central Key Distribution agency before deployment preloads the sensor and special nodes with information that would be required in the later phases for secure communication. After pre-loading the sensors with this information Sn sensor nodes and Sp special nodes are deployed in a uniform random fashion in the monitored area. Once the deployment of nodes has taken place initialization phase begins. In this phase special nodes start transmitting different beacon signals at different transmission ranges which is actually a different random number for different ranges encrypted with common key *K*. they first decrypt the number by using the common key *K* and then by using hashing function Hf()to generates a new set of keys. At the end of key initialization phase we are left with the set of keys that have the diversity based on their location and the initial random distribution. Than in last phase adjacent sensor nodes exchange information to establish trust (i.e. secure communication key) between them. The sensor node broadcasts the handshake message encrypted by a common key *K* to all its neighbours which includes its ID along with the identities of the keys preloaded in its memory which is decrypted by key *K*. After exchange of this information they can find out their common keys. Once the nodes have found their common keys they use their Ids to generate a common seed for Hashing functionis used to generate the secure pair-wise communication key which is used for encrypting communication between the sensor nodes. After which the whole process of key initialization takes place again which leads to next-generation of derived keys and a new pair-wise key. It has to be noted that the original key ring still remains with sensor node and is not deleted it is kept encrypted with common key K already loaded in the memory of sensor node and is done to have unique symmetric key between every pair of nodes in the network

VI. FLOW CHART OF PROPOSED METHOD

The below flow chart shows steps taken for the enhancement of security and detection analysis is done for the LEACH protocol against HELLO flood attacks.



DOI: 10.15680/IJIRSET.2015.0403040

VII. SIMULATION RESULTS

a. Simulation scenario

Matlab simulator has been used for simulation purpose. A square area of 100m × 100m is considered for simulation experiments. The network topology consists of 100 stationary nodes. Initially, the nodes are randomly placed in fixed position. 1% of total number of nodes may have high transmission, receiving and carrier sensing power, one node is a base station. Various parameters taken for simulation and their values are given in Table 1.

Table 1:parameters used for simulation

Parameter Used	Value
Field Dimensions(in meters)	100m x 100m

x and y Coordinates of the Sink	x=0.5*maxfield length
	y=0.5*max field width

Number of Nodes in the field (n)	100 + 1Base station
Optimal Election Probability of a node to become 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 (in meters)	1.5
Percentage of attacking nodes	Upto 1%
Radio range of nodes	Diameter of field*sqrt(log(n)/n)
Maximum number of rounds (r)	100

b. Results

Survey and Implementation of the flow chart has been conducted without the enhancement of security scheme i.e. detection of HELLO flood based on RSS, distance and test packets approaches are made and respected results have been show below.

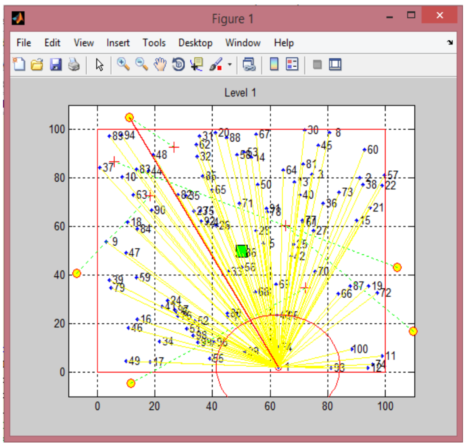


Fig 1:RSS based approach for 1st node.

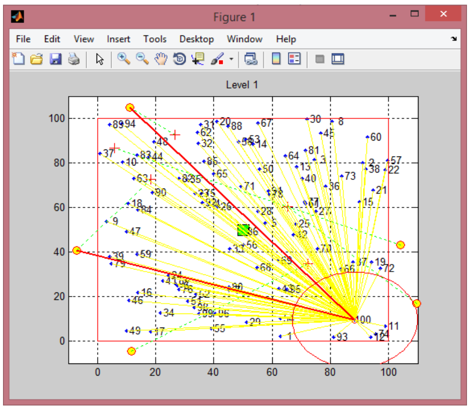
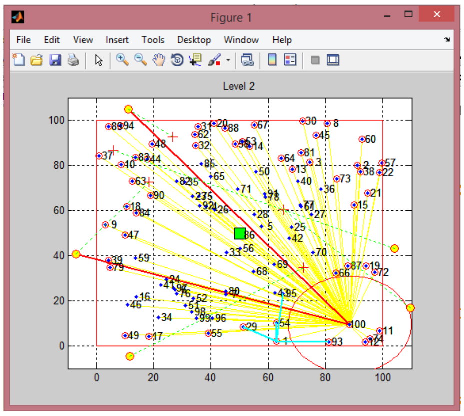


Fig 2: RSS based approch for 100th node

Infig 1&2 shows the calculation of RSS and compared with threshlod RSS (thRSS) of a node is done. if RSS<thRSS is friend orelse its adversary. This is done from 1stnode to 100th node.



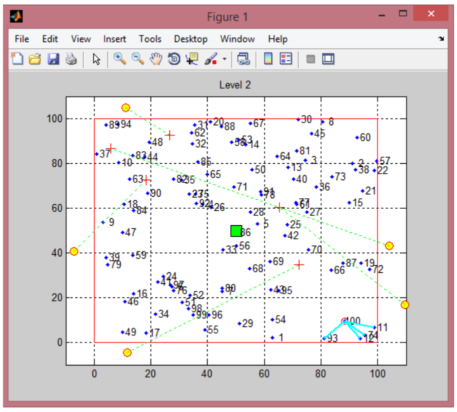


Fig 4:distance based approch for 100th node

In fig 3&4 shows distance based filtering from 1st node to 100th node by using distance equation.if dist < thdist is said to be friend otherwise stranger.

DOI: 10.15680/IJIRSET.2015.0403040

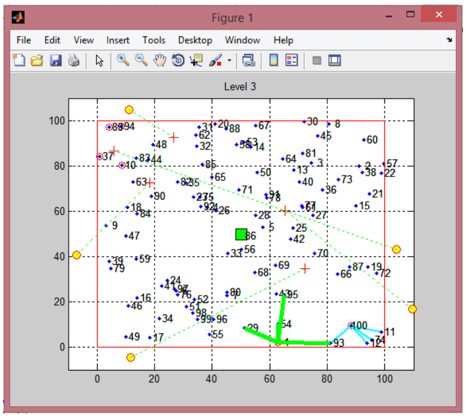


Fig 5: test packet based approch for 1st node

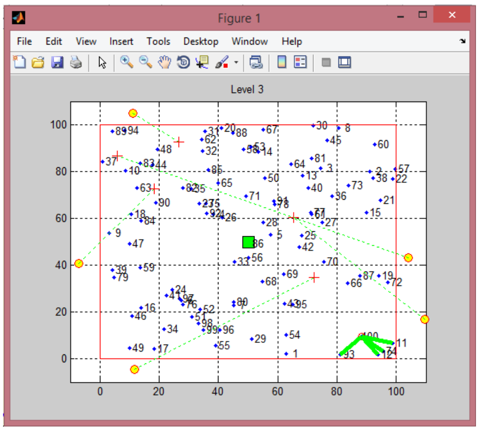


Fig 6: test paacket based approch for 100th node

In Fig 5&6 shows packet based filtering this is done by analysing the RSS and also distance coparison which intends to send the test packets to the receiving node shown in green line.this is done for all nodes.

VIII. CONCLUSION

In this proposed worka new security framework for HELLO Flood is implemented and the results are analyzed which proves that it requires less computational power, hence is suitable for sensor networks. The new algorithm is implemented in Matlab by modifying LEACH protocol. HELLO Flood attack is generated by making selected adversary nodes send HELLO message using high transmission power as compared to regular nodes. The proposed approach is effective in improving the performance of the network. It results in lesser detection time & energy for detection and also results in smooth functioning of LEACH Protocol even under HELLO Flood Attack with minimal communication overhead.

REFERENCES

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

[2] Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H.; "Energy-efficient communication protocol for wireless microsensor networks," System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on, vol. 2, pp.10 pp., 4-7 Jan. 2000.

[3] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks, vol. 1, 2003, pp. 293-315.

[4] 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

[5] Dr. Moh. Osama K., “HELLO Flood Counter Measure for Wireless Sensor Network,” International Journal of Computer Science andSecurity, vol. 2, 2007, pp-57-64.

[6] 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.

[7] Virendra Pal Aishwarya S. Sweta Jain, "Signal Strength based HELLOFlood Attack Detection and Prevention in Wireless Sensor Networks," International Journal of Computer Applications (0975 – 8887), Vol. 62, January 2013.

[8] A. V. Reddy R. Srinath and R. Srinivasan "Cluster based secure routing protocol for wsn," Third International Conference on Networking andServices, pp.45, Washington, DC, USA, 2007.

[9] M.Shankar; M.Sridar; M.Rajani; "Performance Evaluation of LEACH Protocol in Wireless Network," *InternationalJournal of Scientific & Engineering Research*, vol 3, Issue 1, January-2012.

[10] C.Wang K. Zhang and C.Wang "A secure routing protocol for cluster based wireless sensor networks"

[11] Farooq Anjum,"location dependent key management using random key-predistribution in sensor nodes "NJ 08854 ,2007.

[12] W. Du, J. Deng, Y. Han, and P Varsney. A pairwise key pre distribution system for wireless sensor networks. In In Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS 2003), pages 42-51, October 2003.

[13] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge In INFOCOM, 2004, April 2004.

[14] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili. A pairwise key pre-distribution system for wireless sensor networks In ACM Transactions on Information and System Security (TISSEC), 2005.

[15] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks, in Proceedings of the 9th ACM conference on Computer and Communications Security, pages 41-47, November 2002.

[16] S. Basagni, K. Herrin, D. Bruschi, and F. Rosti. Secure pebblenet. Proceedings of the 2001 ACM international Symposium on Mobile Ad Hoc Networking and Computing MobiHoc, 2001, October 2001.

[17] A Perrig, FR. Szewezyk, V. Wen, D. Culler, and J. D. Tygar Spins: Security protocols for sensor networks In Wireless Networks Journal (WINE), September 2002.