A MODIFIED CLUSTERED BASED ROUTING PROTOCOL TO SECURE WIRELESS SENSOR NETWORK FROM ADVERSARY NODE ATTACK

Swathi V[1], Vinaykumar T N[2]

[1]*PG (M.TECH) student, ECE Department, AMC Engineering College, Bangalore, Karnataka, India*
[2]*Assistant Professor, ECE Department, AMC Engineering College, Bangalore, Karnataka, India*

Abstract

Wireless Sensor Network (WSN) comprises of sensor nodes, which form a network by building connections wirelessly, to send detected information from source to destination. Routing Protocols are utilized to shape honest to goodness and littlest routes between a starting node (source) and ending node (destination). Numerous WSN applications use various hierarchical routing protocols. Low Energy Adaptive grouping (LEACH) is the first hierarchical routing protocols and it takes after the standard of forming cluster of nodes and picking a cluster head randomly among the nodes for inter cluster communication. This type of cluster head election leads to attack by adversary node, hence a Modified LEACH algorithm is proposed in this paper. The execution of LEACH and Modified LEACH is assessed utilizing distinctive performance measurements and Modified LEACH was discovered to be extremely compelling in enhancing overall performance of the WSN. MATLAB is made use of, to simulate the undertaking situation.

Keywords: *WSN, LEACH, Hierarchical protocols, Cluster Head.*

--***--

1. INTRODUCTION

The longing for communication, information transfer and connectivity without using wires has grown up a considerable measure as of late and this has prompted the advancement of wireless technology innovations in expansive scale. WSNs are a division of wireless communication/networking technology, which essentially underlines on connection of nodes without utilizing the dreary wired connections. The enthusiasm for the development and improvisation of WSNs are expanding dominatingly; this can be acknowledged by realizing what WSNs genuinely are, they are only a wireless association of vast number of little nodes which are called sensors. Because of wireless interface between nodes, every sensor node has its private battery for power necessities i.e. they are self controlled. The primary function of each sensor node is detecting, preparing and forwarding the information to next node or the sink node.

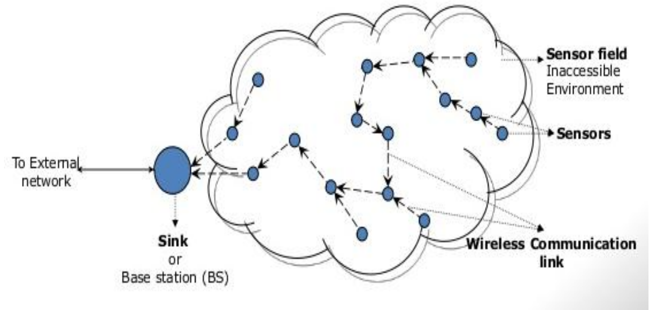

Fig-1: Basic WSN

The basic WSN is as shown in Fig-1. Data is forwarded from source to sink node through the wireless link. The formation of routes between source and destination node, data aggregation, data encapsulation etc, takes place as per designed protocols. There are several parameters to be looked after while designing a wireless network like, battery life, energy consumption, network lifetime, data security and so on since the interface is air usually, security of data is a matter of concern. The following sections give more detailed image of the proposed approach.

1.1 Problem Statement

Wireless sensor network systems are being utilized immensely due to their diminished energy utilization, lower delays and expanded system life time. The connection utilized for trade of information between sensors is wireless, aside from the aforementioned uses; WSN is inclined to security assaults in light of the fact that the interface between nodes is wireless connections. Wormhole, HELLO FLOOD attack, Sybil attack and Sinkhole are few security dangers to specify. Through these attacks, information robberies are becoming relentless in WSN. The information confidentiality issue and absence of security in clustering protocols of WSN have turn into the principle inspiration of this work.

Among existing routing techniques for WSN, Low Energy Adaptive Clustering Hierarchy (LEACH) is the exceedingly energy effective routing protocol, in this protocol Cluster Heads are chosen arbitrarily, as an aftereffect of which adversary nodes can act like Cluster Head and mischief information security. This condition is like Hello Flood attack. The current methodologies for giving security are generally not effective and are cryptographic, which needs high memory to spare authentication keys. This is the fundamental disadvantage in the current types of LEACH, which will be overcome in the proposed Modified LEACH.

In the following sections all the basic knowledge required for understanding the proposed work like components of WSN, design issues, types of routing protocols and simulation results are detailed.

2. COMPONENTS OF WSN

The WSNs are formed by consolidating few components together and making them work productively with mutual consent. The WSNs contain Sensors; which can have ability to move or stationary, protocols; to forward the information and working frameworks and operating systems through which entire WSNs can be controlled for elite operation. Aside from sensors other significant things needed for WSNs to work in a proficient way are suitable topologies and routing protocols. In this paper the fundamental region of concern is the routing protocols. Every constituent of WSN is clarified quickly in the advancing segment.

2.1 Sensors

The sensors basic work is to capture the real world analog signals, process them and modulate it in a form eligible for further processing. To do this a wide variety of sensors are available in numerous shapes and sizes, varying data rate, latency and operating bandwidths. A basic structure is shown in fig-2.

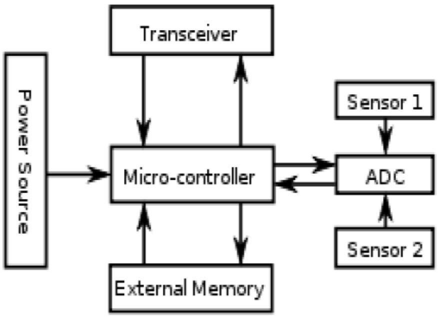

Fig-2: Sensor node basic architecture.

2.2 Operating Systems used in WSN

Operating system plays a huge role in monitoring all the functions and interfacing the hardware and software components of WSN. Generally used operating systems in WSNs are Nano-RK, TinyOS, Contiki, LiteOS etc.

2.3. Routing Protocols

Routing protocols are a set of rules and paths which have to be followed for efficient formation of routes in WSN. WSNs don't have an infrastructure like wired networks hence formulating routing protocols for WSNs is indeed a difficult task. Several routing protocols designed especially for WSNs have been designed and categorized as follows.

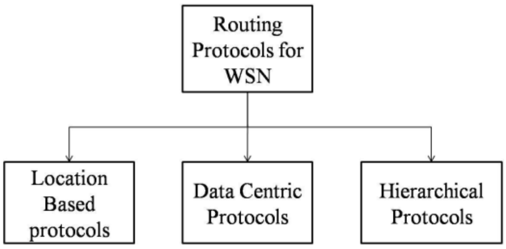

Fig-3: WSN routing protocol classification

The protocol which is of concern in this work is LEACH; it comes under Hierarchical routing protocol. Hierarchical protocol divides the network of sensors into several levels depending on the functions. Like a group of nodes will form first level and are called clusters in second level comes Cluster Head which is the main controlling leader node of the cluster as shown in fig 2.2. LEACH protocol works using this type of leveled architecture. the duty of cluster heads is to just forward the traffic whereas the nodes inside a cluster indulge in functions like data aggregation and processing, instead of wasting energy by all nodes by giving mores tasks to all nodes equally, in hierarchical routing the tasks are divided for different levels thus saving energy. But the major drawback in LEACH is data security which is the concern in this paper.

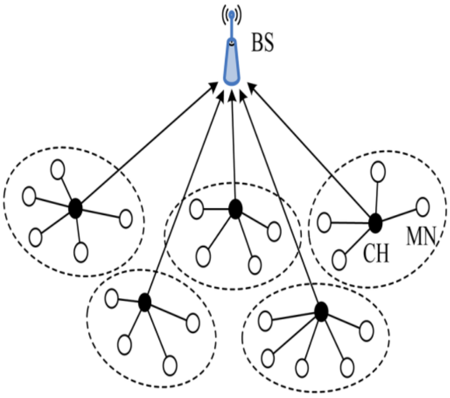

Fig-4: Hierarchical routing protocol, CH clusters Head, BS base station.

3. DESIGN ISSUES

Various design issues are noted while deploying a WSN, they are shown below,

- Production Cost: cost required for formation of network and sensors market cost should be reasonable.
- Energy consumption: since the sensors operate on stored battery power the energy consumption should be as low as possible.
- Reliability: the WSNs must be resistant to errors and faults and must be reliable.
- Scalability: WSNs must be scalable meaning they must be future proof and must be ready to adjust to advancements that takes place in future technologies.

- Security: this is the main design issue which is not being considered much, as all the efforts go into saving energy. Since the interface is wireless many attackers try to hack the network in various ways. Therefore essential measures to make the network safe must be taken.

4. EXISTING APPROACH (NORMAL LEACH) V/S PROPOSED APPROACH (MODIFIED LEACH)

The Existing normal LEACH has several drawbacks in terms of security. The cluster heads are elected randomly for every run of LEACH for every new routing a new cluster head is elected randomly depending on the receiving energy of the signaling packet as a result even if a third party adversary node exhibits itself as node sending high energy packets, it will be chosen as cluster head and the confidential data will pass through this third party cluster head node and we lose data.

The Modified LEACH is proposed to give immense change in security and increment in network lifetime of WSN. In the proposed methodology the Cluster Heads of the clusters are chosen considering the energy remaining in each node, furthermore it includes the distance threshold i.e. position of each node will be noted in the routing table as a result if a new adversary node tries to enter, it will not be entertained as its position is new and not recorded in routing table. A factor F is used to find cluster head a node which has highest value of F behaves as cluster head. The formulas used are shown below.

$$F = \frac{1}{d} + E_u$$

$$d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2}$$

$$E_u = E_c - [2E_{tx} + [E_{gen} \times d^{\delta}]]$$

where,

- F is a factor, involving distance and updated energy.
- d is the distance calculated by Euclidean formula in which x1, x2, y1, y2 are the respective x and y co-ordinates of a nodes.
- E_U is the updated energy of the node after communication.
- E_C is the Current Energy of the node.
- E_{tx} is the energy required for transmission of control packets.
- E_{gen} is the energy required for generation of control packets.
- δ is the attenuation factor within the range $0.1 < \delta < 1$.

This kind of choosing Cluster Head is utilized in the proposed methodology and the execution of Modified LEACH is assessed. Toward the end both normal LEACH and modified LEACH are contrasted with deference with respect to few network parameters like detection time to detect adversary node and energy consumption. The execution flow of the proposed approach is shown below in fig4.

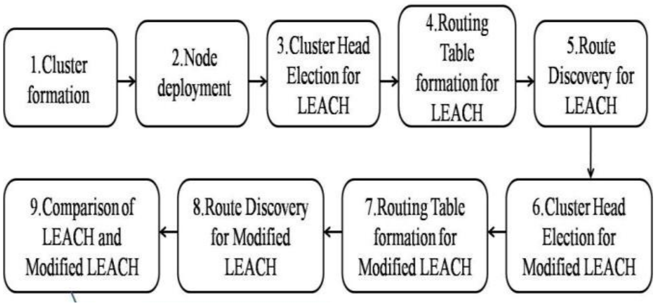
1.Cluster formation
2.Node deployment
3.Cluster Head Election for LEACH
4.Routing Table formation for LEACH
5.Route Discovery for LEACH
6.Cluster Head Election for Modified LEACH
7.Routing Table formation for Modified LEACH
8.Route Discovery for Modified LEACH
9.Comparison of LEACH and Modified LEACH

Fig-5: System process flow

5. SIMULATION RESULTS AND ANALYSIS

The results obtained by simulating the protocol are discussed. All the test cases for normal LEACH and Modified LEACH have been executed. MATLAB is the software used to simulate the project scenario.

Table-1: Simulation parameters considered

PARAMETERS	VALUES
Dimensions of area used	100mx100m
Number of clusters	4 clusters each of area 25mx25m
Total number of sensor nodes	40+1 adversary node
Number of nodes in each cluster	10+1 adversary node in cluster 3
Maximum energy of network	2000mj
Node ID's of cluster1	1,2,3,4,5,6,7,8,9,10
Node ID's of cluster2	11,12,13,14,15,16,17, 18,19,20
Node ID's of cluster3	21,22,23,24,25,26,27, 28,29,30 + 31 (adversary node)
Node ID's of cluster4	32,33,34,35,36,37,38, 39,40

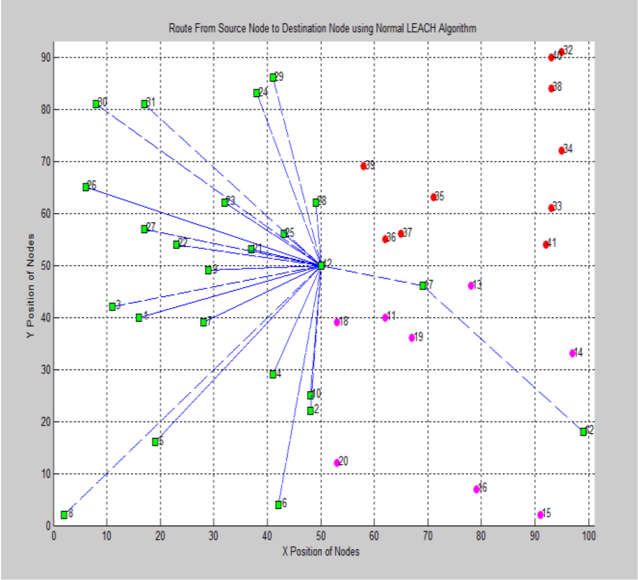

Fig-6: Figure showing source node to adversary node communication in normal LEACH

Fig-6 shows The routing graph obtained when a source node Id 12(cluster 2) which is a Normal non Cluster Head node and sink node Id 31(cluster 3) which is an adversary node were considered. When control packets were sent from source it reached the Cluster Head Id 17 of cluster 2 and then BS, the BS checks if sink node is present in cluster 2 which is "NO", then it scans cluster 1 and doesn't find sink, then it scans cluster 3 and finds sink there, even though it is an adversary node it is added to route and positive reply is given to source that route formation was successful.

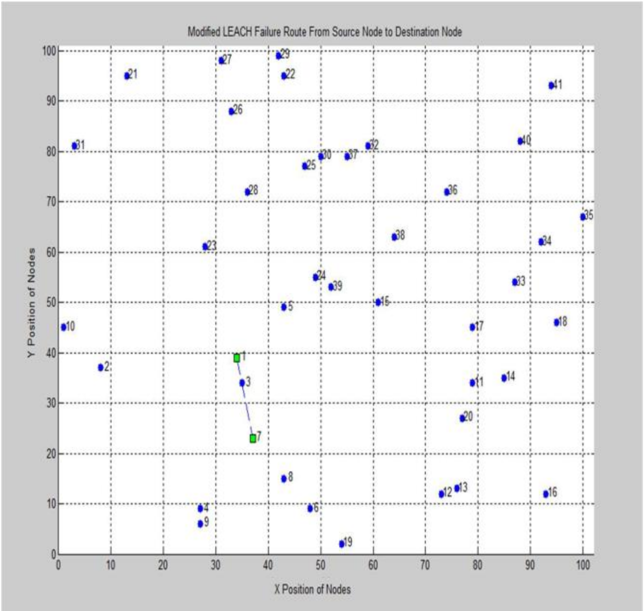

Fig-7: Figure showing source node to adversary node communication in modified LEACH

In this test case a normal node withId1 sends control a packet first to its Cluster Head Id 7 and as said earlier modified LEACH uses globally limited topology i.e. the routing table of Cluster Head 7 will have the node Id and related information of all the other Cluster Heads so node 7 checks its routing table and finds that node 31 is not an genuine node and its information is not present with any of the Cluster Heads therefore the routing stops at Cluster Head 7 itself as shown by taking only one hop. The Cluster Heads communicate directly with out need of BS. This is shown in Fig-7.

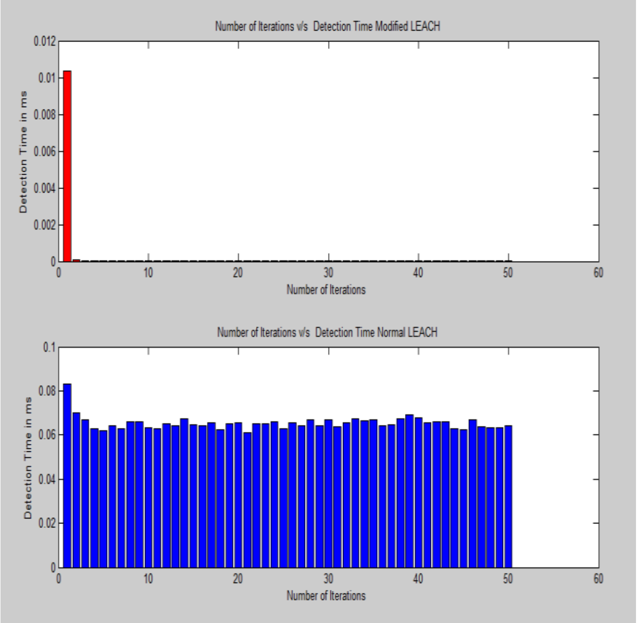

Fig-8: Detection time of normal LEACH v/s Modified LEACH.

Detection time is the time taken to detect the adversary sensor node it is seen that modified leach detects the adversary node in just 0.01ms (mille seconds) and once the adversary node is detected it is isolated and from the next iteration lesser than 0.002ms was taken to detect the adversary node. In the case of normal LEACH, in the first iteration 0.08ms was taken to detect the adversary node which is very much greater than that of modified LEACH and even after first iteration more than 0.06ms is taken to detect the adversary node.

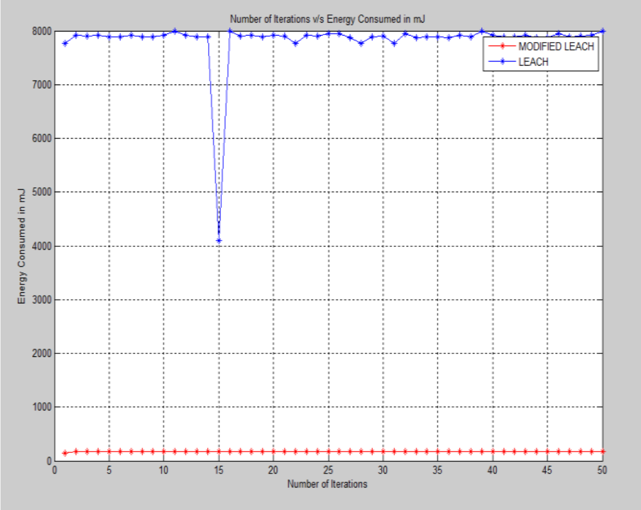

Fig-9: Energy consumption of normal LEACH v/s modified LEACH

The energy consumed in modified LEACH is very less and optimum between zeros to some hundreds of mjllijoules, But in the case of LEACH on an average maximum energy consumed by nodes is almost reaching 8000mj and minimum energy is consumed for 15th iteration which is 4000mj.

6. CONCLUSION

A new framework for security is formed in this project as security is the major concern in WSN. From the approach and upon analyzing results it can be seen that the modified algorithm for LEACH gives best performance. The performance of Normal LEACH and Modified LEACH was compared in terms of energy consumption, detection time. Modified LEACH gave better results in terms of all these parameters. MATLAB was used to simulate the scenario. The adversary node was introduced in which ever cluster as per the requirement and the reaction was studied for all the test cases. The proposed approach on LEACH successfully detects the Adversary node and avoids the involvement of adversary node in the communication. As a result a major security threat is avoided; performance and network life time are also increased.

ACKNOWLEDGEMENTS

The authors would like to extend their heartfelt gratitude to all the friends and faculty members of AMCEC institution for providing support for effective conduction of experiment.

REFERENCES

[1] Shikha Magotra, Krishna Kumar,"Detection of Hello Flood Attack on LEACH protocol",IEEE(IACC)2014.

[2] Jan M .Rabaey, M. Josie Ammer, Da Silva J.L., D. Patel and S. Roundy,"Pico radio supports adhoc ultra-low power wireless networking", Computer, vol.33, no.7, pp.4248, July2000.

[3] Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing" ,third Quarter 20051531-636x/05/IEEE circuits and system smagazine 19.

[4] S.Misraetal.(eds.), "Guide to Wireless Sensor Network" ,Computer Communications and Networks, DOI:10.1007/978-1-84882-218-44, Springer-Verlag London Limited 2009.

[5] Shio kumar Singh, MP Singh and DK Singh, "Routing Protocols in WSN-A Survey" ,IJCSES,NOV2010.

[6] CF Wang, J D Shih, B H Pan and T Y Wu, "A Network Lifetime Enhancement Method for Sink Relocation and its Analysis in WSN",IEEE sensorsjournal,June2014.

[7] W R Heinzelman, Anantha Chandrakasan and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks" ,Hawaii international conference,Jan2000.

[8] C. Dhivya Devi and B.Santhi, "Studies on Security Protocols in Wireless Sensor Networks" International Journal of Engineering and Technology (IJET), Vol 5 No1 Feb-Mar 2013.

[9] Holger Karl and Andreas Willig. "Protocols and Architectures for Wireless Sensor Networks "John Wiley & Sons, 08-Oct-2007.

[10] Daniele puccinelli and Martin Haenggi "Wireless Sensor Networks: Applications and Challenges of Ubiquitous sensing" IEEE Circuits and Systems Magazine, Third Quarter 2005.

[11] Shio Kumar Singh, M P Singh and D K Singh "Routing Protocols in Wireless Sensor Networks – A Survey" IJCSES, Vol.1, No.2, November 2010.

[12] Gurbhej Singh and Harneet Arora "Design and Architectural Issues in Wireless Sensor Networks" IJARCSSE, Volume 3, Issue 1, January 2013.

[13] Chu-Fu Wang, Jau-Der Shih, Bo-Han Pan, and Tin-Yu Wu," A Network Lifetime Enhancement Method for Sink Relocation and Its Analysis in Wireless Sensor Networks", IEEE sensors journal, VOL. 14, NO. 6, June 2014

[14] Samer A B Awwad, Chee K Ng, Nor K. Noordin and Mohd. Fadlee A. Rasid "Cluster Based Routing Protocol for Mobile Nodes in Wireless Sensor Network", IEEE, 2009

[15] Satwinder Kaur Saini and Mansi Gupta "Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks" , IJAIEM, Volume 3, Issue 5, May 2014

[16] Silicon labs "Evolution of Wireless Sensor Networks".

[17] Madhavi, S. and K. Duraiswamy, "Flooding Attacks Aware Secure Aodv", Journal of Computer Science, 9 (1): 105-113, 2013.

BIOGRAPHIES

Swathi V completed her BE in ECE from City Engineering College, Bangalore, Karnataka in 2013. She is pursuing 4th semester Master of Technology, Dept of ECE at AMC Engineering College, Bangalore, and Karnataka. Her areas of interest are Networking, Digital communication and Digital Electronics

Mr. Vinaykumar T N completed his M.Tech in ECE from Malnad Engineering College, Hassan, and Karnataka. He is working as Assistant Professor, Dept of ECE at AMC Engineering College, Bangalore, Karnataka. He has guided several students of BE and M.Tech in his teaching tenure. His area of interest is Wireless Sensor Networks