RLEC: Recursive Leach based Energy Conservation in WSN's using clustering technique

Prof. Raghavendra Reddy
School of C and IT, REVA UNIVERSITY
reddycs2004@gmail.com

Prof. G. C. Sathish
School of C and IT, REVA UNIVERSITY
sathish_gc@reva.edu.in

ABSTRACT-

Wireless sensor network turns out to be extremely prevalent however have exceptional qualities, for example, constrained battery, distributed deployment, and storage limitation will make the energy saving as a one of the major challenge. These systems exposed to DoS assaults such as greedy and jamming assaults. In such cases overall system performance are degraded. Here we are proposing one of the best solutions as a energy stabilizing solution to discover compromised nodes in wireless sensor networks. The suggested technique is established on the hierarchical clustering algorithm. It will helps us to select the suitable Controlled node (Cnode), that is able to analyze the information traffic in the given clusters and it was able to transfer the threatening massage if an unusual conduct is found. The projected system is changing as the Cnodes are intermittently chosen among common nodes on each cluster group. This will effect on enhanced energy saving solution. This is based on the distance among nodes and its associated CH in a given clusters.

Keywords: WSN, Clustering, Leach, Recursive Leach.

1. INTRODUCTION

Wireless Sensor Networks is a type of computer network. WSN comprises of huge amount of small-sized sensor nodes, and these are having limited battery power and are capable of wireless communications. Sensor nodes are considered as basic unit of the WSN. When a WSN is deployed in a sensing field, these sensor nodes will be responsible for sensing abnormal events (e.g., a fire in a forest) or for collecting the sensed data (temperature or humidity) of the environment. A sensor node consists of other components for analysis, and transmitting the gathered information they are: memory, power unit, controller unit, sensor unit, GPS, communication unit, and camera and so on.

Fig.1 shows the general WSN Architecture. The WSNs are mainly operates on batteries. Because of less energy storage capacity of a sensor battery, WSNs can usually remain operational only for a specific period of time. However, in many applications, such as earthquake, soil monitoring and glacial movement monitoring, due to the harshness of the environment, a long period of unattended operability is required. Although there has been a flourish of research efforts on prolonging the lifetime of WSNs, network lifetime remains a performance bottleneck of WSNs and one of the key factors that hinder their very large scale deployment. Due to their small size, the sensors having many limitations such as storage, processing capacity, energy and limited power source. WSNs must be designed to have built-in mechanism that helps the sensor network to reduce power consumption and increase the lifespan of network for end users. Energy saving is considered as one of the major issue while designing the WSN architecture.

Power for sensor nodes can get by using either batteries or in the form of solar cells. A node life period is usually depends on the battery lifetime. Nodes of the sensor network reduce the communication cost and energy cost by performing local processing. WSN provides wide range of applications like environment monitoring, fire detection, traffic detection, military applications etc.

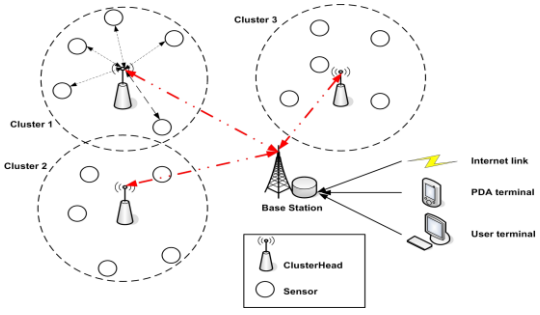

Fig.1 General WSN Architecture with clusters

Following are the various physical factors of nodes need to be considered for many WSNs applications:

- Light
- Sound
- Humidity
- Pressure
- Temperature

In WSN, more energy is used for receiving and transmitting of information as compare to the

processing and information gathering. While a lot of energy is wasted as to information interchanges, which is bring up underneath.

We believe that hierarchical clustering model is the one of the best and effective routing schema for WSN. The main reasons behind the clustering scheme are to make the network scalable and effective information routing within a network. The network lifetime, scaling of network, load balancing can be affected by clustering. Using this clustering scheme, communication bandwidth can be conserved; duplicate message transmissions can be reduced. Example, HEED and LEACH are reflected as best energy effective routing protocols. The cluster construction can plays very important rule in the reduction of cost, and this cost includes all the cost of topology establishment as well as preservation of the given systems. In wired systems, devices are influenced by pre-configured server that will support to form relations. However in WSN, this is not true, since nodes have inadequate memory, limited energy as well as limited processing power.

Designers of the WSNs must be considering the following key attributes:

1. Cost of Clustering

Various resources are required for creating and maintenance of the given network. The costs required for these resources are not related to the costs of data transfer or sensing of data.

2. Selection of Clusters and Clusterheads

Schema of clustering provides more assistances for WSNs. While planning for a specific application, designers must more focus on how clustering is formed. For a given application, the physical size of the cluster as well as number of nodes in that clusters will play very important role in its operation. This influence on the selection of CHs in the given application.

3. Real-Time Operation

Lifespan of data is considered as fundamental criterion in designing WSNs. applications like habitat monitoring we simply receive the data and is sufficient for analysis, because delay is not important here. But for military tracking application, real-time data gathering is very important and it is critical requirement also. While selecting clustering algorithms, we must need to pay more attention to clustering formation delay as well as the time required for cluster recovery mechanisms.

4. Synchronization

Energy capacity of the sensor node is the one of the primary limitations of the WSNs. Slotted transmission methods (like TDMA), allow nodes to be scheduled properly to minimize energy usage. This requires synchronization to setup as well as preserve the transmission strategy. Synchronization as well as scheduling can play very important role while considering a clustering scheme and these are effect on network lifetime as well as performance.

5. Data Aggregation

Data aggregation is the one of the major advantage of WSNs. In some network numerous nodes detecting comparative data. Data aggregation makes the difference among detected information and useful information. Processing task consumes more power as compare to communication task. Quantity of information that need to be sent in network should be reduced as much as possible. Generally all the clustering methods support data aggregation features. While choosing a clustering schema data aggregation should be considered properly. Data fusion combines the various undependable information to generate a additional precise signal and reducing the uncorrelated noise. By using data fusion or characterization calculation provincially, tremendous measures of vitality additions are accomplished.

6. Repair Mechanisms

WSNs suffer from intervention, node immobility, and node death Due to its nature. So that there is more chances of occurring of link failure. While selecting clustering patterns, it is very important to consider the mechanisms for link recovery as well as reliable data communication.

7. Nature of service

QoS requirements can play very important role in Wireless sensor network. A significant number of these prerequisites are application subordinate. We need to consider these metrics while selecting clustering methods. Implementations can change widely in terms of these metrics, so that the designing process should consider these aspects.

In DoS attack, the attacker interferes with the normal operation of the network and they may try to make the actual resources are not available for the required destination. DoS attack has becomes a very serious problem in network security.

2. LITERATURE SURVEY

There are many works carried out related to this project, some are discussed here.

According to authors [7], in WSNs very few security mechanisms are implemented, some of

them may be used in real deployments. As sensor nodes are having less number of resources so that security in WSNs is very hard. Exchange off in the middle of security and reasonableness should be considered. These frameworks incorporate distinctive sorts of data and correspondence innovation frameworks, for example, WSNs, to do control forms progressively. Careful protocol design is needed as well.

According to authors [10], WSN provides reliable monitoring for different environments. Communication protocols are having a large effect on the all energy dispersal of a given systems. Existing protocols are not ideal for sensor systems, so they proposed LEACH. It offers the versatility and power for a given systems. And it also provides data combination during data transmission to sink. LEACH performs static clustering method. High energy nodes have been chosen as a CH. For a given different instances of time, every node has become a bottleneck for getting information from the nodes in the cluster, getting the aggregating signal by fusing information, in addition to sending this signal towards sink.

The authors [11], suggest very good and sufficient criteria for the connectivity of CHs asymptotically almost surely and a tighter bound on various CHs in HEED.

According to authors [13], an ad hoc network can also be organized in the form of clusters. CHs acts as a virtual backbone and it can help to transmit the data from one node to another node. Past heuristics confined to one-hop clusters. We have shown least d-hop commanding set issue is NP-complete. Nodes are expected that they have non-deterministic portability design. When the heuristic termination condition is occurs, then a node can become either Cluster Head or else at best d remote hops which is far from its Cluster Heads. Important characteristics of the heuristic is that, it will re-select the same existing CHs which is already selected as one of the CH even if network topology changes. As it generates a small number of CHs compared to other heuristics so that solution becomes scalable. A low variance of cluster sizes will provides better load balancing among the CHs.

The authors [15], briefly discuss the operations of the clustering algorithms, and they compared various clustering schemes by considering their performance. The performance is analyzed in the form of power and quality aspects. They discussed various improvements to the existing clustering schemes. Here it provides a basis for research in clustering schemes for WSNs to the reader.

The authors [16], suggest the effects of heterogeneity of nodes, in the form of energy, in WSNs. Here some of the nodes become cluster-heads, and then aggregating and fusing of data can be done and then transmit it to sink. Here the sensors uniformly spread across the field, location of the sink node and area of the sensor field are known. But these networks are going to become unstable when the first node dies, specifically in the presence of node heterogeneity. In order to avoid this, SEP is used to draw out the time period before the demise of the leading sensor. These are very important for various applications where the feedback from the given network must be reliable.

The authors [18], suggest avoiding of DoS assaults in WSNs as a repetitive game intermediate an intrusion finder in addition to node of given network, in which few nodes behave maliciously. They use concept of game theory to identify the presence of nodes that agree to forward packets but fail to do so. This protocol categorizes different nodes by considering dynamic behavior.

The authors [19], focus on diminishing the utilization of force in remote small scale sensor systems. Hence, modification to LEACH is necessary. So that CHs selection algorithm can be done by using deterministic nature. They suggest 3 new criteria for defining a lifespan of sensor networks they are: FND (First Node Dies), HNA (Half of the Nodes Alive), and LND (Last Node Dies). Also, the measurements HNA, LND and FNA are used to define the lifespan of the sensor of a given network.

3. PROPOSED SYSTEM

LEACH:

In this paper we have proposed a mechanism based on clustering. Clustering of sensor nodes provides two major advantages: reduces the complexity of network and intra-cluster coordination which reduces the network traffic by establishing efficient communication schemes.

Low Energy Adaptive Clustering Hierarchy (LEACH) [7], [10], [11] protocol for sensor networks minimizes the energy dissipation in wireless sensor networks. The LEACH routing protocol is various leveled, probabilistic, conveyed one-hop protocol. It uses clustering method so as to circulate the energy utilization equally and to boost

the survival time of sensor devices in WSNs. All nodes perform the role of a CH in turns. Consequently the energy is adjusted equally. Following figure shows the LEACH network model.

Clusters are formed amongst the sensor devices in the systems and in each cluster a CH is selected. Every sensor devices in a cluster transfers their data to the CH and CHs thus send the information to the sink.

LEACH displays a few properties which empowers the conventions to decrease the energy utilization. Energy prerequisite in the LEACH is disseminated over all sensor devices.

The cluster administration is accomplished locally, which eliminates the requirements for worldwide system learning. Besides, information aggregation by the group likewise contributes significantly to energy preservation, as clusters are no more needed to send their data specifically to the base station.

The basic operations of LEACH are organized into two stages The setup stage consists of CH choice and cluster arrangement. And The steady state stage consists of information accumulation; aggregation and which is in turn send to sink.

Here we consider a control node named "Cnode" chosen to filter and analyze the messages sent to the CH of the cluster it belongs to. Therefore, each Cnode can detect a compromised node with an abnormal behavior. Compromised nodes [5], [6], [17], [18] are those with significant activity with suspicious behavior compared to normal nodes. It generates malicious traffic that has the capacity to flood the entire network by sending periodic packets created arbitrary, or by redounding messages or diverted data flows from its intended target. The aim of this study is to identify a new method for selecting control nodes that allows better network monitoring and also to determine the distance between each Cnode from the other nodes belonging to the subset formed. The first step of the method use Leach algorithm for constructing clusters. Afterwards for each obtained cluster, we reapplied leach algorithm recursively. The heads from the clusters obtained will be considered as control node.

LEACH is probably one of the easiest algorithms to apply to partition the network. It is a dynamical clustering and routing algorithm. It splits a set of nodes into several subsets, each containing a cluster head. This CH is the only node to assume the cost-expensive transmissions to the BS. Here is the LEACH detailed processing. Let P be the average percentage of clusters we want to get from our network at an instant t. LEACH is composed of cycles made of 1/P rounds. Each round r is organized as follows:

1. Node i can be computes the threshold T(i) as:

$$T(i) = \begin{cases} \dfrac{P}{1 - P.\left(r \bmod \frac{1}{P}\right)} & \text{if } i \text{ has not been CH yet} \\ 0 & \text{if } i \text{ has already been CH} \end{cases}$$

2. Once CH is identified, then it will broadcast its status to all other nodes. For this it uses CSMA MAC.

3. Other sensor devices will combine with clusters from which CH they receive the signal with most power. They inform same back to CH (using CSMA MAC protocol).

4. CH allocates time space to every sensor devices of a given cluster by using TDMA.

5. CH keeps listening for the results. Sensors will gather the data from its surrounding environment and send it to the intermediate node or sink. At the point when a node doesn't have any information to send, then it will switch to sleep mode, so that it will save the energy. This will avoid the Collision between the nodes from different clusters by using code division multiple access (CDMA) protocol.

6. CHs can perform the aggregation, compression of the collected data and then which is intern sent to the base station. Then data transmission can be done either direct, or multi-hopped (transmitting data by using intermediate CH).

7. Repeat stages 5 as well as 6 till all the cycles ends.

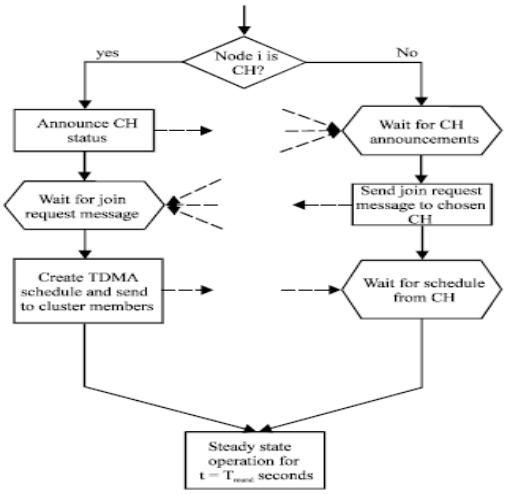

Fig.2 LEACH Process

Recursive -LEACH

Initially we apply the LEACH algorithm for finding first set of clusters, and then we are reapplying this LEACH algorithm recursively on each obtained cluster. One of the best examples of recursive LEACH algorithm is K-cluster. i.e. we are applying LEACH algorithm K times recursively as shown in below figure. This is called K-LEACH algorithm. Generally we consider K=2, because:

- Spare extra energy than using LEACH-1.
- Have a better partitioning of the system.

4. RESULT

Here we have used C# programming language for the purpose of study of LEACH and random clustering protocols. Every node originally has the capacity to send information to every other node or they may sent to BS directly. Initially the given cluster will include all the sensor nodes. Later during the simulation, each node may changes its association with one cluster to another cluster. The sensor nodes are arbitrarily scattered crossways the simulation area and the BS is situated outside the field. In all the simulation scenarios are examined by selecting different set of nodes with energy of 1000 joule for each node, were randomly scattered within a 735m×507m field.

Simulation process generates log files namely: ES_EnergyLog.csv and PS_EnergyLog.csv. We plot the graph by considering sum of 10, 20, 30 set of output values at a time from log file. A comparison of energy consumed by the network at various simulation intervals for random and recursive LEACH clustering model are shown in below graphs.

The performance of random clustering protocol is compared with the LEACH protocol. During simulation, remaining energy and average distance after close of simulation for stable time are determined. In this section result analysis consists of 2 parts:

A. Energy efficiency analysis

B. Average distance between CH and its neighbor nodes.

A] Energy Efficiency Analysis

Energy was and is an interesting issue. This factor affect directly the lifetime of the network. The simulation investigation demonstrated in the below snapshots indicates the aggregate energy remaining in the recursive and random protocol. Complete energy expended is the general energy utilized by the sensor devices as a part of the WSN information stream amid the recreation time.

Fig. 3 shows the average energy remaining is estimated by varying the number of nodes as 40, 80,120,160,200,240. Number of nodes: 240.

Fig. 4 shows the average energy remaining is estimated by varying the number of nodes as 50,100,150,200,250,300,350. No. of nodes: 350.

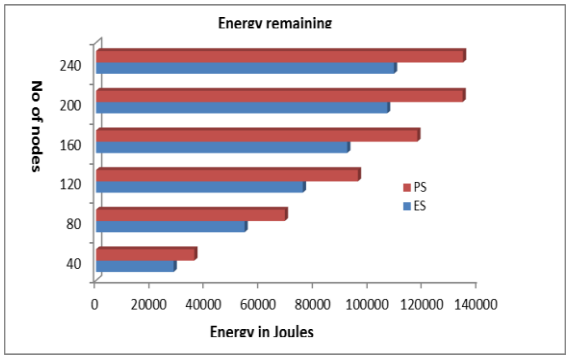

Fig. 3 Shows simulation result with 240 nodes

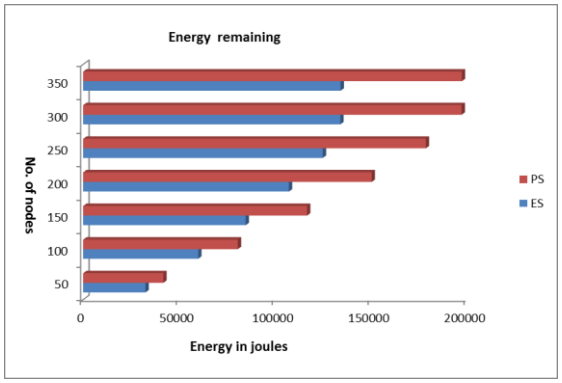

Fig. 4 Shows simulation result with 240 nodes

From the above graphs, the remaining energy in a given network in a LEACH is very high as equated to random protocol. It can be observed that the energy consumed by the WSN is comparatively less for the LEACH protocol. In Recursive LEACH protocol, all the CH's do not communicate with the BS directly and hence resulting in reduced energy consumption. From the simulations, we can say that LEACH can achieve decreases in energy scattering when contrasted with customary directing conventions. Furthermore, LEACH will convey energy scattering uniformly among all the sensor nodes in given WSN. So that system lifetime for the networks is doubled.

B] Average distance between CH and its neighbor nodes.

Following figure 5 shows comparison graph of Average distance calculation by varying the number of nodes 80, 100, 120 respectively.

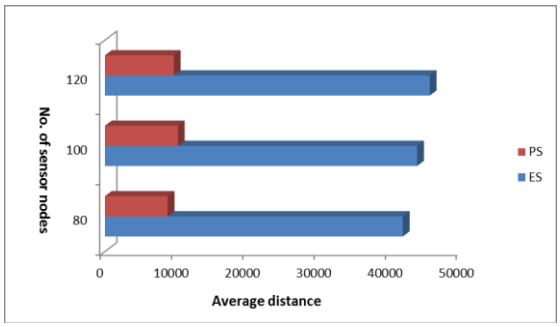

Fig. 5 Comparison graph of Average distance.

From the above graph we can say that average distance with respect to random clustering is very high as compare to the proposed recursive LEACH method.

5. CONCLUSION

Here in this paper we suggest a clustering based technique to improve the security vulnerability and energy efficiency of node in wireless sensor network. This technique is based on LEACH clustering algorithm which is an efficient clustering algorithm. Here we applied recursive LEACH for each level of already obtained cluster nodes. The energy weight of being a CH is equitably dispersed amongst the devices. Improve the detection of DoS attacks with less computation cost. The efficiency of detecting attack is improved by using LEACH recursively.

We compared LEACH system with the random based cluster model. The experiment analysis shows that the proposed model achieves better security and good energy efficiency and increase the network lifetime and it also reduce average distance of Cnodes. In future we will further analyze the simulation model and check how it performs on other parameter like network throughput, latency, and delivery ratio etc. and we will also like to compare this model with other type of clustering model.

6. REFERENCES

[1] B. Yahya and J. Ben-Othman. Energy Efficient and QoS Aware Medium Access Control for Wireless Sensor Networks. Wiley (Concurrency and Computation: Practice and Experience), 22:1252–1266, July 2010.
[2] B. Yahya and J. Ben-Othman. Towards a Classification of Energy- Aware MAC protocols for Wireless Sensor Networks. Wiley Wireless Communications and Mobile Computing (WCMC),), 9:1572–1607, Feb 2009.
[3] Ben-Othman J. Yahya B. Mokdad, L. and S. Diagne. Performance Evaluation tools for QoS MAC Protocol for Wireless Sensor Networks Ad Hoc Networks. Elseiver Adhoc Networks, In Press.
[4] J. Ben-Othman and B. Yahya. Energy Efficient and QoS based Routing Protocol for Wireless Sensor Networks. Elseiver Journal of Parallel and Distributed Computing (JPDC)), 70(8):1572–1607, August 2010.
[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. ACM.
[6] A. Hamieh and J. Ben-Othman. Detection of jamming attacks in wireless ad hoc networks using error distribution. IEEE International Conference on Communications,(ICC), June 2009.
[7] M. Shankar, M. Sridar, and M. Rajani. Performance evaluation of leach protocol in wireless network. 3, January 2012.
[8] G. Hsin Lai and C.-M. Chen. Detecting denial of service attacks in sensor networks. Journal of Computers, 4(18), January 2008.
[9] S. Fouchal, Q. Monnet, D. Mansouri, L. Mokdad, and M. Ioualalen. A clustering method for wireless sensors networks.In Computers and Communications (ISCC), 2012 IEEE Symposium on, pages 000888– 000892.IEEE, 2012.
[10] W. R. Heinzelman et al. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the IEEE Hawaii international conference on system sciences, 2000.
[11] O. Younis and S. Fahmy. HEED: a hybrid, energy-efficient distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mobile Comput., 3(4):366–379, 2004.
[12] D. Baker and A. Ephremides. The architectural organization of a mobile radio network via a distributed algorithm. IEEE Transactions on Communications, 29(11):1694–1701, 1981.
[13] A. D. Amis, R. Prakash, T. H. P. Vuong, and D. T. Huynh. Max-min dcluster formation in wireless ad hoc networks. In Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, volume 1, pages 32–41. IEEE, 2000.
[14] Lehsaini M. Diffusion et couverture basees sur le clustering dans les reseaux de capteurs : application a la domotique. Phd. thesis, University of Franche-Comte, 2009.
[15] A. A. Abbasi and M. Younis. A survey on clustering algorithms for wireless sensor networks. Computer Communications, 30:2826–2841, June 2007.
[16] G. Smaragdakis, I. Matta, and A. Bestavros. Sep: A stable election protocol for clustered heterogeneous wireless sensor networks. Technical report, Boston University Computer Science Department, 2004.
[17] G.H. Lai, C.M. Chen, and B. Jeng. Dos detection in cluster-based sensor networks. In Proceedings of the Fourth IASTED International Conference on Communication, Network and Information Security, pages 109–115. ACTA Press, 2007.
[18] A. Agah and S.K. Das.Preventing dos attacks in wireless sensor networks: A repeated game theory approach. International Journal of Network Security, 5(2):145–153, 2007.
[19] M. J. Handy, M. Haase, and D. Timmerman. Low energy adaptive clustering hierarchy with deterministic cluster-head selection.In Proceedings of the 4th IEEE Conference on Mobile and Wireless Communications Networks, Stockholm, Sweden, 2002.