IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 2, Ver. I (Mar-Apr. 2014), PP 06-15
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Evaluation of Stability and Optimum Energy Consumption In Wireless Sensor Network

A.Kalyan[1],K. Chaitanya[2], B.N.S.Chaitanya[3] and R. Divya kanti[4]
1,2,3: (B.Tech) 4: Asst.Professor
Department of Electronics and Communication Engineering Lendi Institute Of Engineering And Technology

Abstract: *Sensor network consists of tiny sensors and actuators with general purpose computing elements to cooperatively monitor physical or environmental conditions such as temperature, pressure, etc. Wireless Sensor Networks are uniquely characterized by properties like limited power they can harvest or store, dynamic network topology, large scale of deployment. To increase the network lifetime we used energy efficient communication protocol known as Low Energy Adaptive Clustering Hierarchy (LEACH). Low Energy Adaptive Clustering Hierarchy (LEACH) is an energy-efficient hierarchical-based routing protocol. Our prime focus was on the analysis of LEACH based upon parameter network lifetime reducing the power consumption of wireless sensor networks. The performance of the proposed protocol has been examined and evaluated with the MATLAB. Nodes would send the packets to the near by cluster head in its cluster. As a result of simulation, we have confirmed that our proposed algorithm shows the better performance in terms of lifetime. Also if we use a simulation mode of large number of nodes ,we expect that our protocol will clearly make network lifetime much longer.*

I. Introduction

Like living organisms, a variety of modern devices and equipments 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 to monitor physical or environmental conditions, such as temperature, vibration, pressure, sound or motion, and then collectively send these information to a central computing system, called the base station or sink. Different routing protocols govern the movement of this information. Broadly the routing protocols can be classified as at-based routing, hierarchical-based routing, and location-based routing. LEACH (Low Energy Adaptive Clustering Hierarchy) is a hierarchical-based routing protocol which use random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. A sensor network can be made scalable by assembling the sensor nodes into groups i.e. clusters. Every cluster has a leader, often referred to as the clusterhead(CH). A CH may be elected by the sensors in a cluster or pre assigned by the network designer. The cluster membership may be fixed or variable. A number of clustering algorithms have been specifically designed for WSNs for scalability and efficient communication. The concept of cluster based routing is also utilized to perform energy routing in WSNs. In a hierarchical architecture, higher energy nodes (cluster heads) can be used to process and send the information while low energy nodes can be used to perform the sensing.

Heinzelman introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH arranges the nodes in the network into small clusters and chooses one of them as the cluster-head. Node first senses its target and then sends the relevant information to its cluster-head. Then the cluster head aggregates and compresses the information received from all the nodes and sends it to the base station. The nodes chosen as the cluster head drain out more energy as compared to the other nodes as it is required to send data to the base station which may be far located. Hence LEACH uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. After a number of simulations by the author, it was found that only 5% of the total number of nodes needs to act as the cluster-heads. TDMA/CDMA MAC is used to reduce intercluster and intra-cluster collisions. This protocol is used were a constant monitoring by the sensor nodes are required as data collection is centralized (at the base station) and is performed periodically.

1.2 AIM OF THE PROJECT

Our work is inspired and motivated by a number of research efforts. Due to the space limitation, we only briefly review the work closely related to our proposal. In networks with abundant resources, such as the Internet, link quality is usually estimated by sending passive probing packets using Internal Gateway Routing Protocol. The aim of our work is to evaluate the link in wireless sensor network by electing energy efficient protocol called Low Energy Adaptive Clustering Hierarchy(LEACH) i.e., study of transfer of information from node(source) to base station(destination) in an efficient way to increase the network lifetime. The wireless local area network (e.g., IEEE 802.11) and sensor networks share similar qualitative communication patterns [1]. The link qualities of wireless ad hoc and local networks are studied in [5], [04], which demonstrate that shortest path routing may not yield a satisfactory performance, due to the variance of communication links. However, these work have not explored the research issues in estimating link quality that varies over time and locations, especially given the unique characteristics of sensor networks (e.g., high node deployment density) and restrictions on energy. Links with high packet loss and link asymmetry have been studied in [6], [04] However, the number of messages generated for link quality estimation has a direct impact on the expected lifetime of the networks. For instance, a typical sensor network may last for about one month if each sensor node broadcasts a beacon message every 30 seconds, but the network lifetime may be increased to more than ten months if each sensor node broadcasts.

II. Methodology

Link evaluation involves two phases:-
1. Setup phase
2. Steady phase
In the setup phase, the clusters are formed and a cluster-head (CH) is chosen for each cluster. While in the steady phase, data is sensed and sent to the central base station.

2.1 WIRELESS SENSOR NETWORK

Sensor networks refers to a heterogeneous system consisting of multiple detection stations called sensor nodes with a communications infrastructure intended to monitor and record conditions at diverse locations. Sensor nodes, also known as mote, are small, lightweight and portable devices equipped with a transducer, microcomputer, transceiver, and power source. The transducer produces electrical signals based on the sensed physical phenomena. The microcomputer processes and stores the sensed information. The transceiver receives instructions from the base station/central computing system and sends data to it. Each sensor nodes derives its energy usually from a battery or any other embedded form of energy harvesting. The size of the sensor nodes vary from that of a shoebox to that of a minute sand-particle. Similarly their cost also varies from hundreds of dollars to a few pennies. Size and cost constraints result in corresponding constraints on energy, memory, computational speed and communications band width.

Wireless Sensor Networks are characterized by :
1) Limited power they can harvest or store
2) Ability to cope with node failures
3) Heterogeneity of nodes
4) Large scale of deployment
5) Mobility of nodes
6) Communication failures
7) Dynamic network topology
8) Ability to withstand harsh environmental conditions

NODE, CLUSTERHEAD AND CLUSTERING:

Sensor nodes are small, lightweight and portable devices equipped with a transducer, microcontroller, transceiver, and power source. A clusterhead is a node within a cluster that is responsible for routing of packets to other clusters/base station and data aggregation.Data aggregation refers to removal of redundancy bits. The process of grouping similar nodes is called clustering.

2.3 TYPES OF ROUTING PROTOCOLS

Depending upon the network structure, routing in wireless sensor networks can be classified as atbased routing, hierarchical-based routing, and location-based routing. In at-based routing, all the nodes in the topology are assigned the same functionality or role. In hierarchical-based routing, nodes are assigned different roles or functionalities according to the hierarchy. In location-based routing, routing path for the data is decided according to the sensor nodes position in the field. Depending on how the source finds a route to the destination, routing protocols can be classified into three categories, namely, proactive, reactive, and hybrid protocols. In proactive protocols, all routes are computed before they are actually needed. In reactive protocols, routes are computed only when they are needed. While hybrid protocols are combination of the above two ideas. Depending on the protocol operation, routing protocols can be classified into multipath based, query-based, negotiation-based, QoS-based, or coherent-based routing. In multipath-based routing, multiple paths are used to enhance network performance i.e. fault tolerance, balance energy consumption, energy-efficiency and reliability. In query-based routing, destination nodes propagate a query for data. Usually these queries are described in natural language or high-level query language

2.4 TYPES OF RESOURCE HETEROGENITY

There are three common types of resource heterogeneity in sensor nodes: computational heterogeneity, link heterogeneity, and energy heterogeneity.

Computational heterogeneity means that the heterogeneous node has a more powerful microprocessor, and more memory, than the normal node. With the powerful computational resources ,the heterogeneous nodes can provide complex data processing and longer term storage.

Link heterogeneity means that the heterogeneous node has high bandwidth and long distance network transceiver than the normal node. Link heterogeneity can provide a more reliable data transmission.

Energy heterogeneity means that the heterogeneous node is line powered, or its battery is replaceable. Among above three types of resource heterogeneity, the most important heterogeneity is the energy heterogeneity because both computational heterogeneity and link heterogeneity will consume more energy resource.

Impact of Heterogeneity on Wireless Sensor Networks

If we place some heterogeneous nodes in sensor network it shows the following benefits:

Response time: Computational heterogeneity can decrease the processing latency and link heterogeneity can decrease the waiting time, hence response time is decreased.

Lifetime: The average energy consumption will be less in heterogeneous sensor networks for forwarding a packet from the normal nodes to the sink, hence life time is increased. Further, it is also known that if in a network, heterogeneity is used properly then the response of the network is tripled and the network's lifetime can be increased by 5fold

2.5 PERFORMANCE MEASURES

Some performance measures that are used to evaluate the performance of clustering protocols are listed below.

Network lifetime: It is the time interval from the start of operation (of the sensor network) until the death of the first alive node.

Number of cluster heads per round: Instantaneous measure reflects the number of nodes which would send directly to the sink, information aggregated from their cluster members.

Number of nodes per round: This instantaneous measure reflects the total number of nodes and that of each type that has not yet expended all of their energy.

Throughput: This includes the total rate of data sent over the network, the rate of data sent from cluster heads to the sink as well as the rate of data sent from the nodes to their cluster heads.

2.6 ATTACKS ON ROUTING PROTOCOLS

Since the sensor network protocols are quite simple, they are susceptible to a number of network layer attacks.

A few of these attacks are:

1) Spoofed, altered, or replayed information
2) Selective forwarding
3) Sinkhole attack
4) HELLO flood attack
5) Sybil attack
6) Wormholes

Spoofed, Altered, Or Replayed Information:

The most direct and most effective way of attacking any routing protocol is to target the information being exchanged between the nodes. By altering or replaying routing information, adversaries can achieve a number of motives like creating routing loops, extending or shortening routing paths, attracting or repelling network traffic, increasing end-to-end latency, partitioning the network, generating false error messages, etc.

1) Selective Forwarding:

An honest node would always faithfully forward 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 neighboring nodes would consider them as dead nodes and would seek another route. So, adversaries adapt a more subtle form i.e. intelligently forward only certain messages. Hence, the risk of getting caught is minimized. 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.

2) Sinkhole Attack

In sinkhole attack, a compromised node is made to look very attractive to the surrounding nodes with respect to the routing algorithm. (For example, adversary can advertise a very high quality routing path and hence divert the path through it.)Hence a metaphorical sinkhole is created with the adversary at the center. And now since the routing path is diverted through this adversary node, severe damages can be done by it. Sinkhole is a very effective way of implementing selective forwarding. Altering or replaying the routing information can also be done by the adversary. The reason why sensor networks are highly susceptible to sinkhole attack is because all message packets being transmitted have a single ultimate destination, the base station. A Compromised node only needs to provide a single high quality route to the base station and hence, effecting severe damages.

3) Hello Flood Attack

Many protocols require broadcasting HELLO packets by the sensor nodes to announce it to the neighbors, thereby alerting them that its 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

.

4) Sybil Attack

In Sybil attack, a single node presents multiple identities to the other nodes in the network. Routes believed to be passing through multiple nodes would actually be passing through the same adversary node and hence thereby running the risk of an endless loop. Sybil stack pose significant threats to location-based routing protocol. Protocols which require exchange of location information would be adversely affected as adversary nodes ,using Sybil attack, would be exchanging multiple sets of coordinates, rather than a single set of coordinates and hence can
be in more than one place at a time.

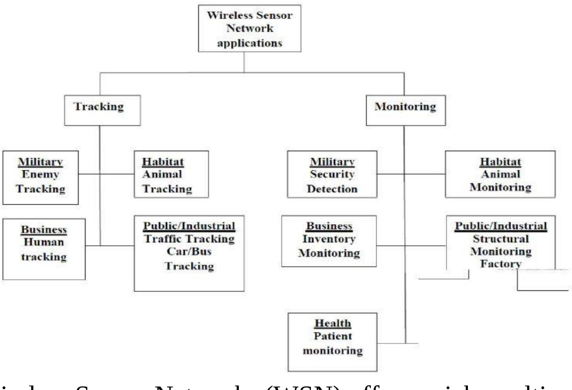
5) Wormholes

In wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different path. Wormhole attack normally involves two distant malicious nodes, misleading others to understate the distance between them by relaying packets along an outer channel, which is available only to the attacker. An attacker situated close the base-station may completely disrupt the routing by creating a well-placed wormhole. This attack is likely to be used in combination with eavesdropping or selective forwarding. Detecting Wormhole attack is difficult when used along with Sybil attack. Wormholes can be intelligently used to create sinkholes.

2.7 APPLICATION OF WIRELESS SENSOR NETWORK

Wireless Sensor Networks (WSN) offers a rich, multi-disciplinary area of research, in which a number of tools and concepts can be applied to address a whole diverse set of applications. Sensor networks may consist of many different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar.

FIGURE:


Wireless Sensor Network applications
Tracking
Monitoring
Military Enemy Tracking
Habitat Animal Tracking
Business Human tracking
Public/Industrial Traffic Tracking Car/Bus Tracking
Military Security Detection
Habitat Animal Monitoring
Business Inventory Monitoring
Public/Industrial Structural Monitoring Factory
Health Patient monitoring

Applications are as follows Wireless Sensor Networks (WSN) offers a rich, multi number of tools and concepts can be applied to address a whole diverse set of applications. Sensor networks may consist of many different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to m sensor nodes can be put for continuous sensing, location sensing, motion sensing and event detection. The idea of micro many new application areas.

2.7.1 Area Monitoring Applications

Area monitoring is a very common application of WSNs. In area monitoring, the WSN is deployed over a region where some physical activity or phenomenon is to be monitored. When the sensors detect the event being monitored (sound, vibration), the event is re-ported to the base station, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can be deployed in security systems to detect motion of the unwanted, traffic control system to detect the presence of high-speed vehicles. Also WSNs finds huge application in military area for battlefield surveillance, monitoring friendly forces, equipment and ammunition, reconnaissance of opposing forces and terrain, targeting and battle damage assessment.

2.7.2 Environmental Applications

A few environmental applications of sensor networks include forest fire detection, green-house monitoring, landslide detection, air pollution detection and flood detection. They can also be used for tracking the movement of insects, birds and small animals, planetary exploration, monitoring conditions that affect crops and livestock and facilitating irrigation. External air quality monitoring needs the use of precise wireless sensors, rain & wind resistant solutions as well as energy reaping methods to assure extensive liberty to machine that will likely have tough access.

2.7.3 Health Applications

Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, monitoring the movements and internal processes of insects or other small animals, monitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.

2.7.4 Industrial Applications

WSNs are now widely used in industries, for example in machinery condition-based maintenance. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors. They can also be used to measure and monitor the water levels within all ground wells.

III. Low Energy Adaptive Clustering Hierarchy (Leach)

Hence LEACH uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. After a number of simulations by the author, it was found that only 5% of the total number of nodes needs to act as the cluster-heads. TDMA/CDMA MAC is used to reduce intercluster and intra-cluster collisions. This protocol is used were a constant monitoring by the sensor nodes are required as data collection is centralized (at the base station) and is performed periodically. Then the cluster head aggregates and compresses the information received from all the nodes and sends it to the base station. The nodes chosen as the cluster head drain out more energy as compared to the other nodes as it is required to send data to the base station which may be far located

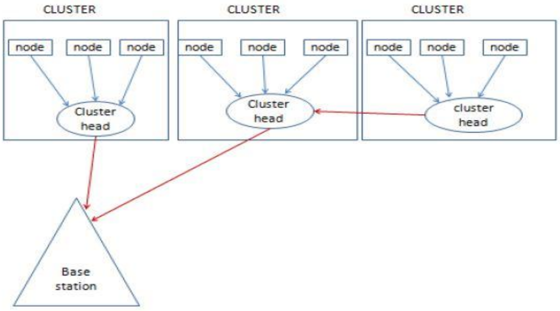


Figure 2.Block diagram of transmission of packets

3.2 Operation

LEACH operations can be divided into two phases:-

1. Setup phase
2. Steady phase

In the setup phase, the clusters are formed and a cluster-head (CH) is chosen for each cluster.
While in the steady phase, data is sensed and sent to the central base station.The steady phase is longer than the setup phase. This is done in order to minimize the overhead cost.

1. Setup phase :-

During the setup phase, a predetermined fraction of nodes, p, choose themselves as cluster-heads. This is done according to a threshold value, T(n). The threshold value depends upon the desired percentage to become a cluster-head- p, the current
round r, and the set of nodes that have not become the cluster-head in the last 1/p rounds, which is denoted by G. The formulae is as follows :

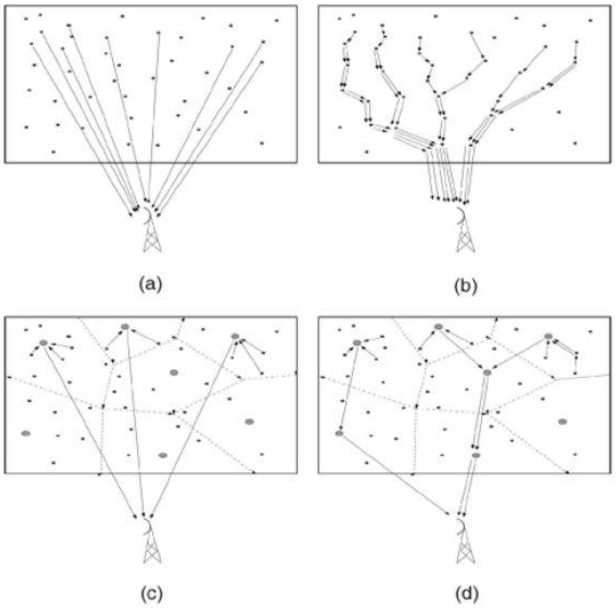
T(n) = p/(1-((R*MODULUS(1/P))) n € G

T(n)=0 n€ G

Every node wanting to be the cluster-head chooses a value, between 0 and 1. If this random number is less than the threshold value, T(n), then the node becomes the cluster-head for the current round. Then each elected CH broadcasts an advertisement message to the rest of the nodes in the network to invite them to join their clusters. Based upon the strength of the advertisement signal, the non-cluster head nodes decide to join the clusters. The non-cluster head nodes then informs their respective cluster-heads that they will be under their cluster by sending an acknowledgement message. After receiving the acknowledgement message, depending upon the number of nodes under their cluster and the type of information required by the system (in which the WSN is setup), the cluster-heads creates a TDMA schedule and assigns each node a time slot in which it can transmit the sensed data. The TDMA schedule is broadcasted to all the cluster-members. If the size of any cluster becomes too large, the cluster-head may choose another cluster head for its cluster. The cluster-head chosen for the current round cannot again become the cluster-head until all the other nodes in the network haven’t become the cluster head.

IV. Steady phase :-

During the steady phase, the sensor nodes i.e. the non-cluster head nodes starts sensing data and sends it to their cluster-head according to the TDMA schedule. The cluster head node, after
receiving data from all the member nodes, aggregates it and then sends it to the base-station. After a certain time, which is determined a priori, the network again goes back into the
setup phase and new cluster-heads are chosen. Each cluster communicates using different CDMA codes in order to reduce interference from nodes belonging to other clusters.



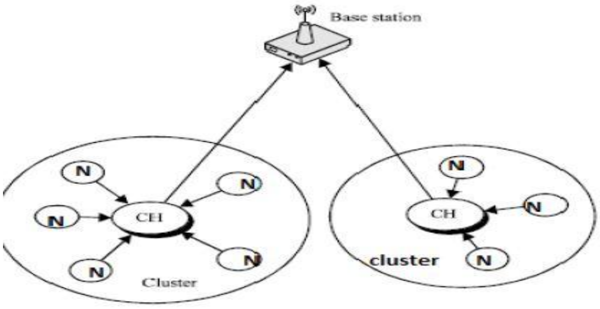


Figure4.clustering

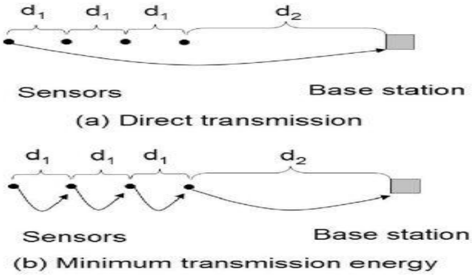
ATTACKS

LEACH protocol is difficult to attack as compared to the more conventional multi-hop protocols. In the conventional multi-hop protocols, the nodes around the base station are more attractive to compromise. Whereas in LEACH, the CHs are the only node that directly communicate with the base station. The location of these CHs can be anywhere in the network irrespective of the base station. And more over the CHs are periodically randomly changed. So spotting these CHs is very difficult for the adversary. However, because it is a cluster-based protocol, relying fundamentally on the CHs for data aggregation and routing, attacks involving CHs are the most damaging. If any adversary nodes become a CH, then it can facilitate attacks like Sybil attack, HELLO flood attack and selective forwarding. The intruder can broadcast a powerful advertisement to all the nodes in the network and hence, every node is likely to choose the adversary as the cluster-head. The adversary can then selectively forward information to the base-station or modify or dump it. Key management is an effective method to improve network security. These schemes typically assume that a node interacts with a quite static set of neighbors and that most of its neighborhood is discovered right after the deployment. However, clusters in LEACH are formed dynamically (at random) and periodically, which changes interactions among the nodes and requires that any node needs to be ready to join any CH at any time. There are a number of standard key distribution schemes but most of them are ill suited to WSNs: for example, public key based distribution requires a lot of processing; global keying is quite vulnerable; and, complete pair wise keying requires a huge memory [13]. And since WSNs consists of sensors with small computational power and negligible memory they are unable to incorporate these security mechanisms.

ASSUMPTIONS

LEACH protocol takes into a number of assumptions which may create a lot of problemsin the real-time systems. A few of these assumptions are as follows:

1) All nodes can transmit with enough power to reach the base station if needed.
2) Each node has computational power to support different MAC protocols.
3) Nodes always have data to send.
4) Nodes located close to each other have correlated data.
5) All nodes begin with the same amount of energy capacity in each election round, assuming that being a CH consumes approximately the same amount of energy for each node.



(a) Direct transmission

(b) Minimum transmission energy

Figure 5: Comparison between direct transmission and minimum transmission energy hopping. energy hopping using a case that there are only 4 collinear sensors and one base station. In figure 2(a), the radio transmission energy used to transmit message from the leftmost sensor to the base station is ε ^{2}*ampk*(3*d*1 + *d*2)2. In figure 2(b), the radio transmission energy used to transmit message from the leftmost sensor to the base station is ε^{2}*ampk*(3*d*2 1 + *d*2 2), which is a lot less than the direct transmission. Figure 2 uses a very simple settings. To apply minimum transmission hop-ping method to sensor network shown in figure 1 is not as straightforward. There are two problems. One is how to find a minimum transmission energy hoping route and the other is how to keep track of energy speed on transmitting and routing.

IMPLEMENTATION

ALGORITHM

The algorithm for the Low Energy Adaptive Clustering Hierarchy (LEACH) implemented is :

Setup phase :

1. CN=> r

2 .If r < T(n) then, CH = CN else, goto step1

3. CH => G : id(CH) , join adv

4. A(i) CH(j) : id(A(i)) , id(CH(j)) , join req

5. CH(j) A(i) : id(CH(j)) , < t(i) , id(A(i)) >

Steady phase :

1. A(i) CH(j) : id(A(i)) , id(CH(j)) , info

2. CH BS : id(CH) , id(BS) , aggr info

The various symbols used here are :

CN : candidate node to become the cluster head.

r : randomvariable(0 < r < 1)

T(n) : threshold value

CH : cluster head

G : all nodes in the network

id : identification number

join adv : advertisement to join the cluster

A : normal node

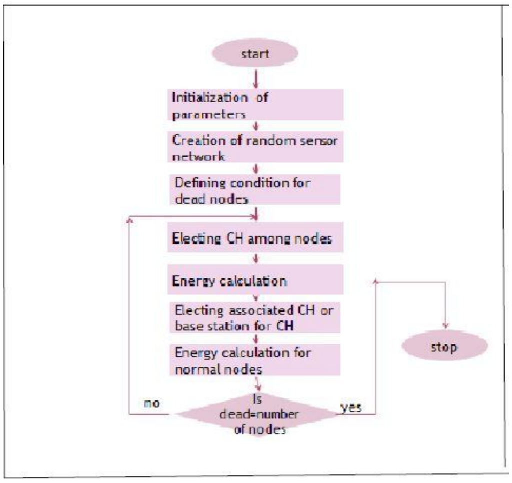
join adv : request to join the cluster

t : time-slot to send the sensed data

=> : broadcast

: unicast

FLOW CHART


start
Initialization of parameters
Creation of random sensor network
Defining condition for dead nodes
Electing CH among nodes
Energy calculation
Electing associated CH or base station for CH
Energy calculation for normal nodes
Is dead=number of nodes
no
yes
stop

4.3 NETWORK CONFIGURATION

Here we have considered a heterogeneous network. A heterogeneous network is one in which all the nodes doesn't have equal energy. Let us assume that m fraction of the nodes

have times more energy than the other nodes and the total number of nodes be n. They are called as advanced nodes. Therefore,

Number of normal nodes = (1-m) * n

Energy per normal node = e0

Number of advanced nodes = m * n

Energy per advanced node = e0 * (1 + α)

Hence the total energy of the network is equal to ((1-m) x n) x e0 + (m x n) x (e0 x(1 + α)

The network configuration for the first simulation is as follows :

Field size = 100m * 100m

Number of nodes = 100

Energy per node = 1 joules

Election probability for a node to become the cluster-head = 0.15

Message size = 3000bits

5% of the nodes have double energy.

A few of the above parameters were changed for the required analysis.

The energy spend by any transmitter to send a L-bit message over a distance d is, where Eelec is the amount of energy spent to run the circuit(of receiver or sender) for 1bit data, Efs and Emp are the transmitter constants and depend upon the type of transmitter used and, do=sqrt(Efs/Emp); The above network configuration, formulae and values of various parameters were referred from [11] A few of the nodes in the network were compromised and selective forwarding was done. The cluster-heads were the nodes that were compromised. Now, the malicious nodes would only forward only certain messages and dump the other. Hence the network throughput is expected to decrease and also abnormal characteristics of the network lifetime.

V. Results

After a number of simulations, the following results were gathered. Based upon these results, a detailed analysis is presented.

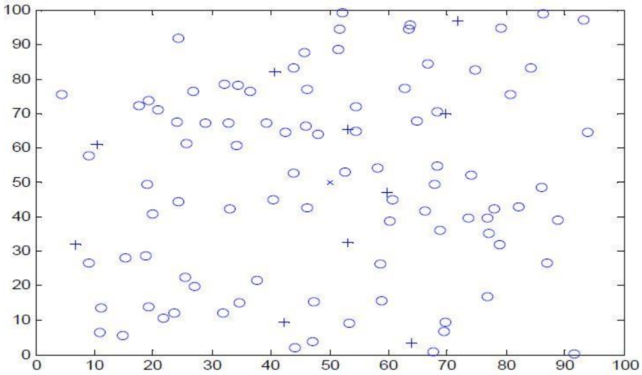


FIGURE 6: FIELD DISTRIBUTION-1

Figure-1 show the initial field distribution of the network, where LEACH protocol is implemented. A 100m*100m field is taken and nodes are randomly placed in it. The sink/base station, which is denoted by a x, is placed at the center of the field (50, 50).Placing the base station at the center is convenient so that no node finds it out of itstransmission range. Here, the advanced nodes are shown by a plus symbol (+) and the normal nodes by a circle (o) [11].

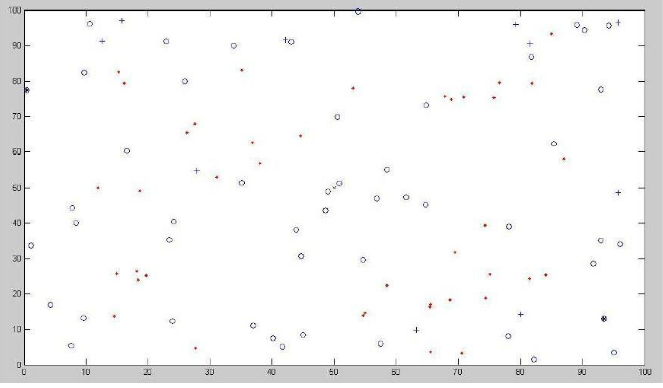


FIGURE 7: FIELD DISTRIBUTION-2

After a few rounds, a few of the nodes drains out all their energy. Such dead nodes are shown by the dot symbol (**.**) [11]. Such scenario is shown in Figure-7. The reason why some of the nodes drained out their energy before the others is because these nodes would have become the clusterheads in the initial rounds of the data transmission. Since the cluster-heads have to aggregate the data and send it to the base station, which might be located far from the base-station, the clusterheads use up their energy faster as compared to the non-cluster head nodes.

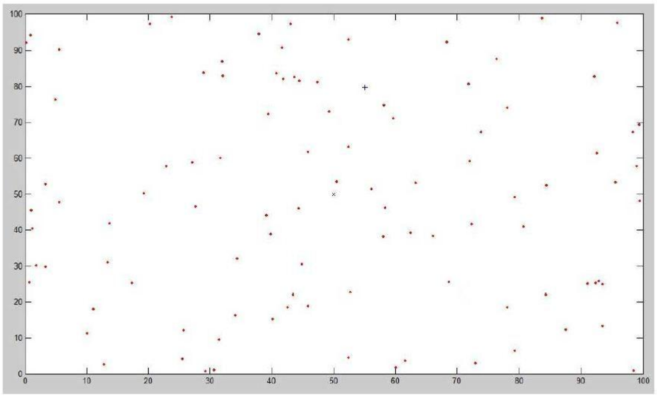


FIGURE 8: FIELD DISTRIBUTION-3

Figure-8 shows when all the nodes in the network die.
The network ceases to work.No data is being transmitted or received either by the cluster-heads or the base-station.

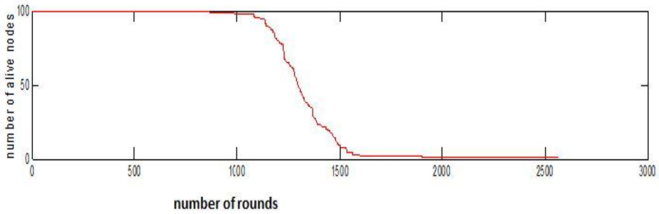


Figure 9 shows the plot number of rounds versus number of alive nodes. As the number of rounds increases the number of alive nodes decreases because of decrease in its energy during Transmission

VI. Conclusion

Clustering is a good technique to reduce energy consumption and to provide stability of network in wireless sensor networks. Energy is one of the valuable resource in wireless Sensors. Data transmission to Base Station(stationary) from different positions in Wireless Sensor Networks using LEACH algorithm gives one of the efficient mechanism for effective routing in Wireless Sensor Networks

References:

[1] L. B. Oliveira E. Habib H. C. Wong A. C. Ferreira, M. A. Vilaa and A. A. Loureiro. Security of cluster-based communication protocols for wireless sensor networks. In 4th IEEE International Conference on Networking (ICN05), volume Lecture Notes in Computer Science, pages 449{458, Washington, DC, USA, 2005.

[2] Jamal N. Al-karaki and Ahmed E. Kamal. Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications, 11:6-28, 2004.

[3] Y. Geng C. Hong-bing and H. Su-jun. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. China Universities of Posts and Telecommunications, September 2008.

[4] G. Hu D. Wu and G. Ni. Research and improve on secure routing protocols in wireless sensor networks. In 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008).

[5] Wendi Rabiner Heinzelman, Anantha Ch, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. pages 3005-3014, 2000.

[6] H. Zhang J. Chen and J. Hu. An eciency security model of routing protocol in wireless sensor networks. In 2008 Second Asia International Conference on Modeling and Simulation, pages 59{64, Washington, DC, USA, 2008.

[7] C.Wang K. Zhang and C.Wang. A secure routing protocol for cluster-based wireless sensor networks using group key management. In 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM08).

[8] 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. (87(12)):2882-2895, December 2007.

[9] 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. In Fifth IEEE International Symposium on Network Computing and Applications, pages 145-154, Washington, DC, USA, 2006.

[10] A. V. Reddy R. Srinath and R. Srinivasan. Ac: Cluster based secure routing protocol for wsn. In Third International Conference on Networking and Services, page 45, Washington, DC, USA, 2007.

[11] Georgios Smaragdakis, Ibrahim Matta, and Azer Bestavrosl. Sep: A stable election protocol for clustered heterogeneous wireless sensor networks. Proc. of the Intl Workshop on SANPA, 2004.

[12] C. Karlof and D. Wagner. Secure routing in sensor networks:attacks and counter measures.Ad Hoc Networks, 1:293_315, May 2003.

[13] S.Zhu, S.Setia, S.Jajodia, LEAP:efcient security mechanisms for large scale distributed sensor networks,10thACM Conference