A Comparative Study on Routing Protocols Used in LEACH

Neha Sanadhya
M.Tech Student, Communication & Information System
SSITM, Aligarh, INDIA

Abstract **- Wireless Sensor Networks are group of low cost and extreme power limited sensor nodes. The various applications of wireless sensor networks include sensing the environment to collect the data and send it to the base station or server in single or multiple hops. The basic target of WSN is to achieve maximum network life using the minimum battery power as limited battery backup is available for any WSN. The first part of this paper presents the comparative study of leach protocol. The second part includes a new routing protocol in LEACH using Fuzzy Logic. The third part includes a comparison based on simulation between AODV, DSR and Fuzzy Logic.**

Index Terms **- Wireless Sensor Network, LEACH, FEEPRP, Fuzzy Logic, AODV, DSR**

I. INTRODUCTION

Wireless Sensor Network [1] is one of the results of the recent developments and advances in micro-electro-mechanical system techniques, digital electronics and wireless communication. The basic idea of these sensor networks are based on the collective efforts of large number of small size, low cost, low power, multi-functioning sensor nodes which sense, collects, process the data and are capable of communicating the base station and other devices in short-range distances. These nodes are deeply deployed near or at the place where phenomenon is taking place. Since the position of theses nodes are not pre-defined therefore they posses the self- organizing and co-operative effort capabilities. Because of these capabilities the responsibility of the wireless sensor network is to send the processed or semi-processed data to the base station. There are many recent improvements in the sensor network over the traditional networks. These improvements can be deployed in two ways [2]:-

- Sensors positioned away from the exact position where actual phenomenon is taking place.
- Sensors are deployed at the same place where the phenomenon is going on.

In first situation, large sensors with the capacity of distinguishing data from noise are required whereas in second situation, the sensors deployed perform only the function of sensing and collecting data.

The basic components of sensor nodes includes: - a sensing unit, a data processing unit, a transceiver unit & a power house. Additional components include location finding system, a power generating system & a mobilizing unit. Sensing units sense the environment using sensors, but since the signals are analog in nature, they are converted to digital using ADC [3]. The output of ADC is send to the processing unit, which processes the data and transfers it to the transceiver. The transceiver then connects to the base station and transfers the data to them[4]. All these functions where power which is supported by a power house which contains a power generating unit which contains scavenging units like solar panels.

II. LEACH PROTOCOL

Low- Energy Adaptive Clustering hierarchy (**LEACH**) [5][9] is one of the most important and widely used routing approaches for Wireless Sensor Networks. The main concept of this algorithm is to rotate the cluster heads per communication interval among the various sensor nodes, so that the energy dissipated is distributed among all the sensor nodes during communication with the base station [6]. As this is a hierarchical protocol, its operation is iterative and can be divided into many rounds. Each round is divided into two phases: - a set-up phase and a steady-state phase.

Set-Up Phase

In this phase every node selects a random number between 0 and 1. The node becomes the cluster head for the current round if it select the number below the threshold value T(n).

$$T(n) = \begin{cases} P/1\text{-}P(r \bmod (1/P)), & \text{if } n \text{ belongs to } G \\ 0 & \text{, otherwise} \end{cases}$$

Where P is the required percentage of CHs, r is the current round and G is the set of nodes that have not been selected as CH in last 1/P rounds**.**

The successfully selected CHs then advertise their selections in the network which are received by the remaining sensor nodes. According to the received signal strengths from various CHs, the sensor nodes select their own Cluster Head and form a cluster for one round of communication with the base station.

Steady-State Phase

After this phase, the nodes collect and send the data to their respective CHs. CHs then process the data and send them to the BS. After each round, the cluster again return back to the set-up phase and CHs are again formed from the remaining sensor nodes which were not selected earlier. Leach uses TDMA and CDMA protocols for inter-cluster and intra-cluster communication for avoiding collisions [1].

III. ROUTING PROTOCOLS USED IN LEACH

In this paper we will study three types of routing protocols used in Leach for the data transmission between base station, cluster heads and other nodes. After that we will discuss the advantages and disadvantages of all protocols over others.

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

The AODV routing protocol is a reactive routing protocol; therefore, routes are determined only when needed. Figure 1 below shows the message exchanges of the AODV protocol. Hello messages may be used to detect and monitor links to neighbours. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbours receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbour, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen[7].

As data flows from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table. If data is flowing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary.

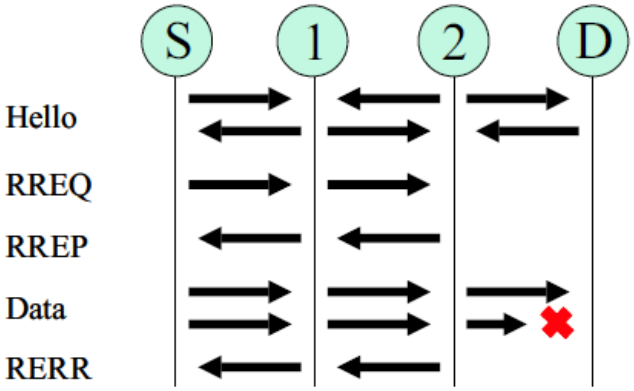

Figure 1: AODV protocol Messaging

Dynamic Source Routing (DSR)

DSR is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The

major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbours of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding RouteRequest packets in the network. The destination node, on receiving a RouteRequest packet, responds by sending a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received.
Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a RouteRequest packet. This RouteRequest is flooded throughout the network. Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbors if it has not forwarded it already, provided that the node is not the destination node and that the packet's time to live(TTL) counter has not been exceeded. Each RouteRequest carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a RouteRequest packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate RouteRequest. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same RouteRequest by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination forward a RouteRequest packet during the route construction phase. A destination node, after receiving the first RouteRequest packet, replies to the source node through the reverse path the RouteRequest packet had traversed. Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase[8].

Fuzzy Logic Based Energy Efficient Packet Loss Preventive Protocol (FEEPRP)
The concept of Fuzzy Logic centers on the idea of partial set membership, instead of crisp or discreet set membership [10]. Initially, it was introduced as an alternative approach to processing data that has behavior defined by a "fuzzy" set , which contains elements whose degree of membership vary in the set. Fuzzy Logic varies from conventional control methods by the fact that it incorporates simple *if- then* structure, rather than complicated mathematical model. It is fundamentally dependent on the experience of an operator in cooperating human reasoning process rather than the technical understanding of the system.
A fuzzy control system consists of three basic components: a Fuzzifier, an Inference System governed by a rule base, and a Defuzzifier. The Controller takes input in the crisp/discrete form and feeds it to the Fuzzifier, which converts the crisp inputs into fuzzy variables using membership functions, which, in turn,map the crisp input into fuzzy variables and calculates the degree of membership of those variables. Fuzzy variables are conceived to be objects or words rather than numbers and are expressed as adjectives such as "high", "low", "medium", "very high" and "very low". The Fuzzifier normalizes the fuzzy variables in the range between 0-1 depending on the crisp input and is termed as the degree of membership[12]. The fuzzy input is then fed into the inference system governed by a rule base in which the fuzzy variables are mapped to fuzzy output. The mapping of the fuzzy variables to the inference system is not discrete and can be partial or overlapping. The set of fuzzy outputs is combined together and is applied to the Defuzzifier, which reverses the effect of fuzzification. Different techniques can be used to obtain the crisp output from the fuzzy output, after applying them to the membership function. The transformation of this set to a crisp number is termed as defuzzification. The basic defuzzification methods include: Centroid method, Mean of maximum and Centre of sums [11].
This algorithm works on fuzzy logic to decide appropriate path by using certain parameters whose values are extracted from nodes. The values are then analyzed and fuzzy logic is implemented to decide a path. The Concept of this algorithm contains two phases: - **Route Discovery** & **Choice of Route [11].**

Route Discovery
For sending information to a particular destination node, a source node requires to find a route to the destination. For this purpose, source node advertises the request packet in the network which contains the source address and the destination address, a sequence number and some vacant space for saving the addresses of intermediary nodes, residual energy, hop counts and packets dropped.
In this algorithm, after advertising the request packet by the source node, the sequence number of all the intermediary nodes are maintained which help in avoiding the loop formation and short route distances. After finding all the routes, the route selection algorithm is run to finalize a route.

Choice of Route
After getting all the routes, a route from source to destination node is finalized using the fuzzy logic algorithm [11]. Since we use a fuzzy logic, it become unpredictable for an outsider to know which route is finalized which adds a security aspect to the information transmitted. Along with the probability of selection of same route is also very low which adds energy efficiency in the network as different nodes will be used every time. The final route is selected on the basis of membership graph and a rule base.

Membership Graph
Membership graph is constructed for all the nodes on three metrics: "residual energy", "packets dropped" and "hop count". On these metrics, the nodes are given values as "LOW","HIGH" and "AVERAGE". As this algorithm is based on the concept of energy efficient, packet loss preventive route discovery, the routes are determined after monitoring the values from all the three metrics for all the intermediary nodes.

Rule Base

This is an intuitive output that is based on the previous experiences of an operator. Along with the experiences, it also incorporates the human reasoning process. The fuzzy input to the rule base includes Low, High and Average for hop count, residual energy and packets dropped, which gives the fuzzy output as "very low", "very high", "average", "low", "high" and "medium".

Defuzzification

After getting inference from the rule base, again a membership graph for deffuzification is generated to get the crisp output. This output is generated using the centroid method and the areas defined in the membership graphs [11].

IV. RESULTS AND DISCUSSIONS

Simulation tool used in this approach is Matlab. Platform is windows on which this tool has been installed. To run this simulation firstly we have to configure the installation.

The Graphs are representing the energy dissipation of nodes during the communication. The blue line is representing energy dissipation of nodes in the original Leach Protocol. The red line is presenting the FEEPRP algorithm. Green Line represent the life time of network using AODV routing protocol.

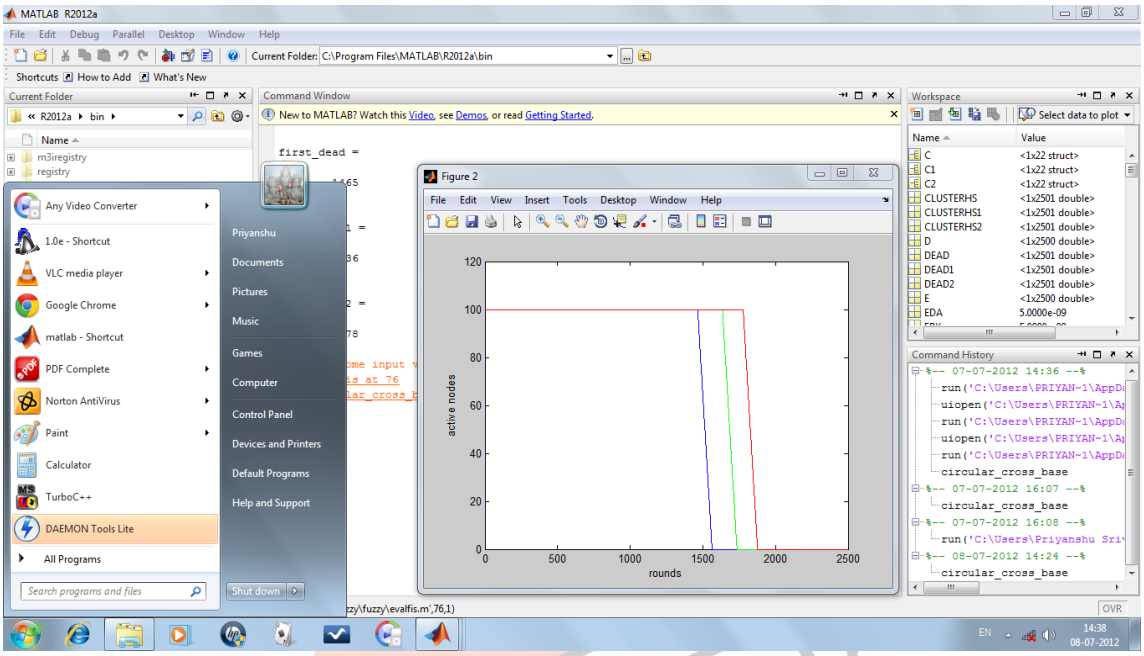

Fig.2: The result of simulation (red line) in number of rounds vs node graph (test 1)

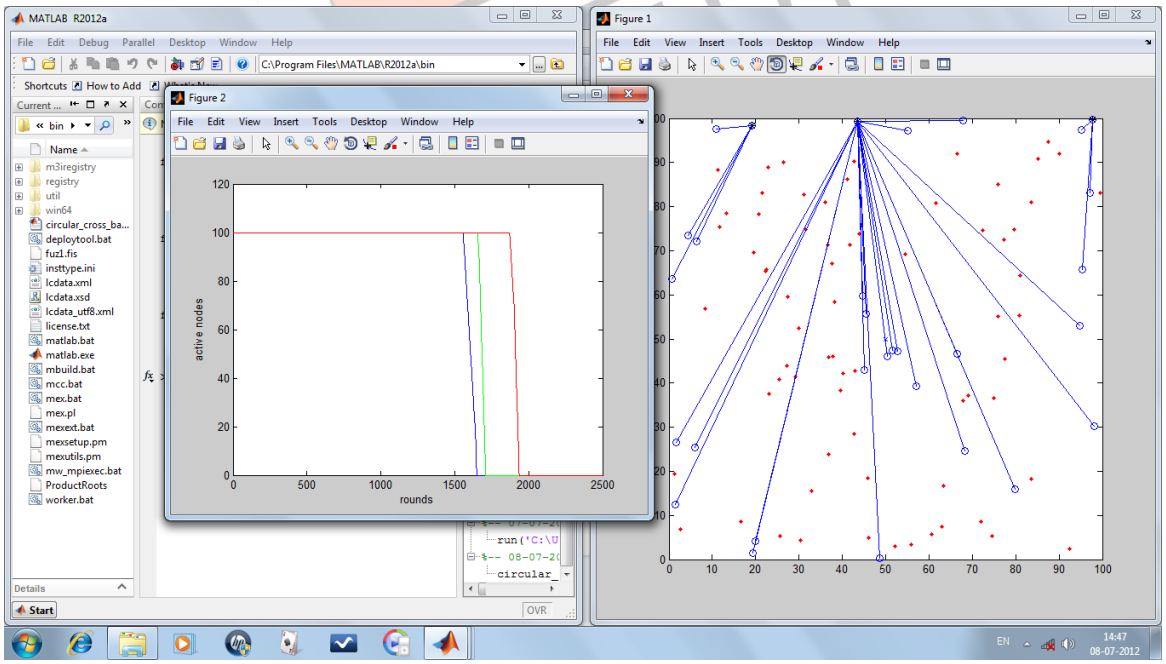

Fig.3 The result of simulation (red line) in number of rounds vs node graph (test 2)

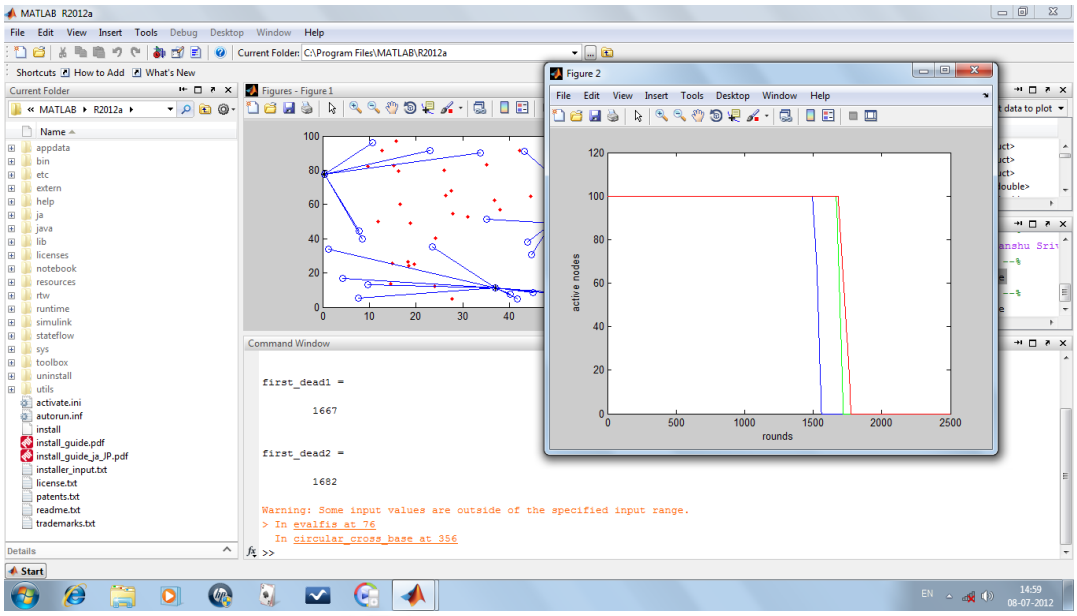

Fig.4 The result of simulation (red line) in number of rounds vs node graph (test 3)

V. SUMMARY AND CONCLUSION

In this paper, we analyze an energy aware packet loss preventive routing protocol, for WSNs using a Fuzzy control mechanism. Applications of Fuzzy Logic in WSN have been encountered in interesting ways in various other pioneering works. Contemplating with the restraints of sensor nodes, FEEPRP is designed to impart security to the network to some extent in terms of avoiding malicious nodes, prevent data loss, control congestion and save energy at the same time. Different from leach, FEEPRP designs a fuzzy control to monitor the past records of the residual energy, packets dropped at each node and hop count to decide which route to select for sending messages. A different route is selected each time according to the output given by the fuzzy logic. As residual energy of each route is given as one of the inputs in the fuzzy control to assure energy conservation and nodes are let to sleep when idle. The graphs above show that energy conservation is much higher in FEEPRP as compared to LEACH protocol.

VI. REFERENCES

[1] I.F. Akyildiz, W.Su, Y.Sankarasubramaniam, E.Cayirci, "Wireless Sensor Network: A Survey".
[2] C.Intanagonwiwat, R.Govindan, D.Estrin, "Directed Diffusion: A Scalable & Robust Communication paradigm for Sensor networks", proceedings of the ACM mobiCom'00, Boston MA, 2000 pp56-67.
[3] R. Kravets, K.Schwan, K.Calvert, "Power-aware Communication for Mobile Computers", proceedings of MOMUC'99, San Diego, CA, Nov-1999, pp64-73.
[4] G.J.Pottie, W.J.Kaiser, "Wireless Integrated network sensors", Communication of the ACM 43(5) (2000)551-558.
[5] W.R.Heinzelman, Anantha Chandrakasan, Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Netwroks", proceedings of 33rd Hawaii International Conference on System Sciences-2000.
[6] Xuxun Ciu, "Survey on Clustering Rounting Protocols in Wireless Sensor Networks", Sensor 2012, 12, 11113-111153.
[7] Charles E. Perkins, Elizabeth M. Royer, "Ad-hoc Demand Distance Vector Routing".
[8] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad hoc Wireless Networks", Mobile Computing, Kluwer Academic Publishers, pp. 153-181, 1996.
[9] Chunyao FU, Zhifang JIANG, Wei WEI, and Ang WEI, "An Energy Balanced Algorithm of LEACH Protocol in WSN", International Journal of Computer Sceince, 2013.
[10] J.Mendel, "Fuzzy Logic Systems for engineering: a tutorial", proceedings of the IEEE, 83(3):345-377, Mar 1995.
[11] Sudip Mishra, Sanchita Roy, Mohammad S. Oaidat, Debashish Mohanta, "A Fuzzy Logic Based Energy Efficient Packet Loss Preventive Routing Protocol", SPECTS 2009.
[12] Mortaza FAhimi Khaton Abad, Mohammad Ali Jabraeil Jamali, "Modify LEACH Algorithm for Wireless Sensor Network", International Journal of Computer Sciences,September 2011.