PERFORMANCE EVALUATION OF SELF ORGANIZATION PROTOCOLS USING AODV ROUTING PROTOCOL

A. Maizate, N. El Kamoun and M. Agnaou
STIC Laboratory, Chouaib Doukkali University, El Jadida, Morocco
E-Mail: maizate@hotmail.com

ABSTRACT
Recent advances in wireless sensor networks have led to many new protocols for self organization specifically designed for sensor networks where energy awareness is an essential consideration. It is one of the major research areas in computer network field today. The WSN has important applications such as disaster management, combat field reconnaissance, border protection and security surveillance. Sensed data need to be delivered to the base station using multihop and must cope with the network unreliability problem and the energy consumption. For minimum energy consumption, all the steps from node deployment to network architecture (Clustered Network) and from environment sensing to communicating the sensed data to base station (routing) should carefully be designed. Few routing and self organization protocols take into consideration of these problems. It is a great challenge of the hierarchical self organization protocols to provide network survivability through redundancy features. In this paper, a short literature review of the existing self organization protocols and routing protocols are carried out. Then, a comparison of self organization protocol was performed using a reactive routing protocol, Ad hoc On Demand Distance Vector (AODV). This comparison addresses network survivability and redundancy issues. Finally, conclusion was drawn based on the research and future direction for further research is identified.

Keywords: software wireless sensor network, routing protocol, AODV, self-organization, clusterhead, clustering energy-efficiency.

INTRODUCTION
The Wireless Sensor Network (WSN) is an emerging field of wireless network comprising a few autonomous tiny sensors nodes. The Sensor Nodes can be deployed at various geographical locations for data aggregation and dissemination. The WSN consist of number of small sensor nodes, with limited processing, limited memory, limited battery power, and limited bandwidth and wireless transmission capabilities. The lifetime of the sensor node depends on the battery power.

Clustering and data dissemination has been widely used for saving the energy of sensor nodes in WSNs and many prominent protocols have been reported in the literature. Clustering sensor nodes is an effective technique for achieving multi-hop communication. Clustering facilitates distribution of control over the network. Each cluster has a cluster head (CH) which acts as a coordinator and also some member nodes. Cluster head has a responsibility to aggregate the data received by the nodes of respective group and send it to the base station (BS) through other CHs. Because CHs often transmit data over longer distances, they lose more energy compared to the member nodes. So the network is re-clustered periodically in order to select energy abundant nodes to serve as CHs, thus distributing the load uniformly on all the nodes. Besides achieving energy efficiency, clustering reduces network contention and packet collisions, resulting in better network throughput under high load.

In the literature of WSN several cluster based protocols are proposed like [1-8] etc. Its various applications like target tracking, environmental monitoring and habitat monitoring require only the aggregated value to be reported at the base station. This extra responsibility leads to early death of cluster head due to high energy dissipation. One of the most accepted cluster based routing protocol LEACH [1], rotates the responsibility of cluster head randomly among all sensor nodes to minimize this effect. Although in LEACH selection of cluster head is done in a distributed way, but it consumes lots of energy of sensor Many researchers have found that the hierarchical routing and specifically the clustered based routing play an important role in reducing energy depletion and increasing the network lifetime.

A WSN is a made up of only wireless sensor nodes, communicating with each other without any centralized control. Nodes within the radio range, communicate directly else communicate through multi-hop. Thus, each node acts as either host or router in the network. Routing protocols try to find the shortest path to the destination. Routing protocols should be able to handle the dynamic nature, and the limited resources of the nodes while maintaining Quality of service. It should also be distributed in nature and loop free for efficient communication.

In this paper we are going to discuss about various clustering algorithms used in WSN. The rest of this paper is organized in the following manner: Section II will introduce the main advantages and objectives of self organization protocols based clustering. Section III will present the energy model and the network. In Section IV, we compare the performance of self organization protocols. Finally, Section V concludes this paper and proposes future research directions.

RELATED WORK
Routing protocols
The routing protocols are classified as reactive protocols and proactive protocols. In reactive routing protocols, the routes are discovered only when necessary i.e., on demand, from the source to the destination, and these routes are maintained as long as it is required. Ad hoc On Demand Vector (AODV) is the most popular reactive routing protocol.

AODV [9] is an approach of on-demand for detecting path. The path is set up as soon as the source node is prepared for the transmission of data packets. Routing table is maintained to store the next-hop address. Each intermediate node in the network forwards the Route Request (RREQ) message until it reaches the destination node. The destination node responds to the RREQ message by transmitting the Route Reply (RREP) message.

As the RREP flows through the network, it determines the route from source node to destination node. The sequence number is increased by each originating node and used to determine whether the received message is the most recent one. The older routing table entries are replaced by the newer ones. Active nodes in the networks are determined by broadcasting a “Hello” message periodically in the network. If a node fails to reply a link break is detected and a Route Error (RERR) message is transmitted which is used to invalidate the route as it flows through the network. A node also generates a RERR message if it gets message destined to a node for which a route is unavailable. Types of messages in AODV:

- **Route Request (RREQ) message**: It is used to form a route from one node to another node in a network.
- **Route Reply (RREP) message**: It is used to connect destination node to source node in a network.
- **Route Error (RERR) message**: It is used to indicate any route broken or node failure.
- **HELLO message**: It is used to determine the activeness of the network.

The transmission of data depends on route discovery and route maintenance in AODV. The route discovery depends on RREQ and RREP messages, if a node initiate’s request of route it will form route after getting the RREP. The route will be maintained by sending HELLO messages to neighbour nodes, if any link failure it will indicate using RERR message.

AODV has greatly reduced the number of routing messages in the network. AODV only supports one route for each destination. This causes a node to reinitiate a route request query when it’s only route breaks. But if mobility increases route requests also increases.

Dynamic Source Routing (DSR) Protocol: DSR [10] is an On-Demand Routing protocol. The major difference between DSR and the other on demand routing protocols is that, it is beacon less and hence does not require periodic hello packets. Consider a source node that does not have a route to the destination. When it has a data packet to be sent to that destination, then it initiates a Route Request packet. This Route Request is flooded throughout the network. The key features of DSR are:

- **Source Routing**: The sender of a data packet knows the complete hop-by-hop route to the Destination. These routes are stored in a route cache. Data packets sent by the source node carry the complete route in the packet header. Intermediate nodes forward the packet based on the route in its header. In most cases, the only modification that an intermediate node may make to the header of a packet is to the hop count field. The fact that all data packets are routed from the source has widely perceived security benefits.
- **On-Demand**: DSR attempts to reduce routing overhead by only maintaining routes between nodes taking part in data communication. The source discovers routes on-demand by initiating a route discovery process only when it needs to send a data packet to a given destination.

Proactive routing protocols maintain up-to-date routing information in its tables and this information are periodically updated using control messages. The proactive routing protocols are based on the link-state routing algorithm. Optimized Link state routing (OLSR) is commonly used proactive routing protocol.

The OLSR [11] is a table driven, proactive protocol, i.e., regularly exchanging topology information with other network nodes. It inherits the stability of a link state algorithm and with the additional advantage of having routes available immediately as and when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol which minimizes the overhead from control traffic flooding through use of selected nodes, called MPRs which in turn retransmit control messages. This greatly reduces the number of retransmissions needed to flood a message to all network nodes. Secondly, OLSR needs only a partial link state to be flooded to ensure shortest path routes. The minimal link state information required is that all nodes, selected as MPRs, should declare links to their MPR selectors. Additional topological information is used for redundancy purposes.

**Self organization protocols**


PCEEC (Passive Clustering for Efficient Energy Conservation in Wireless Sensor Network) [7] use the principles of passive clustering [12] to propose a new mechanism for selecting clusterheads. This mechanism allows the election of an alternate for each cluster head and a dynamic balancing of the role of clusterhead to the alternate when leaving or failure. Thus, it provides several advantages network reliability, stability of clusters and reduces energy consumption among the sensor nodes. Comparison with the existing schemes reveals that the mechanism for selecting an alternate for clusterhead
nodes, which is the most important factor influencing the clustering performance, can significantly improves the network lifetime.

PCEEC uses the same principles as passive clustering for the construction and maintenance of clusters in wireless sensor networks. It also inherits the characteristics of the algorithm GRIDS [13] by giving nodes with the highest level of energy to become a critical node, i.e., Cluster Head, Alternate or Gate Way. PCEEC reduce the amount of energy consumed by the network in comparison with well-known protocols based clustering.

**EDED (Enhanced distributed, energy-efficient, and dual homed clustering)**

EDED [8] is a protocol for self organization in WSN based clustering. EDED algorithm has been designed with the following principles:

- Cluster formation is initiated and maintained in distributed manner, through self organization of sensor nodes.
- Minimum numbers of cluster are created throughout the lifetime of the network.
- Each node has a backup path to the base station.
- Network coverage must be done with a minimum number of clusterheads.
- CHs should be evenly distributed throughout the network.
- Clustering process should terminate within a finite interval.
- Energy consumption should be well distributed among sensor nodes by rotating the role of the CH.

Each node should have a primary Clusterhead and a secondary backup which may be either another Clusterhead or an ordinary node. Data is forwarded to the secondary destination in case the primary Clusterhead fails. Figure-1 shows how sensors may be dual homed.

![Figure-1. Cluster structure with EDED.](image)

Here, nodes 8 and 11 are backed up through the directly reachable CH of a different cluster. Since no such CH is found for node 3, it is backed up by an ordinary node of a neighboring cluster. In the third case, as for node 5, the backup is a neighbor 3 who has the same primary Clusterhead (thus using the neighbor’s backup). Otherwise, which may occur when the CH is the only neighbor of an ordinary node, an ordinary node itself may become a CH after its designated CH fails.

We note that there are two approaches to protect the structure of clusters and avoid triggering of reclustering. The first approach is to protect the cluster as a whole through a CH backup which involves exchanges between clusterhead and the backup clusterhead and packages to notify members therefore, an additional consumption of energy by different clusters. The second approach provides protection for each sensor node independently which performs fault management of a distributed and decentralized manner and enables fault tolerance especially when multiple failures.

The CH selection process in EDED is performed in two steps: first a few nodes advertise themselves as tentative CHs according to value of PCH and the number of neighbors. Then ordinary nodes select from these advertised nodes as final CHs.

The algorithm starts by initializing the parameters and variables. At the start of clustering, the set of neighbors is needed to compute PCH and the number of neighbours for each node. The minimum value for PCH is set to a predetermined threshold Pmin to ensure a constant time complexity of the algorithm. The equation of PCH is:

$$P_{CH} = \max \left\{ \frac{E_{rem}}{T \times E_{rate}}, P_{min} \right\},$$

where T is a constant that indicates the upper bound of the duration for which a node can continuously work as a CH. The value of T should be chosen such that the maximum energy of a node in the WSN is not greater than T $\times$ Erate.

**EPC (Enhanced Passive Clustering algorithm)**

EPC [6] is a clustering algorithm, which evenly distributes the energy dissipation among the sensor nodes to maximize the network lifetime. This is achieved by using residual energy, number of neighbors and distance between nodes in the selection of nodes clusterheads and election of clusterhead backup.

EPC present provides several advantages. It uses balanced energy consumption among network nodes, minimizes the number of clusters (Clusterhead) and provides effective coverage of the network, thus it keeps longer the structure of clusters and minimize the consumed energy. As a result, the network stability is preserved and the lifetime of the network is significantly increased.

EPC (Enhanced Passive Clustering) defines a protocol for cluster formation and election of clusterheads based on the following principles:

- There are six possible states: dead, initial, ordinary, clusterhead ready, custerhead, gateway and clusterhead-Backup.
Initially, all nodes are in the 'initial' state. This state does not change as long as a node does not receive a packet from another node.

When a node receives a packet and if the state of a sender is Cluster Head the node switches to state ordinary or gateway. Otherwise, the receiver's state switches to ClusterHead_ready.

A node in ClusterHead_ready state will switches to Cluster Head, when its coefficient $K(i)$ is best.

The node Cluster Head_ready switches to state gateway when the number of Cluster Heads is greater or equal to the number of Gateways. Otherwise, the node becomes an Ordinary Node or an alternate node.

The node Cluster Head_ready switches to clusterhead-backup status when the number of clusterheads is greater than or equal to the number of gateways and the number of clusterheads is greater than the number of backups and the coefficient $K(i)$ is the second best. Otherwise, the node becomes an Ordinary Node.

The cluster head node selects the second best $K(i)$ node as clusterhead-backup in case of failure of the previous one. The cluster head checks periodically the presence of his backup. In case of failure of the backup, the cluster head replays the selection process of a new backup.

Similarly, if the clusterhead-backup discovers the leaving of the cluster it switches to state ClusterHead and launch the procedure to select a backup.

An ordinary node switches to clusterhead-backup if its $K(i)$ is higher. The clusterhead-backup node switches to state ordinary.

To calculate the weight of each node, we use the following formula:

$$K(i) = \frac{(E_n(i) \times NN_n) + D_n}{E_{\text{Initial}}(i)}$$

Where

- $D_n(i) = \frac{\text{The average distance between the node } i \text{ with all other nodes in the same cluster}}{\text{The maximum range of a node}}$
- $NN_n(i) = \frac{\text{the number of neighbors}}{\text{The maximum number of neighbors supported}}$

EPC reduce the amount of energy consumed by the network in comparison with others protocols based clustering.

HDED (hybrid distributed, energy-efficient, and dual homed clustering Algorithm)

HDED [5] is derived from DED [14] which aims some changes on this protocol to increase its performance. Better coverage, energy efficiency, minimum traffic from nodes to base station, balanced energy consumption are the main features of HDED to improve life time of WSN.

HDED starts by electing nodes critical for the formation of clusters. In addition, the system considers node connectedness, the distance between nodes of the same cluster and remaining energy of cluster head election, and at the same time it sets the cluster head backup for each clusterhead and the path backup for nodes non clusterhead. HDED consists of three parts as shown in Figure-2.

![Figure-2. Clustering formation.](image)

To achieve energy efficiency, the criterion in the selection of Clusterhead is the remaining energy, connectless and the distance between nodes in the same cluster. To reduce the load (or overhead) of Clusterhead, the HDED regulates the size of the clusters. The clustering phase is comprised of four steps: broadcasting step, clusterhead election step, clusterhead backup election step, and clustering step.

For the cluster head election, each node $(i)$ calculates its weight based on several parameters. Weight of node is associated with it’s the current remaining energy, the distance between nodes in the same cluster and the number of neighbors (connectedness). The connectedness can be obtained from broadcasts of neighboring nodes.

Each node $i$ calculates its weight and broadcasts to its neighboring nodes, and at the same time it updates neighboring node information list based on broadcast information of their responses. Then, node $i$ compare the weights of this node with all other one-hop neighboring nodes and select the node with maximum weights as the cluster head, the node that has the following weight will be cluster head backup. If the maximum weight of the nodes is same, the node with maximum remaining energy is elected; else the node with the smallest ID shall be selected as the cluster head. Then, the clusterhead node sends a message to recruit all one-hop neighbor nodes, upon receiving the broadcast message all neighboring nodes join the cluster and updates neighboring node information list. The structure of HDED is shown in Figure-3.
HDED improves the utilization rate of energy and prolongs the lifetime of the network significantly. The main reasons for this are as follows: (1) the clustering process is based on the nodes backup and paths backup, (2) cluster formation is based on multi-criteria cost, and (3) algorithm complexity is negligible.

ENERGY AND NETWORK MODEL

In this section, we present the energy model for communication and the network model that will be used in the performance evaluations section.

Energy model

The energy model used is same with that in Ref. [15]. Equation (1) represents the amount of energy consumed for transmitting $l$ bits of data to $d$ distance. Equation (2) represents the amount of energy consumed for receiving $l$ bits of data which is caused only by circuit loss.

$$E_{TX} (l, d) = \begin{cases} \frac{l}{E_{elec}} + \frac{l \cdot \varepsilon_{fs} \cdot d^2 \cdot d < d_0}{E_{elec}} \\ \frac{l \cdot \varepsilon_{amp} \cdot d^4 \cdot d \geq d_0}{E_{elec}} \end{cases}$$

$$E_{RX} (l, d) = l \cdot E_{elec}$$

where

- The energy consumption per bit in the transmitter and receiver circuitry;
- $\varepsilon_{fs}$: Free space model’s amplifier energy consumption;
- $\varepsilon_{amp}$: Multiple attenuation model’s amplifier energy consumption;
- $d_0$: a constant which relies on the application environment.

SIMULATION AND PERFORMANCE EVALUATIONS

This section describes the simulation results obtained during the investigation phases of the simulation. We used C/C++ language-based event-driven simulator [16, 17] and the same simulation model as in [15] to implement different protocols.

The simulator takes an area of 1500 x 1500 square meters. Numbers of Nodes are increased from 10 to 50 in multiples of 10. The time for which the simulation is performed is 60 seconds. The node mobility model is set up as Random Waypoint Mobility. A total of 100 data packets are sent over the CBR traffic with an individual payload of 512 bytes. The routing protocol is set as AODV. After running the test, we study the graphs in the Analyser mode of the simulator. Hence we get the required performance parameters: Average end to end delay, Average throughput, average PDR (packet delivery ratio) and total number of packets received.

Others parameters considered in this simulation are given in Table-1.

<table>
<thead>
<tr>
<th>Table-1. Parameter settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>$E_{elec}$</td>
</tr>
<tr>
<td>$E_0$</td>
</tr>
<tr>
<td>$\varepsilon_{fs}$</td>
</tr>
<tr>
<td>$\varepsilon_{amp}$</td>
</tr>
</tbody>
</table>

THROUGHPUT

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. Throughput is usually measured in bits per second (bits/sec) [20]. High throughput is always desirable in a communication system. Here the graph shows that we have a better throughput in HDED and EDED in comparison to PCEEC and EPC.
The above figure shows that throughput show that, the total number of data messages received in HDED and EDED are greater than other protocols. Likewise, the throughput increases with the node density and is maximum in case of HDED due to the less of control overhead traffic.

END TO END DELAY

End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination. Usually a data packet may take few extra second to reach the client or the server’s end, which happens due to congestion in the communication network in the situation of a queue or when different routing paths are chosen by the routing protocol [18]. The graph below shows the end to end delay is greatest in IERP as compared to the others which are very small.

END TO END DELAY increases with the increase in number of node. Because when number of node increases, more delay occurred because of node processing time, more queue management time. For better performance it should be low.

Figure-5 shows that the end to end delay is greatest in EPC and PCEEC as compared to the others which are very small.

PACKET DELIVERY RATIO

Packet delivery ratio is the fraction of packets sent by source that are received by the destination and is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source [19]. Its higher value indicates good performance of DED and HDED. The graph below shows the best packet delivery ratio is in the case of HDED and EDED as compared to PCEEC and EPC.

TOTAL NUMBER OF PACKETS RECEIVED

Total number of packets received at the destination. Its count tells us the total number of packets received out of total number of packets sent, in this case 100 data packets were sent. The graph shows the best protocol to deliver the data packets to the destination are HDED and EDED in comparison to PCEEC and EPC.
CONCLUSIONS

The above results give us a combine and comparative study of four types of protocols of self organization namely: PCEE, EPC, EDED and HDED. These comparisons use a proactive routing protocol AODV which is more adapted to the context of wireless sensor networks.

The main concern of this survey is to examine the energy efficiency and throughput enhancement of these self organization protocols. We compare the lifetime and data delivery characteristics with the help of analytical comparison and also from our simulation results.

The overall conclusion is that HDED and EDED like self organization protocols are best choice with AODV routing protocol to move towards a network with less energy consumption as it involves energy minimizing techniques like multihop communication, clustering, redundancy futures and data aggregation. For applications where energy utilization is more critical, HDED et EDED are the best choice. They use both inter cluster as well as intra cluster communication. The power usage, latency and success rate in theses protocols can further improved by increasing probability of clustering.

We can still minimize the energy consumption and extend the network life time by improving the clustering technique. Significant research work has been done in these different clustering protocols in order to increase the life time and data delivery features. Certainly further energy improvement is possible in future work especially in optimal guaranteed cluster-heads selection.

REFERENCES


http://www.cs.binghamton.edu/kang/teaching/cs580s/.

