Advance Power Saving in MANET

Author

[1]Puneet Shukla [2]Vinay Yadav

[1](Research Scholar (M. Tech)/ SR Institute of Technology and Management, Lucknow/India)
[2](Assistant professor/Department of CSE/ SR Institute of Technology and Management, Lucknow/India)

Abstract : *The latest advancement in wireless technology and its applications received a lot of attention. An ad hoc network is one such recent technology, which gives a new paradigm for wireless self-organized networks. Ad hoc networks are simple peer-to- peer networks, self-organized and with no fixed infrastructure. They are used in military oriented tactical operations, for emergency law enforcement, and in rescue missions. We have proposed On Demand Based Energy Efficient Routing Protocol (ODBEERP). The main aim of proposed protocol is to discover the minimum power-limitation route. The power limitation of a route is decided by the node which has the minimum energy in that route. So compared with the minimum node energy in any other route, the minimum node energy in the minimum power-limitation route has more energy. We have also proposed a more accurate analysis to track the energy consumptions due to various factors, and improve the performance during path discovery and in mobility scenarios. The proposed protocol is evaluated with object oriented discrete event simulator environment. Simulation results shows that the ODBEERP achieves good throughput, less delay, high packet delivery ratio and good energy efficiency than the existing protocol PEER.*

Keywords- *MANET, Packet Delivery Ratio, Energy Efficiency, throughput and delay, ODBEER*

1. **Introduction:** A Mobile Ad hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication. Some special characteristics of MANET like dynamic topology, fast deployment, robustness make this technology an interesting research area. Each node in MANET can work as a sender, receiver as well as router. Communication in the network depends upon the trust on each other. Communication can work properly if each node co-operate for data transmission.

The following algorithm depicts the communication in any ad hoc network:

1. Sender node sends the signal to the neighbouring nodes within the vicinity.
2. Neighbouring nodes communicate with the sender node
3. Sender node sends the message to the destination node.
4. If destination node is within the vicinity then message received by the destination node else an intermediate node receives the message.
5. Restart the process of forwarding the message from step no 1 till the destination node is reached.

Confidentiality, integrity, availability, non-repudiation and authentication are the basic requirements of information security. Ad hoc network's dynamic topology with no centralized administration makes it highly vulnerable for its security-breach. Particularly secure routing in ad hoc networks has been a challenging task for researchers

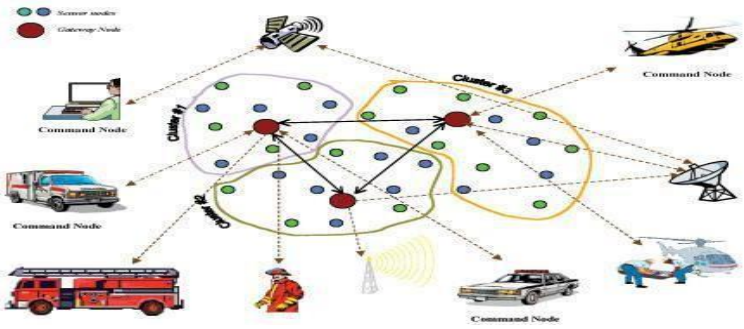

Figure 1 : Mobile Ad-hoc Network

The illustration of mobile ad hoc network is shown in figure.1. The main characteristics of ad hoc networks are as follows:

Dynamic Topology: Because nodes in the network can move arbitrarily, the topology of the network also changes.

The Bandwidth of the Link is unstrained, and the capacity of the network is also tremendously variable. Because of the dynamic topology, the output of each relay node will vary with the time, and then the link capacity will change with the link change. At the same time, compete-collision and interference make the actual bandwidth of ad hoc networks smaller than their bandwidth in theory.

Power Limitation in mobile devices is a serious factor. Because of the mobility characteristics of the network, devices use batteries as their power supply. As a result, advanced power conservation techniques are very necessary in designing a system.

The Safety is limited in a physical aspect. The mobile network is more easily attacked than the fixed network. Overcoming the weakness in safety and the new safety trouble in wireless networks are on demand.

2. Previous Work

For conserving energy, many energy-efficient routing protocols have been proposed. These protocols can be generally classified into two categories: Minimum Energy routing protocols and Maximum Network Lifetime routing protocols. Minimum Energy routing protocols search for the most energy-efficient path from the source to the destination, while Maximum Network Lifetime routing protocols attempt to balance the remaining battery-power at each node when searching for the energy-efficient path. Since Minimum Energy routing scheme is also an important part in most recent Maximum Network Lifetime routing protocols such as Conditional Max-Min Battery Capacity Routing (CMMBCR) and Conditional Maximum Residual Packet Capacity (CMRPC) routing, we will focus on developing more efficient Minimum Energy routing protocols in this research work. Li and Wan described a distributed protocol to construct a minimum power topology and develop an algorithm which directly find a path whose length is within a constant factor of the shortest path. The length of the path is measured in term of energy consumption. This proposed algorithm used only local information.

A topology based on minimum spanning tree, called localized minimum spanning tree (LMST) was proposed by Li et al. It is a localized distributed protocol with the following properties:

(1) the protocol generates a strongly connected communication graph;
(2) the degree of any node is at most six, and
(3) the topology can be made symmetric by removing asymmetric links without impairing connectivity.

An energy efficient dynamic path is maintained to send data from source to destination for MANET is proposed in Sheu, Tu, and Hsu. Due to mobility existing paths may not be energy efficient. So, each node in a data path dynamically updates the path by adjusting its transmission power. Each node in the

networks determines its power for data transmission and control packets transmission according to the received beacon messages from its neighbors. In dynamic path optimization technique protocols dynamically select energy efficient path as per the requirement of dynamic topological changes in the network.

3. Energy Management of Ad hoc Networks

In ad hoc networks, the equipment always uses exhaustible energy such as batteries. The fact is that mobile computing is sprouting quickly with proceeds in wireless communications getting smaller and more efficient; advances in battery technology have not yet accomplished the stage. So, advanced power saving techniques is necessary. A variety of techniques can be used to cope with power insufficiency. Table 1 lists some of power saving techniques at ad hoc networks' protocol layers. Based on the analysis of multicast routing in ad hoc networks, we propose a distributed multicast routing protocols—the On Demand Based Energy Efficient Routing Protocol (ODBEERP), which is based on the device's energy

Table 1 : Power Saving Techniques at ad hoc networks Protocol layers

Protocol Layer	Power Saving Techniques
Application Layer	Adopt an adaptive mobile quality of service (QoS) framework
Transport Layer	Avoid repeated retransmissions. Handle packet loss in a localized manner
Network Layer	Consider route relaying load. Optimize size of control headers
Data-Link Layer	Avoid unnecessary retransmission. Turn radio off (sleep) when not transmitting or receiving

4. Overview of ODBEERP Protocol:

The ODBEERP is a source-initiated, on-demand routing scheme. The main aim of proposed scheme to discover the minimum power-limitation route. The power limitation of a route is decided by the node which has the minimum energy in that route. So compared with the minimum node energy in any other route, the minimum node energy in the minimum power-limitation route has more energy. In other words, the value of that node's energy is the maximum of all minimum node energy in all selectable routes. In routing Process of on Demand Based Energy Efficient Routing Protocol (ODBEERP), The following assumptions are made:

1. A node can find the value of its current energy.
2. Links are bidirectional.

4.1. Route Discovery

In ODBEERP, nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. The route discovery of the EECS is as follows.

Step1:

When the source node wants to send a message to the destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. The source node disseminates a route request (RREQ) to its neighbors. The RREQ includes such information as destination Internet ID, power boundary (the minimum energy of all nodes in the current found route), destination sequence number, hop count, lifetime, Message Authentication Code (MAC) is for providing certificate authority to the nodes and Cyclic Redundancy Code (CRC) for error detection and correction. The destination sequence number field in the RREQ message is the last-known destination sequence

number for this destination and is copied from the destination sequence number field in the routing table. If no sequence number is known, the unknown sequence number flag must be set. The power boundary is equal to the source's energy. The hop count field is set to zero. When the neighbor node receives the packet, it will forward the packet if it matches.

Step 2:

When a node receives the RREQ from its neighbors, it first increases the hop count value in the RREQ by one, to account for the new hop through the intermediate node. The creator sequence number contained in the RREQ must be compared to the corresponding destination sequence number in the route table entry. If the creator sequence number of the RREQ is not less than the existing value, the node compares the power boundary contained in the RREQ to its current energy to get the minimum. If the creator sequence number contained in the RREQ is greater than the existing value in its route table, the relay node creates a new entry with the sequence number of the RREQ If the creator sequence number contained in the RREQ is equal to the existing value in its route table, the power boundary of the RREQ must be compared to the corresponding power boundary in the route table entry. If the power boundary contained in the RREQ is greater than the power boundary in the route table entry, the node updates the entry with the information contained in the RREQ.

During the process of forwarding the RREQ, intermediate nodes record in their route tables the addresses of neighbors from which the first copy of the broadcast packet was received, so establishing a reserve path. If the same RREQs are later received, these packets are silently discarded.

Step 3:

Once the RREQ has arrived at the destination node or an intermediate node with an active route to the destination, the destination or intermediate node generates a route reply (RREP) packet. If the generating node is an intermediate node, it has an active route to the destination; the destination sequence number in the node's existing route table entry for the destination is not less than the destination sequence number of the RREQ. If the generating node is the destination itself, it must update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet immediately. When generating an RREP message, a node smears the destination IP address, creator sequence number, and power boundary from the RREQ message into the corresponding fields in the RREP message.

Step 4:

When a node receives the RREP from its neighbors, it first increases the hop count value in the RREP by one like,

$$\text{Hop count} = \text{Hop count} + 1$$

When the RREP reaches the source, the hop count represents the distance, in hops, of the destination node from the source node. The creator sequence number enclosed in the RREP must be compared to the corresponding destination sequence number in the route table entry. If the originator sequence number of the RREP is not less than the existing value, the node compares the power boundary contained in the RREP to its current energy to get the minimum, and then updates the power boundary of the RREP with the minimum. The power boundary field in the route table entry is set to the power boundary contained in the RREP.

4.2. Route Maintenance

A node uses a Hello message, which is a periodic local broadcast by a node to inform each mobile node in its neighborhood to maintain the local connectivity. A node should use Hello messages if it is part of an active route. If, within the past delete period, it has received a Hello message from a neighbor and then does not receive any packets from that neighbor for more than allowed-Hello-loss Hello-interval

milliseconds, the node should assume that the link to this neighbor is currently lost. The node should send a route error (RERR) message to all precursors indicating which link is failed. Then the source initiates another route search process to find a new path to the destination or start the local repair.

4.3. Analysis of the Proposed Protocol

The ODBEERP is a pure on-demand routing protocol, as nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. It allows mobile nodes to obtain routes quickly for new destinations and respond to link breakages and changes in network topology in a timely manner. The operation of ODBEERP is loop free and, by avoiding the "counting to infinity" problem, offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network) . When links break, ODBEERP causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. As in the AODV, the shortest routing is found when the source initiates a route discovery with a new destination sequence number. But one distinguishing feature of ODBEERP is its use of a power boundary as a selection criterion. The power boundary is the minimum of all nodes' energy in the route. Using a power boundary ensures the updated route has the greater power boundary. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest power boundary. The ODBEERP selects the shortest path at first, which decreases the average relaying load for each node and therefore increases the lifetime of most nodes. At the same time, the ODBEERP updates the route using the power boundary as metrics, which can prevent nodes from being unwisely overused by extending the time until the first node powers down and increasing the operation time before the network is partitioned. This avoids additional control overhead and power consumption to perform a new route discovery process to find a path to the destination. When the energy is nearly exhausted, the Operating System (OS) and Basic Input– Output System (BIOS) will take actions in preparation for power down, which needs more power. So the maximum power boundary route can reduce the additional information operations and conserve energy. In a word, the ODBEERP can optimize power utilization. We have also proposed one more scheme which is used to reduce the energy consumption of the MANET.

5. Energy Consumption Reduction Using Topology Control Approach

Due to the dynamic topology, node consumes more energy while roaming. For this, the topology control approach has been introduced. In this approach, we have considered two cases,

i) Energy consumption of the node and routes.
ii) Link stability and location stability.

Case i)

In first case, the dynamic and adaptive topology is proposed. It will adopt, according to the node moves with in the network. For this each node will keep on nearest level with in the cluster. The number of links connected to a node is very kept low. The link with the low transmission power is also taken in to the consideration for the energy consumption of the route.

Case ii)

For link stability and location stability, each node carrying link with highest density and efficient transmission power with adaptable location. The location stability which implies node is on the stable state which is ready state to send the number of packets to the intended destination node with degrading the network performance. While implementing these two cases, the energy consumption of the whole network can be effectively reduced.

6. Performance Evaluation

6.1. Simulation Model and Parameters

The Proposed protocol is implemented with the object oriented discrete event simulator. In our simulation, 50 mobile nodes move in a 1200 meter x 1200 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 2

Table 2 : Simulation Setting & Parameter

No. of Nodes	50
Area Size	1200 X 1200 m^2
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	Constant Bit Rate (CBR)
Packet Size	512 bytes
Mobility Model	Random Way Point
Max.& Min.Speed	10 & 0.5 m/s

6.2. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Throughput and Delay: Throughput is generally measured as the percentage of successfully transmitted radio-link level frames per unit time.

Transmission delay is defined as the interval between the frame arrival time at the MAC layer of a transmitter and the time at which the transmitter realizes that the transmitted frame has been successfully received by the receiver.

Data Packet Delivery Ratio: The data packet delivery ratio is the ratio of the number of packets generated at the sources to the number of packets received by the destinations

End-To-End Delay: This metric includes not only the delays of data propagation and transfer, but also all possible delays caused by buffering, queuing, and retransmitting data packets.

Energy Consumption per Packet: It is defined by the total energy consumption divided by the total number of packets received. This metric reflects the energy efficiency for each protocol.

Energy Efficiency: Energy efficiency can be defined as :

$$Energyeffic\quad ency = \frac{Totla\ Number\ of\ Bits\ Transmitted}{Total\ Energy\ Consumed}$$

7. RESULT

The simulation results from NS2 with respect to the following performance metrics are shown in the following figures.

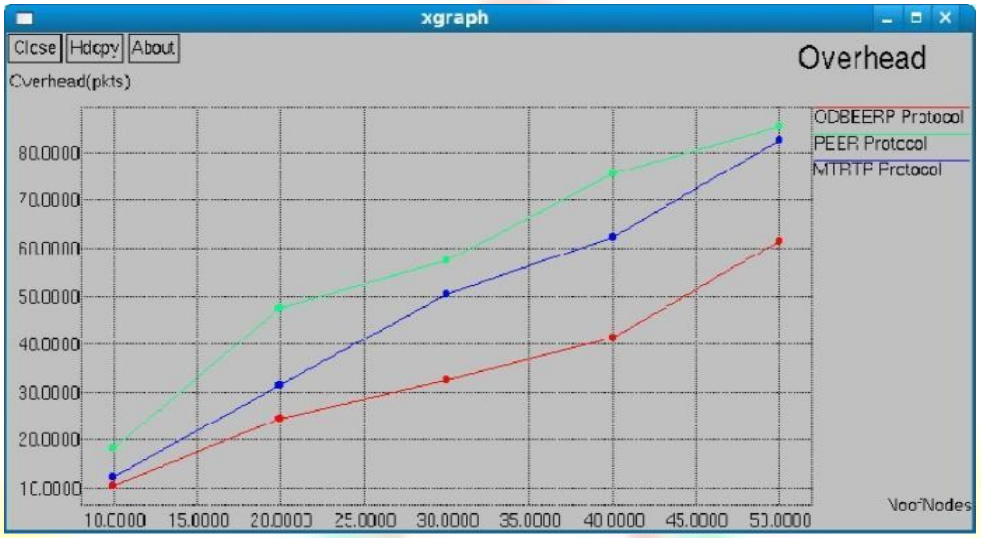

Figure 2. No. of Nodes Vs Overhead

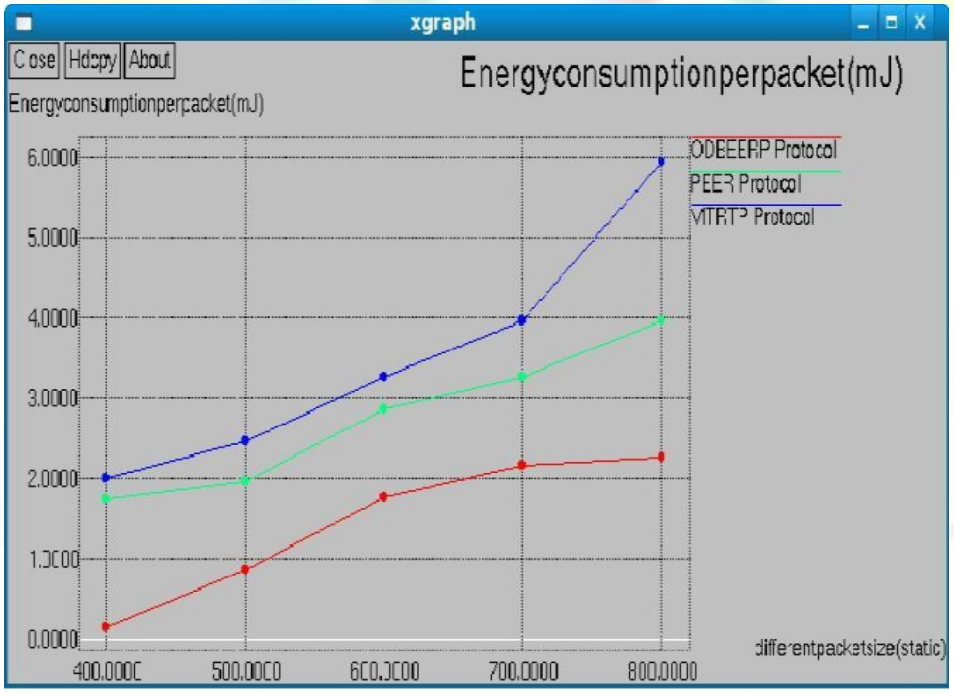

Figure 3 : Energy Consumption per Packet

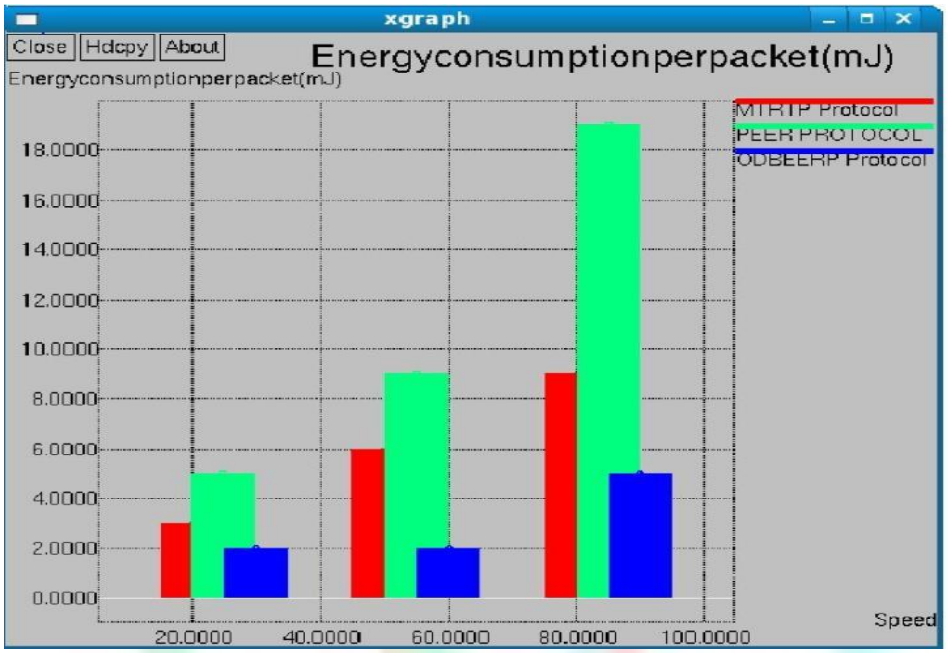

Figure 4 : Speed Vs Energy Consumption

8. Conclusion

In MANET, it is very important to design energy-efficient routing protocols. Incase if we have not considered a careful design, an energy-efficient routing protocol could have much poor performance than a normal routing protocol. In this paper, we first derived an analytical model to more track the energy consumption. We have also discussed the energy consumption technique using Topology Control Approach. Based on these observations and our analysis, we propose a ODBEERP protocol with a quick and low overhead path discovery scheme and an efficient path maintenance scheme for reducing energy consumption. Our performance studies show that ODBEERP protocol reduces routing overhead and path setup delay as compared to PEER and MTRTP, and is highly adaptive to the environment change. ODBEERP performs much better than normal energy-efficient protocol in both static scenario and mobile scenario, and under all circumstances in terms of node mobility, network density, and load. In mobile scenarios, ODBEERP can reduce transmission energy consumption up to 50 percent in all simulation cases compared to the conventional energy efficient routing protocol MTRTP and PEER.

References

[1]. Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2- 17)
[2]. Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang [2005]. "Resisting Flooding Attacks in Ad Hoc Networks". Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'05).
[3]. Anand Patwardhan, Jim Parker and Anupam Joshi**.** "Secure Routing and Intrusion Detection in Ad Hoc Networks". [On-line] accessed on 6th November, 2005 at URL http://csrc.nist.gov/mobilesecurity/Publications/nist-umbc-adhocids-ipv6.pdf
[4]. Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02)
[5]. Panagiotis Papadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002