Novel Approach for Efficiency benchmarking of Routing Protocols for Mobile Ad-Hoc Networks

Dr.T.Manjula[1], Dr.P.K.Poonguzhali[2]
[1,2]*Associate Professor (EEE), Hindusthan College of Engineering and Technology, Department of ECE, Coimbatore, India*

***Abstract*—Routing problems in mobile ad-hoc Networks have become challenging issue amidst the compelling requirements to preserve power in mobile ad-hoc Networks as the network topologies and data traffic may change rapidly in an unpredictable way.Ideally the mobile ad-hoc networks need to maintain all the nodes in active state and should exchange keep-alive packets with its neighbors. The slip side of this topology is waste of energy to keep the nodes alive also takes the toll computational complexity and extra overhead. To overcome these drawbacks there are number of protocols are being proposed to arrive Energy Efficient network with improved performance. The effectiveness of the topology control algorithms are compared with some other protocols in terms of energy consumption and throughput and other performance parameter of interest as required by the algorithms proposed. There is no universal benchmarking mechanism to evaluate the effectiveness of the algorithms. This work is trying to devise a generic effectiveness measuring method for the two important network performance parameters viz. Energy consumption and throughput by proposing the test environment parameters. Elemental node properties are derived by statistical means of exhaustive study of commonly available wireless nodes. And the routing algorithm's performances are validated against the elemental node properties. The simulated results of the AEERG (Adaptive Energy Efficient and Reliable Gossip Routing Protocol) and AODV (Ad-hoc On Demand Distance Vector) will be computed and compared.**

***Index Terms*—Efficiency benchmarking, Energy efficiency, AEERG.**

I. INTRODUCTION

Routing problems in mobile ad-hoc Networks have become challenging issue amidst the compelling requirements to preserve power in mobile ad-hoc Networks as the network topologies and data traffic may change rapidly in an unpredictable way.Ideally the mobile ad-hoc networks need to maintain all the nodes in active state and should exchange keep-alive packets with its neighbors. This work is trying to devise a generic effectiveness measuring method for the two important network performance parameters viz. Energy consumption and throughput by proposing the test environment parameters.

A. MOBILE AD-HOC NETWORKS

A mobile ad-hoc network (MANET) is a collection of many mobile nodes with no infrastructure. To form a network over radio links, the mobile nodes are self-organized. Extending mobility into the self-organized, mobile and wireless domains is the main objective of MANETs where a set of nodes form the network routing infrastructure in an ad-hoc fashion. MANETs are used in those areas where wired network is unavailable and where rapid deployment and dynamic reconfiguration are necessary. These include military battlefields, emergency search, rescue sites, classrooms and conventions, where the participants share information dynamically using their mobile devices.

B. EXISTING ROUTING PROTOCOLS

Generally the existing routing protocols are either

- Table-driven (proactive) routing protocol or
- On-demand (reactive) routing protocol
- Proactive MANET protocol (PMP)

C. PROACTIVE MANET PROTOCOL (PMP)

A proactive MANET protocol (PMP) detects the layout of the network which is active. PMP maintains a routing table at every node. From the routing table, a route can be determined with minimal delay. The PMP can provide good reliability and low latency. This protocol cannot update the route information immediately for a node moving with high speed. Also for a node moving occasionally, updating the

unchanged entry continuously in the routing table results in much traffic overhead and wastage of network resources.PMP is not appropriate for large scale MANETs . PMP is used in DSDV, OLSR.

D. Reactive MANET protocol (RMP)

In Reactive MANET protocol (RMP) when the source node request to communicate with the other node, only then a route between a pair of nodes is found. For nodes with high mobility and for nodes which transmit data occasionally, this on-demand approach is quite suitable. But in RMP the disadvantage is, the source node broadcasts route requests throughout the network and has to wait for the response. This route discovery procedure results in a major delay [2]. RMP is used in, DSR[12], AODV [13] and TORA[15].

E. GOSSIP ROUTING PROTOCOL

For location discovery or for secure routing applications, most ad hoc routing algorithms depend on broadcast flooding. Though flooding is a robust algorithm, because of its extreme redundancy, it is unfeasible in dense networks. The use of flooding algorithms may lead to broadcast storms in large wireless networks where the number of collisions is so high it could cause system failure. Since the packet retransmission is based on the outcome of coin tosses, Gossip [3] is a probabilistic algorithm. The main objective of gossip is to minimize the number of retransmissions, while maintaining he main benefits of flooding.

F. GOSSIP ROUTING IN AD HOC NETWORKS

Flooding is a basic element in many of the ad hoc routing protocols. But the use of flooding algorithms may lead to broadcast storms in large wireless networks, where the number of collisions is so high, causing system failure. Since the packet retransmission is based on the outcome of coin tosses, the main objective of gossip is to minimize the number of retransmissions, while maintaining the main benefits of flooding. A message is normally transmitted as a broadcast rather than a unicast communication in ad-hoc networks. So the message is received by the entire nodes one hop away from the sender. Since wireless resources are expensive, it will be better if we use this physical-layer broadcasting feature of the radio transmission. In the gossiping protocol, we control the probability with which this physical-layer broadcast is sent.

The basic gossiping protocol is simple. A source sends a route request with probability 1. When a node first receives a route request, with probability p it broadcasts the request to its neighbors and with probability 1-p it discards the request; if the node receives the same route request again, it is discarded. Thus, a node broadcasts a given route request at most once. Thus, in almost all executions of the algorithm, either scarcely any nodes receive the message, or most of them do. Ideally, we could make less number of executions where the gossip dies out relatively low while also keeping the gossip probability low, to reduce the message overhead.

The gossip routing protocol satisfies the following conditions:

- The main portion of the protocol involves periodic, pair wise, inter-process communications.
- During these communications the information exchanged is of bounded size.
- When agents interact, just to intimate the state of the other agent(at least the change in the state of one agent)
- A gossip communication does not occur when A pings B, to compute the response time, as this does not involve the transmission between agents.
- Reliable communication is not implicit.
- The protocol costs are insignificant since the frequency of the communications is low compared to classic message latencies.

As we mentioned earlier, the current ad hoc network routing protocols require all the nodes to be awake and keep listening. This wastes a lot of energy.

G. ADAPTIVE ENERGY EFFICIENT AND RELIABLE GOSSIP (AEERG) ROUTING PROTOCOL

Optimizing energy consumption in these networks has given high priority, since most of the mobile hosts are not connected to a power supply and battery recharging is tough. Even if there is no traffic or heavy traffic (neighbor nodes are totally redundant for each other), the traditional ad hoc routing protocols necessitate all nodes to continue listening, thereby wasting the energy. Hence this reduces the

lifetime of the nodes as well as the network's lifetime [3].The major objective as proposed in (GSP) is to achieve energy efficiency by putting some nodes in a sleep mode. The potential disadvantage of this approach is that packets may go through longer paths if the nodes sleeping are on the shortest paths between source and destination nodes, resulting in more energy consumption in the network-wide communication. Also, paths will be broken more often due to mode change of the nodes. Therefore, more overhead is generated to overcome the path failures and this will consume some extra energy. So we are concerned if the energy saved by GSP is larger than the extra energy, consumed by non-optimal paths and extra routing overhead. In addition, sleeping of nodes results in decrease of the network throughput and increase of end to end delay. Hence both energy consumption and reliability cannot be achieved. The major objective of [9] is to achieve energy efficiency and reliability. But in this work, since all the nodes are kept in active state, it results in energy wastage.

The existing energy efficient routing protocols and topology management schemes increase the computing complexity and acquire extra overhead. In this paper, based on the gossip-based ad hoc routing, we propose an Adaptive Energy Efficient and Reliable Gossip Routing Protocol to achieve energy efficiency and reliability in mobile ad hoc networks, to overcome the above discussed drawbacks. In this protocol, the nodes can be in active mode withprobability p or sleep mode with probability 1-p which is fixed at the initial stage. We set a counter B to adapt the number of neighbors to which a packet is forwarded. B represents the current number of neighbors at each node which are kept in active state. The value of B is adaptively adjusted based on the packet delivery ratio. This results in more energy consumption and reliability in the network-wide communication.

H. ADAPTIVE ENERGY EFFICIENT AND RELIABLE GOSSIP (AEERG) ROUTING PROTOCOL

Our observation is that if gossiping can make all the nodes receive a message, then the nodes forwarding the message are connected at least by the paths the message passes through. Therefore, in a static network without mobility (e.g., a sensor network), with certain probability p' , gossiping protocols can make almost all nodes in the network receive the message. Then if all nodes go to sleep with probability $p = (1-p')$, almost all the awake nodes stay connected. Thus, we can safely put a percentage (p) of the nodes in sleep mode without losing network connectivity. We term p the gossip sleep probability.

Let us assume that every node in the ad hoc network chooses an equally distributed random time interval, known as gossip interval. When the time is up, the node will immediately choose another random interval independently. To make it possible, we assume the feasible maximum gossip interval is much smaller than the lifetime of the network

1) Each node independently generates a random time interval and chooses either going to sleep with probability p or staying awake with probability $1-p$ for the interval.

2) Every sleeping node wakes up at the end of its interval

3) Every node repeats the above process for every random interval independently

A node (which wants to communicate) maintains a control variable called B which represents the current number of neighbors at each node which are kept in active state. The rest of the nodes will be in either p or $1-p$ state. The higher – B is the more power the node uses to send packets and thus the communication is more reliable. When node X needs to broadcast a data packet, X looks up its neighbor list for the distance between itself and its neighbors numbered B. X then calculates the amount of power needed to send the packet to that neighbor.

Every node initializes B to one. This means that a node initially broadcasts data packets only to its closest neighbor, thus requiring the least power. After sending data packet, node X waits for a feedback from destination. While receiving packets at the destination, the delivery ratio D is calculated and it will be sent as a feedback to the source. If X hears a feedback D for the data packet below a reliability threshold RT, X increases the value of B thereby increasing the probability of active nodes. This assures the increased delivery ratio. When D becomes greater than or equal to RT, the value of B is decreased adaptively to decrease the number of forwarding nodes and there by decrease the probability of active nodes. This process continues until either X hears a feedback for the

packet or the value of B reaches reliability threshold RT, which is determined by the total number of neighbors. Upon receiving a feedback, X starts to decrease the value of B (after a certain number of acknowledged data packets) to a minimum value of one.

Algorithm:

1) Let sleep probability P(s) = p and awake probability A(s) = 1−p .
2) Let initial value of B −1 .
3) X broadcasts data packets toY .
4) At Y , calculate delivery ratio,
D = Number of packets received /Number of packets sent
5) Y sends D as a feedback to X .
6) At X , If D <RT then,
6.1. B = B +δ, where δis the scale factor.
6.2. Repeat from 3.
7) Else. If D ≥RT , then,
7.1. If B >1, then,
7.1.1. B = B −δ
7.1.2. Repeat from 3.
7.2. End If
8) End If
9) Repeat from 3.

To summarize, AEERG routing protocol has the following salient features:

- Unlike existing routing schemes, AEERG is neither single-path nor multi-path; rather each node exploits the multiplicity of paths based on its observed loss conditions.
- Under AEERG, only for low packet delivery ratios, a node uses high-powered transmissions to reach farther neighbours. For high packet delivery ratios, a node adapts to low-powered transmissions. Thus, AEERG sensibly consumes power based on local error conditions, which maximizes the lifetime of the network and minimizes the cost of the power consumed per successfully delivered data.
- AEERG aggressively probes for possible routes to deliver data packets, thus reacting quickly within unreliable areas of the network.

I. AODV

AODV is a method of routing messages between mobile computers. It allows these mobile computers, or nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed. AODV makes sure these routes do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in routes and can create new routes if there is an error.

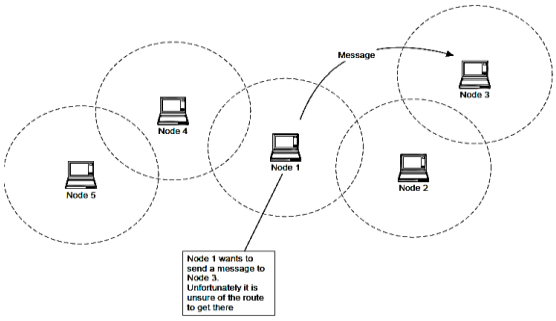

Fig: 1.1. Ad-hoc network nodes

The diagram to the left shows a set up of four nodes on a wireless network. The circles illustrate the range of communication for each node. Because of the limited range, each node can only communicate with the nodes next to it.Nodes you can communicate with directly are considered to be Neighbors. A node keeps track of its Neighbors by listening for a HELLO message that each node broadcast at set intervals. When one node needs to send a message to another node that is not its Neighbor it broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number which serves as a unique ID. In the example, Node 1 wishes to send a message to Node 3. Node 1's Neighbors are Nodes 2 + 4. Since Node 1 cannot directly communicate with Node 3, Node 1 sends out a RREQ. The RREQ is heard by Node 4 and Node 2.

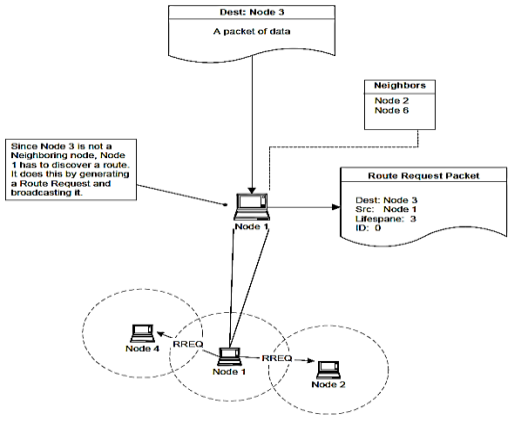

Fig: 1.2. Route Request (RREQ) message

When Node 1's Neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to Node 1, otherwise they will rebroadcast the RREQ to their set of Neighbors. The message keeps getting rebroadcast until its lifespan is up. If Node 1 does not receive a reply in a set amount of time, it will rebroadcast the request except this time the RREQ message will have a longer lifespan and a new ID number. All of the Nodes use the Sequence Number in the RREQ to insure that they do not rebroadcast a RREQ In the example, Node 2 has a route to Node and replies to the RREQ by sending out a RREP. Node 4 on the other hand does not have a route to Node 3 so it rebroadcasts the RREQ.

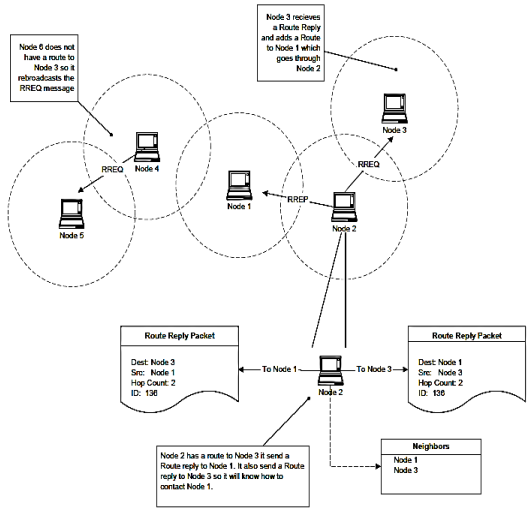

Fig: 1.3. Route discovery

Sequencenumbers serve as time stamps. They allow nodes to compare how "fresh" their information on other nodes is. Every time a node sends out any type of message it increases its own Sequence number. Each node records the Sequence number of all the other nodes it talks to. A higher Sequence numbers signifies a fresher route. This it is possible for other nodes to figure out which one has more accurate information. In the example, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in it's Routing List.

Node 1 then replaces the route it currently has with the route in the Route Reply

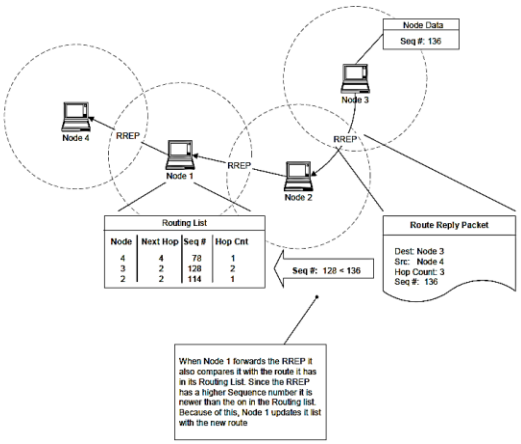

Fig: 1.4. Sequence numbers

Error Messages

The Route Error Message (RERR) allows AODV to adjust routes when Nodes move around. Whenever a Node receives RERR it looks at the Routing Table and removes all the routes that contain the bad Nodes. The diagrams to the left illustrate the three circumstances under which a Node would broadcast a RERR to its neighbors. In the first scenario the Node receives a Data packet that it is supposed to forward but it does not have a route to the destination. The real problem is not that the Node does not have a route; the problem is that some other node thinks that the correct Route to the Destination is through that Node. In the second scenario the Node receives a RERR that cause at least one of its Route to become invalidated. If it happens, the Node would then send out a RERR with all the new Nodes which are now unreachable In the third scenario the Node detects that it cannot communicate with one of its Neighbors. When this happens it looks at the route table for Route that use the Neighbor for a next hop and marks them as invalid. Then it sends out a RERR with the Neighbor and the invalid routes .

AODV Characteristics:

- Will find routes only as needed
- Use of Sequence numbers to track accuracy of information
- Only keeps track of next hop for a route instead of the entire

II .PERFORMANCE METRICS

Our proposed Adaptive Energy Efficient and Reliable Gossip Routing (AEERG) protocol is compared with Ad-hoc On-demand Distance Vector (AODV)

protocol. The evaluation is mainly based on performance according to the following metrics:

- Throughput: It is the number of packets received successfully.
- Average Energy: It is the average energy consumption of all nodes in sending, receiving and forward operations.
- Drop: It is the number of packets dropped.
- Packet Delivery Fraction: It is the ratio of the fraction of packets received successfully and the total number of packets sent.

A. *Power Management in mobile ad-hoc networks*

Since a wireless network is idle most of the time, it is not necessary to keep the WLAN card fully powered all the time. Software intelligence can be added to put the WLAN card hardware into a low-power "sleep" mode whenever possible while maintaining high data transfer performance.

To sustain network connectivity, the WLAN card must have power to listen for traffic, including beacons, periodically. However, the circuitry responsible for sending and receiving packets can be turned off or set to "sleep" when there is no traffic to send or receive. This can lead to considerable power savings. In fact, this is how power saving works in current WLAN cards. When power save is enabled, the WLAN card will follow a periodic "sleep-awake-sleep-awake" pattern to minimize the power drawn by the card.

When the WLAN card is sleeping, incoming packets will be buffered at the AP. Periodically, the card wakes up to listen to beacons from the AP, which the AP uses to tell the card if incoming traffic is queued. Once the card notices incoming traffic is available, it tells the AP to deliver the traffic. After that, the card goes to sleep again.

The penalty for saving power via sleep is greater latency on the delivery of new incoming packets. Moreover, depending upon the implementation, if only a few packets are delivered before the card goes to sleep again, the data rates will be significantly reduced.

Thus, it is necessary to seek a balanced implementation that optimizes for both power efficiency and throughput performance.

B. *Measuring Platform for Power Consumption*

There are five physical states that the AP can be in:

- Off. The device is completely powered off.
- Sleep. A majority of the circuitry is turned off, except for certain critical parts.
- Listen. The radio is listening for traffic but is not passing any data to the host.
- Receive. The AP is detecting, demodulating and passing packets to the host.
- Transmit. The AP is modulating and sending packets onto the air.

Although the five physical states of the WLAN card are useful, conceptual tools, their individual power consumptions will not actually be measured. Instead, the focus should be on the actual usage scenarios, which abstract many of the lower-level details and are more relevant to the end user. Actual usage scenarios are linear combinations (weighted averages) of the above physical states. That is, in the normal course of WLAN operation, the user will put the system into all of the above states at various times.

The basic usage scenarios are:

- Baseline: there is no WLAN peripheral attached to the laptop. This is the same as the WLAN card always being off. There should be no active computations or peripheral accesses in progress. The Windows3 Task Manager or similar utility can be used to monitor any unusual application or background task activity. Once it is determined that the laptop is in a steady state, the power consumption can be recorded.
- Searching/Roaming: the laptop is searching for an available network. The laptop is in this state if the WLAN card is enabled but cannot associate with an access point. After the initial failure to associate, the device actively scans the channels of all the supported bands once every preset interval. In this usage scenario, the card is not only in the Listen and Receive states on a periodic basis, but is also in the Sleep state some of the time.
- Associated and Idle: the laptop is associated with the access point but is not passing data This is an important test scenario because laptops are in this state the majority of the time. There are two sub-categories to test:
- Power Save Off. The WLAN card never enters Sleep. It is always in Listen unless it is actively receiving or transmitting.

- Power Save On. The WLAN card enters Sleep after a certain elapsed period of inactivity. It wakes up after a preset interval to check for traffic queued for it at the access point. It is thus briefly in the Listen and Receive states on a periodic basis, but is in the Sleep state the vast majority of the time.
- TCP Uplink: the laptop is actively transmitting data. The device is thus in Transmit most of the time. However, according to the 802.11 standard, it must listen for an acknowledgement packet (physical layer ACK) and listen to sense if the channel is busy immediately after sending each packet. This is true even when it is sending consecutive packets. Thus, the device might be in the Transmit state perhaps 60% of the time and in Listen and Receive the rest of the time.
- TCP Downlink: the laptop is actively receiving data. The device is thus in Receive most of the time. However, according to the 802.11 standard, it must transmit a physical layer ACK, listen to sense if the channel is busy immediately after receiving a packet, and also transmit TCP ACKs and receive their physical-layer ACKs. Thus the station will be mostly in the Receive and Listen states, and briefly be in the Transmit state.

Here is an example of the composition of the power consumption in the TCP Uplink scenario in terms of the WLAN physical states:Given the following WLAN physical power consumption: Transmit = 2 W, Receive = 0.9 W, Listen = 0.8 W, Sleep = 40 mW, TCP Uplink Power Consumption = 0.6 x Transmit + 0.2 x Listen + 0.2 x Receive + 0 x Sleep = 0.6(2 W) + 0.2(0.8 W) + 0.2(0.9 W) = 1.54 W

C. *Decomposition of Energy Consumption in IEEE 802.11*

The total energy J(n) that a station's radio consumes when it transmits 1 MB of data in an IEEE 802.11 network with n stations is calculated as below. It is assumed that all nodes are one hop away from each other and use the CSMA/CA DCF protocol.

The formulas also divide the total energy among six different MAC operations: (a) successful transmission; (b) successful reception; (c) overhearing (reception of packets intended for other stations); (d) idle listening (when the channel is idle); (e) unsuccessful (colliding) transmissions; and (f) reception of collisions. Only operations (a) and (b)—the successful transmission and reception of 1 MB of data—usefully consume energy. This energy is a constant, which depends on the bit rate and packet size. The others, (c)-(f), waste energy. This waste depends on several factors: the number of stations, n; the pattern of traffic, assumed here to be symmetric and saturated, i.e., destinations are uniformly selected and every station has data to send; whether the basic access or the RTS/CTS mechanism is used; the packet size and bit rate; and the power consumed in different radio states, transmit, receive, etc.

Most energy is wasted in overhearing packets intended for other destinations. For n = 15 (using radio data from [1]), overhearing wastes 60 percent of the total energy for the basic mechanism, and 75 percent for the RTS/CTS mechanism. Because the RTS/CTS packets contain the destination address and information about the duration of the transmission (NAV), stations could avoid overhearing, saving significant energy. The three other wasteful operations (d)-(f) cannot be avoided without major changes in the protocol.

The energy calculations presented here are unimportant for a laptop PC platform in which the radio consumes only 9 percent of the total energy. However, an 802.11 radio in a PDA, cell phone, or wireless sensor, will consume a larger portion of the total energy, so these calculations would be more significant for these devices.

III. SIMULATION OF AEERG AND AODV PROTOCOLS

NS2 is used to simulate the AEER algorithm. In this simulation, the channel capacity of mobile hosts is set to 2 Mbps. In the simulation, mobile nodes move in a 500 meter x 500 meter region for 50 seconds simulation time. The number of mobile nodes is kept as 40. It is assumed that each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the speed is set as 20m/s. The simulated traffic is Constant Bit Rate (CBR). The pause time of the mobile node is kept as 10 sec.

The simulation settings and parameters are summarized in table 3.1.

SIMULATION PARAMETERS

No. of Nodes	40
Area Size	500 X 500
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Rate	100,200,300,400 and 500kb
Mobility Model	Random Way Point
Speed	20m/s
Pause time	10 sec
Transmit Power	0.660 w
Receiving Power	0.395 w
Idle Power	0.035 w
Initial Energy	15.1 J

Table: 3.1. Simulation Parameters

A. SIMULATION RESULTS OF AEERG

Fig 3.1 shows the results of energy consumption for the number of flows 1,2,3,4. From the results, we can see that AEERG scheme has less energy than AODV scheme, since it has the energy efficient routing.

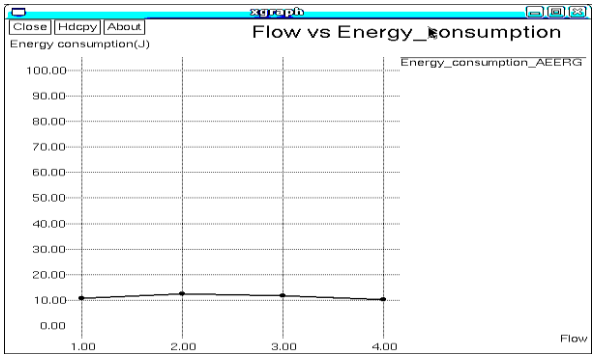

Fig: 3.1. Energy consumption Vs Flow

Based on Flow (number of neighbor nodes) in the experiment, the number of flows as 1, 2, 3 and 4. Fig 3.2 gives the throughput of protocols when the number of flow is increased. As we can see from the figure, the throughput is more in the case of AEERG than AODV.

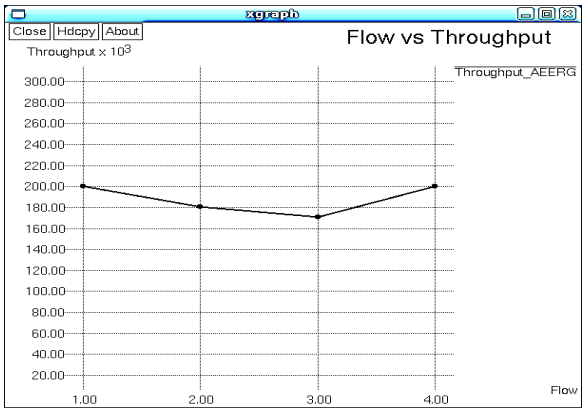

Fig: 3.2. Throughput Vs Flow

IV. RESULT AND DISCUSSION

A. AEERG AND AODV PROTOCOLS - SIMULATION RESULTS COMPARED

The Energy consumption of the AEERG and AODV are compared for the similar experimental setup. The AEERG is found to be utilizing almost one-third of the energy used by AODV.

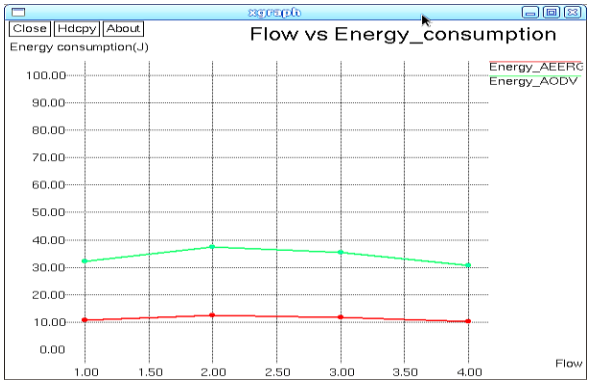

Fig: 3.3. Energy consumption Vs Flow – Compared

The Throughput of the AEERG and AODV are compared for the similar experimental setup. The AEERG is found to have 35 percent increase in throughput compared to AODV.

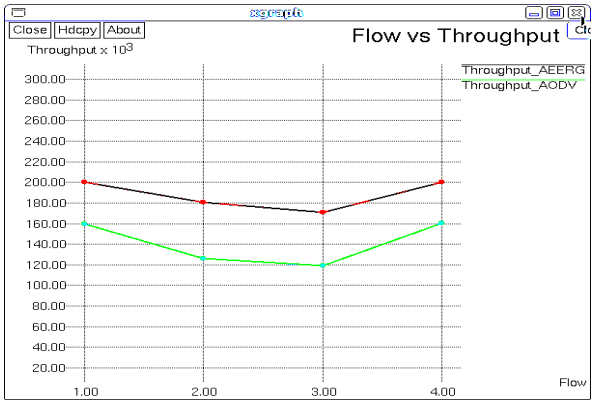

Fig: 3.4. Throughput Vs Flow - Compared

B.BENCHMARKING METHODOLOGY

The benchmarks used to profile the network topology and routing protocols, comparing the two supported wireless subsystems highlights the performance, power efficiency, and suitability of different wireless technologies for the various applications.

Seven different benchmarks to measure the power consumption and performance of the system, exploring various quiescent modes of the processor and typical media-access capabilities:

- *Sleep*: low power deep-sleep mode, where the processor is unable to perform any computation. Wake-up is achieved by either a timer event or external interrupt (*e.g.*, wake-on-wireless).

- *Idle*: A low power mode that offers less power saving than the Sleep mode, but has a very low time to transition to Active state. The processor is awake, but since the system clock is frozen, it is not executing any instructions. All the I/O subsystems are fully functional.
- *CPU*: A synthetic micro-benchmark designed to exercise the processing and storage subsystems. This benchmark involves the processor performing a search of the local file system and does not use any communication.
- *Put &get*: These benchmarks use the SSH program to continuously encrypt and transfer a 3 MB file to and from the device, respectively.
- *Audio &video*: Streaming audio and video from the mobile device to an access point. These benchmarks use the Darwin Streaming Server [11] and standard MP4 encoding at 110 kbps and 410 kbps, respectively. Each benchmark is run using one of several radio configurations:
- *None*: Both radios are disconnected from the system.
- *BT*: Only the Bluetooth radio is connected; the Wi-Fi radio is physically removed from the system.
- *Wf*: Only the Wi-Fi radio is connected; the Bluetooth radio is physically removed from the system.
- *Both*: Both radios are connected to the system.

Each radio, when physically connected to the system and not actively transferring data, is in one of the following states:

- *Off*: The radio is in a software-controlled shutdown state.
- *Scan:* The radio is scanning for nearby devices to connect to.
- *Conn:* The radio has established a connection to a nearby device, but is not actively communicating data.

C. IETF BENCHMARKING GUIDELINES

Efficiency of a routing protocol is evaluated as per the IETF guidelines

- Network lifetime
- Delivery Ratio
- Control Overhead
- Propagation delay

From routing perspective

- Route setup
- Routing overhead
- Route maintenance

D. THE ELEMENTAL NETWORK AND NODE PROPERTIES FOR BENCHMARKING

Based on the study of various network setups for various routing protocols performance comparison, the following elemental network parameters are proposed to simulate and compare the results.

Table: 4.1. Elemental network Parameters

Node Properties	Quantity
No. of Nodes	40
Area Size	500 X 500
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Rate	100,200,300,400 and 500kb
Mobility Model	Random Way Point
Speed	20m/s
Pause time	10 sec
Transmit Power	0.660 w
Receiving Power	0.395 w
Idle Power	0.035 w
Initial Energy	15.1 J

V. CONCLUSIONS AND FUTURE ENHANCEMENT

The Efficiency of the routing protocols of AEERG and AODV is compared for Energy consumption and throughput. The two protocols were simulated in the similar network metrics and access point parameters.The network scheme and Access point parameters could be used as the elemental values for comparing and benchmarking any other new routing protocols proposed in future.Other network parameters of interest like Packet delivery Ration and latency can also be compared with the simulation of similar network setup.The network and mode parameters proposed can be extended to other IEE 802.11x.

REFERENCES

[1] Fahmy, I.M.A.; Hefny, H.A.; Nassef, L.,"PEEBR: Predictive Energy Efficient Bee Routing algorithm for Ad-hoc wireless mobile

networks " Informatics and Systems (INFOS), 8th International Conference -2012

[2] Jinhua Zhu and Xin Wang,"Model and Protocol for Energy-Efficient Routing over Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, NOVEMBER 2011

[3] S.Rajeswari and Dr.Y.Venkataramani "An Adaptive Energy Efficient and Reliable Gossip Routing Protocol For Mobile Adhoc Networks" International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010 1793-8201

[4] Pi-Cheng HsiuandTei-Wei Kuo," A Maximum-Residual Multicast Protocol for Large-Scale Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 11, NOVEMBER 2009

[5] Ramana Rayudu Real Time Systems Group, "Wireless Sensor Node Design Considerations", UBICOMP India 2008, C-DAC, Bangalore

[6] Mustafa Ergen and PravinVaraiya," Decomposition of Energy Consumption in IEEE802.11", IEEE 2007

[7] Xiaoping Hou and David Tipper," Gossip-based Sleep Protocol (GSP) for Energy Efficient Routing in Wireless Ad Hoc Networks", WCNC 2004 / IEEE Communications Society, March 2004

[8] Vijay Raghunathan, Trevor Pering, Roy Want, Alex Nguyen and Peter Jensen," Experience With A Low Power Wireless Mobile Computing Platform", Proceedings of the 2004 International Symposium on Low Power Electronics and Design (ISLPED'04)

[9] Marcelo M. CarvalhoCintia B. Margi Katia Obraczka J. J. Garcia-Luna-Aceves," Modeling Energy Consumption in Single-Hop IEEE 802.1 1 Ad Hoc Networks", IEEE 2004

[10] Power Consumption and Energy Efficiency Comparisons of WLAN Products. White paper, Atheros Communications, Inc, 2003.

[11] Network Simulator, http://www.isi.edu.nsnam /ns

[12] IETF MANET Working Group AODV Draft :http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt