iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5229

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Proposed Energy Conservation Technique in Wireless Sensor Network

Sarang Kharpate[1], Ankita jain[2], Neelesh Gupta[3]
[1, 2,3]*Department of Electronics and Communication, Rajiv Gandhi Proudyogiki Vishwavidyalaya*

Abstract: Wireless Ad hoc network has a lack of infrastructure and decentralized network. It is a collection of mobile nodes which has energy, some restricted bandwidth and computational functionality also. Due to its mobility behavior rigorous kinds of vulnerabilities may get compromised from the nodes which consumes the energy mostly and exploits the bandwidth of the transmitting node. The energy consumption is momentous issue as mobile nodes have battery power. To extend the lifetime of ad hoc network, it is serious issues to minimize the energy consumption of mobile nodes. In this work, proposes an efficient energy conserving scheme which use election algorithm and key management techniques. This approach is much more efficient in preserving the energy of mobile nodes and also prevents it from the exploitation of bandwidth. The experimental analysis of proposed approach is done in network simulator NS2.34. For measuring the performance of the proposed approach different performance measuring parameter such as Packet Delivery Ratio (PDR), Routing Load and Energy Consumption and Delay is used.

Keywords: Bandwidth, Computational Capacity, Energy, Network Simulator, Overhead, PDR, Throughput

I. INTRODUCTION

Wireless ad hoc network is a self-organized and infrastructure less network which does not have any central coordination. In such network each nodes are free to move and share their link among nodes. Each nodes act as host or routers which has the capability to transmit packets from one end to another end. Wireless network uses the dynamic topology to form the connection and because of this structure of the network changes haphazardly which consumes energy while each node has limited battery power. This network is used in many areas of application such as military application, scientific purpose, research application, Rescue Operations etc. wireless ad hoc network uses routing concepts to transmit the packets which are classified into three categories specifically: proactive routing protocol, reactive routing protocol and hybrid routing protocol.

In proactive routing protocol [2] is analogous to the connectionless approach of forwarding packets, with no regard to when and how recurrently such routes are preferred. The routing information is continuously propagated and maintained in table-driven routing protocols; a path to every other node in the ad hoc network is forever available, regardless of whether or not it is needed. Examples of this protocol are DSDV (Destination Sequence Distance Vector), CSGR, GSR (Global State Routing) and FSR (Fisheye State Routing) etc.

In reactive protocols [2] are also called on demand routing protocols because they don't uphold routing information or routing movement at the group nodes if there is no announcement. If nodes wish to send a packet to a different node then this protocol investigates for the route in an on-demand method and founds the association in order to broadcast and acknowledge the packet. The examples of this protocol are AODV and DSR etc.

Hybrid routing protocols [3] combine the best feature of proactive and of reactive routing. This routing is principally recognized with a few proactively prospected routes and next serves the stipulate from furthermore activated nodes through reactive flooding. The fundamental proposal is that each node has a pre-defined zone centered at itself in terms of number of hops. The examples of this protocol are ZRP (Zone Routing Protocol). To route the packet from one end to another it requires energy for transmission but due to its dynamic change in network it consume much energy than wired network. So, the efficient node-energy utilization in mobile ad-hoc networks is an indispensable role. Death of node due to energy exhausted in ad hoc network escorts to the network partition and causes communication breakdown in the network. Because energy is limited in wireless mobile ad hoc networks, designing energy conscious routing protocols has become a foremost issue. The endeavor of these protocols is to decrease the energy consumption of the mobile nodes in the network in order to maximize the lifetime of the network.

In this work, we use election algorithm and key management techniques by considering the transmission power of nodes and residual energy as energy metrics in order to maximize the network lifetime and to decrease energy expenditure of mobile nodes. The experimental analysis of proposed work is done on network simulator NS-2.34 and it is found that this propose scheme gives better outcomes than other scheme. The remaining section of research paper is done as follows: In section II presents the related work which has already been done and pertinent to our scheme. Section III we present or proposed scheme in detail. In Section IV, the simulation results and analysis of proposed scheme is presented and Last section presents conclusion of the proposed work.

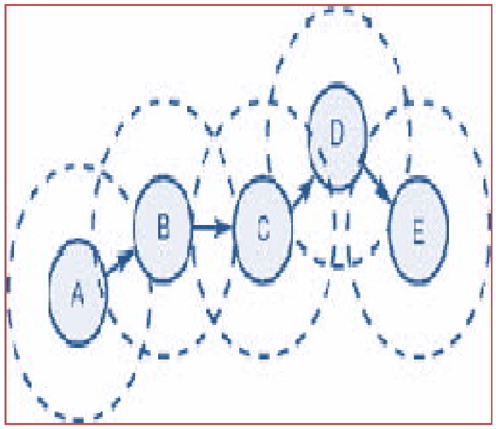

Fig.1 Architecture of Wireless Ad Hoc Network

A. *Energy Management in MANETs*

Energy is a sparse resource in ad hoc wireless networks and it is of overriding importance to use it resourcefully when establishing communiqué patterns.

Energy Management [12] is defined as the progression of managing the sources and clients of energy in a node or in a network as an intact for enhancing the lifetime of the network.

Energy Management can be classified into the subsequent categories:

1) *Transmission Power Management:* The power frenzied by the radio frequency (RF) module of a mobile node is determined by numerous factors such as the state of operation. The transmission power, and skill used for the RF circuitry. The state of operation refers to transmit, receive, and sleep modes of operation. The broadcast power is determined by the reachability requirement of the network, the routing protocol and the MAC protocol employed. The RF hardware design must guarantee minimum power expenditure in all the three stages of operation.
2) *Battery Energy Management:* The battery supervision is intended at extending the battery life of a node by taking benefit of its chemical assets, discharge patterns, and by the assortment of a battery from a set of batteries that is offered for redundancy.
3) *Processor Power Management:* The clock speed and the number of instructions accomplished per unit time are a few of the processor parameters that influence power consumption. The CPU can be put into dissimilar power saving modes during small processing load conditions. The CPU power can be absolutely turned off if the machine is inactive for a long time. In such cases, disruption can be used to turn on the CPU upon recognition of user interaction or other events.
4) *Devices Power Management:* An intelligent device management can diminish power utilization of a mobile node considerably. This can be done by the operating system (OS) by selectively powering down interface devices that are not used or by putting devices into dissimilar power-saving modes depending on their usage.

II. RELATED WORK

Zhang et al. (2009) [4] presented an energy-efficient dynamic key management method in which novel sensor nodes can link a sensor network steadily and compromised nodes can be isolated from the network in time. Contrasting in centralized and location-based key management schemes, their method doesn't depend on such infrastructure as base stations and robot; therefore it possesses a high level of suppleness. By using a pseudo-random function and the elliptic curve digital signature algorithm in their scheme, energy consumption can be reduced appreciably in key establishment and maintenance phases. Analysis showed that their method had an extremely low overhead in terms of computation, communication, and storage. Wei et al. (2010) [5] presented an energy-efficient distributed deterministic key management method (EDDK) for resource-constrained wireless sensor networks. EDDK generally focuses on the establishment and safeguarding of the pair-wise keys as well as the local cluster keys and can repair some flaws in some existing key management methods. Not simply can the neighbor table constructed during key establishment present the security for key maintenance and data transfer, but it can also be used to successfully administer the storage and update of the keys. By using the elliptic curve digital signature algorithm in EDDK, both novel and mobile sensor nodes can connect or disconnect a sensor network securely. Dissimilar some centralized and location-based key management method, EDDK does not depend on such infrastructure as base stations and robots and thus has a high level of flexibility. Experimental analysis showed that

EDDK had a very low overhead. Priya S et al. (2014) [6] presented a Low Energy Adaptive Reliable Routing (LEARR) to find routes which entails least amount of energy for consistent packet transfer in ad hoc networks. It describes the energy cost of packet forwarding by a node as the fraction of remaining battery energy which is obsessive by a node to forward a packet. It comprises the energy consumed for retransmission of the packet as well, while the packet or its acknowledgment is misplaced. It is found that LEARR can successfully diminish the energy consumption of nodes and balance the traffic load amongst them. Additionally, LEARR is able to discover reliable routes, in which ingredient links require less number of packet retransmissions due to packet loss. It in turns diminishes the latency of packet delivery and saves energy as well. To extend the network lifetime, power supervision and energy-efficient routing techniques become obligatory. Energy-aware routing is an effectual way to extend the operational lifetime of wireless ad hoc networks. Loganatha et al. (2013 [7] proposed a trust authority based key management and authentication method for multicasting in ad hoc networks. Primarily they construct an energy proficient topology aware key tree which mostly aimed to decrease the re-keying load by pre-processing the joining members during the redundant re-keying interval. Key management is processed based upon Diffie-Hellman key-pair and RSA secret public key pair. A trust authority ascertains public key certificates for each group member by signing the public key with its secret key. By the simulation results it showed that this key management guarantees key substantiation, enhances fault-tolerance and defends the tree from impersonation attacks. Mekkakia et al. (2014) [8] anticipated a single-path routing technique; a novel path-discovery course is required once a path break down is detected, and this procedure causes delay and exhaustion of node resources. A multipath routing technique is an unconventional to exploit the network lifetime. In this paper, they proposed an energy-efficient multipath routing protocol, called ad hoc on-demand multi-path routing with life span maximization (AOMR-LM), which preserve the enduring energy of nodes and steadiness the consumed energy to enhance the network lifetime. To attain this target, they used the residual energy of nodes for manipulating the node energy level. The multipath selection method used this energy level to categorize the paths. Two constraints are analyzed: the energy threshold β and the coefficient α. These parameters are indispensable to categorize the nodes and to make certain the perpetuation of node energy. Their protocol improved the performance of mobile ad hoc networks by extending the life span of the network. This novel protocol had been compared with other. Sylvia et al. (2015) [9] proposed a protocol which utilizes abundant metrics such as residual energy and link superiority for route selection and also comprise a monitoring method which initiates a route innovation for a poor link, thereby tumbling the overhead involved and humanizing the throughput of the network though maintaining network connectivity. Power control is also implemented not only to accumulate energy but also to improve the network performance. Using recreations, they showed the performance improvement attained in the network in terms of packet delivery ratio, routing overhead, and remaining energy of the network. Gouda et al.(2013) [10] presented an energy optimal AODV (EO-AODV) routing protocol based on reactive routing protocol. In this proposed mechanism, source node does not send any RREQ; no adequate energy (battery life time) and received RREP until the node density in its neighbouring go beyond a meticulous threshold. While applying routing discovery and needs to evade the superfluous information sending proficiently Aye et al.(2014) [11] anticipated an energy efficient multipath routing protocol for choosing energy proficient path. This system also considers transmission power of nodes and remaining energy as energy metrics in order to exploits the network lifetime and to diminish energy consumption of mobile nodes. The objective of their proposed system was to uncover an optimal route based on two energy metrics while choosing a route to transfer data packets. This system is implemented by using NS-2.34. Simulation outcomes showed that the proposed routing protocol with transmission power and remaining energy control mode can lengthen the life-span of network and can accomplish higher performance when compared to conventional ad-hoc on-demand multipath distance vector (AOMDV) routing protocol.

III. PROPOSED SCHEME

Our leader election algorithm is based on the traditional termination-detection algorithm for disseminating computations by Dijkstra and Scholten [10]. In this section, we explain a leader election algorithm based on diffusing computations. In later sections, we will confer in detail how this algorithm can be adapted to a mobile situation.

A. *Leader Election in a Static Network*

We primary explain our election algorithm in the context of a static network, under the postulation that nodes and links never fail. The algorithm operates by primary "expanding" and next "Diminishing" a spanning tree rooted at the node that initiates the election algorithm. We submit to this computation-initiating node as the *source node*. As we will observe, after the spanning tree shrinks absolutely, the source node will have passable information to find out the most-valued-node and will then broadcast its uniqueness to the rest of the nodes in the network. The algorithm uses three messages, viz. *Election*, *Ack* and *Leader*.

1) *Election: Election* messages are used to "extend" the spanning tree. As soon as election is triggered at a source node *s* (for instance, upon exodus of its current leader), the node commences a *diffusing computation* by sending an *Election* message to all of its direct neighbors. Each node, *i*, other than the source, designates the neighbor from which it primary receives an *Election* message as its *parent* in the spanning tree. Node *i* then propagates the received *Election* message to every of its neighboring nodes (children) excluding its parent.
2) *Ack:* As node i accept an *Election* message from a neighbor that is not its parent, it instantaneously responds with an *Ack* message. Node i do not, On the other hand, instantly return an *Ack* message to its parent. Instead, it stays until it has received *Ack*s from all of its children, by sending an *Ack* to its parent. As we will see abruptly, the *Ack* message sent by i to its parent encloses leader-election information based on the *Ack* messages i has received from its children. Once the spanning tree has totally developed, the spanning tree "shrinks" back toward the source. Specifically, once all of i's outgoing *Election* messages have been accredited sends its pending *Ack* message to its parent node. Tree "contraction" instigates at the leaves of the spanning tree, which are parents to no other node. Ultimately, each leaf accepts *Ack* messages for all *Election* messages it has sent. These leaves hence finally send their imminent *Ack* messages to their relevant parents, who in turn send their pending *Ack* messages to their own parents, and so on, until the source node receives all of its imminent *Ack* messages. In its imminent *Ack* message, a node announces to its parent the identifier and the value of the most-valued-node amongst all its downstream nodes. Therefore the source node finally has adequate information to conclude the most-valued-node from among all nodes in the network, since the spanning tree extents all network nodes.
3) *Leader:* As the start node for a computation has received *Ack*s from all of its children, it then broadcasts a *Leader* message to all nodes publicizing the identifier of the most valued-node.

B. Key Management

A keying relationship is the state in which network nodes distribute keying material for utilize in cryptographic mechanisms. The keying objects can comprise public/private key pairs, secret keys, initialization parameters, and non-secret parameters supporting key management in diverse instances. Key management can be defined as a set of methods and procedures supporting the institute and maintenance of keying relationships among authorized parties. In précis, key management amalgamates techniques and procedures to ascertain a service supporting.
1) Initialization of system users inside a network
2) Creation, sharing, and installation of keying material;
3) Control over the use of keying substance;
4) Update, revocation, and obliteration of keying substance;
5) Storage space, backup/recovery, and archival of keying material, and
6) Bootstrapping and protection of trust in keying substance.

Substantiation is the basis of protected communication. Exclusive of a vigorous authentication mechanism in place, the remaining security purpose (confidentiality, data integrity, and non-repudiation) are in most instances not attainable. Authentication can only be realized by means of verifying somewhat known to be associated with individuality. In the electronic domain, the owner of the identity must have a publicly demonstrable secret associated with its identity; if not, the node can be impersonated. Authentication in general depends on the context of usage. Key management is apprehensive with the authenticity of the identities associated with the six services given over; it is a notion which may appear trivial at primary, but one that is not easily achieved. Authentication of users is predominantly intricate (and in most network settings impossible) devoid of the help of a trusted authority. The elementary function of key management schemes is the establishment of keying material. Key institution can be subdivided into key agreement and key transfer.

Key agreement permits two or more parties to originate shared keying material as a function of information contributed by or connected with, each of the protocol participants, such that no party can pre conclude the resulting value. In key transport protocols, one party creates or if not obtains keying substance, and securely transfers it to the further party or parties. Both key agreement and key transfer can be accomplished by using either symmetric or asymmetric techniques. A fusion key establishment method makes use of both symmetric and asymmetric method in an endeavor to utilize the benefits of both techniques.

IV. SIMULATION RESULTS & ANALYSIS

The simulation of the proposed scheme for the energy efficient routing is done using network simulator NS-2.34. This simulation tools uses the TCL scripting language to test our approach. Performance analysis of the proposed approach is done using measuring parameter PDR, Routing Load, Energy and Delay. It is an object oriented (OO) simulation written in C++, with OTCL interpreter as a front end. The simulation area for the proposed system is 1000 X 1000m and the parameter used for simulation is illustrated in table 1.

Parameters	Value
Network Simulator	NS2.34
Topology Size	1000 X 1000
Mac Layer	IEEE 802.11
No. Of Nodes	28
Packet Size	512 bytes
Initial Energy	1000 Joules
Idle Energy	.1
No. Of Source	1
No. Of Destination	1

Table1: Simulation Environment

A. *Result Analysis*

The comparative study of our proposed approach is done using different performance measuring parameters: energy, packet delivery ration, delay and routing load.

B. *Energy Expenditure*

Energy expenditure is calculated as the total expends energy divided by the total number of packets received. Our proposed approach in case of energy it gives better outcomes than the existing technique. This means that it helps to save more energy which is shown through graph and results in table 2.

Table 2: Energy expenditure result

Node	Energy Left-Existing	Energy Left-Proposed
0	0.313413	0.946665
1	0	0.537607
2	0.080009	0.646898
3	0	0.538627
4	0	0.55127
5	0	0.575807
6	0	0.591148
7	0	0.560346
8	0.093086	0.758617
9	0	0.550218
10	0	0.597383
11	0	0.543415
12	0	0.566334
13	0	0.552611
14	0	0.545841
15	0.038893	0.606696
16	0.076841	0.644756
17	0.110064	0.678046
18	0.185923	0.85167
19	0.027349	0.594811
20	0.096103	0.66739
21	0.023143	0.597488

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

22	0	0.546376
23	0.035211	0.602664
24	0.087703	0.655477
25	0	0.554594
26	0	0.541718
27	0	0.540395
28	0.006832	0.589492
29	0.004369	0.572358

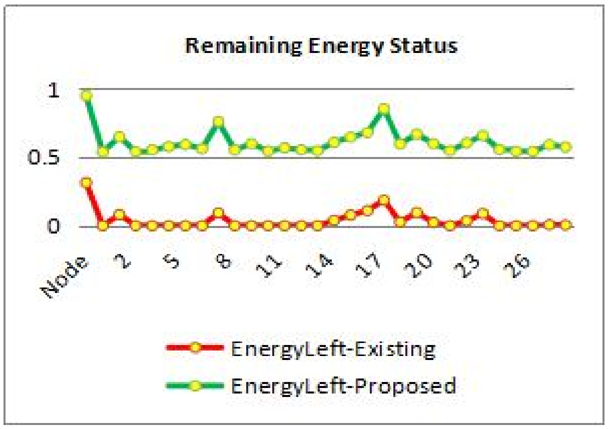

Fig. 4.1 Comparison of energy expenditure between proposed and existing approach Vs nodes

C. Packet Information

This parameter is used to evaluate the no of packet transmitted, packet receives and packet loss at the receiver end. Figure 4.2 and figure 4.3 shows the comparison of the proposed and existing system between the information and simulation time.

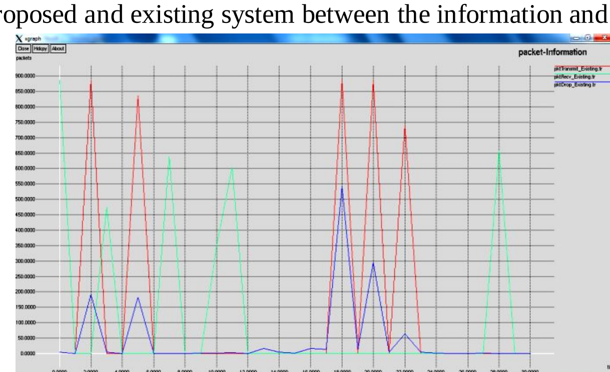

Fig. 4.2 Packet information for existing approach

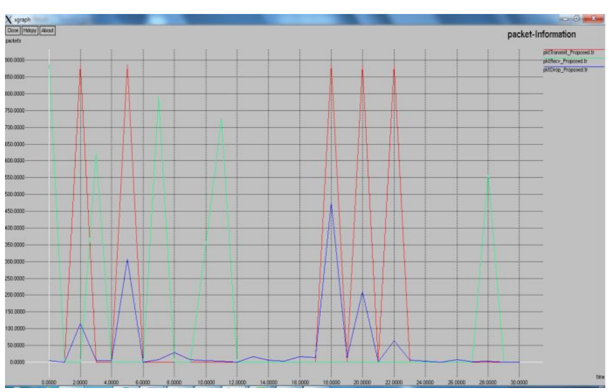

Fig. 4.3 Packet information for proposed approach

D. Packet Delivery ratio (PDR)

It is the ratio of number of packets effectively delivered to destination as the number of packets transmitted by source node. Simulation outcomes for PDR of proposed system are much more than the existing system which is shown in fig. 4.4.

Fig. 4.4 Packet Delivery Ratio Vs Simulation Time

E. Routing Load

It is the fraction of the entire routing control packets sent by all nodes over the number of received data packets at the receiver nodes. The routing load of the proposed approach is much optimal than the existing system in 1000 X 1000m grid area.

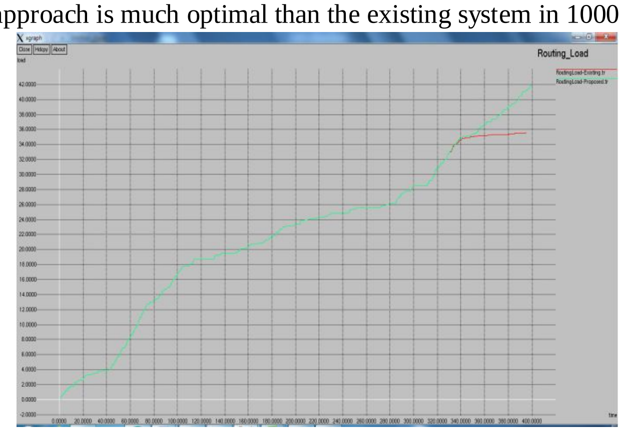

Fig. 4.5 Routing Load comparison between proposed and existing system

V. CONCLUSION

In this paper we use election algorithm and key management technique to preserve energy and make our network secure from the different threats. For simulation of our approach NS-2.34 network simulator uses and performance measurement is done using PDR, Energy, Delay, Routing Load and Packet information parameters The comparative analysis of our approach and existing approach is performed in which our approach outperforms than the existing ones and gives very good results. Our approach helps to save energy as well as makes the network secure.

REFERENCES

[1]. Amruta Kodole, P. M. Agarkar, " A SURVEY OF ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS", Multidisciplinary Journal of Research in Engineering and Technology, Volume 2, Issue 1, Pg.336-341: ISSN:2348-6953.

[2]. Tseng Y.C., Shen C.C, and Chen W.T. "Mobile IP and ad hoc networks: An integration and implementation experience" Technical report, Department of Computer Sci. and Inf. Eng., Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.

[3]. Vipan Chand Sharma, Atul Gupta, Vivek Dimri, "Detection of Black Hole Attack in MANET under AODV Routing Protocol", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[4]. X. Zhang, J. He ; Q. Wei "An Energy-Efficient Dynamic Key Management Scheme in Wireless Sensor Networks", Pervasive Systems, Algorithms, and Networks (ISPAN) on 14-16 Dec. 2009 Page(s):238 - 242 Print ISBN: 978-1-4244-5403-7 in proceeding of IEEE explore.

[5]. Xing Zhang, Jingsha He and Qian Wei "EDDK: Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks", EURASIP Journal on Wireless Communications and Networking 2010 in proceeding of Springer open access.

[6]. Sebastin Christhu Raj A, Helensupriya M, Shanmuga Priya S, "Reliable Energy Efficient Routing Algorithms In Wireless Ad Hoc Networks", International Journal Of Scientific & Technology Research Volume 3, Issue 4, April 2014 ISSN 2277-8616.

[7]. Pavithira Loganatha and T. Purusothaman, "An Energy Efficient Key Management And Authentication Technique For Multicasting In Ad Hoc Networks", Journal of Theoretical and Applied Information Technology 10th July 2013. Vol. 53 No.1 ISSN: 1992-8645.

[8]. Omar Smail, Bernard Cousin, Rachida Mekki and Zoulikha Mekkakia, "A multipath energy-conserving routing protocol for wireless ad hoc networks lifetime improvement" EURASIP Journal on Wireless Communications and Networking 2014, 2014:139.

[9]. Jeevaa Katiravan, D. Sylvia and D. Srinivasa Rao, "Energy Efficient Link Aware Routing with Power Control in Wireless Ad Hoc Networks", Hindawi Publishing Corporation the Scientific World Journal, Volume 2015, Article ID 576754, 7 pages.

[10]. Bhabani Sankar Gouda, Pinaki Prasad Panigrahi, "A New Optimal Approach for Improving Energy Efficiency in Wireless Ad-hoc Networks" Proceedings of IEEE Conference on Information and Communication Technologies 2013.

[11]. May Cho Aye and Aye Moe Aung "Energy Efficient Multipath Routing For Mobile Ad Hoc Networks" International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3, August 2014.

[12]. Annapurna P Patil, Dr K Rajani kanth , BatheySharanya, M P Dinesh Kumar, Malavika J "Design of an Energy Efficient Routing Protocol for MANETs based on AODV", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online): 1694-0814.

[13]. Sudarshan Vasudevan, Jim Kurose, Don Towsley, "Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks", National Science Foundation under grants ANI-0085848 and EEC-0313747001, and by the Defense Advanced Projects Research Agency under contract N66001-99-C-8616.

[14]. Abu Taha Zamani, Syed Zubair, "Key Management Scheme", International Journal of Emerging Research in Management &Technology in Mobile Ad Hoc Networks", ISSN: 2278-9359 (Volume-3, Issue-4)