Efficient Trusted Secure Ad-Hoc On-Demand Multipath Distance Vector In Manet

[1]A.Praveena, [2]R.Sangeetha, [3]P.E.Prem
[1]PG Scholar, [2]Assistant Professor, [3]Assistant Professor
[1]IT Department,
[1]Vivekanandha College of Engineering for Women (Autonomous), Tiruchengode, India

Abstract— **A mobile adhoc network is a continuously self configuring infrastructure less network of mobile device connected wirelessly. Each device in Manet is free to move independently in any direction. Routing in MANET is extremely challenging because of MANETs dynamic features, its limited bandwidth and power energy. Therefore Manet is exposed to series attack. This paper extends an Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing protocol is based on the nodes routing manners. The proposed Trusted Secure AOMDV aims at identifying and separating the attacks such as flooding, black hole, and gray hole attacks and given that energy saving in MANET. TS-AOMDV using Intrusion Detection System (IDS) and trust-based routing, to identify the attacks and seclusion are carried out in two phases of routing. The IDS friendly with each node performs operations in both the route discovery and data forwarding phases. To improve the routing performance, the IDS integrates the measured information into the TS-AOMDV routing protocol for the detection of attackers and using energy saving routing to save energy by coloring model. The sensor node get changed the colour by the node performance. This facilitates the energy efficient TS-AOMDV to provide better energy saving security in MANET.**

***Index Terms*— MANET,AOMDV,TS-AOMDV,ENERGY EFFICIENCY**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless nodes, which works well only if those mobile nodes are good and behave cooperatively. The lack of infrastructure support and resource constraint is the key issue that causes dishonest and non-co-operative nodes. Therefore, MANET is vulnerable to serious attacks [1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes.

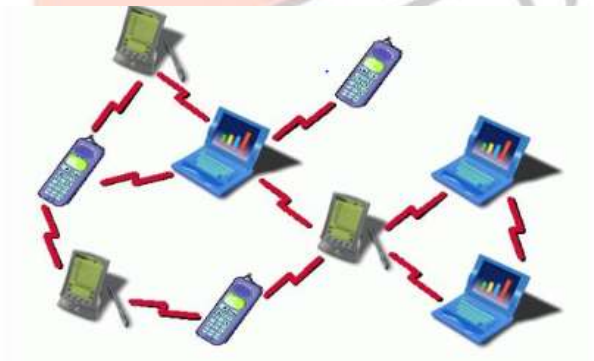

Fig 1: Mobile Ad-hoc Network

MANETs are a breed of wireless ad hoc network that habitually has a routable networking milieu on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. The MANET is a multi-hop distributed communication network comprising of a collection of mobile nodes that operate in a dynamic and self-organized manner [2].Each mobile node performs the data forwarding only through single or multihope communication due to the limited transmission range[3][4].

The nodes are free to moving about and categorize themselves into a network. These nodes frequently change the position. The network topology is quickly changing the wireless and it makes more difficult to make routing decision. since MANETs are infrastructure less, self organizing and self managing, network topology changes wireless, multihope, power constraint ,band width optimization, physical security, they are highly suitable for applications involving special outdoor events, commercial field, emergencies and natural disasters, and military operations, education field, network based on sensor, and device network.

The routing protocols design is used to find an appropriate path to route the data packet from the source to the destination. The routing process has to evolve capably and efficiency of the routing process in the attendance of dynamic network conditions, volatile mobility, limited energy, autonomous architecture, and resource constrained environment. The lack of infrastructure and

short communication range are the major reasons for mutual communication model. The ad-hoc on-demand multipath routing is the most popular advance in the MANET. However, these protocols is support multipath in Manet. The Ad-hoc On-demand Multipath Distance Vector (AOMDV) [5] routing protocol is a multipath extension of the AODV routing protocol.

Exploitation of ad-hoc network leads to many technical challenges such as limited wireless range, hidden terminals, packet loss, route changes, limited battery power, low quality communication, dynamic topology, and security [6]. But, the major issue in MANET is energy consumption and security since nodes are usually mobile and battery-operated. Power failure of a mobile node affects its functionality thus the overall network lifetime. Energy efficient routing is very essential in MANET.

Energy efficient and TSAOMDV routing techniques play a important role in saving the energy consumption, and providing better routing performance of the network. We decided to design an energy efficient routing protocol and TSAOMDV which reduces the total energy consumption, and providing high security to maximize the life time of the network.

II. RELATED WORK

Mobile Ad Hoc Networks (MANETs) is a wireless communications-less network, where nodes are free to move at any direction. The node co-operation is a crucial requirement in multi- hop routing for mobile ad-hoc network. The behavior of non-co-operation of nodes is egotistical and malicious. The mischievous nodes drop some of the packets. The battery power for the node is too low. The energy efficient routing protocols to optimize network concert Energy conservation is a major issue in the ad hoc networks for economy network life time with limited battery power. The lack of federal supervision and resource constraint is the key issue that causes dishonest and non-co-operative nodes. Therefore, MANET is vulnerable to serious attacks [7][8]. Some of the usual routing attacks are a gray hole, flooding, black hole, stealthy, and rushing attack [1][9][10].

The Manet needs to provide some application like commercial, education, healthcare and military. Due to lack of infrastructure, security in Manet is a challenging task, especially in multipath MANET [11].Attack can easily prevent data forwarding by breaking the wireless links among any mobile nodes located in the routing path [12]. The security issues in multipath routing are not considered in the conventional routing techniques [13]. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network [14].

The route discovery phase to determine the new routes to the destination from the source in case of route failure. This factor is initiate used for the conventional routing techniques. MANET is mainly alert on the problem of security and energy consuming problem on mobile nodes. For conserving energy, many energy-efficient routing protocols have been proposed [15], [16], [17], [18], [19], [20], [21], [22]. The energy efficient routing protocols can be generally classified into two categories:

Minimum Energy routing protocols [15],[16],[17],[18], [19],[20] and Maximum Network Lifetime routing protocols [21],[22]. The most energy-efficient path from the source to the destination, is near explore the minimum energy efficient routing protocol and while the energy-efficient routing protocols to provide increase the Network Lifetime and balance the remaining battery-power at each node in mobile ad-hoc network. we propose a ODBEERP protocol with a quick and low overhead path discovery scheme and an efficient path maintenance scheme for reducing energy consumption [23]. Power management system basically decides what time to deactivate radio transceiver of the mobile node to save energy [24]. The transmission range is stronger toward reduces the number of hops, while transmission power is low near topology slender resulting in network partitioning and high end-to-end delay due to hefty hop count [24].

III. SYSTEM MODEL

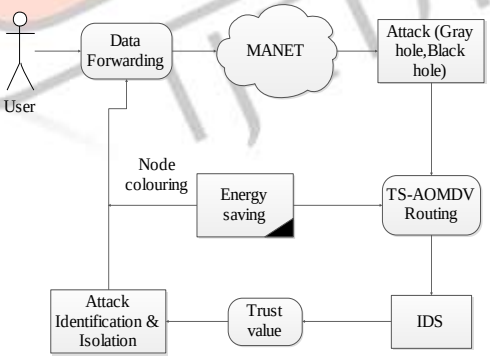

Fig 2: The Architecture for Energy Saving TS-AOMDV

The proposed Energy saving TS-AOMDV routing protocol aims to identify and isolate the attacks and saving the energy by using coloring model. The attacks are black hole, gray hole, flooding attacks in Manet. In the TS –AOMDV routing protocol using on IDS (Intrusion Detection System) and trusted based routing. The two phases of routing such as route discovery phase and data forwarding phase is also to identification and isolation of the attacks. The Route request flooding attack is launches within the route discovery phase. The blooding attack is toward attack the routing packet with the unreal destination address in the network.

An IDS monitors the packet generation rate of the source and assigns trust value of the corresponding source. The trust value of the source is lesser than the threshold, the consequent source is dropped. The second phase is data forwarding phase, an attacker is easily to attack the router and drop the packets. The IDS is monitoring the data forwarding activity and router assign the trust value for the entire router. When the trust value of the router is low from threshold it select from the interchange the path from further data forwarding.

The Energy saving routing is also included in TS-AOMDV routing to save node energy. Based on the common routing protocol, energy-saving routing introduces new measures related to power consumption in order to save energy after considering energy consumption factors. Node energy and data fusion should be considered during the routing protocol design.

IV. PROPOSED SCHEME

The proposed Energy saving TS-AOMDV routing protocol aims to identify and isolate the attacks and saving the energy by using coloring model. An IDS specifically looks for disbelieving activity and events that might be the result of an attack. The IDS is used to identification and isolation of the attacks. The two phases of data forwarding and route discovery process is using on the IDS.

In TS-AOMDV, the IDS run on the each node and monitoring the neighboring nodes of the routing activities toward informs network layer. The network layers to detect the routing attackers in the progression. The IDS is continuously monitoring the routing packet generation rate and data forwarding process to identify the behavior of the nodes.

The route identification and data forwarding phases is based on the control packets and data packets. When the intrusion detection system to provide inclusive routing security by both control packets and data packets of two phases. The measured statistics are integrated into the AOMDV routing protocol for the detection of attackers. Energy efficient TS-AOMDV routing protocol to improve the routing performance provides the security and consuming the energy. The IDS measured the trust value for route discovery and data forwarding phases.

1. Trust Evaluation for Source and Router

TS-AOMDV routing protocol using IDS. The IDS measure the source and router trust value for each nodes. The source trust value assign the inverse proportion of the RREQ count and router trust value is ratio between forwarded packet count and the received packet count. The trust value is stored in the trust table. The data forwarding process router are selected the most trusted routers.

Source-trust = (RREQ packet count)-1

Router-Trust= Forward packet Count/ Received packet Count. A node identifies the attackers when using the trust value. The source or router trust value is exceeds than threshold and identifies moreover isolates the attacker from the neighbor list.

2.TS-AOMDV routing progression

The proposed TS-AOMDV routing protocol aims to identify and isolate the attacks such as flooding, black hole, and a gray hole in a MANET. With the relieve of an IDS (intrusion detection system) and a trust-based routing. The IDS to identify the attack and isolation are carried out in two phases of routing such as route discovery phase and data forwarding phase.

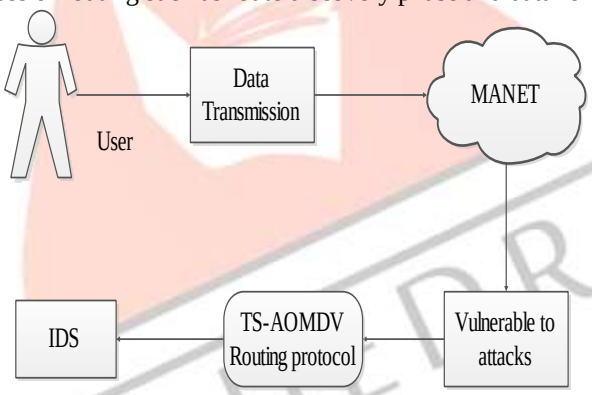

Fig 3: TS-AOMDV routing process

The route identification and data forwarding phases is based on the control packets and data packets. When the intrusion detection system to provide inclusive routing security by both control packets and data packets of two phases. TS-AOMDV routing protocol to improve the routing performance and providing the high security.

A. Trust Based Route Discovery Process

The Route request flooding attack is launches within the route discovery phase. The blooding attack is toward attack the routing packet with the unreal destination address in the network. An IDS monitors the packet generation rate of the source and assigns trust value of the corresponding source. Initially each node assigns the trust value like one. According to the route discovery of these node the IDS measures the original trust value and informs to the network layer. When IDS check the trust value for all the neighboring nodes. The source node sends the RREQ packet the neighbors, every node checks for the trust value of the source. If the source trust value is lower than the threshold value, then the source is dropped to block the blooding activity of the attacker. If the trust value of the source node is different from all the nodes. The source trust value is lower than threshold value, so the source do not forwarded the RREQ packet of the source node into the destination node.

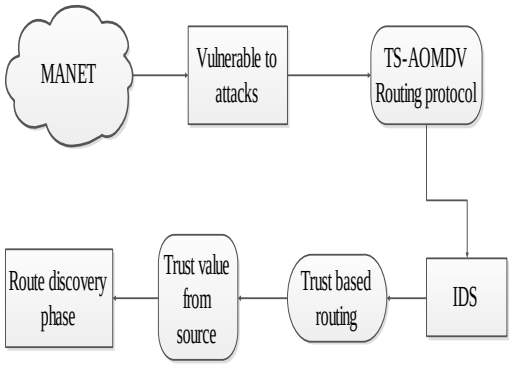

Fig 4: Route Discovery Phase: Route Request Flooding Attack Detection and Isolation

B.Trust Based Data Forwarding Process

The data forwarding process is conceded out based on the router. This process phased on the two attacks, black hole and gray hole. The attacker is blocked to only for the router. If the router forwarding the data packet, for every node checks the trust value of the router. The router trust value is lower than threshold; the current data transmission through malicious router is blocked.

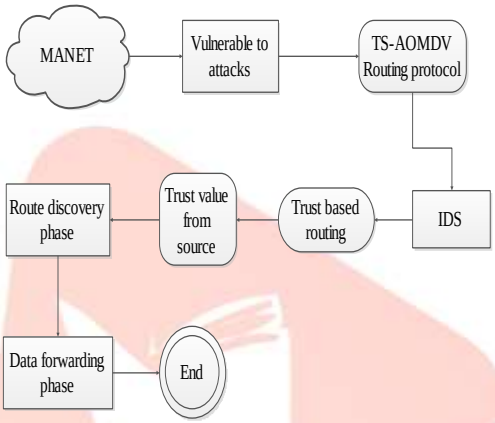

Fig 5: Data Forwarding Phase: Data Dropping Attack Detection and Isolation.

It consist of two neighboring nodes such as router A and router B .The trust value of router A is 0.0 and router B trust value is 1.0. The current node of router A trust value is lower than threshold, so the IDS is monitored and discarded the data. The trust value of the node B is higher than node A. When the data forwarding this source node is selects for router B. Thus the TS-AOMDV routing protocol improve the routing performance and providing the security in Manet with a help of IDS.

V. PERFORMANCE ANALYSIS

The Proposed protocol is resistant to two types of routing attacks launched over data packets and control packets such as data dropping attack and a request packet flooding attack. The IDS attached with each node performs operations in both the route discovery and the data forwarding phases. The performance of the TS-AOMDV protocol is evaluated using Network Simulator (NS2) in terms of overhead, packet delivery ratio, end to end delay, packet loss and energy consumption.

1. Experimental Setup

The NS2 simulation is employed to evaluate the performance of proposed Energy saving TS-AOMDV routing protocol. The simulation model consists of 50 to 90 deployed nodes within the square network area of 600m x 600m to transmit data packets of 1024 bytes. The node communication range is 250m, and it is capable of communicating directly with others in the range of 250m. The network is simulated for 30 seconds. The performance of the proposed Energy saving TS-AOMDV is evaluated and compared with the existing AOMDV. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 2

2. Performance Metrics

We evaluate mainly the performance according to the following metrics.

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

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.

Results:

Figure 5 shows the results of No.of Nodes Vs overhead. From the results, we can see that ODBEERP scheme achieves low overhead than the PEER and MTRTP protocol.

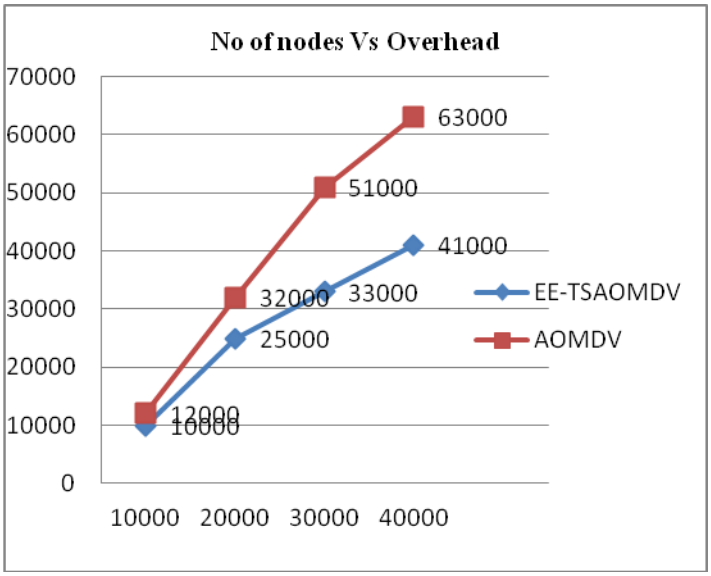

Fig 5: No of nodes Vs Overhead

Figure 6 show the results of packet delivery ratio for the throughput. Clearly our EETSAOMDV achieves more packet delivery ratio than the AOMDV.

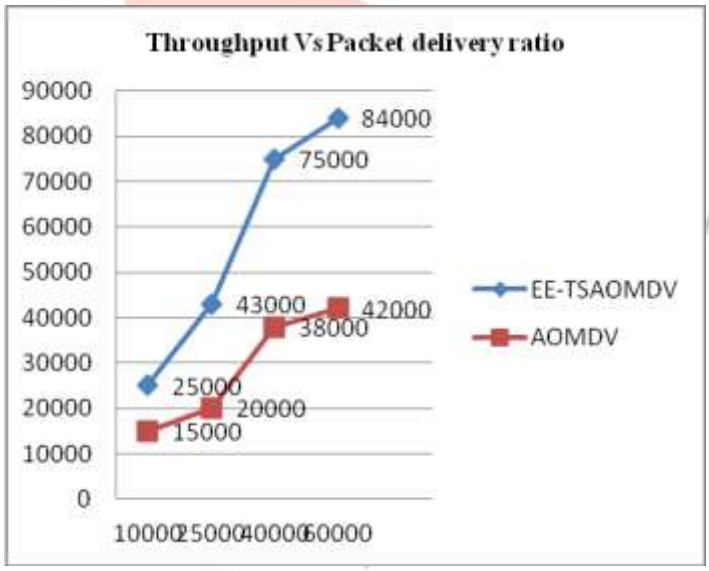

Fig 6: Throughput Vs Packet delivery ratio

Figure 7 show the results of Speed Vs Energy Consumption per packet (mJ) under Different Node density (Static) scenarios for the 10, 20,30,40,50 …..100 speed. Clearly our EETSAOMDV Protocol consumes less energy per packet than the AOMDV protocol.

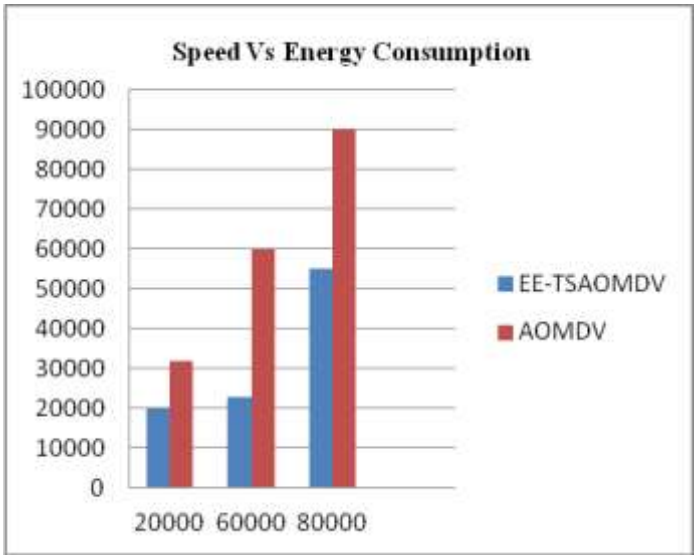

Fig 7: Speed Vs Energy consumption

Table 1 Parameters

No. of Nodes	50 to 90
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	30 sec
Traffic Source	Constant Bit Rate (CBR)
Packet Size	1024 bytes
Mobility Model	TwoRayGround model

V. CONCLUSION

T In this paper, we proposed an energy efficient Trusted Secured Ad-hoc On-Demand Multipath Distance Vector, TS-AOMDV was clearly intended to accomplish security and trim down energy consumption in order to maximize the lifetime of the network. The proposed TS-AOMDV routing protocol is flexible and aggressive with two types of routing attacks launched over data packets and control packets, such as gray hole and black hole, and request packet flooding attack. The IDS attached with each node, performs two operations such as route discovery and data forwarding process. The IDS measured and comparing the trust values with the threshold, and easily captures the different types of attackers in various routing phases. Moreover, the performance of the proposed protocol is simulated using NS2. The proposed Energy Efficient Trust based Secured AOMDV (EETS-AOMDV) is compared with the existing AOMDV in terms of throughput, energy consumption and overhead through the simulation model. The simulated results show the superiority of the proposed protocol in various scenarios.

REFERENCES

[1] Abrar Omar Alkhamisi, Seyed M Buhari, "Trusted Secure Ad-hoc On-Demand Multipath Distance Vector Routing in MANET",2016 IEEE 30th International Conference on Advanced Information Networking and Applications, pp.212-219,2016.

[2] Erciyes, K. "Distributed Graph Algorithms for Computer Networks", Computer Communications and Networkss, London: Springer, pp. 259- 275, 2013.

[3] S.Abdel Hamid, H. Hassanein and G. Takahara, "Routing for Wireless Multi-Hop Networks: Unifying Features", Springer Briefs in Computer Science, pp. 11-23, 2013.

[4] Hamid, S. A., Hassanein, H., & Takahara, G., "Routing for Wireless Multi Hop Networks–Unifying and Distinguishing Features", School of Comp.—Queen's University, Canada, report 583, 2011.

[5] Mahesh K. Marina, and Samir R. Das, "Ad hoc on-demand multipath distance vector routing," Wireless Communications and Mobile Computing, Vol 6, No. 7, pp. 969-988, November 2006.

[6] Imrich Chlamtac, Marco Conti & Jennifer J.-N. Liu, (2003) "Mobile ad hoc networking: imperatives and challenges", Ad-hoc Networks, Elsevier, pp 13-64.

[7] Habib, S., Saleem, S., & Saqib, K. M., "Review on MANET routing protocols and challenges", IEEE Student Conference on Research and Development SCOReD, pp. 529-533 , 2013.

[8] Mahmoud, Mohamed MEA, and Xuemin Sherman Shen. "Secure routing protocols." Security for Multi-hop Wireless Networks. Springer International Publishing, pp. 63-93, 2014.

[9] Shanmuganathan, V., and T. Anand. "A Survey on Gray Hole Attack in MANET." IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), pp. 2250-3501, 2012.

[10] Tayal, S., & Gupta, V., "A Survey of Attacks on Manet Routing Protocols", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, No.6, pp. 2280-2285, 2013.

[11] Vaidya, Binod, et al. "Secure multipath routing scheme for mobile ad hoc network." Third IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 163-171, 2007.

[12] C. Tachtatzis and D. Harle, "Performance evaluation of multi-path and single-path routing protocols for mobile ad-hoc networks", Performance Evaluation of Computer and Telecommunication Systems,2008. SPECTS 2008. International Symposium on, pp. 173-180, 2008.

[13] Eliana Stavrou, Andreas Pitsillides,"survey on secure multipath routing protocols in WSNs," Computer Networks, vol. 54, no.13,pp 2215–2238, 2010. Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks

[14] Nidal Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks," IEEE Communications Society subject matter experts for publication in the ICC, pp 1154-1159, 2007 .

[15] K. Scott and N. Bambos, "Routing and Channel Assignment for Low Power Transmission in PCS," Proc. Fifth IEEE Int'l Conf.Universal Personal Comm. (ICUPC '96), Oct. 1996.

[16] S. Doshi, S. Bhandare, and T.X. Brown, "An On- Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, July 2002.

[17] V. Rodoplu and T. Meng, "Minimum Energy Mobile Wireless Networks," IEEE J. Selected Areas in Comm., vol. 17, no. 8, pp. 1333-1344, Aug. 1999.

[18] S. Banerjee and A. Misra, "Minimum Energy Paths for Reliable Communication in Multi-Hop Wireless Networks," Proc. ACM MobiHoc, June 2002.

[19] J. Gomez, A.T. Campbell, M. Naghshineh, and C. Bisdikian, "Conserving Transmission Power in Wireless Ad Hoc Networks," Proc. IEEE Ninth Int'l Conf. Network Protocols, Nov. 2001.

[20] J. Zhu, C. Qiao, and X. Wang, "A Comprehensive Minimum Energy Routing Protocol for Wireless Ad Hoc Networks," Proc. IEEE INFOCOM, Mar. 2004.

[21] C.K. Toh, H. Cobb, and D. Scott, "Performance Evaluation of Battery-Life-Aware Routing Schemes for Wireless Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '01), June 2001.

[22] A. Misra and S. Banerjee, "MRPC: Maximizing Network Lifetime for Reliable Routing in Wireless Environments," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '02), Mar. 2002.

[23] Gopinath.S1, Sureshkumar.N2, Vijayalakshmi.G3, Natraj.N.A4, Senthil.T5 & Prabu.P6, "Energy Efficient Routing Protocol for MANET," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 ,pp.292-298.

[24] M.Siddappa, Sridhar.H.S, "A Survey of Energy Efficient Routing Protocols In Mobile Ad-Hoc Network," IJEEAR Vol 03, Issue 03; July-Sep2012.