Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P) Vol.9 No.2, 2020, pp.1-8

DOI: https://doi.org/10.51983/ajes-2020.9.2.2549

Secure And Energy Efficient Stochastic Optimized Routing Protocol for Mobile Ad Hoc Network

Krunal Sudhirbhai Bhavsar
Coordinator, BCA & BBA Department ,
V.S. Patel College of Arts & Science, Bilimora, Gujarat, India
E-mail: bhavsar_tk@yahoo.co.in
(Received 2 May 2020; Revised 24 May 2020; Accepted 26 June 2020; Available online 3 July 2020)

***Abstract* - Mobile Ad-hoc Network is a wireless mobile nodes network, which forms a network without any pre existing fixed network infrastructure support. MANET permits versatile communication between hosts that are moving around. MANETs have numerous advantages compared to traditional wireless networks. In MANET, each mobile node needs the cooperation of other nodes in the network for forwarding data packets from source to destination node. Mobile Ad-hoc Network includes different routing protocols for communication and in MANET each mobile node can act as host as well as sender or receiver at the same time. MANET is design to smartly react to network changes and operates without human interference to support nodes mobility. Mobile Ad-hoc Networks are designed to sustain its survivability in unfriendly and hostile conditions such as natural disasters and other emergency conditions. However unique characteristics of MANETs topology such as open peer-to-peer architecture, dynamic network topology, shared wireless medium and limited resource (battery, memory and computation power) pose a number of non-trivial challenges to security design. These challenges and characteristics require MANETs to provide broad protection and desirable network performance. Due to dynamic nature of MANET it is very challenging work to employ a secure route. The routing protocols play important role in transferring data. Mobile Ad Hoc Networks (MANETs) pose challenges in terms of energy control, due to their fixed transmission power, the mobility of nodes and a constantly changing topology. High levels of energy are needed in wireless networks, particularly for routing. In order to address this problem, energy enhancement is analyzed with the proposed dynamic AODV cluster base trust protocol, with the aim of maximizing the lifetime of the network. We have performed simulation of our approach to justify our research work on network simulator-2 (NS-2). Simulation result presents that our proposed approach result is improved the performance of network than the existing Mobile Ad hoc Network protocol.**
***Keywords*: MANET, Routing Protocol, Energy Efficient.**

I. INTRODUCTION

A. Wireless Mobile Networks

Electromagnetic waves are used by Wireless technology to communicate data from one point to another. In the late 1990's after the definition of wireless standards by IEEE, wireless networking turns out to be viable for a widespread range of personal and business applications and subsequently, it has been utilized in particular applications for decades. Wireless networks have developed more common because of better accessibility of technologies and lower costs. In addition to mobility, wireless networking offers several other benefits over wired connections such as adaptability, ease of connectivity, and usage in locations that forbid wiring. A wireless mobile network usually mentions to a telecommunication network, which is employed by means of radio frequency. Most common method of wireless mobile communication is the cellular phones. Moreover, that, other standards for wireless networks are Bluetooth and WLAN etc.

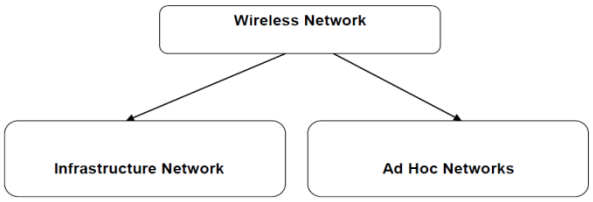

Fig. 1 Wireless network classification

Based on two different methods to communication between mobile devices, wireless mobile networks can be sorts in two types:

1. Infrastructure Based Network or Single Hop (Ex: Cellular, WLAN)
2. Infrastructure Less Network or Multi-hop (Ex: Ad hoc)

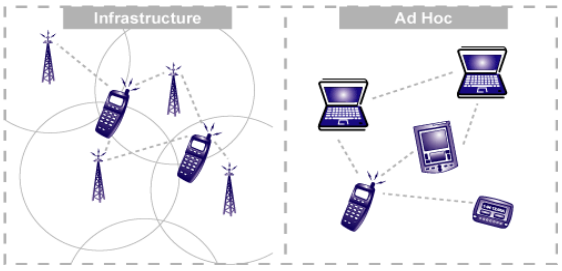

Fig.2 Infrastructure based cellular topology and Ad Hoc network

B. Infrastructure Based Networks

Typically wireless mobile networks depended on the cellular idea with great infrastructure support in which mobile hubs correspond with each other by means of access points where the access points give an infrastructure in

terms of immobile network availability. Indeed, the source mobile hub corresponds with its closest base station, in order, transmits the data to the closest base station of the objective hub. Be that as it may, when a mobile hub is situated at a crossing point of the scope range of two base stations, it is changed to the base station with the more grounded signal with no interruption in the communication and without the user getting to be mindful of it. Hence in this course of action, every hub dependably lies in the transmission scope of some base station rendering the network a solitary bounce model. Distinctive examples of infrastructure base wireless mobile networks are GSM, UMTS, WLL, and WLAN and so forth. (Safwat, A., et.al, 2002)

C. Infrastructure less Networks

Infrastructure less networks are another kind of wireless mobile networks based on radio to radio multi-hopping model. Each hub imparts without utilizing any prior altered network base wherein all hubs are able to perform like virtual routers taking part both in figuring and keeping up the routes. The prior wireless ad hoc networks supported by DARPA in the mid-1970s were likewise alluded to as packet radio multi-hop networks. These networks are getting prevalent these days because of simplicity of setup and nonappearance of cabling problems. As a result of transmission power limitation, nodes that communicate with different hubs specifically or by implication through intermediate hubs that rely on its packets. Such networks serve a developing number of uses which depend on a quickly deployable, multi-hop, wireless infrastructure. (Saadawi, T., and Hussein, O. 2005).

Wireless mobile networks with infrastructure less approach can be further categories in two types:

1. Smart Sensor Networks (SSN)
3. Mobile Ad hoc Networks (MANET)

A brief discourse of the above networks is given in the following sections.

D. Smart Sensor Networks

A sensor network is a densely organized gathering of minimal cost, minor working together wireless calculating gadgets called sensor hubs shaping an interim network without the guide of any central organization or bolster administrations. Sensor hubs can quantify, assemble, prepare, break down and disperse natural data like light conditions, mugginess, temperature and seismic activities. Users can access the information by means of a gateway, called base station, which sends real questions into the sensor network. Every sensor comprises of detecting and information preparing segments and capable of taking care of mobile communication. So as to support routed communications between two mobile hubs, the routing protocol decides the hub connectivity and routes packets likewise. In a sensor network, the MAC addresses might be a substantial part of the small size packets. This condition has made a mobile ad hoc sensor network exceptionally adaptable so it can be conveyed in all situations. Still, intrinsically these hubs are asset obliged and inclined to blunders. (Akyildiz, I. F., *et.al*, 2002)

Some applications of sensor networks are smart sensors and actuators entrenched in user electronics, chemical/biological detection, data tracking of environmental conditions, precision agriculture, supply chain management, and structural health monitoring (detecting damage in buildings, highways, bridges, factories and aircraft) to recover public safety. Great numbers of sensors, efficient use of the small memory, low energy use, data aggregation, collaborative signal processing, network self-organization, and enquiring capability are the key features of these networks. Thus, wireless sensor networks understand the idea of prevalent figuring by bridging the gap between computer organizations and the real world.

E. Mobile Ad Hoc Network

A Network eases the delivery of files and information between multiple computers. Computer networks can be unified either over Ethernet cables or by means of wireless cards that send and receive data or wireless medium like air. An Ad hoc network founds a connection between numerous nodes without any base station. (Abolhasan, M., *et.al*, 2004) Mobile Ad Hoc Networks (MANETs) are speedily becoming a common mode in telecommunication due to easy placement and fast formation. They are used in disaster circumstances like flooding, earthquake, hurricane, and military.

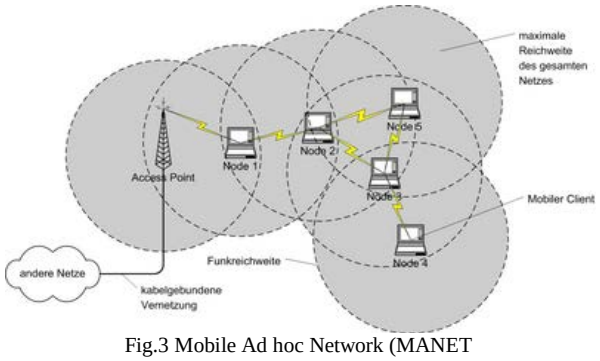

Fig.3 Mobile Ad hoc Network (MANET

A simple classification like the wired and the wireless network is prepared based on assets like wire and air. Wireless communication experiences challenge like link stability, bandwidth constraints, mobility, MAC layer designing, and node energy and so on. The wireless networks are classified into two types. (i) Infrastructure network requires a base station to the function (ii) Infrastructure-free network where all the nodes work without a base station.

A mobile ad-hoc network is a group of mobile nodes that are energetically and subjectively situated in such a way that the interconnections between nodes are able to alter on a repeated basis. These networks are constructed by the wireless nodes which have to perform the routing process as well furthermore to the information exchange. The MANET topology alters frequently as mobile hosts transfer, disappear that is failure or reduction of battery capacity, or regulate their transmission and reception features. (Lee, S. J.,*et.al*, 2000)

These networks use broadcasting as a method for communication, for updating the topology, maintaining the network, giving warning messages. They consist of a group of nodes that communicate with each other over a wireless medium like air without the need for any predefined infrastructure. All the nodes are working as source, router or destination. The topology of the network can change dynamically because the nodes move in different directions, leave or join it. Such change creates problems in maintaining the routing process through energy loss, delay and instability in linking. So, the routing protocol must be designed to provide energy maintenance, avoid delay and make the link stable.

Mobile ad-hoc network discovers incredible applications in calamity retrieval procedures, hybrid mesh networks, collaborative and distributed computing, and military operations in remote areas. Mostly the deployment of MANET is in areas where there is a scarcity of resources. Therefore, it is necessary that the resources in the MANETs be used in an efficient manner. A MANET can exist and work if and only if the participating nodes behave in a cooperative manner wherein the data packets of other nodes are faithfully forwarded. But the problem arises due to following factors:

1. The network topology in MANET is dynamic due to the mobility of nodes leading to the change in the connectivity among the nodes.
2. The connectivity may also vary with time due to departure or arrival of nodes in the network.
3. MANETs are vulnerable to black hole (Packet Dropping) attacks launched by malicious nodes.
4. MANETs are vulnerable to grey-hole (Selective Forwarding) attacks launched by selfish nodes.
5. With the time, the nodes which were earlier cooperative may become selfish due to loss of power.

All these characteristic features of MANETs the design of routing protocol is a challenging task even today. There has always been the need for efficient routing protocols which enable the nodes to communicate over multi-hop paths without centralized routers.

These complex issues have posed many open problems for researchers and provided them opportunities for making significant contributions to this area. The next section discusses the basic characteristics of these networks.

II CHARACTERISTICS OF MANET

1. MANET is a collection of wireless devices that come together to form a self-organizing network without any support from the existing fixed communication infrastructure. (Jubin, J., & Tornow, J. D. 1987) These devices are mobile in nature and are free to move in and out of the network with/without notifying the other nodes in the network.
2. The communication in ad-hoc networks is multi-hop in nature. Each node in the network has to relay data packets between other nodes for the successful communication of MANET as shown in Fig. 4.
3. This strategy of multi-hop communication ensures longer battery life because a lot of transmitting power (proportional to fourth power of the distance between the communicating nodes) is saved (Gregory S. Lauer. 1995). The main characteristics of MANET are as follows:

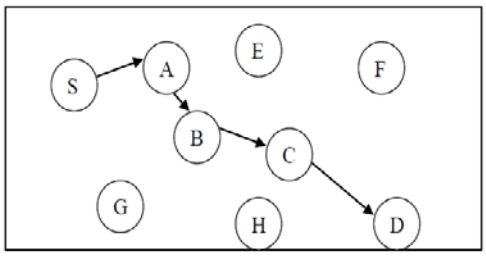

Fig.4 Communication in MANET

Dynamic topology*:* The network topology in MANET is highly dynamic due to movement of nodes; hence an ongoing session suffers frequent path breaks. Disruption occurs either due to the movement of intermediate nodes or due to movement of end nodes. Such situations do not arise in wired networks wherein the nodes are stationary (Mahmud, S. A., et.al, 2006).

Bandwidth constraints and variable link capacity*:* Abundant bandwidth is available in wired networks due to the advent of fiber optics and due to the exploitation of wavelength division multiplexing technologies. But in wireless networks, the radio band is limited, and hence, the data rates available are far less in comparison to wired networks. (Abolhasan, M., et.al, 2009)

Energy constrained nodes*:* Mobile nodes rely on batteries for proper operation. Since an ad hoc network consists of several nodes, depletion of batteries in these nodes will have a great influence on overall network performance. While designing any protocol for MANET this factor is taken into account.

Multi-hop communications*:* Due to signal propagation characteristics of wireless transceivers, ad hoc networks require the support of multi-hop communications i.e. mobile nodes that cannot reach the destination node directly will need to relay their messages through other nodes.

Limited security: In MANETs we don't have centralized devices such as routers and switches which can share the major burden of security. The nodes in these networks must have inbuilt capabilities to avoid resource consumption, denial of service, impersonation, and similar attacks possible against MANET. (Lee, M. H., et.al, 2008)

III. ENERGY EFFICIENCY

Since MANET are a set of nodes that agree upon forming a spontaneous, temporary network with the lack of any centralized administration, any form of infrastructure and nodes are typically powered by batteries with a limited energy supply, each node ceases its function when the battery exhausts. Therefore, given the energy constraints placed on the network's nodes, designing energy efficient routing protocols is an important issue for MANET, maximizing the lifetime of its nodes and thus of the network itself (Li, J., et.al, 2005). Minimum Weight Incremental Arborescence (MWIA) (Lau, K. S, et.al, 2006), RB-MIDP and D-MIDP (Cheng, M. X., et.al, 2006) are examples for energy-efficient multicast routing.

IV. ADVANTAGES OF MANET

Mobile Ad Hoc Network due to its infrastructure-less structure and node mobility possess following advantages:

Fast installation: The level of flexibility for setting up MANET is high since they do not require any previous installation or infrastructure, therefore, can be brought up and torn down in very short time.

Dynamic topologies: Nodes can arbitrarily move around the network and can disappear temporally from the MANET, so the network topology graph can continuously change at undetermined speed.

Fault tolerance: Owing to the limitations of the radio interfaces and the dynamic topology, MANET is robust enough to handle connection failures. The routing and transmission control protocols are designed to manage these situations.

Self-configuring: MANET has decentralized infrastructure, with all mobile nodes functioning as routers and all wireless devices being interconnected to one another. Intuitively, this means that the MANET is also a self-configuring network in which network activities like the discovery of the topology and delivery of messages, are executed by the nodes themselves.

Connectivity: The use of centralized points or gateways is not required for the communication within the MANET and the communication takes place due to the collaboration between the participating nodes.

Mobility: The wireless mobile nodes can move with random speed and can take random direction. Although the routing algorithms deal with this issue, the performance shows that there is a threshold level of node mobility after which the protocol operation begins to fail.

Cost: MANETs are more economical in the case of temporary installation as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes.

Spectrum reuse possibility: Owing to short communication links (node-to- node instead of the node to a central base station) it is possible to use same frequency band in different places of the network.

V. LIMITATIONS OF MANET

The highly adaptive networking technology in the form of MANET still faces various limitations. Some of these limitations are as given below:

Bandwidth constraints: As mentioned above, the capacity of the wireless links is always much lower than in the wired links. Several Gbps are available for wired LAN nowadays while the commercial applications for wireless LANs work typically around 2 Mbps. (Royer, E. M., et.al, 2001)

Processing capability: Most of the nodes in MANETs are devices without a powerful CPU. The network tasks such as routing and data transmission cannot consume the power resources of the device, as it is intended to play other roles such as sensing functions. (Camp, T., et.al, 2002)

Energy constraints: The power of the batteries is limited, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why more energy conserving algorithms have been implemented.

High latency: In an energy conserving design, nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake up. (Divecha, B., et.al, 2007)

Transmission errors: Attenuation and interferences are other effects of the wireless links that increase the error rate. (Bai, F., & Helmy, A. 2004)

Security: The authors divide the possible attacks in passive ones when the attacker only attempts to discover valuable information by listening to the routing traffic; and active attacks, which occur when the attacker injects arbitrary packets into the network with some proposal like disabling the network.

Addressing: The addressing is the another problem for the network layer in MANET since the information about the IP address used in fixed networks offers some facilities for routing that cannot be applied in MANET.

Commercially unavailable*:* MANET is yet far from being deployed on the large-scale commercial basis.

Due to all the above limitations mentioned above, it is always a challenging task for the researchers to develop a routing protocol for MANET. The next section discusses the routing strategies present in the protocols available in the literature for MANET. (Bai, F., *et.al*, 2004)

VI. SIMULATION

System machine broadly speaking called NS2 is simply an incident driven reenactment equipment that has incontestable valuable in examining the active approach of correspondence systems. Reenactment of wired and in addition remote system capacities and conversion (e.g., steering calculations, TCP, UDP) should be possible utilizing NS2. A reenactment study was completed to charge the implementation of MANET steering convention. For example: DSDV, AODV and DSR taking into account the measurements throughput, parcel transportation proportion, and normal end-to-end delay with NS2.

VII. PROBLEM ON HAND

Mobile unexpected system is that the own-configuring, infrastructure less complex cellular phone connected while not wires. Each device in moves severally all told directions. Main challenge to make MANET is to furnish all tools to sustain the knowledge essential to accurately direction traffic. The lively nature of transportable impromptu set-up creates it terribly difficult to use in protected steering. The routing protocol plays a major role in sending knowledge.

Current study inspects the accessible secluded navigation of steering etiquette in MANET to beat the matter in map-reading safety. Belief primarily based secure routing is projected for modeling of safe and energy potency of Mobile ad hoc network. It has several problems in terms of transmission power, force management, & knob quality. The vigor improvement is analyzed supported cluster-based dynamic informal On-demand distance vector that may be a routing protocol for MANET and different systems. Unprepared on demand distance vector is especially employed in ZigBee.

AODV protocol creates network flexibility among nodes only the supply lump requests the routes. Directions stay active only the info. Packets travel along lane between supply & designation. Once the supply stops causing packet, way is stopped. This will support each unicast and multicast protocols.

Ad hoc on demand distance vector doesn't want any central body system for handling secure routing. The protocol has larger information measure share. Main disadvantage of this protocol includes high process demand, consumes additional share of the information measure, and needs longer for construction course-plotting table.

VIII. PROTOCOL PERFORMANCE EVALUATION

A. Choosing the Environment

To evaluate the performance of the designed protocol need was felt to choose a suitable environment which would ensure that the protocol performance has been properly checked and evaluated. There were following alternatives:

1. To take up an actual MANET scenario and evaluate the performance
2. To use NS-2 a freeware software

B. Performance Metrics

The various parameters that were estimated during the simulation are as follows:

Packet Delivery Ratio: It is defined as the ratio of a number of packets received to that of the number of packets sent as in Equation 1.1.

$$\text{Packet Delivery Ratio} = \frac{Totaldatapacketssent}{Totaldatapacketsreceived} \quad (1.1)$$

Control overhead: It is defined as the sum of a number of route requests, route replies & route errors as in Equation 1.2.

Control overhead = RREQ+RREP+RERR in packets (1.2)

Average Remaining Energy: It is taken as the average of the remaining energy levels of all the nodes in the network as in Equation 1.3.

$$\text{Average remaining energy} = \sum \frac{remainingenergyofindividualnodes}{totalnumberofnodes} \quad (1.3)$$

End-to-End Delay: It is the overall average delay experienced by a packet from the source to that of the destination. This is the average time involved in the delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets as given in Equation 1.4.

$$\text{Average end to end delay} = \sum \frac{Timereceived - Timesent}{Totaldatapacketreceived} \quad (1.4)$$

Average Hop Count: Average number of hops for all successful route formation.

Throughput: How fast data can pass through a network. In our simulation scenario, it is the number of bits passing through the network in one second.

Network Lifetime: It is Time at which the first node of the network gets dead.

The simulation input parameters apart from varying values used for study and analysis are given in Table I

TABLE I PARAMETERS USED FOR SIMULATION

PARAMETERS	VALUE
Simulation area	1000*1000
Number of nodes	105
Node communication range	50
Mobility model	Random waypoint
Routing protocols	AODV
MAC	802.15.4
Initial node energy	1000
Node-placement	Uniform

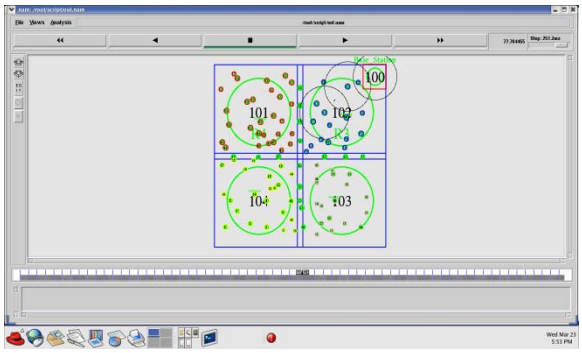

Fig.5 Output for data transmission from novel nodes to base station

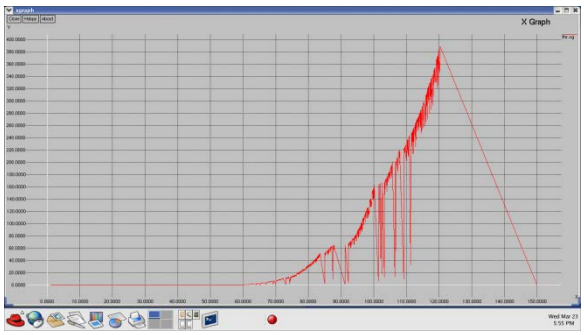

Fig.6 X graph for network throughput

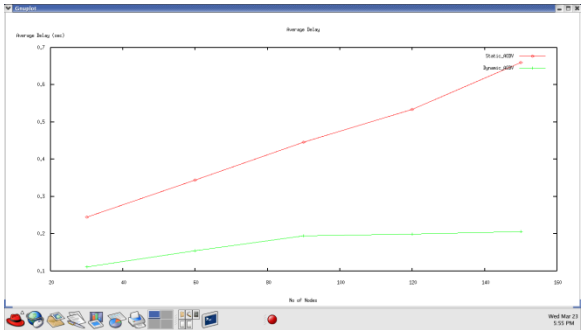

Fig.7 Average delay for static and dynamic AODV

Fig. 8 shows the results of average end-to-end delay for varying the nodes from 20 to 160. From the results, it shows that dynamic AODV scheme has a lower delay than the static AODV scheme because of authentication routes. When the density of the node increases from 20 to 160 nodes the average end to end delay of the end nodes also increases because of the time consumed for route discovery and the increasing number of packets in the buffer. The statistics show that the dynamic protocol reduces the average end to end delay by 28.5% over the static protocol.

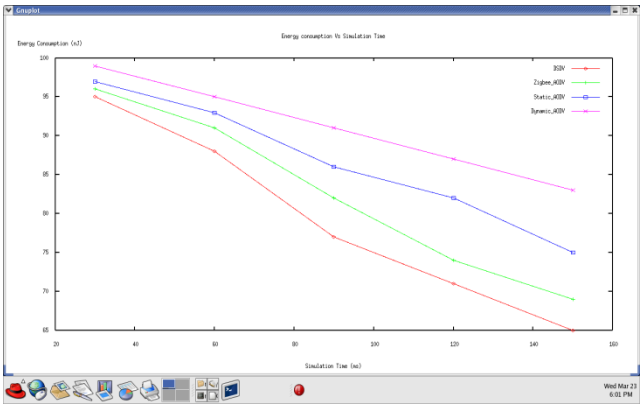

Fig.8 Energy consumption VS simulation time for different protocols

The Network losses comparison is shown in Fig.1.9. The result shows that the network loss is minimum in energy efficient secure dynamic AODV compared to the static AODV.

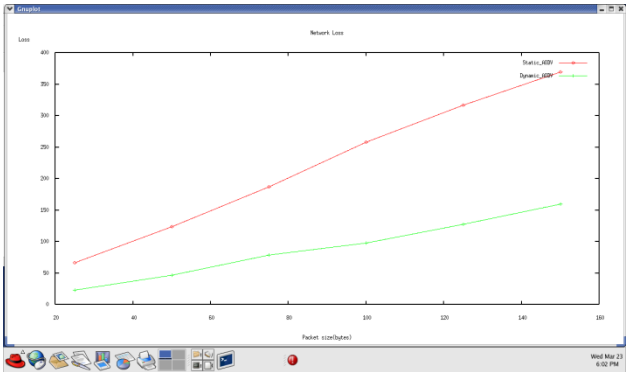

Fig.9 Network loss for static and dynamic AODV

Fig.10 shows the graph between varying number of nodes and the packet delivery ratio for proposed energy efficient routing protocols and the existing DSDV protocol.

When the density of the node increases from 20 to 160 nodes the average packet delivery ratio increases because of the number of routes available to broadcast the packets from the source node to the destination node. The simulation results show the energy efficient dynamic AODV protocols increases the PDR over the DSDV and static AODV protocol.

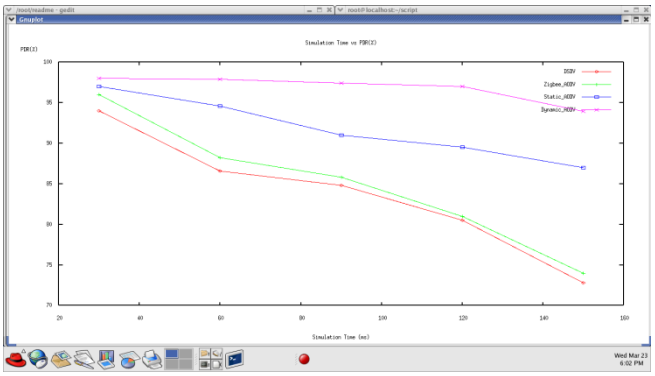

Fig.10 Packet delivery ratio VS simulation time

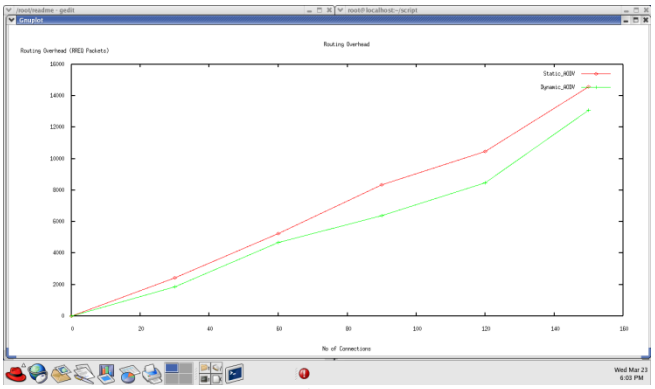

Fig.11 Routing overhead for static and dynamic AODV

Fig. 11 shows the graph between varying number of nodes and the control overhead in packets for the proposed energy efficient routing protocols and compare them with the static AODV protocol. When the density of the node increases from 20 to 160 nodes the average control overhead increases because of the number of control packets used for route discovery and maintenance. The statistics explain that the proposed trust based dynamic AODV protocol shows better performance like reduction of the control overhead by 14.25% over the existing AODV protocol. The results for the throughput are shown in Fig.1.12. The energy efficient cluster-based AODV protocol shows high throughput compared to DSDV, Zigbee AODV, and static AODV.

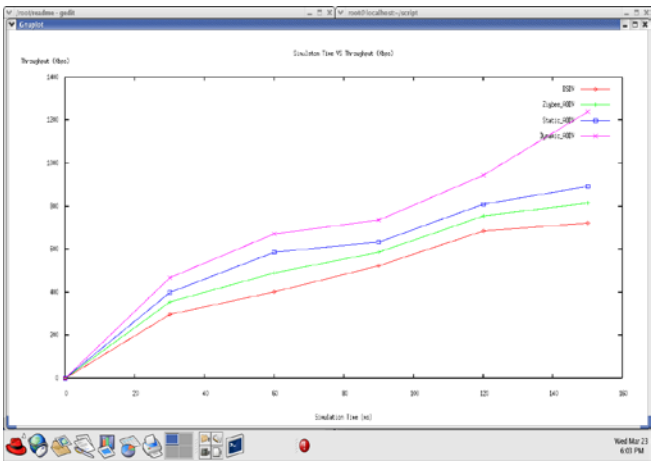

Fig.12 Throughput VS Simulation time

IX. CONCLUSION

Mobile nodes characterize the mobile ad hoc network and that is proficient of communicating over a wireless medium and forming a network deprived of a previously existing infrastructure. In MANETs, the resources like computation power, bandwidth, battery, and memory are to be used to attain improved enactment. Challenges encountered by MANETs comprise routing, Quality of Service (QoS) provisioning, security, energy efficiency, and multicasting. Many difficulties and challenges occur in this field as a consequence of the recurrent topology changes of unpredictable MANET. The recent trends explored that certain topics such as routing and energy management attracted more attention. This paper focused on security issues in the routing protocol and energy efficiency. The security issue in the MANET was analyzed based on the attacks in the network layer and the trust based dynamic AODV protocol was proposed to achieve the better security.

REFERENCES

[1] A.M.A.El-Haleem and I.A. Ali, "TRIUMF: Trust-Based Routing Protocol with a controlled degree of Selfishness for Securing MANET against Packet Dropping Attack," *IJCSI*. 2011.

[2] J. Jubin, and J.D. Tornow, "*The DARPA packet radio network protocols,*" *Proceedings of the IEEE*, Vol.75, No.1, pp.21-32. 1987.

[3] S. Gregory Lauer, "Packet-radio routing in Routing in Communications Networks," edited by Martha E. Steen Strup, Prentice-Hall, Englewood Cliffs.1995.

[4] S.A. Mahmud, S. Khan, S. Khan and H. Al-Raweshidy, "A comparison of MANETs and WMNs: commercial feasibility of community wireless networks and MANETs," In *Proceedings of the 1st international conference on Access networks* (p. 18). ACM. 2006, September.

[5] M. Abolhasan, T. Wysocki and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad hoc Networks*, Vol.2, No.1, pp.1-22. 2004.

[6] M.H. Lee, M. Sarahintu, H. Mohamed, B. Sanugi, S. Olariu, and A. Zaharim, "Performance evaluation of routing protocols for mobile ad hoc networks using statistical Taguchi's experimental design," In S.Kartalopoulos, A. Buikis, N. Mastorakis, & L. Vladareanu (Eds.), WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering (No. 13). *WSEAS*. 2008, December.

[7] E. M. Royer, P. M. Melliar-Smith and L.E. Moser, "An analysis of the optimum node density for ad hoc mobile networks," In Communications, 2001. ICC 2001. IEEE International Conference on Vol. 3, pp. 857-861, IEEE. 2001.

[8] T. Camp, J. Boleng and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless communications and mobile computing*, Vol. 2, No.5, pp.483-502. 2002.

[9] B. Divecha, A. Abraham, C. Grosan and S. Sanyal, "Impact of node mobility on MANET routing protocols models," *Journal of Digital Information Management*, Vol.5, No.1, pp. 19. 2007.

[10] F. Bai and A. Helmy, "The IMPORTANT framework for analyzing and modeling the impact of mobility in wireless adhoc networks," *Wireless Ad Hoc and Sensor Networks, Kluwer Academic Publishers*. 2004.

[11] F. Bai, G. Bhaskara and A. Helmy, "Building the blocks of protocol design and analysis: challenges and lessons learned from case studies on mobile ad hoc routing and micro-mobility protocols," *ACM SIGCOMM Computer Communication Review*, Vol.34, No. 3, pp. 57-70. 2004.

[12] A. Safwat and H. Hassanein, "Infrastructure-based routing in wireless mobile ad hoc networks," *Computer communications*, Vol.25, No. 3, pp. 210-224. 2002.

[13] T. Saadawi and O. Hussein, "Routing method for mobile infrastructureless network *U.S. Patent No. 6,940,832,"* Washington, DC: U.S. Patent and Trademark Office. 2005.

[14] I.F. Akyildiz and W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, Vol. 38,No.4, pp. 393-422. 2002.

[15] M. Abolhasan, T. Wysocki and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad hoc networks*, Vol. 2, No.1, pp.1-22. 2004.

[16] S. J. Lee, W. Su, J. Hsu, M. Gerla and R. Bagrodia, "A performance comparison study of ad hoc wireless multicast protocols. In *INFOCOM 200," Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE* (Vol. 2, pp. 565-574). IEEE. 2000.

[17] K.S. Lau and D. Pao, "Tree-based versus gossip-based reliable multicast in wireless ad hoc networks," In *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE* (Vol. 1, pp. 421-425). IEEE. 2006, January.

[18] E.M. Royer and C.K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *Personal Communications, IEEE*, Vol.6, No.2, pp. 46-55. 1999.

[19] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M.B. Royer, "A secure routing protocol for ad hoc networks," In *Network Protocols*, 2002. Proceedings. 10th IEEE International Conference on (pp. 78-87). IEEE. 2002, November.