ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

A Novel Study on Improved Routing Mechanism with Performance Analysis in MANETs

Er. Deepak Negi[1], Dr. Kishori Lal Bansal[2]

Department of Computer Science, Himachal Pradesh University, Shimla, India[1]

Professor, Department of Computer Science, Himachal Pradesh University, Shimla, India[2]

Abstract: Consumption of energy is a vital design concern in mobile ad hoc networks (MANETs), since nodes are powered by batteries with inadequate energy, whereas in existing dynamic source routing (DSR) does not take the energy restriction of MANET nodes into account. Also there occurs a problem of broken links due to the lack of energy which cause disorder in network system. Such problem occurs due to the unawareness of energy of mobile neighbour nodes. In this study, it proposes an efficient algorithm for MANETs, which maximises the network lifetime. It is used to determine the local link connectivity information for monitoring the link status between nodes along with the incorporation of Dynamic On Demand Routing Protocol to reduce the energy consumption of mobile nodes to certain extent. These protocols use shortest path as a main metric to establish routing between source and destination. The proposed mechanism is implemented with MATLAB.

Keywords: MANET, DSR, AODV, Shortest Path, Reactive Routing Protocol etc.

I. INTRODUCTION

Cellular network technologies were developed to allow mobile phones to connect via base stations and communicate in a circuit switched environment. The area of mobile ad-hoc networking deals with devices equipped to perform wireless communication and networking, but without any existing infrastructure such as base stations or access points [1].

An ad-hoc network is self-organizing and adaptive. Networks are formed on-the-fly; devices can leave and join the network during its lifetime, devices can be mobile within the network, the network as a whole may be mobile and the network can be deformed on the-fly. All this needs to be done without any system administration and without the requirement for any permanent devices within the network. Devices in mobile ad-hoc networks should be able to detect the presence of other devices and perform the necessary set-up to facilitate communications and the sharing of data and services. MANET is a most promising and rapidly growing technology which is based on self-organized and rapidly deployed network.

Mobile Ad Hoc Networks (MANETS) are wireless mobile nodes that cooperatively form a network without infrastructure. In other words, ad hoc networking allows devices to create a network on demand without prior coordination or configuration. Thus, nodes within a MANET are involved in routing and forwarding information between neighbours, because there is no coordination or configuration prior to setup of MANET. MANET is self-configuring networks of mobile nodes without the presence of static infrastructure. They can also be heterogeneous, which means that all nodes don't have the same capacity in term of resources (power consumption, storage, computation, etc.) [2].

Due to its great features, MANET attracts different real world applications areas where the networks topology changes very quickly. A good example is given by military battlefield networks. In that case, mobile devices have different communications capability such as radio range, battery life, data transmission rate etc.

MANET is a type of multi-hop network, infrastructure less and the most important self-organizing. Due to its wireless and distributed nature there is a great challenge for system security designers. In the last few years security problems in MANETs have attached much attention; most of the research efforts focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or intrusion detection and response.

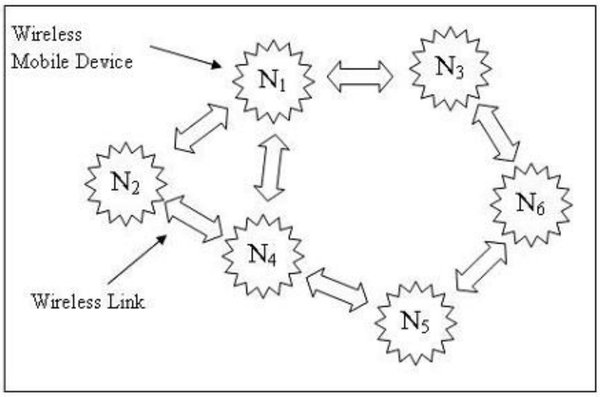

Figure 1: Mobile ad hoc Network (MANET) [2]

One of the main characteristic of MANET's with respect to security design point of view is the lack of clear line defense. In case of wired networks we have dedicated routers; which perform routing functionalities for devices but in case of Mobile ad hoc network are concerned each mobile node acts as a router and forward packets for other nodes. It is also true that the wireless channel is accessible to both network users as well as to attackers. There is no well defined rule or place where traffic from different

DOI 10.17148/IJARCCE.2015.410129

nodes should be monitored or access control mechanisms can be enforced. Due to this way there is no any defense line that separates inside network from the outside network. Due to this way the existing ad hoc routing protocols, like Dynamic Source Routing (DSR) [3] and Ad Hoc On Demand Distance Vector (AODV) [2] typically assumed to be trusted. As a result, an attacker can become a router and disrupt network operations.

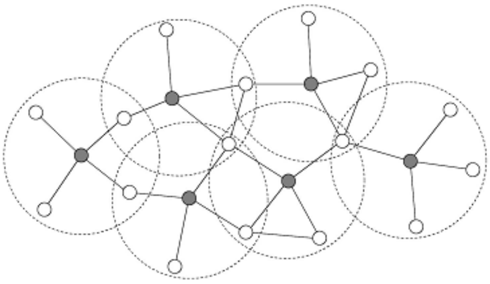

Figure 2: A hierarchy of Network in 2-D [3]

The idea of distributed power control can be used to improve energy efficiency of routing algorithm in MANET. There are some control messages such as RREP in On-Demand Routing Protocol which provide a strong indication that messages should trigger a node to switch to active node from sleep. Since the communication with a neighbour is only possible if the neighbour is in active mode, it is necessary for nodes to track energy modes of neighbours i.e., active, sleep or idle. The neighbour's power mode can be discovered in two ways: the first way is through explicit local HELLO message exchanges with piggybacked information about the energy management mode of a node, and the second way is via passive inference.

The paper is ordered as follows. In section II, we discuss correlated work with routing in MANETs. In Section III, It describes the routing protocols in MANETs. In section IV, it explains the proposed implementation of system. In section V, it describes the results related them. Finally, conclusion is explained in Section VI.

II. LITERATURE REVIEW

Authors proposed a lightweight proactive source routing (PSR) protocol. PSR can maintain more network topology information than distance vector (DV) routing to facilitate source routing, although it had much smaller overhead than traditional DV-based protocols e.g., destination-sequenced DV (DSDV), link state (LS)-based routing e.g., optimized link state routing (OLSR), and reactive source routing e.g., dynamic source routing (DSR). Their tests using computer simulation in Network Simulator 2 (ns2) indicated that the overhead in PSR is only a fraction of the overhead of these baseline protocols, and PSR yielded similar or better data transportation performance than these baseline protocols [3].

Some proposed a new concept by combining two proposed protocols based on geographical location based: ALERT which was based mainly on node-to-node hop encryption and bursty traffic. and Greedy Perimeter Stateless Routing (GPSR), a new geographical location based protocol for wireless networks that used the router's position and a packet's destination to make forwarding of packets. It followed greedy method of forwarding using the information about the immediate neighbouring router in the network. Simulation results had explained the efficiency of the proposed DD-SARP protocol with improved performance when compared to the existing protocols[4].

Some reviewed some current literature on mitigation of the routing attacks. These attacks may lead to either misdirection of data traffic or denial of services. The mitigation techniques to combat the attacks in MANETs have to work under severe constraints, and therefore it was imperative to study the vulnerabilities of the routing protocols and methods of launching the attack in detail [5].

Some authors attempted to develop a mathematical model for throughput of MANETs considering both of the aspects. In addition, they also focused on developing mathematical models for delivery ratio and drop ratio; these metrics limit the maximum throughput of a network. In their analysis, they performed rigorous simulation utilizingns-2 to capture the performance of MANETs under diversified settings [6].

Authors proposed Secured Hierarchical Anonymous Routing Protocol (SHARP) based on cluster routing. In MANETs security is the major concern in applications such as communication and data sharing. These are so many chances of different types of attacks due to self-organizing property of MANETs. Malicious attacker may try to attack the data packets by tracing the route. They may try to find the source and destination through different types attacks. MANETs are vulnerable to malicious attackers that target to damage and analyzed data and traffic analysis by communication eavesdropping or attacking routing protocols [7].

III. ROUTING IN MANETs

Routing is the most fundamental aspect for multi-hop MANETs. Unlike the Internet and infrastructure-based wireless networks, MANETs are characterized by the lack of a dedicated routing infrastructure. MANET nodes depend on each other to forward traffic. This requires nodes to forward traffic on behalf of other nodes, which opens the door for selfish behaviour [8].

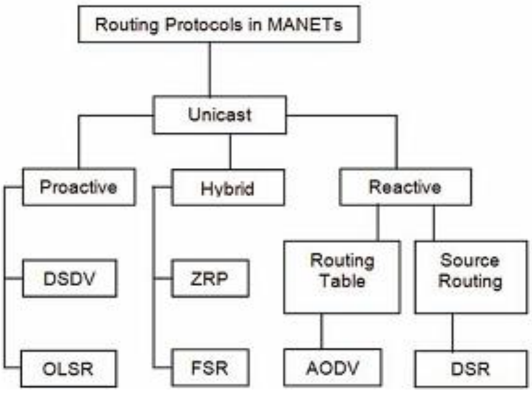

Figure 3: Classification of MANET Routing [8]

DOI 10.17148/IJARCCE.2015.410129

In bandwidth and power-limited environments, it is desirable to minimize routing control traffic when there is no data to be routed. Proactive routing is not particularly suitable for such settings. This is the main motivation behind reactive routing, also called on-demand routing. Such protocols do not maintain routes, but build them on-demand when communication to a certain destination is required. For example, the ad-hoc on-demand distance-vector (AODV) protocol is a reactive adaptation of distance-vector.

1. Dynamic Source Routing protocol (DSR)

The Dynamic Source Routing Protocol is one of the on-demand routing protocols, and is based on the concept of source routing. In source routing, a sender node has in the packet header the complete list of the path that the packet must travel to the destination node. That is, every node in the path just forwards the packet to its next hop specified in the header without having to check its routing table as in table-driven routing protocols. Besides, the nodes don't have to periodically broadcast their routing tables to the neighbouring nodes. This saves a lot of network bandwidth.

- **Route Discovery Phase**

In this phase, the source node searches a route by broadcasting route request (RREQ) packets to its neighbours. Each of the neighbour nodes that has received the RREQ broadcast then checks the packet to determine which of the following conditions apply: (a) Was this RREQ received before (b) Is the TTL (Time To Live) counter greater than zero (c) Is it itself the destination of the RREQ (d) Should it broadcast the RREQ to its neighbours.

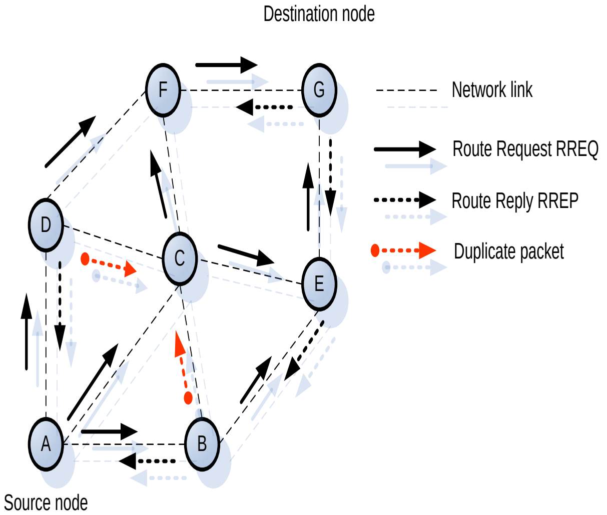

Figure 4: Route Discovery in DSR [10]

- **Route Maintenance**

The route maintenance phase is carried out whenever there is a broken link between two nodes. A broken link can be detected by a node by either passively monitoring in promiscuous mode or actively monitoring the link. As shown in Figure 5, when a link break (F-G) happens, a route error packet (RERR) is sent by the intermediate node back to the originating node. The source node re-initiates the route discovery procedure to find a new route to the destination. It also removes any route entries it may have in its cache to that destination node.

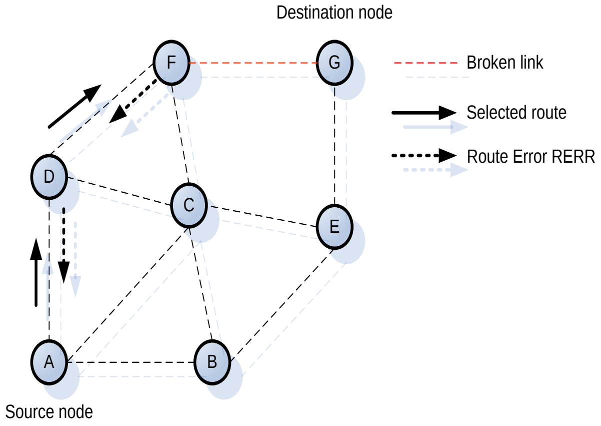

Figure 5: Route Maintenance in DSR [10]

DSR benefits from source routing since the intermediate nodes do not need to maintain up-to-date routing information in order to route the packets that they receive. There is also no need for any periodic routing advertisement messages. However, as size of the network increases, the routing overhead increases since each packet has to carry the entire route to the destination along with it. The use of route caches is a good mechanism to reduce the propagation delay but overuse of the cache may result in poor performance.

2. Ad-hoc On-demand Distance Vector (AODV) Routing Protocol

To find routes, the AODV routing protocol [9] uses a reactive approach and to identify the most recent path it uses a proactive approach. That is, it uses the route discovery process similar to DSR to find routes and to compute fresh routes it uses destination sequence numbers. AODV minimizes the number of broadcasts by discovering routes on-demand as opposed to DSDV (or OLSR) which maintains the list of routes to all destinations. To find a path to a destination, the source broadcasts a route request message (RREQ). Its immediate neighbours, in turn, broadcast the RREQ to their neighbours and so on, until it reaches an intermediate node that has recent route information about the destination or until it reaches the destination itself.

A node discards a RREQ if it has already received it. RREQ-s contains sequence numbers to ensure that the routes are loop free. Sequence numbers also ensure that, if intermediate nodes reply to a RREQ, they reply with the latest information only. If the source moves it can re-initiate route discovery to the destination. If one of the intermediate nodes moves then a neighbour of that node will sense the link failure and sends a notification to its upstream neighbours. Upstream neighbours forward such a notification and it eventually reaches the source. The source then can re-initiate a new route discovery if needed.

- **Route Discovery**

In this phase, RREQ packets are transmitted by the source node in a way similar to DSR. The components of the

DOI 10.17148/IJARCCE.2015.410129

RREQ packet include fields such as the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier, and TTL. When a RREQ packet is received by an intermediate node, it could either forward the RREQ packet or prepare a Route Reply (RREP) packet if there is an available valid route to the destination in its cache.

When a node receives a RREP packet, the information of the previous node is also stored in it in order to forward the packet to it as the next hop of the destination. This plays a role of a "forward pointer" to the destination node. By doing it, each node contains only the next hop information; whereas in the source routing, all the intermediate nodes on the route towards the destination are stored.

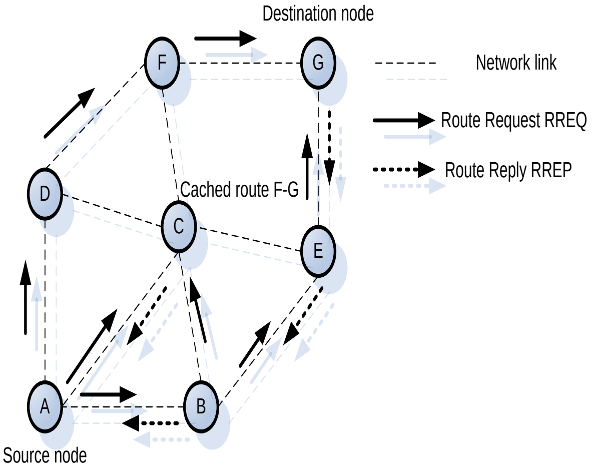

Figure 6: Route discovery in AODV [11]

- **Route Maintenance**

The way that the route maintenance mechanism works is described below. Whenever a node finds out a link break (via link layer acknowledgements or HELLO messages), it broadcasts an RERR packet (in a way similar to DSR) to notify the source and the end nodes. This process is illustrated in Figure 7. If the link between nodes C and F breaks on the path A-C-F-G, RERR packets will be sent by both F and C to notify the source and the destination nodes [11].

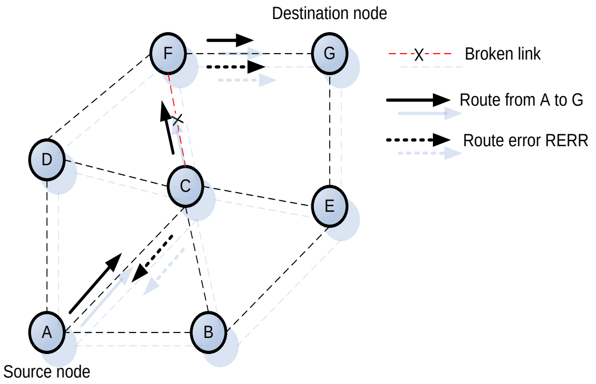

Figure 7: Route Maintenance in AODV [11]

The main advantage of AODV is the avoidance of source routing to reduce the routing overload in a large network. Another good feature of AODV is its application of expanding-ring-search to control the flood of RREQ packets and search for routes to unknown destinations. In addition, it also supplies destination sequence numbers, allowing the nodes to have more up-to-date routes. However, some notes have to be taken into consideration when using AODV. Firstly, it requires bidirectional links and periodic link layer acknowledgements to detect broken links. Secondly, unlike DSR, it needs to maintain routing tables for route maintenance unlike DSR.

IV. IMPLEMENTATION OF SYSTEM

A. Improved On-demand Routing Protocol

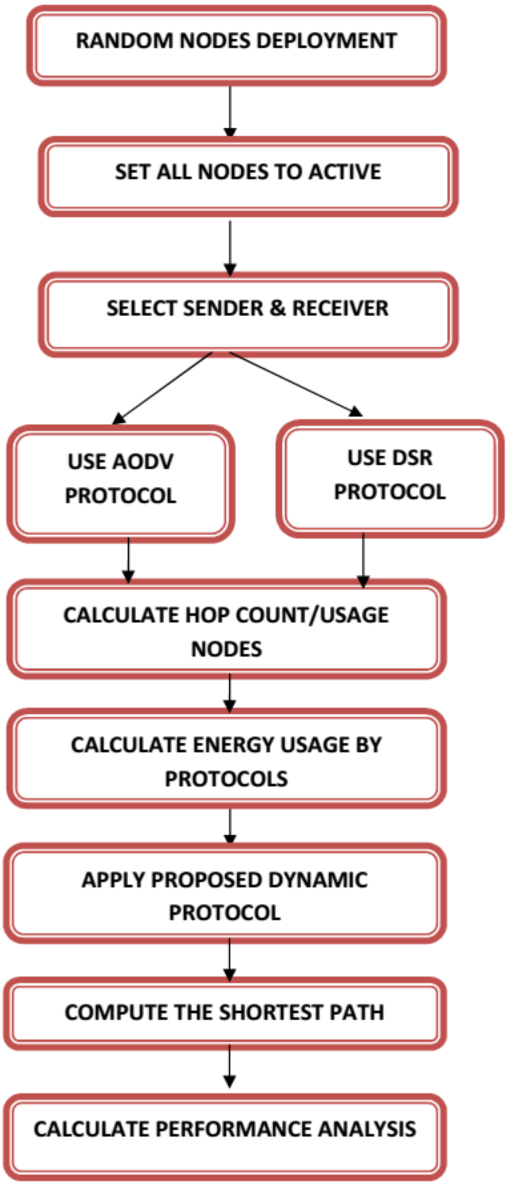
RANDOM NODES DEPLOYMENT
SET ALL NODES TO ACTIVE
SELECT SENDER & RECEIVER
USE AODV PROTOCOL
USE DSR PROTOCOL
CALCULATE HOP COUNT/USAGE NODES
CALCULATE ENERGY USAGE BY PROTOCOLS
APPLY PROPOSED DYNAMIC PROTOCOL
COMPUTE THE SHORTEST PATH
CALCULATE PERFORMANCE ANALYSIS

Figure 8: Proposed Implementation of System

QoS is defined as a set of service requirements that should be met by the network while transmitting a data packet from source to destination. It is a purely reactive protocol in which routes are computed on demand. Unlike AODV, it does not support unnecessary HELLO message transmission; also the operation is purely based on sequence number that is assigned to all the packets. It

DOI 10.17148/IJARCCE.2015.410129

employs sequence numbers to ensure loop freedom. It also enables on demand, multi-hop uni-cast routing among the nodes in a network. The basic operations are route discovery and maintenance to obtain a valid path and also to avoid the existing obliterated routes from the routing table to reduce the packet dropping in case of any route break or node failure.

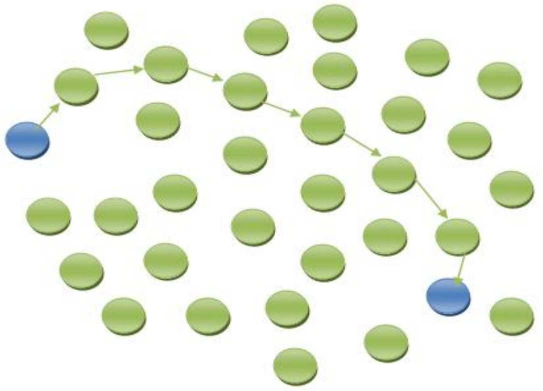

Figure 9: Proposed Improved ON Demand Protocol

V. RESULTS

All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighbouring nodes. During network initiation all nodes are strangers to each other. There are two main things in re-active routing protocols first is that it never take initiative in order to take routes for network, second is that whenever it creates routes it will developed on demand by flooding mechanism. In this system, it works on 50 nodes for presenting the proposed mechanism with comparison to actual system. Initially all nodes are randomly placed in 150*150 area network. Each node has an ID with it.

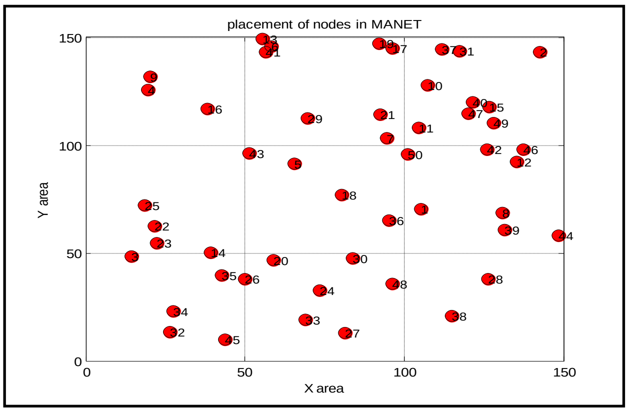

Figure 10: Placement of 50 Nodes in Network

AODV using a classical distance vector routing algorithm. It is also a share DSR's on demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination.

The Dynamic Source Routing Protocol is one of the on-demand routing protocols, and is based on the concept of *source routing*.

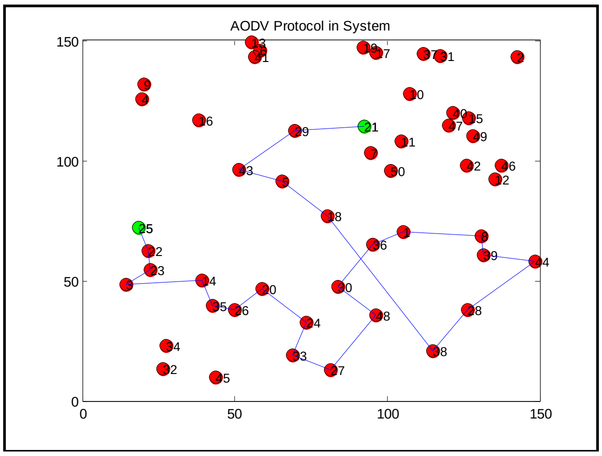

Figure 11: AODV Protocol Response in Network

In source routing, a sender node has in the packet header the complete list of the path that the packet must travel to the destination node. That is, every node in the path just forwards the packet specified in the header without having to check its routing table as in table-driven routing protocols.

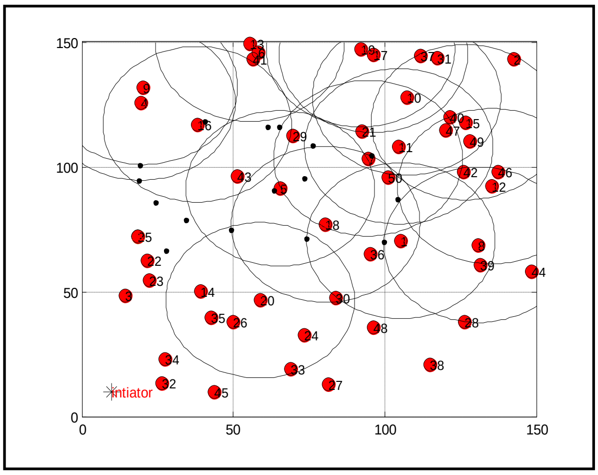

Figure 12: DSR Protocol Response in Network

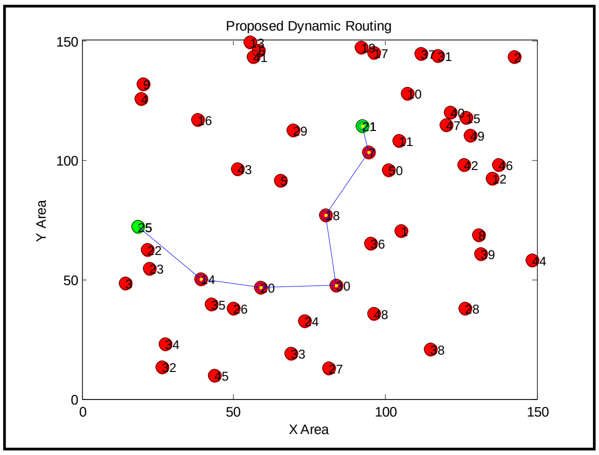

Figure 13: Proposed Dynamic Protocol Response in Network

The routing consists of two basic mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node wishing to send a packet to a destination obtains a source route. To reduce the cost of

Route Discovery, each node maintains a Route Cache of source routes it has learned or overheard. All the nodes are authentic and fault free. Information is securely transferred from sender to the receiver. It selected the shortest path from sender to receiver.

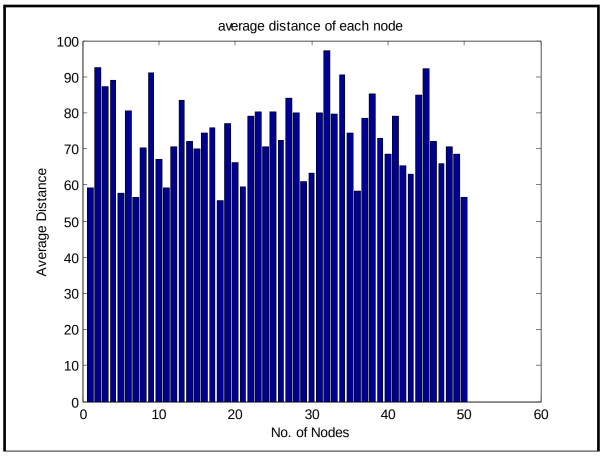

Figure 14: Average Distance of each Node in Network

The figure 15 shows below how the energy is being depleted in the above scenarios when information is transferred from Sender node to the Receiver node in each protocol. As move from sender to receiver, energy is consumed by each node and hence energy gets decreased. The results shows that the proposed protocol consumes less amount of energy as compared to other protocols.

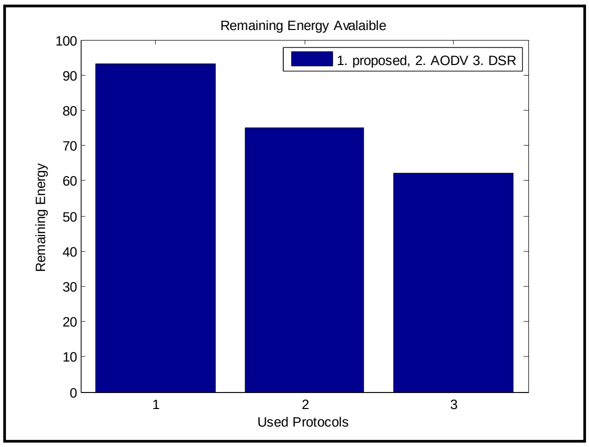

Figure 15: Energy Comparison of Each Protocol

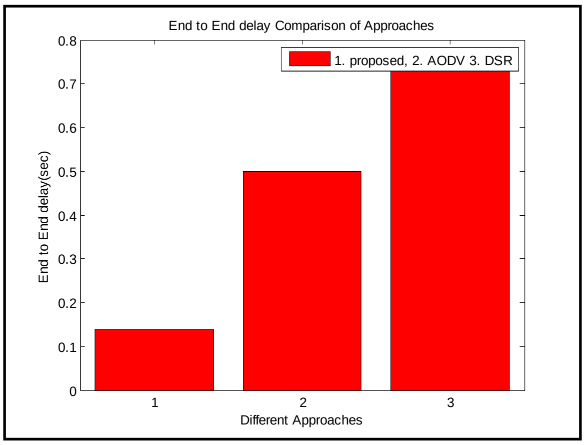

Figure 16: End to End Delay Comparison of System

This figure 16 shows the delay response of scenarios in proposed system i.e. it shows the delay response when data transfer from 1st sender node to sink node. In this, delay is quite high of AODV system as compared to proposed technique. As no. of nodes increases, delay increases as shown but proposed system provides less delay as compared to other systems.

VI. CONCLUSION

There occurs a problem of broken links due to the lack of energy which cause disorder in network system. Such problem occurs due to the unawareness of energy of mobile neighbour nodes. In this study, it proposes an efficient algorithm for MANETs, which maximises the network lifetime. It is used to determine the local link connectivity information for monitoring the link status between nodes along with the incorporation of Dynamic ON Demand Routing Protocol to reduce the energy consumption of mobile nodes to certain extent. These protocols use shortest path as a main metric to establish routing between source and destination. In this, it presents the comparison of proposed protocol with AODV and DSR. The results show that the proposed protocol takes minimum no. of nodes for data transmission. Due to this, it provides high energy efficiency and minimum end to end delay in network.

In the Future, we can compare other existing protocols with this system and some attacks can be detected and prevented by designing IDS system.

REFERENCES

[1] Zehua Wang, Yuanzhu Chen, “PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks”, IEEE Transactions On Vehicular Technology, Vol. 63, No. 2, February2014.

[2] S. Imran, R. Vimal Karthick, “DD-SARP: Dynamic Data Secure Anonymous Routing Protocol for MANETs in Attacking Environments”, IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, May 2015. pp. 39-46.

[3] Raj Kamal Kapur, Sunil Kumar Khatri, “Analysis of Attacks on Routing Protocols in MANETs”, IEEE International Conference on Advances in Computer Engineering and Applications, 2015.

[4] Novia Nurain, Moin Mostakim, “Towards Empirical Study Based Mathematical Modeling for Throughput of MANETs”, IEEE 2015.

[5] Remya S, Lakshmi K S, “SHARP: Secured Hierarchical Anonymous Routing Protocol for MANETs”, IEEE International Conference on Computer Communication and Informatics (ICCCI-2015), Jan. 08 – 10, 2015.

[6] Surendran. S, Prakash. S, “An ACO Look-Ahead Approach to QOS Enabled Fault Tolerant Routing in MANETs”, IEEE China Communications, August 2015.

[7] Gaurav Singal, Harshit Garg, “Impact Analysis of attacks in Multicast Routing Algorithms in MANETs”, IEEE 2014.

[8] Anju Sara Varghese and S. Caroline Jebakumari, “Dynamic Beacon based and Load Balanced Geo Routing in MANETs”, IEEE International Conference on Communication and Signal Processing, April 3-5, 2014.

[9] C.Nishanthini, G.Rajkumar, “Congestion Avoidance Through Cooperative Routing In Manets”, IEEE 2013.

[10] Peng Zhao, Xinyu Yang, Wei Yu, “A Loose-Virtual-Clustering-Based Routing for Power Heterogeneous MANETs”, IEEE Transactions on Vehicular Technology, Vol. 62, No. 5, June 2013.

[11] Shyr-Kuen Chen, Pi-Chung Wang, “Shortcut Anycast Tree Routing in MANETs”, IEEE International Conference on Advanced Information Networking and Applications, 2012.

DOI 10.17148/IJARCCE.2015.410129

[12] Du Zheng, Helen Tang, “A Game Theoretic Approach for Security and Quality of Service (QoS) Co-Design in MANETs with Cooperative Communications”, IEEE 2013.

BIOGRAPHIES

Er. Deepak Negi is pursuing M.Tech in Computer Science from the Department of Computer Science, Himachal Pradesh University, Shimla. He has completed his B.Tech in Computer Science Engineering with Honours from the Himachal Pradesh University, Shimla.

Dr. Kishori Lal Bansal is working as a Professor, Department of Computer Science, Himachal Pradesh University, Shimla. He has completed his Ph.D from the Himachal Pradesh University, Shimla.

DOI 10.17148/IJARCCE.2015.410129