iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Method & Implementation Of Constructing A Backup Method For Mitigating Fault In Manets

Neelam Rani[1], Ms. Amrita Chaudhary[2]
[1]M.Tech Scholar, [2]Asst. Professor, Computer Science & Engineering. Deptt. Galaxy Global Group of Institutes, Ambala

Abstract: ***A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less formed by the dynamic gathering of mobile nodes. The biggest challenge among them is routing. Routing is the process of path in a network along which to send data packets. Path routing and protocol selection are the primary strategies to design any wireless network. Due to the mobility of mobile nodes, the topology of a MANET frequently changes. The dynamic properties of MANETs are therefore challenging to protocol design. To cope with the intrinsic properties of MANETs, a backup node mechanism for quick reconnection during link failures, is proposed in this paper. Due to this, an improved algorithm is proposed to reduce current recovery time by improving reliability of system. In this paper, backup path is provided in the existing AODV routing protocol to ensure secure routing in mobile Adhoc network. All simulations are done in MATLAB.***
Keywords-MANET, AODV, Backup path, Node Failure etc.

I. INTRODUCTION

A Computer networks were originally developed to operate by connecting computers together with wires and transmitting data over these wires. Network sizes and occurrences increased creating a requirement for inter-network communication. This led to the development of the Internet and its suite of protocols. The use of the Internet and its applications became ubiquitous. A need for providing network access to entities while not physically attached to the wired network arose. To enable this wireless networking was developed, providing devices with methods to connect to a wired network using radio wave technologies through wireless access points. Simultaneously, telephone networks were undergoing a similar transformation [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 onthe-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 [2].

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 neighbors, because there is no coordination or configuration prior to setup of MANET. MANET [3] 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.). 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.

Figure 1: MANET Network [1]

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

From the survey, it is concluded that A mobile ad hoc network (MANET) is a wireless communication network, where nodes that are not within the direct transmission range of each other require other nodes to forward data. [4] While alleviating forwarding nodes from table lookup, DSR's source routing is particularly vulnerable in rapidly changing networks. When a data packet is forwarded to a neighbor that no longer exists, it causes link layer retrial, backlogging of subsequent packets, and TCP congestion avoidance and retransmission. Therefore, in research on multi-hop wireless networking, it usually makes sense for us to minimize any impact on the network's communication resources even if there is penalty in other aspects. When it comes to the case when a node should share its updated route information with its neighbors, we chose to delay it until the end of the cycle so that only one update is broadcast in each period. DSR proved to be reliable choice for different traffic classes when throughput metric is our concern. DSDV has the worst performance compared to other protocols, while DSR and AODV have comparable PDF and total dropped packets for different number of nodes.

The paper is organized as follows. In section II, we discuss the applications of MANET. In Section III, It describes major attacks in MANETs. In Section IV, it describes the proposed system. Section V defines the proposed results related to system. Finally, conclusion is given in Section VI.

II. APPLICATIONS OF MANET

Applications	Possible Scenarios/Services
Tactical Networks	• Military communication and operations [5] • Automated battlefields
Emergency Services	• Search and rescue operations • Disaster recovery • Replacement of fixed infrastructure in case of environmental disasters • Policing and fire fighting • Supporting doctors and nurses in hospitals
Commercial and Civilian Environments	• E-commerce: electronic payments anytime and anywhere • Business: dynamic database access, mobile offices • Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks • Sports stadiums, trade fairs, shopping malls • Networks of visitors at airports
Education	• Universities and campus settings [6] • Virtual Classrooms • Ad hoc communications during meetings or lectures
Context Aware Services	1) Follow-on services: call-forwarding, mobile workspace 2) Information services: location specific services, time dependent services
Sensor Networks	• Home Applications: Smart sensors and actuals embedded in consumer electronics • Body area networks(BAN) • Data tracking of environmental conditions, animal movements, chemical/biological detection

III. MAJOR ATTACKS IN MANETs

A. Current ad hoc routing protocols are basically exposed to two different types of attacks:

1) Active attacks

2) Passive attacks

An attack is considered to be active when the misbehaving node has to bear some energy costs in order to perform the threat while passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. On the other side, selfish nodes can severely degrade network performances and eventually partition the network by simply not participating to the network operation [7].

B.Eavesdropping

This attack is used to gain knowledge of the transmitted data. This is a passive attack, which is easily performed, in many networking environments. However using an encryption scheme to protect the transmitted data can prevent this attack.

C. Impersonation

Since current ad hoc routing protocols do not authenticate routing packets a malicious node can launch many attacks in a network by masquerading as another node (spoofing). Spoofing occurs when a malicious node mis-represents its identity in order to alter the vision of the network topology that a benign node can gather. As an example, a spoofing attack allows to create loops in routing information collected by a node with the result of partitioning the network.

D. Modification

Existing routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Malicious nodes can easily cause traffic subversion and denial of service (DoS) by simply altering these fields: such attacks compromise the integrity of routing computations. By modifying routing [8] information an attacker can cause network traffic to be dropped, redirected to a different destination or take a longer route to the destination increasing communication delays.

E.Fabrication

The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages claiming that a neighbor can no longer be contacted.

F.Wormhole Attack

A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private network connection. This exploit allows a node to short-circuit the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

G. Lack of Cooperation

A selfish node that wants to save battery life for its own communication can endanger the correct network operation by simply not participating to the routing protocol or by not executing the packet forwarding (this attack is also known as the black hole attack). Current ad hoc routing protocols cannot cope with the selfishness problem and network performances severely degrade [9].

IV. DESCRIPTION OF PROPOSED SYSTEM

MANET performance is sensitive to mobility, scalability and traffic load, so to examine the different protocol performance while the amount of traffic and speed of nodes varies even plays a crucial role in efficient traffic routing. The reactive protocols determine a route only when necessary. The source node is the one in charge of the route discovery. As a main advantage, the routing overhead is small since the routes are determined only on demand. As a main disadvantage the route discovery introduces a big delay. Due to this, this thesis proposes a routing protocol for MANETs with the objective that each node works using the most suitable features. To achieve that, every node checks periodically its speed and its traffic.

Reactive protocol is identified as On-demand protocols because it creates routes only when these routes are needed. The need is initiated by the source, as the name suggests. When a sender node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined.

Ad hoc On-Demand Distance Vector (AODV) [10] routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand.

AODV is capable of both unicast and multicast routing [11]. It keeps these routes as long as they are desirable by the sources. Additionally, AODV creates trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. The sequence numbers are used by AODV to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV defines three types of control messages for route maintenance:

RREQ-A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.

RREP- A route reply message is uni-casted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR-Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ―precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network [18]. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node getting the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it uni-casts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

It defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In this, a route is chosen based on associatively states of nodes and temporal stability of the links between the nodes. It maintains the Signal Stability (SS) and Routing table. The SS keeps the signal strength of neighboring nodes acquired by periodic beacons from the link layer of every neighboring node. Signal strength is either recorded as a strong or weak channel.

It is a protocol for wireless ad hoc networks that uses position of next-hop neighbor nodes and packet's destination to decide forwarding paths. Sources can determine the destinations' location by Location services. It utilizes greedy forwarding to advance packets to nodes which are nearer to destination. In this approach it deployed sensor nodes which may vary from a few hundreds to thousands. More the number of nodes deployed, more will be the accuracy. To address the described fault and increase network efficiency, a protocol is proposed to provide access to nodes. The proposed algorithm is defined as:

A. Node Initialization

1) Generate the number of nodes (N)
2) Assign node ID to the new node by MANET protocol
3) The new node's initial local table is established by direct transactions.
4) AODV computes the shortest distance for all nodes
5) Provide a routing from source to destination from shortest path (primary).
6) Each Node finds an adjacent node as a backup before failure occurs.
7) While source sends traffic to destination via shortest pat
8) If node/link failure occurs in primary path the
9) Store the location of failures
10) Provide the rerouting through backup node.
11) Select a set of path having minimum path length.
12) Choose available best path for Communication.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

13) End
14) End

V. RESULTS & DISCUSSION

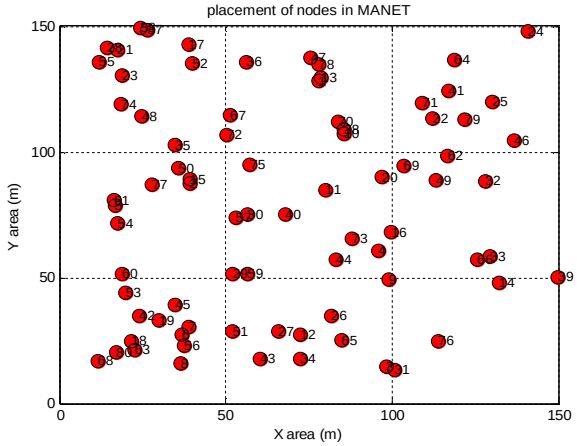


Figure 2: Placement of Nodes in Network

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. All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. During network initiation all nodes are strangers to each other.

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. Each node detects the nodes having direct link with itself.

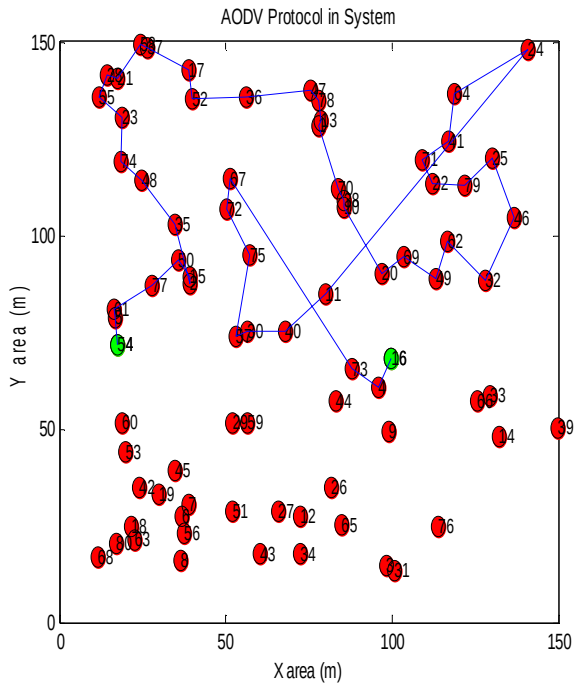


Figure 3: AODV Response of System

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

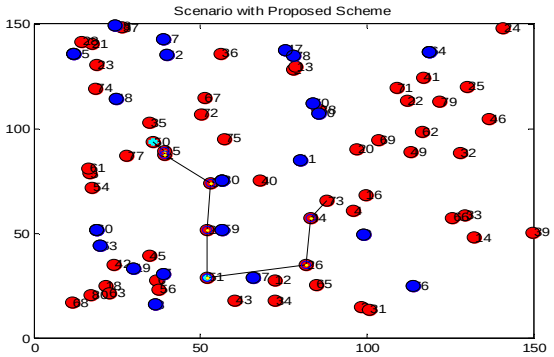


Figure 4: Proposed Scenario of System

These neighbors selected are the only nodes in charge to relay the routing packets and are called MPRs (Multipoint Relays). The rest of the neighborhood processes the routing packets that they receive, but they cannot relay them. Each node decides an optimum path (in number of hops) to each destination using the stored information (in its topology routing table and in of their neighbors ones). Besides each node stores that information in a routing table when a node wants to sent data

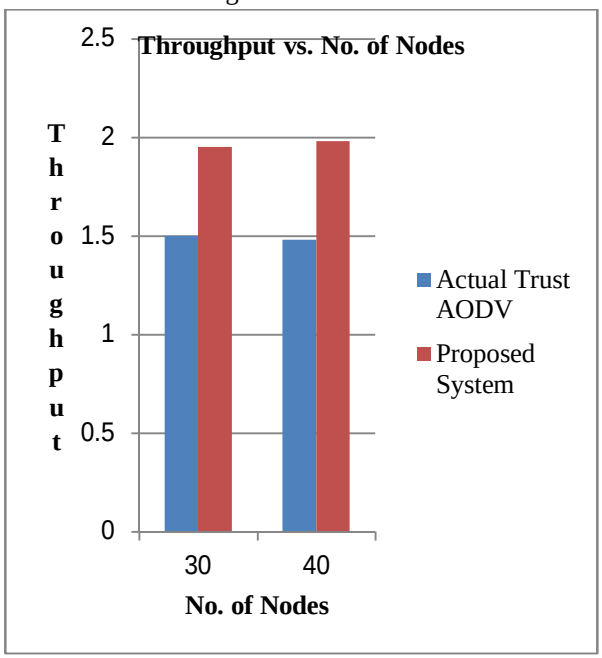


Figure 5: Performance Comparison of System

The network throughput is the main parameter that is used to reflect the network capability. It is the amount of traffic that is leaving the "Network". We measure these statistics in bits per second unit. As we know that throughput use to describe loss rate which usually seen on transport layer. The graph reflects completeness; it also shows accuracy of the routing protocol. It is also clear that throughput is inversely proportional to mobility i.e. throughput decrease and on other side mobility increase.

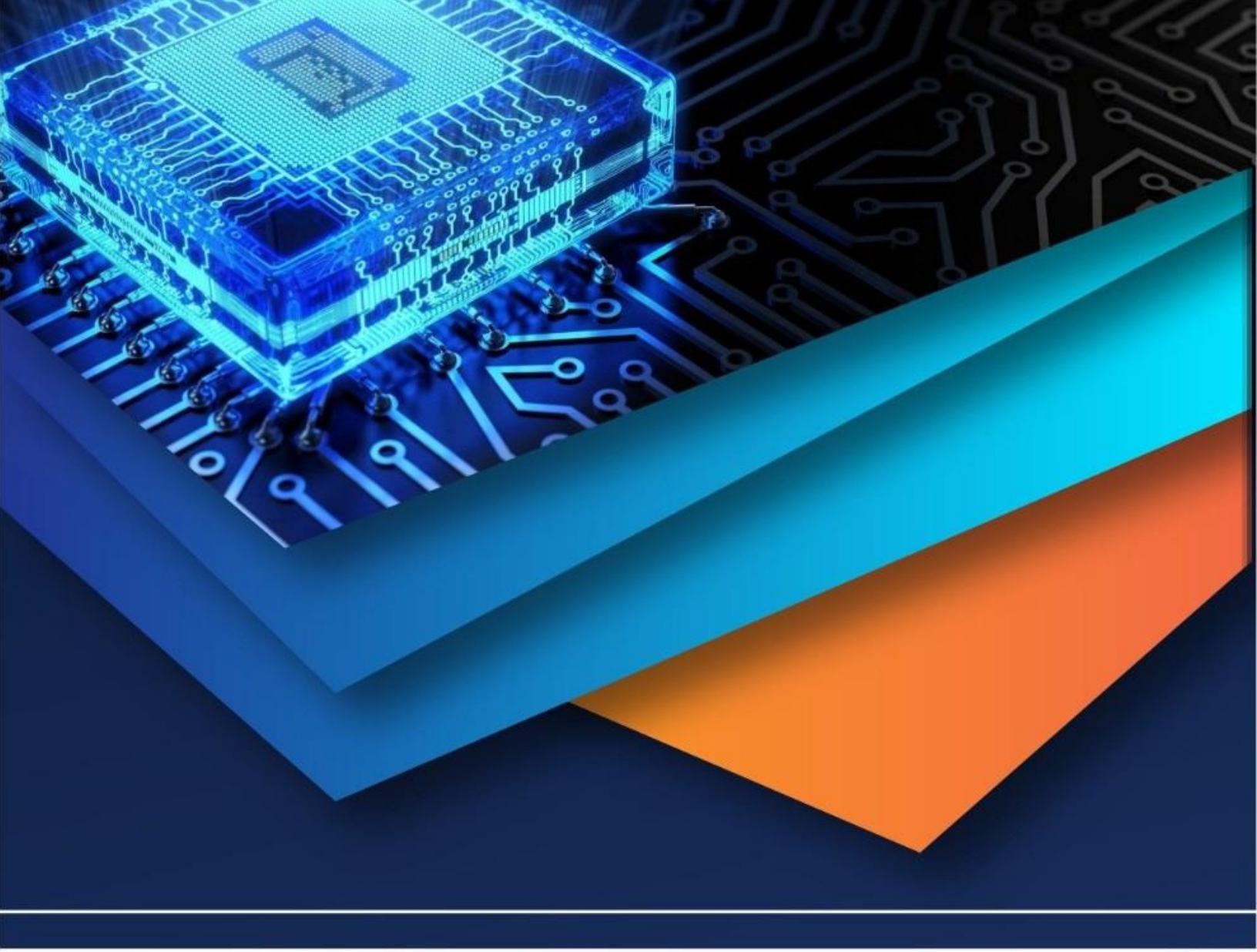
VI. CONCLUSION

In this study, it proposes an efficient algorithm for MANETs, which maximizes the network throughput. 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. It provides the solution to handle node failure and link failure in network. Due to this, it provides a useful backup path in system. The results show that the proposed protocol takes minimum no. of nodes for data transmission. Due to this, it provides high energy efficiency and high throughput in network.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

REFERENCES

[1] Vijaya Singh,Ms.Megha Jain," Analysis of Trust Dynamics in Cyclic Mobile", 2015 IEEE
[2] MitraAhmadi, MohammadShojafar,AhmadiKhademzadehKambizBadieh,RezaTavoli, "A Hybrid Algorithm for Preserving Energy and Delay Routing in Mobile Ad-Hoc Networks",SpringerScience+Business Media, 2015.
[3] Tran The Son, Hoa Le Minh, Graham Sexton, NaumanAslam, , "Self-adaptive proactive routing scheme for mobilead-hoc networks" The Institution of Engineering and Technology 2015. Vol. 4, Iss. 2, pp. 128–136
[4] "Shivashankar, GollaVaraprasad, Suresh HosahalliNarayanagowda "Implementing a new power aware routing algorithm based on existing dynamic source routing protocol for mobile ad hoc networks" The Institution of Engineering and Technology 2014. Vol. 3, Iss. 2, pp. 137–142.
[5] Nabil Nissar ,NajibNaja ,AbdellahJama, "A review and a new approach to reduce routing overhead in MANETs", Springer Science+Business Media, 2014.
[6] Shiva Shankar, GollaVaraprasad, Hosahalli, Narayanagowda Suresh, , "Importance of on-demand modified power awaredynamic source routing protocol in mobile ad-hocnetworks", The Institution of Engineering and Technology 2014, Vol. 8, Iss. 7, pp. 459–464.
[7] V.Hema, M.Mohanapriya, "Routing Overhead Reduction in MANETs", International Journal Of Scientific & Engineering Research,March 2014, Volume 5, Issue 3.
[8] Jyoti Jain1, Roopam Gupta, Tushar K. Bandhopadhyaya, "Performance analysis of proposed local link repair schemes for ad hoc on demand distance vector", The Institution of Engineering and Technology 2014, Vol. 3, Iss. 2, pp. 129–136.
[9] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning" 2013 IEEE.
[10] Zehua Wang, Student Member, IEEE, Yuanzhu Chen, Member, IEEE, Cheng Li, Senior Member, "PSR: a Light-Weight Proactive Source Routing Protocol For Mobile Ad Hoc Networks" 2013 IEEE.
[11] IsraatTanzeenaHaque, "On the Overheads of Ad Hoc Routing Schemes" 2013 IEEE."
[12] Jiajia Liu, Member, Nei Kato, Fellow, Jianfeng Ma, and Toshikazu Sakano," Throughput and Delay Tradeoffs for Mobile Ad Hoc Networks with Reference Point Group Mobility",2013 IEEE.
[13] R.Maheshwari, R.Velumani,"A Recent Survey on Increasing Routing Efficiency in MANET"International Journal of Computer Science and Information Technology & Security, Vol. 2, No.5, October 2012.
[14] S. Mohapatra, P.Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols" Published by Elsevier,2014.
[15] Dr Chandra Shekar Reddy Putta,DrK.Bhanu Prasad, ,DilliRavilla, MuraliNath R.S,,M.L.Ravi Chandra, "Performance of Ad hoc Network RoutingProtocols in IEEE 802.11" 2010 IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY