Jyoti *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 8, August- 2015, pg. 62-79 **ISSN: 2321-8363**

DETECTION AND AVOIDANCE OF CONGESTION CONTROL THROUGH ROUTING PROTOCOLS

Mrs. Sonal Beniwal, Jyoti
Computer Science and Engineering, (Network Security), BPSMV KHANPUR KALN SONIPAT, INDIA

ABSTRACT: In wireless network communication mobile network communication has becomes very important. Manet is a temporary network that means nodes moves without any fixed infrastructure. In Manet nodes are generally communicated with each other over various wireless links and also changes network topologies due to nodes are movable. Routing is a problem in Manet because there is no router between source & destination so; mobile nodes themselves act as the routers. In Manet, routing depend upon topologies, router source etc. This paper describes the research work done in recent and new mechanism to estimates the network congestion and avoiding them, so that network performance will improve. Our goal in this paper is to achieve high throughput and low end to end delay in congested network.

Keywords— MANET, GSR, AODV

1. INTRODUCTION

In Manet, congestion control is a major problem. Congestion means when transmission of number of packets across the network is greater than the capacity of the network then network becomes congested. Due to congestion packets have to be dropped and also decrease the performance of the network. So, finding the congestion free shortest path is a main issue in Manet.

1.1 Ad hoc Network:

In this new era of communications, mobile communication [1] and mobile computing have exhibited a tremendous rise in popularity among researchers and practitioners. The advent of new powerful, efficient and compact devices like Personnel Digital Assistants (PDAs), Pagers, Laptops, Cellular Phones, having extraordinary processing power paved the way for better communication technologies and mobile computations. At the same time, market for the wireless telephones and the Communication devices are experiencing a rapid growth. The availability of Internet and the Internet based applications in these devices delivered through emerging technologies is giving a push to the move. The thirst for information is increasing day to day. An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Mobile ad hoc networks (MANET) [4] do not rely on any fixed infrastructure but communicate in a self-organized way.

1.2 Infrastructured and ad-hoc networks:

Wireless communication between mobile users is becoming more popular than ever before. This is due to the recent technological advances in laptop computers and wireless data communication devices, such as wireless modems and wireless LANs. This has lead to lower prices and higher data rates, which are the two main [2] reasons why mobile computing continues to enjoy rapid growth. There are two distinct approaches for enabling wireless communication between two hosts. The first approach to let the existing cellular network infrastructure carry data. The major problem is that networks based on the cellular infrastructure are limited to places where there exists such a cellular network infrastructure.

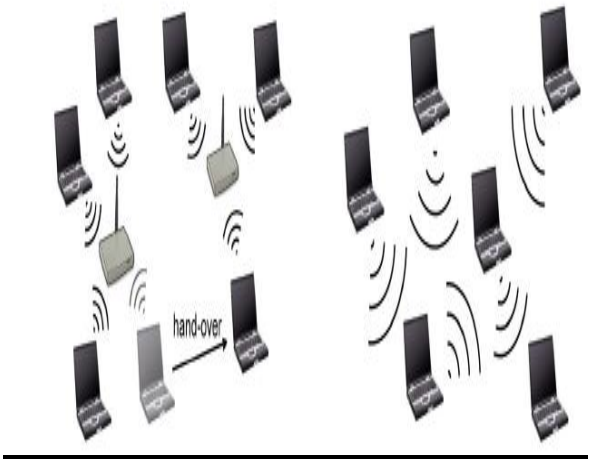
The second approach is to form an ad-hoc network among all users want to communicate with each other. This means that all users participating in the ad-hoc network must be willing to

forward data packets to make sure that the packets are delivered from source to destination. This form of networking is limited in range by the individual nodes transmission ranges and is typically smaller as compared to the range of [1] cellular systems. This does not mean that the cellular approach is better than the ad-hoc approach. Ad-hoc networks have several advantages compared to traditional cellular systems. These advantages include:

- On demand setup
- Fault tolerance
- Unconstrained connectivity

A mobile ad hoc network (MANET) is formed by a group of mobile nodes connected by wireless links. The nodes can talk to each other by direct peer-to-peer wireless communication when they are close to each other. When the sender and receiver are far away, their packets can be forwarded by the intermediate nodes along a multi-hop path.

In contrary to infrastructured networks, an ad-hoc network (Figure 1(b)) lacks any infrastructure. There are no base stations, no fixed routers and no centralized administration. All nodes may move randomly and are connecting dynamically to each other. Therefore all nodes are operating as routers and need to be capable to discover and maintain routes to every other node in the network and to propagate packets accordingly. Mobile ad-hoc networks may be used in areas with little or no communication infrastructure: think of emergency searches, rescue operations, or places where people wish to quickly share information, like meetings etc.



(a) An infrastructured network with two base stations. (b)**A mobile ad-hoc networks.**

2. MANET

Such devices can communicate with another node that is immediately within their radio range or one that is outside their radio range. For the latter scenario, an intermediate node is used to rely or forward the packet from the source toward the destination. [1] An ad-hoc wireless network is self-organizing and adaptive. The term "ad-hoc' tends to imply "can be mobile, standalone, or networked." Ad hoc nodes or devices should be able to detect the presence of other such devices and to perform the necessary handshaking to allow the sharing of information and services. A mobile ad-hoc network (MANET) is self-created [1] and self-organized by a set of mobile nodes called hosts. The nodes are interconnected by single-hop or multiple hop wireless connection, and each node may serve as a packet level router for other nodes in the mobile ad hoc network.

The goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes, [2] which may be combined routers and hosts, they form the network routing infrastructure in an ad-hoc fashion. Examples for the

use of such mobile, wireless, multi-hop ad-hoc networks, which are only called ad-hoc networks here for simplicity, are:

I) Instant infrastructure:

Unplanned meeting, spontaneous [1] interpersonal communication etc. Cannot rely on any infrastructure. Infrastructure needs planning and administration. It would take too long to set up this kind of infrastructure; therefore, ad-hoc connectivity has to set up.

II) Disaster relief:

Infrastructure typically breaks down in disaster areas. Hurricanes cut phone and power lines, floods destroy base station, fires burn serves. Emergency teams can only rely on an infrastructure they can setup themselves. No forward planning can be done and set-up must be extremely fast and reliable.

III) Remote areas:

Even if infrastructure could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely [2] populated areas. Depending on the communication pattern, ad-hoc networks or satellite infrastructures can be a solution.

IV)Effectiveness:

Services provided by existing infrastructure might be too expensive for certain application.[4] Registration procedure might take too long, and communication overheads might be too high with existing networks. Application- tailored ad-hoc networks can offer a better solution.

3. HISTORY OF MANET

The whole life cycle of ad-hoc networks could be categorized into the first, second, and the third generation ad-hoc networks systems. Present ad-hoc networks systems are considered the third generation.

The first generation goes back to 1972. At the time, [3] they were called PRNET (Packet Radio Networks). In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment. The second generation of ad-hoc networks emerged in 1980s, when the ad-hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program. [5] This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

In the 1990s, [3] the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences.

4. CHARACTERISTICS OF MANET

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communication devices), herein simply referred to ad “nodes”, which are free to move about arbitrarily. The nodes may be located in or airplanes, ships, trucks, cars, perhaps even on people. MANETs have several salient characteristics that have to be taken into account when considering their design and deployment:

I) **Dynamic topologies:** Nodes are free to move arbitrarily within the network (or leave and join the network) causing random topology changes [6] which can happen rapidly at unpredictable times.

II) **Bandwidth-constrained variable capacity links:** Wireless links will continue to have significantly lower capacities compared to traditional hardwired links. In addition, the realized throughput of wireless communications, after accounting for the effect of

multiple access, fading, noise and interference conditions, etc, is often much less than a radio's maximum transmission rate.

III) **Throughput:** These networks have lesser throughput than the wired network, because of its lower capacity, noise, interference conditions.

IV) **Limited physical security:** Mobile wireless networks are generally more prone to physical security threats than hardwired networks. The increased possibility of eavesdropping, spoofing, and denial of service attacks should be carefully considered. Existing link [7] security techniques are often applied within wireless network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

V) **Heterogeneity:** There are various types of system from PDA to Laptops. While the above characteristics are common to any kind of wireless network, MANETs are further distinguished by their "Infrastructure less" property. There is no centralized administration or pre-existing infrastructure that takes care of the network management and existence. It is obvious that the routing function is of utmost importance for the viability of an ad hoc network

1.12 Types of Ad-Hoc Routing Protocols : Basically there are two types of routing protocols.

I. Proactive Routing Protocols:

The sender of the packet explicitly mentions the list of all nodes in the packet's header, identifying each forwarding 'hop' by the address of the next node to which to transmit the packet on its way to destination host. In this protocol [8] the nodes don't need to exchange the routing table information periodically and thus reduces the bandwidth overhead in the network. Each mobile node participating in the protocol maintains a 'routing cache', which contains the list of routes that the node has learnt. Whenever the node finds a new route it adds the new route in its 'routing cache. Each mobile node also maintains a sequence counter 'request id' to uniquely identify the requests generated by a mobile host. The pair < source address, request id> uniquely identifies any request in the Ad Hoc network. The protocol does not need transmission between hosts to work in bidirectional.

Here in the nodes keep updating their routing tables by periodical messages. [8]This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

II. Destination Sequence Distance Vector (DSDV)

A) Destination Sequenced Distance Vector Routing (DSDV)25

The Destination-Sequenced Distance [8] Vector Routing Algorithms applies distance vector routing approach to mobile ad-hoc networks. In this each node has a routing table, which maintains a set of distances for each possible destination and the number of hops to each destination. When a node has to select one of its direct neighbours to relay a data packet, it selects the entry with the minimum distance. To keep the set of distances up to date, each node periodically broadcasts its routing table to all neighbours. A node, which receives an update message from one of its neighbours updates its own routing table and applies a shortest path algorithm. When the neighbourhood of a node changes, routing information in table is exchanged. Two types of update packets are transmitted in DSDV protocol full dump, and incremental dump. A full dump contains the whole routing table of a node. In contrast, an incremental dump contains only the changes since the last full dump.

B) Global State Routing (GSR) Protocol 25

This protocol is based on Link State Routing, which has the advantage of routing accuracy, and dissemination method to avoid inefficient flooding in LS routing. Each node maintains a neighbour list, a topology table, a next hop table, a distance table. The neighbour list contains the list of nodes adjacent to the node. [8] The topology table contains the link state information reported by a destination and a timestamp indicating the time at which this is generated. The next hop table and the distance table contain the neat hop and the distance of the shortest path for each destination respectively. Initially, each node learns about its neighbours

and the distance of the link to it (generally hop count equals one) by examining each packet in its inbound queue and broadcasts this information to its neighbour. Upon receiving the link state message from its neighbours, each node updates the link state information corresponding to that neighbour in the topology table to the most up to date information using timestamps. The routing table information is exchanged periodically with the neighbours only. GSR is suitable for a mobile environment where mobility is high and bandwidth is high. The drawback of [10] GSR are the large size of routing message, which consumes considerable bandwidth and the latency of the link state change propagation, which depends on update period.

I) Reactive or On Demand Routing Protocols:

Here the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) [17] and the Ad-hoc On- demand Distance Vector Routing Protocol (AODV).In today's world the most common ad-hoc protocols are the Ad-hoc On-demand Distance Vector routing protocol and the Destination-Sequenced Distance-Vector routing protocol and the Dynamic Source Routing. All these protocols are quite insecure because attackers can easily obtain information about the network topology. This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

Examples of on-demand algorithms are:

- Ad hoc On-demand Distance Vector(AODV) (RFC 3561)
- Dynamic Source Routing (RFC 4728)
- Flow State in the Dynamic Source Routing
- Power-Aware DSR-based

A. Dynamic Source Routing (DSR)

The DSR is a simple and efficient on-demand source routing protocol designed for multi hop wireless ad-hoc networks. DSR doesn't require any existing network infrastructure. DSR allows network to [9] be completely self-organizing and self-configuring. It uses source routing which is a technique in which the sender of a packet determines the complete sequence of nodes through which the node has travel.

B. Ad hoc On-Demand Distance Vector Routing (AODV)

The Ad Hoc On-Demand Distance-Vector Protocol (AODV) is intended for use by the mobile nodes for routing data in Ad Hoc networks. AODV is an extension of Distance-Sequenced Distance-Vector routing protocol a Table Driven routing protocol for Ad Hoc networks that is discussed in the previous section. AODV is designed to improve upon the performance characteristics of DSDV in the creation and maintenance of routes. The primary objectives of AODV protocol are:

- To broadcast discovery packets only when necessary,
- To distinguish between local connectivity management and general topology maintenance and
- To disseminate information about changes in local connectivity to those neighbouring mobile nodes those are likely to need the information.

5. EFFECTS OF CONGESTION

As WSN is a multi-hop network, congestion taking place at a single node may diffuse to the whole network and degrade its performance drastically. Congestion causes many folds of drawbacks:

1. Increases energy dissipation rates of sensor nodes

2. Causes a lot of packet loss, which in turn diminish the network throughput and

3. Hinders fair event detections and reliable data transmission.

4. Large queuing delays are experienced as the packet arrival rate nears the link capacity.

6. OBJECTIVES

Our objective in this paper is to provide efficient data rate throughout the network operation, handling varying traffic rates. Congestion is main factor in degrading network throughput. To satisfy this objective we propose techniques to detect congestion, and take action to maintain a constant traffic rate. Our aim is to try and maintain network in an ideal state in which it will deliver maximum packets allowed by network bandwidth consistently. Initial step towards achieving this goal is to categorize packet loss and congestion types in wireless networks.

7. CNGESTION DETECTION

In our work we have proposed a congestion control technique. But accurate congestion detection is also equally important. AODV routing protocol is used to make a route from source to destination. To show congestion multiple sources to single destination are used, which results in path of common nodes and congestion may occur in that path. Before discussing the detail of congestion detection mechanism a light has been put on AODV protocol.

Table 3.1: Proposed Packet Format

Source ID	Destination ID	Hop Count	MAC	OCS	Queue length	C_{act}

The proposed packet is shown in table 3.1. It contains source id, destination id occupies 2 bytes. Source id is used to identify the node, which is ready to discover the route. Destination node verifies the packet received from route, which contains source id.

- The Hop count is incremented once the packet is successfully sent. It occupies 1 byte field. Hop count determines number of nodes is connected to the particular node.
- Medium Access Control (MAC) is for accessing the particular channel.
- Overall Congestion Standard is used to verify the congestion aware route. It occupies 4-byte field.
- Queue length occupies 2 bytes field, which verifies the packet dropping ratio.
- Channel activity Cact is used to verify the occupation of the channel, which occupies 2 bytes field.

Figure 3.2 shows the path shared by two sources. At node number 34 sharing of paths started as indicated by a blue circle in the figure. The channel bandwidth in WSN is always fixed and can't be altered so nodes have to transmit message within that limit. When message from source 1 is transmitted to destination and after same time source 2 transmits then it senses the path is already acquired by other and no space to transmit the new message to destination. It will wait for some moment at node 34, if this waiting time is high then source node may consider the loss of packets as no feedback from sink node is received within expected time and again new packet will be lost if path is still engaged.

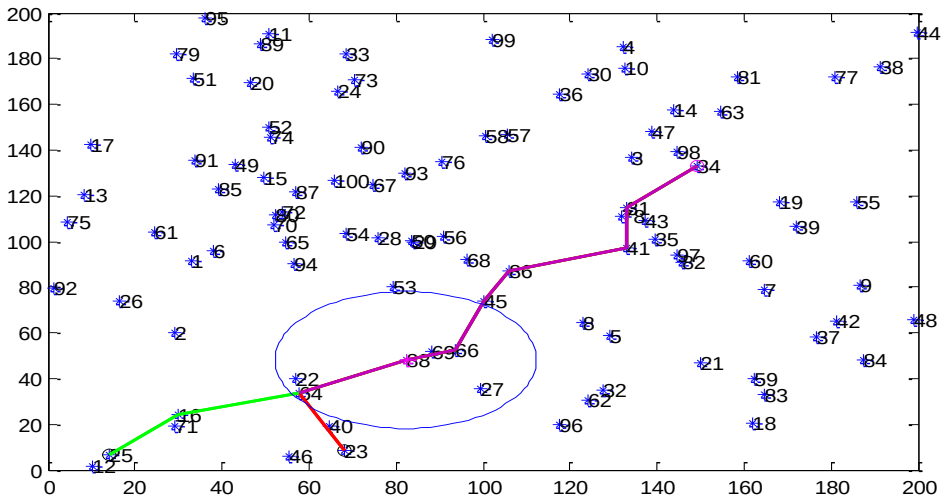


Figure 3.2: Common path for two sources to destination

8. Results & Discussion

In this work we used AODV routing protocol and based on the channel bandwidth and waiting time congestion in the network is found out. To simulate the AODV WSN environment we have used MATLAB as a tool because it provides many toolboxes which helped in simulating the environment of network. Initial parameters considered for it are tabulated in table 4.1 below.

Table 4.1: Initialization parameters considered for the network

Parameters	**Specifications**
Area Size	100x100 mtr
No. of Nodes	100
Mac	802.11
Mobility Model	Random Way Point
Protocol	AODV
Transmission Range	30mtr
Packet Size	512 bytes
Pause time	Yes
Traffic Source	CBR
Radio Range	250m
Simulation Time	50 sec
Channel Bandwidth	2Mbps

The simulation time for the algorithm has been set to 50 seconds, for 50 seconds congestion in the path may occur for some time intervals. The congestion profile for 50 seconds in shown in figure 4.2. When congestion occurs the value is set to 1 otherwise it is 0. Figure shows that maximum continuous congestion time is 43-50 seconds. During this time a new congestion free route is searched by the affected source node. That route doesn't include the affected nodes or nodes already present in present route. To see the congestion condition at respective time intervals a graph for channel bandwidth and total bandwidth requirement for both data channels is plotted in figure 4.3. It shows that when limit is violated and waiting time exceeded, congestion occurred.

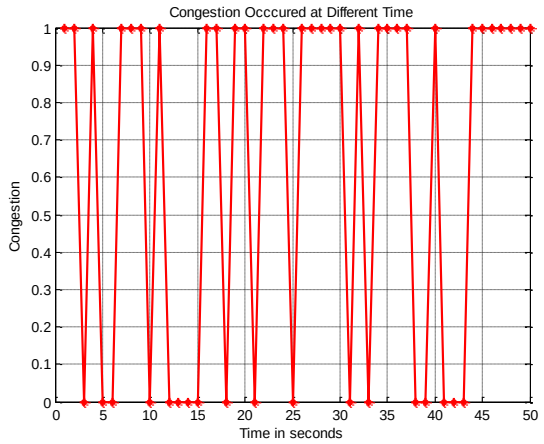


Figure 4.2: congestion profile for the network.

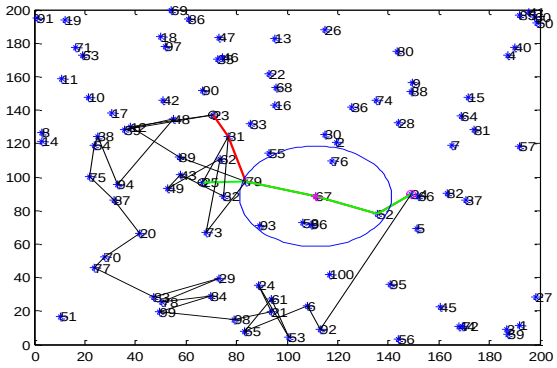


Figure 4.5: New route constructed by source node after congestion in the path

The route may be longer than original and to measure the efficiency of algorithm, data packets received is calculated. In this we have not considered the energy loss of data packets in travelling a long distance. This has been kept for future work. A comparison of packet delivery ratio is shown in figure 4.6. it is the ratio of total number of packets received to total number of packets sent. In this case some packets sent by second path could accommodate in the channel bandwidth and rest raise alarm for congestion in the path. If figure 4.6 is compared with figure 4.2, it shows the congestion is removed by proposed method only when congestion was in the path and packet delivery ratio is highest at that time.

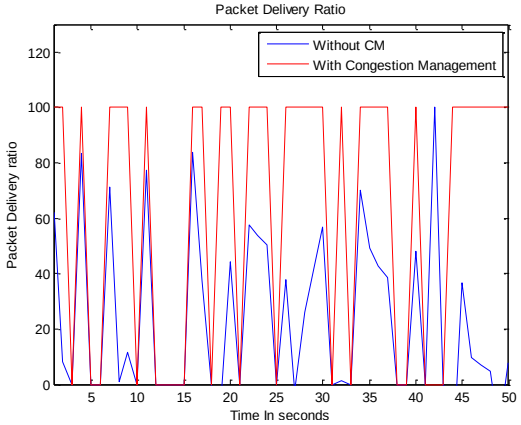


Figure 4.6: Percentage of Packet delivery ratio for proposed algorithm

9 . CONCLUSION

Initially in this paper we prove that traffic bottlenecks is a major issue in WSNs and that queue formation starts very early when bottlenecks appear in the network. Thus, in order to avoid queue formation the data rate of the incoming flow must be severely reduced. In case that this action is omitted, buffer fill-up is going to happen, while the time that passes until the nodes' buffers fill-up depends on the difference between incoming and outgoing flows. In order to solve this issue congestion control algorithms needs to be applied. These algorithms can be based either on traffic or resource control. According to the results of this paper, the traffic control method is an effective method for transient congestion occurrences but can be proven inappropriate when application needs all data to be transferred to sink. For this reason we base our proposed algorithms to the resource control method, a method that has not attracted a lot of interest due to the overhead that it creates. In this paper we addressed all possible problems that resource control methods may face and presented a novel algorithm. Before presenting the two algorithms, we study a number of issues that were raised in relation with topology control algorithms. Specifically, we studied whether source-based trees can provide an effective topology control solution as sink-based trees do. The results show that source based can provide a proper solution under specific circumstances and for specific applications. Source based trees constituted the base for the first novel algorithm that we presented.

10.FUTURE WORK

This research area is never ending area as due to sensor nodes battery constraint, researcher always try to develop algorithm which may consumes very less energy during transmission and reception as well as in detection mechanism executed on that. In our work we have not considered the energy concept at nodes, but in actual the congestion detection is done at node which takes energy of node in processing, decreasing the alive time of node. In future work, energy can be considered as a constraint in the algorithm as it may happen as with our case, after 50n seconds congestion detection. Our work is lacking with the effective new path searched after

congestion. It's a path with many hopes. These should be decreased so that energy of packets don't reduces much.

REFERENCES

[1] H. M. El-Sayed, O. Bazan, U. Qureshi, M. Jaseemuddin" Performance Evaluation of TCP in Mobile Ad hoc Networks", Second International Conference on Innovation in Information Technology (IIT'05).

[2] V.Elamathi, D.Dhivya "To Avoid Congestion by Using Flooding Approach in Wireless Ad Hoc Networks", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[3] S. Floyd and K. Fall, "Promoting the use of end-to-end congestion control in the internet" IEEE/ACM Transactions on Networking, 7(4), August 1999.

[4] Nishu Garg, R.P.Mahapatra "MANET Security Issues ", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[5] Anup W. Burange, PRMIT & R,Badnera,Dr. Vijay T. Ingole "Minimization of Congestion in Mobile Ad-Hoc Network ",International Journal of Advance Research in Computer Science and Management Studies Research Paper Volume 1, Issue 7, December 2013.

[6] L. Xia, Z. Liu, Y. Chang, P. Sun, "An Improved AODV Routing Protocol Based on the Congestion Control and Routing Repair Mechanism", Int. Conf. Communications and Mobile Computing, IEEE, China, 2009, vol. 2, pp. 259-262.

[7] S. Yin, and X. Lin, "MALB: MANET adaptive load balancing", In Vehicular Technology Conf. IEEE, Beijing, China, vol. 4, pp. 2843-2847, 2004.

[8] Special issue on Computational Intelligence, IEEE Journal on Selected Areas in Communications (JSAC), Volume 15, Issue 2, February 1997.

[9] Gasim Alandjani and Eric E. Johnson, "Fuzzy Routing in Ad Hoc Networks" IEEE 2003.

[10] S. Floyd and V. Jacobson. "Random early detection gateways for congestion avoidance", IEEE/ACM Transactions on Networking, 1(4):397–413, 1993.

[11] V. Firoiu and M. Borden, "A study of active queue management for congestion control", In Proceedings of the IEEE Infocom, pages 1435–1444, Tel Aviv, Mar 2000.

