Adaptive Reliable and Congestion Conscious Routing Protocol (RCCRP) using Link Stability Estimation with Bypass Route Mechanism for Mobile Ad hoc Networks

R.Vadivel
Doctoral Research Scholar
of Manonmaniam Sundaranar University,
Assistant Professor, Department of IT, SCSE,
Bharathiar University, Coimbatore – 641 046.

V. Murali Bhaskaran
Principal
Paavai College of Engineering
NH – 7, Pachal
Namakkal - 637 018.

ABSTRACT

In Mobile Ad hoc Networks (MANETs) the main reason for packet loss is due to the link failure or node failure. When the link failure occurs, the upstream node with the cached data in its buffer can retransmit it through the next reliable link by using a bypass route and fault tolerance technique is alone handled. The technique of choosing the bypass route and the way to avoid congestion in the bypass route are not handled. In this paper, we propose an adaptive reliable and congestion control routing protocol to resolve congestion and route errors using bypass route selection in MANETs. When a source node detects congestion on a link along the path, it distributes traffic over alternative paths. The congestion is detected according to the utilization and capacity of link and paths. The distribution of traffic considers the path availability threshold and utilizes a traffic splitting function. If a node cannot resolve the congestion, it signals its neighbors using the congestion indication bit. By using simulation, we show that that the proposed protocol is reliable and achieves more throughput with reduced packet drops.

Keywords

Mobile Ad hoc Networks, Routing, Congestion Conscious Routing, Link Stability Estimation, Bypass Route Discovery.

1. INTRODUCTION

The performance level of a service provided by the network to the user is the Quality of Service (QoS). Most of the multimedia applications have severe QoS requirements which have to be satisfied. Achieving more deterministic network behavior is the aim of QoS Provisioning, where the information from the network can delivered in a better way and the resources of the network can be utilized. But, providing QoS solutions and maintaining end-to-end QoS with end user mobility remains as a major challenge [1].

QoS routing requires a route which satisfies the end-to-end QoS requirement in terms of bandwidth or delay but not only to find a route from source to destination. Calculating paths which are suitable for different type of traffic generated by various applications while maximizing the utilizations of network resources. The following are the major objectives of QoS routing [2]:

- To find a path from source to destination satisfying users requirements
- To optimize the usage of network usage

To decay the network performance when unwanted things like congestion, path breaks appear in the network.

1.1 Failures in Routing

Maximizing the data packet delivery in the face of fast changing network topology devoid of incurring a large routing overhead is the major issue in mobile ad hoc networks. The packet delivery ratio can be reduced by slow detection of broken links which causes the data packets to be forwarded to stale or invalid paths. The main reason for packet loss in ad hoc networks is the link failure or node failure. A MAC failure is caused if there is more than one packet using this link after the physical layer failure. Though after a failure, the routing protocol takes off such packets from the queue, new packets still keep coming into the queue without any checking. If the new incoming packets make use of the failed link, then they will block all other packets resulting in network wide low throughput and long delay [3]. Detection of such failures in an ad hoc network becomes challenging due to the lack of centralized monitoring and management point. This makes the faulty nodes to remain long time in the network, which affects the performance of routing in the ad hoc network. For instance, if a defective node participating in the routing process drops data packets, subsequently a large number of packets will be lost [4].

1.2 Congestion in MANETs

Network congestion is the major problem in the mobile wireless ad hoc networks. Due to limited availability of resources, the congestion occurs in mobile ad hoc networks. In such networks, due to shared wireless channel and dynamic topology, packet transmissions suffer from interference and fading. Due to exhaustive bandwidth the large amount of real time traffic is likely to explode and tends to congestion. Congestion tends to packet losses, bandwidth degradation, wastes time and energy on recovery. Even if the influence of congestion is reduced it is not possible to overcome the congestion problem completely. By using some suitable procedures and rules for traffic flow, the influence of congestion can be reduced [5]. TCP congestion control works very well on the Internet. The design of suitable protocols and protocol stacks in general and particularly the congestion control mechanism are affected severely by some of the unique properties of MANETs. For standard TCP, the widely differing environment in a MANET is highly problematic. Generally congestion is concentrated on a single router when it occurs on the internet.

On the other hand, due to the shared medium congestion in MANET affects the whole area [6]. Due to congestion, none

single sender is capable to collapse the network deliberately due to the comparatively low bandwidth of MANETs. The severe unfairness between the traffic flows are caused because of the extreme effect of a single traffic flow on the network condition.

When compared with the conventional wire line networks like Internet the wireless multihop networks are liable to overload-related problems. Hence it is essential for an appropriate congestion control for network stability and acceptable performance [6].

It can be noticed that when the link failure occurs, the upstream node with the cached data in its buffer can retransmit it through the next reliable link by using a bypass route and fault tolerance technique is alone handled. The technique of choosing the bypass route and the way to avoid congestion in the bypass route are not handled.

This paper is an extension of [14]. In this paper, we propose a technique for selecting the bypass route to resolve the congestion. When a source node detects congestion on a link along the path, it distributes traffic over alternative paths. The congestion is detected according to the utilization and capacity of link and paths. The distribution of traffic considers the path availability threshold and utilizes a traffic splitting function. If a node cannot resolve the congestion, it signals its neighbors using the congestion indication bit.

2. LITERATURE REVIEW

Jun Peng et al [7] have presented a multi-rate multicast congestion control scheme for Mobile Ad-hoc Networks (MANETs). There the proposed scheme overcome the disadvantages of existing multicast congestion control protocols which prevent them from being used in MANETs, but it also achieves good performance in other aspects such as fairness with TCP, robustness against misbehaving receivers, and traffic stability.

Karunakaran et al [8] have presented a Cluster Based Congestion Control (CBCC) protocol that consists of scalable and distributed cluster-based mechanisms for supporting congestion control in adhoc networks. The distinctive feature of their approach is that it is based on the self-organization of the network into clusters. The clusters autonomously and proactively monitor congestion within its localized scope. By exchanging small amount of control packets along the paths, adjustment of node rates and co-operation between cluster nodes are achieved. Clustering helps to determine the interactions between the flows. When compared to end-to-end techniques, our approach improves the responsiveness of the system.

Kazi Chandrima Rahman et al [9] have proposed a novel Explicit Rate-based Congestion Control mechanism (XRCC), where routers provide explicit feedback which allows quick increase of throughput. Since routers are the central places where congestion takes place, they are in a better position to detect and respond to such condition. Hence, an explicit rate-based congestion control where senders' flow is controlled by the explicit information in the feedback packets from the routers can outperform the TCP and TCP like protocols' conservative behavior for multimedia streaming over MANET. Their mechanism supporting applications like multimedia streaming over MANET.

Kazuya Nishimura et al [10] have discussed a routing protocol that uses multi-agents to reduce network congestion for a Mobile Ad hoc NETwork (MANET). They have engaged two kinds of agents in routing. One is a Routing Agent that collects information about network congestion as well as link failure. The other is a Message Agent that uses this information to get to their destination nodes. MAs correspond to data packets and determine their direction autonomously using an evaluation function. They have developed both a simulation environment and protocols, and performed simulations under different conditions of mobility and traffic patterns to demonstrate the effectiveness of their approach. Umut Akyol et al [11] have studied the problem of jointly performing scheduling and congestion control in mobile adhoc networks. They have defined a specific network utility maximization problem and described a wireless Greedy Primal Dual (wGPD) algorithm for combined congestion control and scheduling that aims to solve this problem. They have shown that how the wGPD algorithm and its associated signaling can be implemented in practice with minimal disruption to existing wireless protocols.

3. RELIABLE AND CONGESTION CONSCIOUS ROUTING PROTOCOL (RCCRP) USING LINK STABILITY ESTIMATION WITH BYPASS ROUTE MECHANISM FOR MOBILE AD HOC NETWORKS

3.1 Measuring the Signal Strength

The received signal strength in cross layer designs can be calculated at the physical layer, and it is accessed at the top layers. The procedures at physical layers have to be modified, in order to reassign the measured value of received signal strength to the MAC layer along with the signal [12]. This value is used if required, or to pass the routing layers along with the routing control packets in the calculation of MAC layer. Also this value is stored in the routing/neighbour tables and is used in decision making process. The received signal strength is passed to the top layers, as an interlayer interaction parameter. The received signal strength is used to improve the performance of the mobile ad hoc networks by adjusting the medium access and routing protocols as per the required cross layer design.The IEEE 802.11 is reliable MAC protocol. Since the received signal strength must reach every exposed node, it assumes the fixed maximum transmission power. When a sending node transmits RTS packet, it attaches its transmissions power. The receiving node measures the signal strength received for free–space propagation model while receiving the RTS packet [12].

$$P_R = P_T(\lambda / 4\pi d)^2 G_T G_R \qquad (1)$$

Where λ is the wavelength of carrier, d is distance between sender and receiver, GT and GR are unity gain of transmitting and receiving omni directional antennas, respectively.

3.2 Route Expiration Time (RET)

The RET is the minimum time selected from a set of link expiration times (LETs) designed for the feasible path. LET is the period of time between two nodes. So, minimum value of LET is attained in each path and the maximum number of RET which represents the more reliable routing path is selected.

$$\text{RETi} = \text{Min (LETsi)} \qquad (2)$$

Thus, the RET is the maximum value among LETs of the feasible path. The principle of LET is to estimate future disconnection time with the help of two neighbors in motion and this can be achieved by using the following method. Global positioning system (GPS) determines the motion parameters of two neighboring nodes. Following assumptions are made, a free space propagation model whose signal strength solely depends on the distance to the transmitter and all nodes have their clocks synchronized by using the GPS clock. The duration of time can be calculated for the two nodes which remained connected by having knowledge of the motion parameters of two nodes. These parameters which are obtained from the GPS include speed, direction, and radio range. Given a prediction Tp on the continuously available time for an active link between two nodes at time t0, the availability of this link, L (Tp), is defined as

$$L\ (Tp) = P\ \{\text{to last to } t0+Tp \mid \text{Available at } t0\},$$

which indicates the probability that the link will be continuously available from time t0 to t0+Tp. The calculation of L (Tp) can be divided into two parts: the link availability when the velocities of the two nodes keep unchanged between t0 and t0+Tp, L1 (Tp), and the one for the other cases, L2 (Tp). That is,

$$L\ (Tp) = L1\ (Tp) + L2\ (Tp) \qquad (3)$$

It is easy to calculate L1 (Tp), which is equal to the probability that the epochs from t0 onwards for the two nodes are longer than Tp because Tp is an accurate prediction if the movements of the two nodes keep unchanged. Since nodes' movements are independent of each other and exponential distribution is 'memoryless', L1 (Tp) is given by

$$L1\ (Tp) = [1 - E\ (Tp)]\ 2 = e^{-2\lambda Tp} \qquad (4)$$

However, it is difficult to give an accurate calculation for L2 (Tp) because of the difficulties in learning changes in link status caused by changes in a node's movement.

3.3 Node Remaining Energy

It is assumed that all nodes are equipped with a residual power detection device and know their physical node position. The packet transmitting energy for a packet can be computed as

$$Energy_{tx} = \frac{Psize \times Power_{tx}}{LBW} \qquad (5)$$

where Psize is the data packet size, Powertx is the packet transmitting power and LBW is the wireless link bandwidth. When a mobile node performs power control during packet transmission, the transmitting energy for one packet relative to the node distance is given as

$$Energy_{tx} = kd^{\alpha} \qquad (6)$$

Where k is the proportionality constant, d is the distance between the two neighboring nodes, and α is a parameter that depends on the physical environment (generally between 2 and 4). The shorter distance between the transmitter and the receiver, the smaller amount of energy required. At each node, the total required energy is given by

$$Energy_{tot} = p \times (Energy_{tx} + Energy_{pro}) \qquad (7)$$

where p is the number of packets. The energy required for packet processing ($Energy_{proc}$) is much smaller than that required for packet transmitting. The node remaining energy or the residual energy is the energy left after the packet transmission (i.e.) residual energy $Energy_{res}$ is given by

$$Energy_{res} = Energy_{initial} - Energy_{tot} \qquad (8)$$

3.4 Node Velocity

Consider a node N1 which can always communicate with another node N2 until it reaches position p3, which is at a distance R from N1, where R is the transmission range of each node.

Tp = Tp1p3, where Tp1p3 is the time taken by node N1 to move from p1 to p3.

It is clearly the continuous available time of the wireless link between nodes N1 and N2. Knowing Tp, the probability that a link is available during the time period of Tp can be calculated. By assuming a random walk-based mobility model during a time interval called mobility epoch, each node moves in a constant direction at a constant speed. The epoch length of every node is exponentially disseminated with mean . The route is evenly distributed over [0, 2π] and the speed is also uniformly distributed in a known range. It is assumed that, speed, direction, epoch length, and mobility of nodes are uncorrelated and the links fail autonomously. A conservative prediction of the link being available in the time period of Tp is given based on all the assumptions above as [13]

$$L_2(T_p) = \frac{1 - e^{-2\lambda T_p}}{2\lambda T_p} + \frac{\lambda T_p e^{-2\lambda T_p}}{2} \qquad (9)$$

A metric is needed to reflect this aspect and whose value should lie in the range [0, 1] for accounting the reliability of a link while selecting routes. It is impossible to combine the L (Tp) of each link along a path for estimating the path availability, because each link has a different Tp. The term Tp x L (Tp) is used in the place of L (Tp) which is an evaluation of average available time of a link. We can detain our interest of the estimation within Tr, by assuming that estimation will be carried out regularly with period Tr. The ratio of Tp x L (Tp) to Tr. is very much concerned. A new routing metric is developed based on the above reasoning which is referred to as normalized link availability (LAN) and it can be defined as follows: [13]

$$LA_N = \min\left[\frac{T_p\ x\ L_2(T_p)}{T_r}, 1\right] \qquad (10)$$

3.5 Combined Metric

Finally, the combined metric for finding the link life time is given by

$$CRM = PR + L1\ (TP) + Energyres + LAN \qquad (11)$$

The node status is adaptively determined based on the value of CRM as given below.

Node status is Green, if CRMmin > CRM < CRMmax

Node status is Yellow, if CRM = CRMmin

Node status is Red, if CRM < CRMmin

where CRMmin and CRMmax are the maximum and minimum combined routing metric values. Then Bypass Route Discovery is performed as described in our previous work. When a link is likely to be broken, the previous node will cache the subsequent packets in its data buffer. When a link failure occurs, the upstream node with the cached data in its buffer can retransmit it through the next reliable link by using a bypass route.

3.6 Bypass Route Technique to resolve Congestion

It is described a set PG of common link paths between N and D to create a multipath route which includes the property that any two paths p,q PG have almost G common links, i.e.,

$$|Ln(p) \cap Ln(q)| \leq G \quad (12)$$

Algorithm 1 defines the PG group. Generally the pair wise disjoint paths from N to D are included in the set of group-0 paths. The property of the group 1 paths is that the every pair in the paths shares almost a single common link whereas in group 2 paths it shares two common links. This can be explicitly expressed as for group-1 paths, a link (f,d) where f is a neighbor of node d and for the group 2 paths (f,d) and (f',f) which form a sub path {f',f,d}. Similarly the set of group-3 and group-4 paths can be described. We can observe that in the set of group (G+1) paths for G = 1,2,.. the set of group-G paths are included. Hence, we have

P(0)ND P(1)ND P(2)ND …. PG PND, For G > 2 (13)

Input: AP, G, N, D Output: PG
PG ← {P}
While AP ≠ δ do
$\hat{P}$ ← argmin {d(q): q $\in$ AP
AP ← AP\ {$\hat{P}$}
Size ← | PG|
for each p $\in$ PG do
if |Ln($\hat{P}$) ∩ Ln(P) ≤ G, then
size ← size-1
else
break
end if
end for
if size = 0, then
PG ← PG U {p}
end if
end while

In Algorithm 1, the set PG is initialized to contain the shortest path P. The other paths in PG are selected from the set of alternative paths AP in increasing order of path length. The while loop iterates over all paths in the set APND. In lines 4 and 5, the shortest path in the (current) set APND is removed from the set. In lines 6-13, the candidate path is tested against all of the paths in the (current) set PG to check whether the condition (3) is satisfied. If satisfies for all paths p PG, then is added to the set PG (lines 14-16).

By using Algorithm 1, we develop a method to resolve the network congestion by distributing the traffic over group-G multipath routes. Node N calculates the multipath routes to destinations D when it detects congestion on a local outgoing link Ln for which the path pND contains link Ln. Some part of the traffic to node D is then transferred to alternative paths p PG. If the utilization of a local link exceeds a local congestion threshold TH then the congestion is detected in the local link. The main goal is, by shifting a portion of the traffic to the alternative paths the utilization has to be reduced adequately and this part of traffic as bypass traffic.

A node calculates a set of alternative paths and distributes the bypass traffic over these paths whenever it detects local link congestion or receives an ACI (Absolute Congestion Index) bit from a neighbor. A node produces signals to its neighbors using the ACI bit when a node is not able to solve the congestion in the former method. The following is the procedure for congestion-triggered multipath traffic distribution to resolve congestion at the local link.

1) When node N detects local congestion on outgoing link l, PUT(Ln) > TH), or receives an ACI=1 bit from a neighbor node on link l, it tries to move bypass traffic onto alternative paths that avoid this link. The alternative paths are group-G paths determined using Algorithm 1.

2) Let SP = {p PG : PUT(p) < μ}, where μ is called the path availability threshold.

3) Distribute traffic over the path set SP.

For its active path Pa, the node N load balances its current traffic on the entire available path. Let the current load of node N be 100kbit/s. Let P1,P2,P3, and P4 be the available paths in SP. Node N will use the multiple paths P1, P2, P3 and P4 in addition to its primary path Pa on reception of ECI and will send on each of these paths with equal amount of data rate (i.e.) 100/4 = 25kbit/s of data.

4. SIMULATION SETTINGS AND PERFORMANCE METRICS

4.1 Simulation Settings

We use NS2 [16] to simulate our proposed technique. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, we keep the number of mobile nodes as 150. The mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). The CBR flows are varied as 2, 4, 6 and 8. Our simulation settings and parameters are summarized in table 1.

Table 1. Simulation Settings

No. of Nodes	50,75,100,125 and 150
No. of Flows	2, 4, 6 and 8.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Speed	10m/s
Rate	100,150 ,200 and 250 Kb.
No. of Nodes	50,75,100,125 and 150
No. of Flows	2, 4, 6 and 8.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec

4.2 Performance Metrics

We evaluate mainly the performance according to the following metrics.

- Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.
- Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.
- Drop: It is the average number of packets dropped.
- Overhead: It is the number of control packets exchanged during the entire transmission of data packets.

The simulation results are presented in the next section.

5. RESULTS AND DISCUSSIONS

In this experiment in NS2 [16], we vary the network size by increasing the number of nodes as 50, 75, 100, 125 and 150. We keep the number of flows as 8 and data rate as 250kb. From the figure 1 we can see that, when we increase the number of nodes, the delay is increased linearly. It can be observed that AODV has the highest delay followed by Hop-by-Hop [15]. ARCCRP has significantly less delay than the Hop-by-Hop and AODV. When we increase the number of nodes, the number of packets dropped increases and hence the packet delivery ratio decreases slightly. From Fig 2, we can see that ARCCRP has high delivery ratio followed by Hop-by-Hop, while AODV has the least delivery ratio. Figure 3 shows that the packet drop is less in ARCCRP followed by Hop-by-Hop whereas AODV has the highest packet drop. When the number of nodes is increased, the control packets exchanged will increase resulting in the increased overhead. But from figure 4, we can see that, ARCCRP has slightly less overhead than the existing Hop-by-Hop protocol.

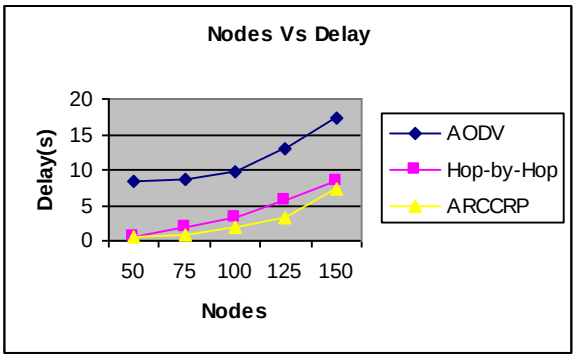

Fig. 1. No. of nodes Vs Delay

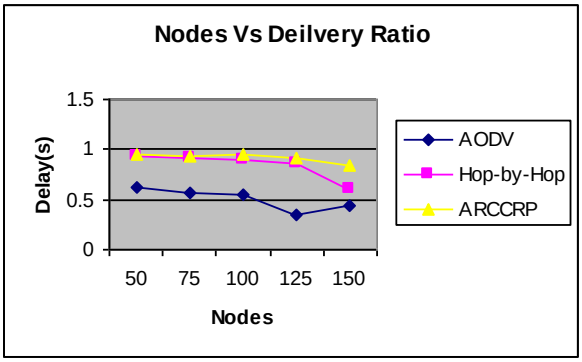

Fig. 2. No. of nodes Vs Delivery Ratio

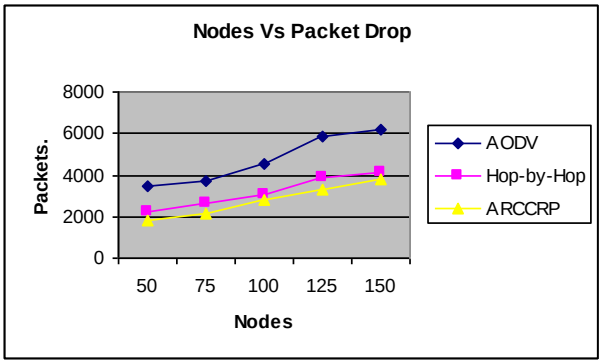

Fig. 3. No. of nodes Vs Packet drop.

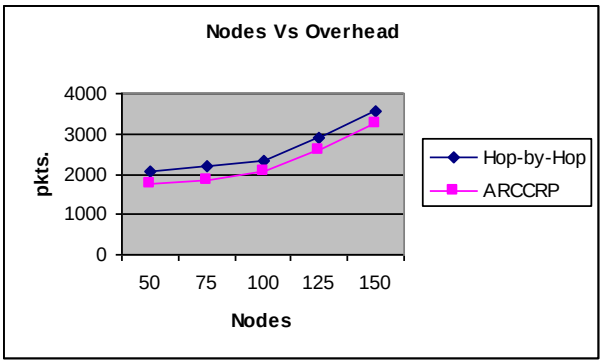

Fig. 4. No. of nodes Vs Overhead

6. CONCLUSIONS

In this paper, we have proposed an enhanced technique to resolve congestion using bypass route selection in MANETs. When a node detects congestion on a local outgoing link L, it calculates the multipath routes to destinations for which the path contains link L. Some portion of the traffic to node is then shifted to alternative paths. Congestion is detected on a local link if its utilization exceeds a local congestion threshold TH. The objective is to minimize the utilization to a more acceptable level by shifting a portion of the traffic to the alternative paths and this part of traffic as bypass traffic. A node calculates a set of alternative paths and distributes the bypass traffic over these paths whenever it detects local link congestion or receives an Explicit Congestion Indication (ECI) bit from a neighbor. A node produces signals to its neighbors using the ECI bit. By simulation results, we have shown that the proposed protocol is reliable achieves more throughput with reduced packet drops.

7. ACKNOWLEDGEMENTS

The authors thanks UGC for allocating Minor Research Project grant during Feb 2011 to Feb 2013 Grant Number 39-947/2010 (SR).

8. REFERENCES

[1] G. Santhi and Alamelu Nachiappan, "A survey of QoS routing protocols for mobile ad hoc networks", International journal of computer science & information Technology (IJCSIT) Vol.2, No.4, August 2010.

[2] Chunxue Wu, Fengna Zhang, Hongming Yang, "A Novel QoS Multipath Path Routing in MANET", International Journal of Digital Content Technology and its Applications Volume 4, Number 3, June 2010.

[3] Xiaobing Hou and David Tipper, "Impact of Failures on Routing in Mobile Ad Hoc Networks Using DSR".

[4] Yuan Xue and Klara Nahrstedt, "Fault Tolerant Routing in Mobile Ad Hoc Networks", IEEE 2003.

[5] Laxmi Shrivastava, G.S.Tomar and Sarita S. Bhadauria, "A Survey on Congestion Adaptive Routing Protocols for Mobile Ad-Hoc Networks", International Journal of Computer Theory and Engineering, Vol. 3, No. 2, April 2011.

[6] Christian Lochert, Bjorn Scheuermann and Martin Mauve, "A Survey on Congestion Control for Mobile Ad-Hoc Networks", Wiley Wireless Communications and Mobile Computing, June 2007.

[7] Jun Peng and Biplab Sikdar, "A Multicast Congestion Control Scheme for Mobile Ad-Hoc Networks".

[8] S.Karunakaran and P.Thangaraj, "A Cluster Based Congestion Control Protocol for Mobile Ad hoc Networks", International Journal of Information Technology and Knowledge Management, July-December 2010.

[9] Kazi Chandrima Rahman and Syed Faisal Hasan, "Explicit Rate-based Congestion Control for Multimedia Streaming over Mobile Ad hoc Networks", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 10 No: 04, July 2010.

[10] Kazuya Nishimura and Kazuko Takahashi, "A Multi-Agent Routing Protocol with Congestion Control for MANET", Proceedings 21st European Conference on Modelling and Simulation, ECMS 2007.

[11] Umut Akyol, Matthew Andrews, Piyush Gupta, John Hobby, Iraj Saniee and Alexander Stolyar, "Joint Scheduling and Congestion Control in Mobile Ad-Hoc Networks",

[12] B. Ramachandran and S.Shanmugavel, "Received Signal Strength-based Cross-layer Designs for Mobile Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network security, VOL.9 No.1, January 2009.

[13] Xueyuan Su, Sammy Chan and King-Sun Chan, "RLAR: Robust Link Availability Routing Protocol for Mobile Ad Hoc Networks", IEEE International Conference on Communications, ICC '07, 4759 – 4766, 24-28 June 2007.

[14] R.Vadivel and V. Murali Bhaskaran, "Adaptive Reliable Routing Protocol Using Combined Link Stability Estimation for Mobile Ad hoc Networks" , INTERNATIONAL CONFERENCE ON MODELING, OPTIMIZATION, AND COMPUTING (ICMOS 20110) West Bengal, India, AIP Conf. Proc. 1298, pp. 625-632.

[15] Yung Yi and Sanjay Shakkottai, "Hop-by-Hop Congestion Control Over a Wireless Multi-hop network", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 1, FEBRUARY 2007.

[16] Network Simulator, http://www.isi.edu/nsnam/ns.