

A Fault Tolerant Congestion Aware Routing Protocol for Mobile Adhoc Networks

¹Rajkumar, G. and ²K. Duraiswamy

¹Department of ECE Shanmuga Arts, Science,
Technology and Research Academy, Thanjavur

²Department of Computer Science and Engineering,
K.S.R College of Technology, Tiruchengode

Abstract: Problem statement: The performance of ad hoc routing protocols will significantly degrade when there are faulty nodes in the network. Packet losses and bandwidth degradation are caused due to congestion and thus, time and energy is wasted during its recovery. The fault tolerant congestion aware routing protocol addresses these problems by exploring the network redundancy through multipath routing. **Approach:** In this study, it is proposed to design a fault tolerant congestion aware multi path routing protocol to reduce the route breakages and congestion losses. The AOMDV protocol is used as a base for the multipath routing. This proposed scheme enables more nodes to salvage a dropped packet. **Results:** Simulation results show that the proposed protocol achieves better throughput and packet delivery ratio with reduced delay, packet drop and energy. **Conclusion:** An effective congestion control technique proposed in this study proactively detects node level and link level congestion and performs congestion control using the fault-tolerant multiple paths.

Key words: Mobile Ad-Hoc Network (MANET), Congestion Control and Fairness (CCF), In-Network Packet Scatter (IPS), End-to-End Packet Scatter (EPS), Biased Geographical Routing (BGR), Packet Sending Rate (PSR)

INTRODUCTION

Routing in Mobile Ad-Hoc Network (MANET): A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links, to form an arbitrary topology. The nodes are free to move arbitrarily. Thus, the network's wireless topology may be random and may change quickly. Such a network may operate in a standalone fashion, or may be linked to the larger Internet. An ad Hoc network is formed by sensor networks consisting of sensing, data processing and communication components. Due to be deficient in infrastructure support, each node acts as a router, forwarding data packets for other nodes. Its application area includes Tactical Networks, Emergency Services, Commercial Environments Educational Applications and entertainment (Akhter and Sanguankotchakorn, 2010).

Routing is performed for many kinds of networks, including the telephone network (Circuit switching), electronic data networks (such as the Internet) and transportation networks. The following limitations are observed for routing traffic in mobile ad hoc networks:

- Nodes in traditional wired networks do not route packets, while in MANET every node is a router
- Nodes transmit and receive their own packets and forward packets for other nodes also
- Due to mobile nodes, topologies are dynamic in MANET, but are relatively static in traditional networks
- Connectivity and interference are indicated by link layer information
- A traditional router has an interface for each network to which it connects, while a MANET "router" has a single interface
- Routed packet sent forward when transmitted, but also sent to previous transmitter
- MANETs may have gateways to fixed network, but are normally "stub networks"

Fault tolerant routing: The performance of ad hoc routing protocols will significantly degrade because of faulty nodes in the network or route failures. The main cause of route failures is node mobility. Another factor that can lead to router failures is the link failures due to the contention on the wireless channel. A route includes

Corresponding Author: Rajkumar, G., Department of ECE Shanmuga Arts Science Technology and Research Academy, Thanjavur

a sequence of links. Even if only one link in the sequence fails, the route no longer works. That is, route stability is heavily affected by link stability. Whenever a route fails, consequent route maintenance is triggered and thus the network throughput degrades (Khazaei and Berangi, 2009). Node failure due to power shortage is significant cause of route failure. In MANET, users communicate by relaying in multi-hop. A multi-hop route breaks because of the movement of relative nodes, burst error in wireless channels or hidden terminal collisions. The route failure leads to unnecessary route maintenance, route error diffusion and upper layer multi-hop retransmission. This process significantly increases routing overhead and prolonged end-to-end delay (Saxena and Sinha, 2011)

The fault tolerant routing protocol addresses these problems by exploring the network redundancy through multipath routing. Guaranteed Packet delivery in the presence of faulty nodes will be provided by fault tolerant routing algorithm.

Fault Tolerant Routing protocols can be classified into 2 categories.

Proactive: They provide protection proactively (before the fault occurs) by:

- Suitably selecting optimum paths with least possibility of faults
- By caching important data
- By using erasure codes or redundant data

Reactive: They provide protection reactively (after the fault occurs) by:

- Using Retransmission techniques
- Using Effective Route maintenance techniques
- Using Alternate path techniques

Multipath routing protocols can be used for fault tolerance in which proactive or reactive techniques can be used. Multipath routing protocol provides fault tolerance with redundant information routed to destination via alternative paths. Thus probability is reduced saying communication is disrupted in case of link failure. The source coding can be employed in order to reduce the traffic overhead caused by more redundancy, also maintaining the same degree of reliability (Manjre and Gulhane, 2011)

Congestion: Congestion takes place in MANETs with limited resources. In these networks, shared wireless channel and dynamic topology leads to interference and fading during packet transmission. Packet losses and

bandwidth degradation are caused due to congestion and thus, time and energy is wasted during its recovery (Narasimhan and Baboo, 2009).

Congestion detection: Congestion can be prevented using congestion-aware protocol through bypassing the affected links. Congestion control is the major problem in mobile ad hoc networks. Congestion control is related to controlling traffic entering into a telecommunication network. To avoid congestive collapse or link capabilities of the intermediate nodes and networks and to reduce the rate of sending packets, congestion control is used extensively.

Congestion collapse in wireless networks has particularities such as spatial correlation that cause even idle nodes to become congested when the wireless area around them is busy. Unlike the Internet where congestion is mostly situated at the border of the network, in wireless networks with point-to-point communication congestion usually builds in the center. Fortunately, the connectivity of most wireless networks is rich enough to allow routing packets on alternate paths that avoid the congested areas (Lakshmi and Bindhu, 2011).

Congestion detection types: Congestion detection protocols can be implemented by the following main schemes:

- Open-loop hop-by-hop backpressure technique-In this technique, backpressure is generated as long as congestion is detected when an upstream node (toward the source) receives a backpressure message it decides whether or not to further propagate the backpressure upstream based on its own local network conditions
- Closed-loop multi-source regulation technique-In this technique, when the source event rate is less than some fraction of the maximum theoretical throughput of the channel, the source regulates itself. However a source is more likely to contribute to congestion and therefore closed-loop congestion control is triggered, the source only enters sink regulation if this threshold is exceeded
- Hop-by-hop Backpressure-In Hop-by-hop Backpressure, if the sink is congested, backpressure spatially spreads the congestion and helps alleviate congestion quickly. Once congestion is detected, the receiver will broadcast a suppression message to its neighbors. The hop-by-hop backpressure could immediately response to the congestion at the intermediate node without incurring the round trip delay that reduces feedback's effectiveness

- **Queue Occupancy-**It is a simple way to detect congestion which relies on monitoring a sensor's queue size. If the fraction of space available in the output queue falls below a high water mark, the congestion bit of outgoing packets is set; otherwise the congestion bit is cleared
- **Receiver Based-**It uses a combination of the present and past channel loading conditions and the current buffer occupancy, to infer accurate detection of congestion at each receiver side. Once congestion is detected, nodes signal their upstream neighbors via a backpressure mechanism
- **Event to Sink Reliable Transport-**In Event to Sink Reliable Transport, a sensor sets a congestion notification bit in the packet header if its buffer is full. The sink periodically computes a new reporting rate based on a reliability measurement, the received congestion notification bits and the previous reporting rate

Congestion Control and Fairness (CCF): It uses packet service time to deduce the available service rate and detects congestion. Each sensor node uses rate adjustment based on its available service rate and number of child nodes. CCF provides simple fairness for all nodes with same throughput. But fairness can maintain, while each node gets same priority (Chakravarthi *et al.*, 2010).

Effects of congestion: Packet loss in MANETs is mainly caused due to congestion. The packet loss can be reduced by involving congestion control over a mobility and failure adaptive routing protocol at the network layer. The congestion non-adaptive routing protocols, leads to the following difficulties.

Long delay: The congestion control mechanisms take much time for detecting congestion. Usage of new routes in some crucial situations is advisable. In an on-demand routing protocol, the major problem is the delay occurring for route searching.

High overhead: It takes effort in new routes for processing and communication for discovering it. It also takes effort in multipath routing for maintaining the multi-paths, though there is an alternative protocol

Packet losses: The packets may be lost when the congestion is detected. To reduce the traffic load, a congestion control solution is applied either by decreasing the sending rate at the sender, or dropping packets at the intermediate nodes or by both methods. But high packet loss rate or a small throughput occurs at the receiver (Valarmathi and Chandrasekaran, 2010).

Proposed protocol: The performance of ad hoc routing protocols will significantly degrade when there are faulty nodes in the network. The fault tolerant routing protocol addresses this problem by exploring the network redundancy through multipath routing. In the previous work (Rajkumar and Duraiswamy, 2011), a fault-tolerant multipath routing protocol has been designed to reduce packet loss due to route breakage. In this protocol, nodes determine multiple disjoint routes using AOMDV (Manjre and Gulhane, 2011) having more battery power and residual energy, to every active destination. In fault-tolerant mechanism, the received signal strength is measured and based on its value; it can send warning packets to the previous node. When a downstream node encounters a forwarding error, an upstream node with the same data in its buffer and alternative route can retransmit the data. The faults have proactively detected and provided fault-tolerant routing but didn't consider the losses due to congestion. Hence an effective congestion detection and control mechanism is required to reduce the congestion losses.

In this study, it is proposed to design an effective congestion control technique which proactively detects node level and link level congestion and perform congestion control using the fault-tolerant multiple paths. The AOMDV (Manjre and Gulhane, 2011) protocol is used as a base for the multipath routing. In existing reactive routing protocols, only the node encountering the error can salvage or retransmit a data packet. (i.e..) packet salvaging is centralized. This proposed scheme enables more nodes to salvage a dropped packet, (i.e..) packet salvaging is distributed.

Related work: Narasimhan and Baboo (2009) have proposed a hop-by-hop congestion aware routing protocol which employed a combined weight value as a routing metric, based on the data rate, queuing delay, link quality and MAC overhead. They have selected the route with minimum cost index, among the discovered routes, which was based on the node weight of the entire nodes in the network. They have used a multipath on demand routing protocol which discovered multiple disjoint routes from a source to destination. Among the discovered routes, the route with minimum cost index was selected by them, which was based on the node weight of all the in-network nodes from the source node to the destination node.

Venkatasubramanian and Gopalan (2009) have proposed QoS based robust multipath routing (QRMR) protocol for mobile ad hoc networks. Their protocol assigns weights to every link depending on the link quality, channel quality and end-to-end delay. Since the these weight values assists the process of routing, the

balanced traffic and enhanced network capacity is obtained. Then, the proportion of traffic to be routed to each neighbor is selected in such a way that node weight is minimum. The security issues are not considered in this approach.

Fard *et al.* (2011) have proposed an end-to-end threshold based algorithm that improves congestion control to address link failure loss in MANET. Their algorithm holds two phase. First, threshold-based loss classification algorithm distinguishes losses due to link failure by estimating queue usage based on Relative One-way Trip Time (ROTT). Second phase adjusts RTO for new route by comparing capabilities of new route to the broken route using available information in Transport layer such as ROTT and number of hops. The accuracy of loss classification algorithm should be enhanced to prevent misinterpreting losses only as link failure losses.

Yi *et al.* (2011) have proposed the Multipath Optimized Link State Routing (MP-OLSR) protocol. The multipath is obtained using multipath dijkstra algorithm. This algorithm gains great flexibility and extensibility by employing different link metrics and cost functions. Also they implement route recovery and loop detection in MP-OLSR to enhance quality of service. Their protocol improves the performance of the network especially in the scenarios with high mobility and heavy network load and also be compatible with OLSR. The end-to-end delay and jitter occurring during MP-OLSR for quality of service are more accurately required for significant multimedia services.

Liu and Liu (2010) have proposed a delay-aware multipath source routing (DMSR) protocol to offer end-to-end delay requirement in wireless ad hoc networks. Their protocol includes two parts. Firstly the accumulation delay is considered as the admission metric to choose the paths. Secondly the node delay is considered as the metric to measure the end-to-end delay and determine the best routing path. The metric takes into account the number of the neighbor nodes of the forwarding nodes, the channel busy time and the number of packets in the send buffer.

MATERIALS AND METHODS

Fault-Tolerant Congestion Aware Multi-Path Routing (FTCAMR) protocol: In the previous work (Rajkumar and Duraiswamy, 2011), a fault-tolerant multipath routing protocol have been designed to reduce packet loss due to route breakage. In this protocol, nodes determine multiple disjoint routes having more battery power and residual energy, to every active destination.

The battery power E^b is given by Eq. 1:

$$E = \sum_{i=1}^n B_i \quad (1)$$

E^{av} , the average energy of the nodes is given by Eq. 2:

$$E = \frac{\sum_{i=1}^n E_r}{n} \quad (2)$$

where, E_r is the residual energy of node i and n is the number of nodes along the path. Now the energy level of node E^{el} is given by Eq. 3:

$$E = \frac{E_r}{E^{av}} \quad (3)$$

The smaller the value of the battery power is, the better the path runs. Each RREQ is modified to include two additional fields, E^b and E^{av} to indicate the value of battery power and the average energy along a path.

In fault-tolerant mechanism, the received signal strength is measured and based on its value; it can send warning packets to the previous node.

The receiving node measures the signal strength received for free-space propagation model while receiving the RTS packet which is given by Eq. 4:

$$P_R = P_T (\eta / 4\pi d)^2 \theta_T \theta_R \quad (4)$$

Where:

η = Wavelength of the carrier

d = Distance between sender and receiver

θ_T and θ_R = Unity gain of transmitting and receiving omni directional antennas respectively

Congestion detection algorithm: The algorithm shown below states the proposed congestion detection and notification strategies. The congestion detection algorithm is buffer based. On reception of a data packet, each intermediate node monitors its current buffer size (C_{tBs}) and calculates a running average value (Avg_{Bs}) using exponential weighted moving average (EWMA) formula. If this average value becomes greater than a predefined threshold (Thr) then the congestion is detected. Here, w_t represents the weight factor given to the current size of the buffer. Once the congestion is detected, the intermediate node empties its buffer of all pending data packets in order to reduce the amount of backlogged packets. This also boosts up the forwarding of current data packet and it would be routed

with minimum delay. After then, the node sends a congestion notification packet towards to source. Before sending the current data packet to a designated next hop node, the congested node resets its EWMA variable.

Algorithm:

1. For the detection of congestion,
 - 1.1. $Avg_{Bs} = (1 - wt) * Avg_{Bs} + w * Ct_{Bs}$
 - 1.2. If ($Avg_{Bs} > Thr$)
 - 1.2.1. Congestion is detected
 - Else
 - 1.2.2. No congestion.
2. If Congestion is detected,
 - 2.1. Empty the buffer of all pending data packets,
 - 2.2. Send the Congestion packet to the source,
 - 2.3. Reset EWMA variable to zero value.
3. Send the data packet to downstream.

Congestion control: Whenever the source node receives the congestion control packet sent by the congested node, it executes the congestion control algorithm. At first, the source node stops the forwarding of packets over the active paths. Then it reduces the Packet Sending Rate (PSR) to the next higher rate. Before resuming the transmission of data packets at this new reduced rate, the source node sets a timer for the duration at which this new rate will be activated. If the source node does not receive any congested packet during this period, it will switch to the next higher PSR. If the link qualities of any of the active paths deteriorate, eventually the source node starts to load at the lowest possible rate over that path. In the event of further deterioration of that path quality, the source node will receive more congested packets but it has no option to decrease the PSR further. In this case, the source attempts to switch the congested path with the backup path if possible. Otherwise, the source has to reinitiate path discovery again.

Overall algorithm: Consider residual energy and battery power in paths selection and the energy balance in data transmission to maximize the lifetime of networks. Let S and D be the source and destination nodes.

Algorithm:

Consider the sample topology given in Fig. 1.



Fig. 1: Sample topology

1. Calculate battery power E_b using (1)
2. Compute the average energy of the nodes E_a using 2)
3. Calculate the Energy level of node E_{cl} using (3)
4. $RREQ_{modified} = (RREQ + (E_b + E_{av}))$
5. If S requires a route to destination, then
 - 5.1 Check routing table
 - 5.2 If Path is invalid, then
 - 5.2.1 S performs route discovery (with network-wide flood of RREQ)
 - End if
6. If node receives RREQ, then
 - 6.1 If RREQ is from D and RREQ has route to the D, then
 - 6.1.1. Stores the first received RREQ in buffer
 - 6.1.2. Starts the timer
 - Else
 - 6.2 Process proceeds as conventional AOMDV
 - End if
7. If Node receives other copies of RREQ, then
 - 7.1 If RREQ provides new disjoint path, then
 - 7.1.1 RREQ is stored in the buffer of the node.
 - Else
 - 7.1.2 Dropped.
 - End if
 - 7.2 If timer expires, then
 - 7.2.1 Node drops all copies of RREQ
 - End if
 - 7.3 If Battery power is minimum
 - 7.3.1 The destination node replies with k copies of RREQ in buffer
 - End if
 - End if
8. If intermediate node does not have valid route to destination, then
 - 8.1 forward fist received RREQ.
 - End if
9. If $E_{cl} > E_{th}$
 - 9.1 intermediate nodes forward the RREQ.
 - Else
 - 9.2 drop RREQ
10. Calculate received signal strength P_R using (4) and check for the congestion.
11. If congestion is detected,
 - 11.1. Source node stops the forwarding of packets through active paths
 - 11.2. Then it reduce the PSR to the next higher rate
 - 11.3. If source node does not receive any congested packet for particular time

11.3.1. It switched to the next higher rate

11.3.2. If the rate is reduced to the lowest,

11.3.2.1. Go for the possible back up path.

12. If $PR = T_{min}$

12.1 Node C is about to fail shortly

12.2 Node D informs node B about status of node C

12.3 B starts caching the data packets in its data buffer

End if

13. If $PR = T_{min}$,

13.1 Node C is completely failed

13.2 Node D informs node B about the status of node C

13.3 Node B salvages all packets that are still in its data cache through the established alternate path.

End if

RESULTS AND DISCUSSION

Simulation model and parameters: The NS2 Network Simulator is used to simulate our proposed protocol in our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs is used as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In this simulation, 50 mobile nodes move in a 1500 × 300 m rectangular region for 50 sec simulation time. It is assumed that each node moves independently with the same average speed. All nodes have the same transmission range of 250 m. In our simulation, the speed is set as 5 m sec. The simulated traffic is Constant Bit Rate (CBR). The pause time of the mobile node is varied as 0-40.

The simulation settings and parameters are summarized in Table 1.

Table 1: Simulation parameters

No. of nodes	50
Area size	1500×300
Mac	802.11
Radio range	250 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Mobility model	Random way point
Speed	5m sec
Pause time	0,10,20,30 and 40
Flows	2,4,6,8,10
Sending power	0.660
Receiving power	0.395
Idle power	0.035

Performance metrics: The FTCAMR protocol is compared with the Congestion Avoidance Routing Protocol (CARP) (Mbarushimana and Shahrabi, 2008) protocol. The performance is mainly evaluated 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 sent

Throughput: It is the number of packets received successfully.

Drop: It is the number of packets dropped.

Results:

Based on flow: In the first experiment the number of flows is varied as 2-10.

Figure 2 presents the packet delivery ratio of both the protocols. Since the packet drop is less and the throughput is more, FTCAMR achieves good delivery ratio, compared to CARP.

From Fig. 3, it can be seen that the average end-to-end delay of the proposed FTCAMR protocol is less when compared to the CARP protocol.

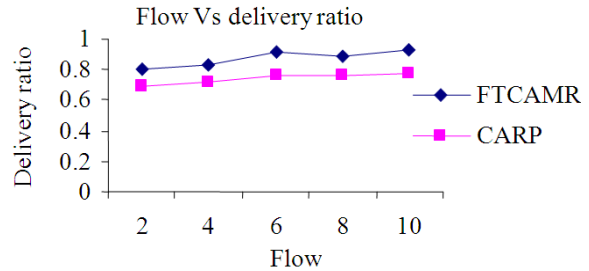


Fig. 2: Flow Vs delivery ratio

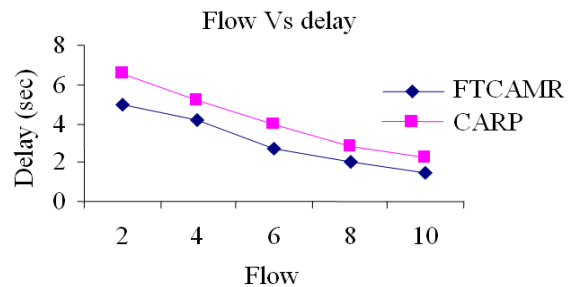


Fig. 3: Flow Vs delay

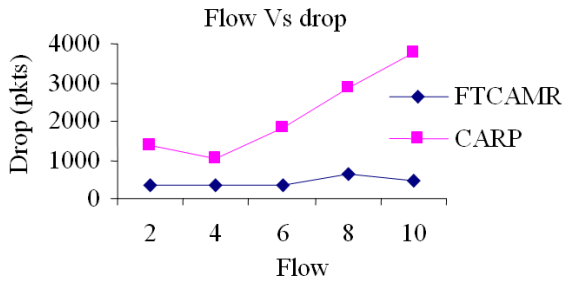


Fig. 4: Flow Vs drop

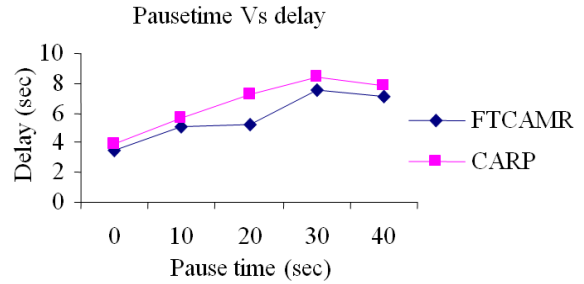


Fig. 7: Pausetime Vs delay

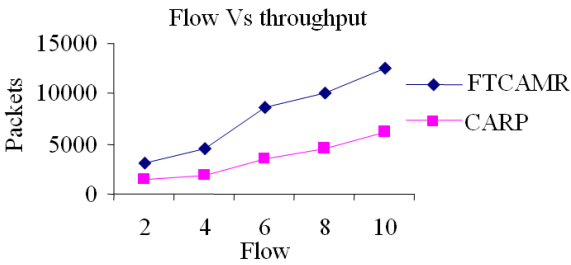


Fig. 5: Flow Vs throughput

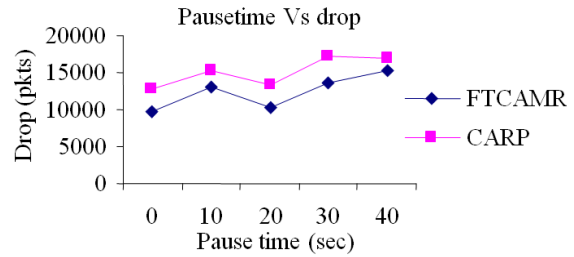


Fig. 8: Pausetime Vs drop

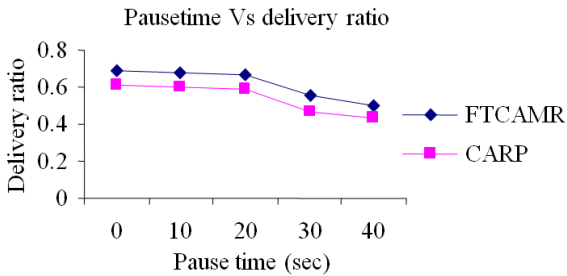


Fig. 6: Pausetime Vs delivery ratio

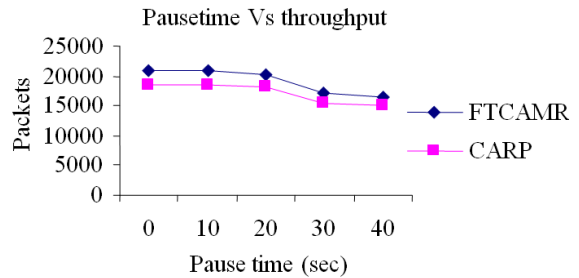


Fig. 9: Pausetime Vs throughput

From Fig. 4, it can be ensured that the packet drop is less for FTCAMR when compared to CARP.

Figure 5 gives the throughput of both the protocols when the pause time is increased. As it is seen from the figure, the throughput is more in the case of FTCAMR, than CARP.

Based on pause time: In the second experiment the Pause time is varied as 0-40.

Figure 6 presents the packet delivery ratio of both the protocols. Since the packet drop is less and the throughput is more, FTCAMR achieves good delivery ratio, compared to CARP.

From Fig. 7, it can be seen that the average end-to-end delay of the proposed FTCAMR protocol is less when compared to the CARP protocol.

From Fig. 8, it can be ensured that the packet drop is less for FTCAMR when compared to CARP.

Figure 9 gives the throughput of both the protocols when the pause time is increased. As it can be seen from the figure, the throughput is more in the case of FTCAMR, than CARP.

CONCLUSION

In this study, a congestion aware multi path routing protocol has been designed to reduce the congestion losses. In this protocol, a congestion control technique is followed which proactively detects node level and link level congestion and performs congestion control using the fault-tolerant multiple paths. The congestion detection algorithm is buffer based. On reception of a

data packet, each intermediate node monitors its current buffer size and calculates a running average value using exponential weighted moving average formula. If this average value becomes greater than a predefined threshold, then the congestion is detected. Whenever the source node receives the congestion control packet sent by the congested node, it executes the congestion control algorithm. The AOMDV protocol is used as a base for the multipath routing. This proposed scheme enables more nodes to salvage a dropped packet, (i.e.) packet salvaging is distributed. From simulation results it is shown that the proposed protocol achieves better throughput and packet delivery ratio with reduced delay, packet drop and energy.

REFERENCES

- Akhter, A. and T. Sanguankotchakorn, 2010. Modified AODV for multi-constrained qos routing and performance optimization in MANET. Proceedings of the International Conference on Electrical Engineering/Electronics Computer Telecommunications and Information Technology, May 19-21, IEEE Xplore Press, Chaing Mai, pp: 234-238.
- Chakravarthi, R., C. Gomathy, S.K. Sebastian, K. Pushparaj and V.B. Mon, 2010. A survey on congestion control in wireless sensor networks. *Int. J. Comput. Sci. Commun.*, 1: 161-164.
- Fard, M.A.K., S. Karamizadeh and M. Aflaki, 2011. Enhancing congestion control to address link failure loss over mobile ad-hoc network. *Int. J. Comput. Netw. Commun.*
- Khazaei, M. and R. Berangi, 2009. A multi-path routing protocol with fault tolerance in mobile ad hoc networks. Proceedings of the 14th International CSI Computer Conference, Oct. 20-21, IEEE Xplore Press, Tehran, pp: 77-82. DOI: 10.1109/CSICC.2009.5349359
- Liu, S. and J. Liu, 2010. Delay-aware multipath source routing protocol to providing QoS support for wireless ad hoc networks. Proceedings of the 12th IEEE International Conference on Communication Technology (ICCT), Nov. 11-14, IEEE Xplore Press, Nanjing, pp: 1340-1343. DOI: 10.1109/ICCT.2010.5689050
- Lakshmi, G.V. and C.S. Bindhu, 2011. Congestion Control avoidance in ad hoc network using queueing model. *Int. J. Comput. Technol. Appl.*, 2: 750-760.
- Manjre, B.M. and V.A. Gulhane, 2011. Secure and reliable ad-hoc on demand multipath distance vector routing protocol for mobile ad hoc networks. Proceedings of the 2011 International Conference on Information and Network Technology, (IPCSIT' 11), IACSIT Press, Singapore, pp: 79-83.
- Mbarushimana, C. and A. Shahrabi, 2008. Congestion avoidance routing protocol for QoS-Aware MANETs. Proceedings of the International Wireless Communications and Mobile Computing Conference, Aug. 6-8, IEEE Xplore Press, Crete Island, pp: 129-134. DOI: 10.1109/IWCMC.2008.23
- Narasimhan, B. and S.S. Baboo, 2009. A hop-by-hop congestion-aware routing protocol for heterogeneous mobile ad-hoc networks. *Int. J. Comp. Sci. Inform. Security.*
- Rajkumar, G. and K. Duraiswamy, 2011. A fault tolerant multipath routing protocol to reduce route failures in mobile adhoc networks. *Eur. J. Sci. Res.*, 50: 394-404.
- Saxena, S. and M. Sinha, 2011. A study of Adaptive Replication Technique in routing time-constrained messages (VoIP) in MANET. *Int. J. Comput. Sci. Eng.*, 3: 2273-2285.
- Valarmathi, A. and R.M. Chandrasekaran, 2010. Congestion aware and adaptive dynamic source routing algorithm with load-balancing in MANETs. *Int. J. Comput. Appl.*, 8: 1-4.
- Venkatasubramanian, S. and N.P. Gopalan, 2009. A QoS-based robust multipath routing protocol for mobile adhoc networks. *IACSIT Int. J. Eng. Technol.*, 1: 391-396.
- Yi, J., A. Adnane, S. David and B. Parrein, 2011. Multipath optimized link state routing for mobile ad hoc networks. *J. Ad Hoc Netw.*, 9: 28-47. DOI: 10.1016/j.adhoc.2010.04.007