

# OCC: Ordered congestion control with cross layer support in Manet routing

T.Suryaprakash Reddy

Professor

Department of CSE

Krishna Chaitanya Institute of Technology & Sciences  
Markapuram,Prakasam(dist),A.P,INDIA.

Dr.P.Chenna Reddy

Associate Professor and HOD

Department of CSE

JNTU College of Engineering  
Pulivendula,Kadapa(dist),A.P,INDIA

**Abstract**—In the recent times many accessible congestion control procedures have no capability to differentiate involving two major problems like packet loss by link crash and packet loss by congestion. Consequently these resolutions effect in form of wastage of possessions because they target only on the packet drop by link crash that has a needless importance. Consumption of energy and possessions in order to make the basis node attentive regarding the congestion occurring in routing path is the supplementary drawback in most of the accessible procedures. This way of concentrating mainly on standardizing the outlet load at the basis node stage is the boundary to the present accessible procedures. It is already known that as a reason of link crash and congestion packet loss in the network routing largely occurs. In this article a new cross layer and path restoration procedure has been put forward. We also put forwarded two algorithms namely Path discovery Algorithm and congestion handling algorithm. In this approach of cross layer it comprises of 3 kinds of layers called network, MAC and transport layers. In this introduced approach the MAC and network layers have dynamic functionalities in identifying the congestion and standardization where the functionalities of network and transport layers are distinguished in bearing the congestion i.e. congestion endurance. The produced tentative results illustrate an enhanced management of congestion and its endurance by this approach.

**Keywords**- manet; routing protocol; congestion control; zone; occ; cross layer.

## I. INTRODUCTION

MANETs are recognized for their influence on protocols and protocol stacks of managing methods and they are naturally unsuited for customary TCP [17]. As a result ordinary TCP congestion management that is applies for the internet is not apposite method. In MANETs the nodes move fundamentally through a different means that is not known which generally is an effect of communal wireless multi hop channel and it does not get interpreted as the congestion is vanished. As a result the packet delivery delay and crash takes place. “An individual node can be transferred in its intrusion series” is the principal policy of the wireless multi hop channel. Coming to the MANETs network the whole region in the medium is packed and congested as it is common region, but coming to the internet the crowd is on main Pathr [17]. The significant character of the MANETs is that the region may be packed full but not the nodes [17].

The contrast between ordinary TCP and MANETs is due to verity that crash and losing of packets is constantly not due to the congestion in the network and the transfer periods (along with round trip periods) diversify creating complexity in identifying the lost packets. Distinct consumer is able to turn out a congestion ensuing in relatively lesser bandwidth of mobile ad-hoc networks, due to which it is complicated origin of congestion in a multi hop network. A reasonable congestion control scheme should be in use effectively to be firm and for greater functionality [17] of the wireless system as a reason of vulnerability towards congestion troubles in contrast with conventional wire line systems.

The multi-hop wireless networks are unable to attain a distinct and integrated procedure for the trouble in the congestion as they are heterogeneous character of function protocols. As an alternative an appropriate model of congestion control should be intended that mainly concentrates on the characteristics that are associated with the network [17]. Eventually these schemes serve as division of the procedures for the troubles that are recognized instead of an absolute immediately utilized method. They create themselves as the head of the customized application protocol stacks. But there are only fewer characters that work with a huge series of functions [17] and these are rare cases.

Congestion managing techniques focused mainly on the modeling, analysis, algorithm improvement of clogged loop control formats (e.g. TCP) have been observed in the latest times preparing them to get customized to the mobile hoc networks by stipulating constraints concerned to routing path and bandwidth algorithms that hold the capability to unite and improve functions are developed. There is one more chief part that should be taken into the view in the field of wireless hoc network is by reason of the MAC [Media access Control] layer [17]. That condition is that maximum wireless MACs consist a time restraint which allows the customer to utilize the physical medium but in the provided time period.

This article is structured in the method as given: The section II looks at the mainly quoted works in the field of literature. The conversations of the projected procedures are featured in section III and section IV exposes the replications and the corresponding outputs that are tagged by end conclusion and references.

## II. RELATED WORK

The mechanism for QOS centric congestion management is present in [1]. Et al, [2] initiated metrics to evaluate data-rate, MAC overhead along with buffer interruption, that assists in recognizing and manage the congestion conflicted region in network system. Hongqiang Zhai, et al, [3] put forwarded a procedure opposing that congestion and strict means conflict is interconnected. Metrics based solution on congestion aware routing was introduced in [4]. Hop stage congestion managing design was projected by Yung Yi et al, [4]. Tom Goff, Nael et al, [5] conferred a group of algorithms that instigates substitute pathways utilization in case of uncertainty in the value of a pathway that is being utilized. Xuyang et al, [6] obtained a cross-layer hop-by-hop congestion control method which was modeled for the TCP functioning in multi-hop wireless networks. Dzmityr et al [7] introduces the crash congestion at the transport layer which minimizes the functioning of the system. Duc et al [8] has discovered that the models that exist in present days cannot be adjustable for the congestion.

Discovering the congestion clearance in routing pathway is the main goal of present day methodologies. The packet crash is the cause for the link collapse. The efficient way is to work on the method to manage the packet losing which is the reason for the link collapse. Standardizing the way out near every node involving in routing is one more costly methodology. The management of congestion is near hop stage [4] [15] in most of the situations. As a result the standardizing way out method at every node in the network includes the usage of the costly possessions. This article shows the effectiveness in discovering the crash of the packets which are recurring as a reason of conflict or by buffer filled up or by malevolent fail. So the method of managing the congestion through standardizing the way out can be evaded in the conditions like the link collapse and in bitter situations this is handled by using substitute pathway restitution. We can also urge that a situation may arise where the hop stages cannot standardize themselves for which only hop stage congestion management is not enough. The way of managing the outlet force that is being followed in origin stage standardization design, can also be followed as well in the management of the congestion by using the similar possessions.

In this article introduction to a new cross layer congestion control design has been made which involves:

- The node capability and possession's heterogeneity.
- Congestion related packet crash being confirmed by cross layer design.

## III. OCC: ORDERED CONGESTION CONTROL USING CROSS LAYER SUPPORT IN MANET ROUTING

We know that in MANETs crashing of the packets happen frequently. The main causes for this to happen are as follows:

- Link collapse during transfer.
- Minimizing the packet entrance power by utilizing conditional Transfer with overwhelmed Ingress. This is also named as packet sinking because of congestion near routing.

- Medium usability conflict.
- Malevolent sinking near the recipient.

A concise explanation on introduced OCC is as given: The congestion control methodology that was put forward is attained in stratified way.

In our methodology, at first reduce channel current near the pathway node  $pn_p$  antecedent to pathway node  $pn_c$  that is affected by congestion. This step is voluntary and probable delay threshold at  $pn_p$  and functional part of buffer capability. If there is any situation of error or crash in the functioning of the primary step, then automatically this gives rise to the functioning of the secondary step of the methodology. Coming to the secondary step the MAC layer makes the adjacent nodes  $pn_p$  attentive that are also present in that particular region. As a result the outcome of all the other adjacent nodes  $pn_p$  will be reduced at a time, so that there will be no delay in the group of threshold value.

Even if the affected node has not improved after the commencement of the first steps of the methodology then the thirds step gets instigated. The procedure in this step is that the MAC checks the inward rush of the nodes I near the particular pathway  $pn_p$  in a given period of the time span  $\tau$ , then the nodes that are present in that particular zone  $C_c$  of the routing path will be intimated about the affected node  $pn_v$  by the MAC. Now all the rest of the nodes reduce their outward rush in order to make the delay of the threshold group gets decreased. When the MAC checks the inward rush of the nodes I near the particular pathway  $pn_p$  in a given period of the time span  $\tau$ , if  $I' \geq I$  and the affected node is not improved then the pathway is re-established by making a link among the nodes  $pn_p$  and  $rpnc$ , where  $rpnc$  is the pathway node that is held back, which is a consideration node for  $pn_c$ . As a result the routing information avoids the affected node  $pn_v$ , that is  $pn_c$ .

### A. Dividing the network in to zones

Mohammad M. Qabajeh et al [8] explained a methodology, which was chose by us. By understanding the already present nodes, the total area is separated into divisions. In general the outline of the zone is preferred as hexagon. By considering the hexagon the benefit is that the outline touches the larger area and along with it the correspondence with adjacent nodes is also easier as the outline is similar to that of the transmitter. The point-based is applicable in the MANETs due to the accessibility of reasonably cheap and portable less consumable GPS receiver. The series of the transfer for the node is represented using R and the length of the hexagon by using L. For the correspondence of the zones amongst them a relation between R and L is generated as  $L=R/2$ .

All the zones have their identification as ( $cid$ ). The zones are provided with couple of alternative units. They are:

1) If a node is involved in the routing and its zone is present in the routing path, if that node has entered into the given series region then that from then is referred as pathway node.

2) If the node  $rp_n$  of the pathway node  $pn$  is recognized as the substitute node for the node  $pn$  by the transport layer then that node is named as the reversed pathway node.

If the placement of the node is found, that is at which point it is present then, nodes can execute our self-mapping algorithm of the substantial site on present zone and compute the  $cid$  with no trouble. Figure 1.shows the Common outline of the Zone divisions in network.

Pathway nodes and their respective reserved pathway nodes are present for every zone.

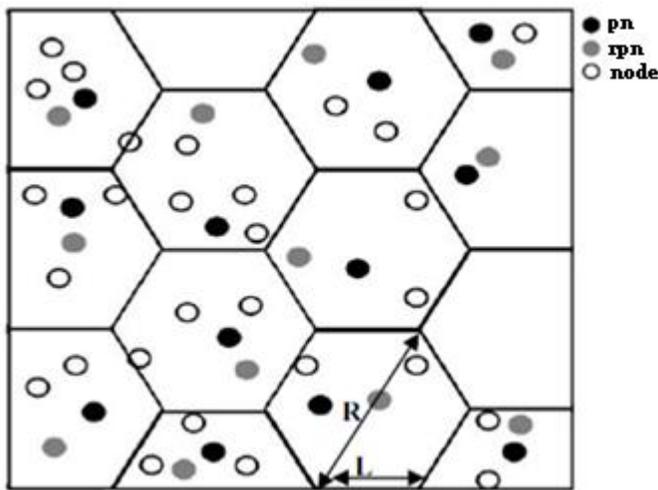


Figure 1. Common outline of the Zone divisions in network[8]

### B. Path Detection

This practical methodology is termed as DSR policy for Path detection. A distributed technique is utilized in order to determine the path to the end node  $n_d$  by the source node  $n_s$ . The appealed packet  $rreq$  that is being transmitted will take the node related data like the involvement in the routing path and its id value  $cid$  of that node that is communicating. While the packets are transferring the, transport layer checks the zone stage nodes of every node that is communicating and holds the data with the packet  $rreq$ . After the final end node gets this packet  $rreq$  from the origin then it gets ready to send the reply packet  $rrep$  which includes the record of all the pathway nodes and their communicating nodes in the area of the zone. At the time when the reply packet is acknowledged than all the communicating nodes make the necessary changes in their routing table and revise it with the antecedent and descendant node data. It also revises with the other communicating nodes of that particular node and its descendant node in the pathway of the pathway.

When the reply packet  $rrep$  finally reaches the origin node  $n_s$ , then the most desired path will be chosen. Then the origin node  $n_s$  delivers an acknowledgement  $ack(pn)_i$  for every path node for the routing desired path. After the acknowledgement packet  $ack(pn)_i$  is delivered then ahead the pathway node  $pn_i$  determines the desirable paths among the node  $pn_i$  and the both hop stage descendant node  $pn_{i+2}$ . In this step the main path node  $pn_i$  delivers an appeal  $rreq$  to  $pn_{i+2}$ . This appeal  $rreq$  communicates by using only the communicating nodes of the main node  $pn_i$  and the node  $pn_{i+1}$ . When this appeal is delivered to  $pn_i$ , then  $pn_{i+2}$  acknowledges it by using the packet  $rrep$  and transfers it to the  $pn_i$  on the same path that used by the  $rreq$ . When the acknowledgement  $rrep$  is delivered then  $pn_i$  chooses the desired path among the nodes  $pn_i$  and  $pn_{i+2}$ , lastly accumulating it into the routing tables. The desired path that was chosen is utilized for the re-establishment among the nodes  $pn_i$  and  $pn_{i+2}$ , on the basis of a condition that the congestion is obvious at the adjacent descendant node  $pn_{i+1}$  of the main node  $pn_i$ .

### Path detection algorithm

1.  $n_s$  Creates  $rreq$  and transmit it to adjacent units.
2. When  $rreq_i$  is delivered, hop stage node  $n_i$  confirms that whether retransmitting of  $rreq_i$  is previously completed on their own or not.
3. If retransmitting is previously completed then rejects the  $rreq_i$ , or else  $n_i$  gathers the particulars of communicating nodes from transport layer and along with that it includes its own recognition and particulars of its communicating nodes to  $rreq_i$ , then retransmits. This procedure continues until  $rreq$  is delivered to the end node  $n_d$ .
4. Then end node  $n_d$  creates acknowledgement packet  $rrep_i$  that includes the particulars of the nodes that are present in the pathway. By utilizing this acknowledgement  $rreq_i$  navigated to arrive at  $n_d$  and it's communicating nodes. The acknowledgement

packet  $rrep_i$  transfers in reverse to the origin node  $n_s$  on the same desired path of the packet  $rreq_i$ .

5. Every transitional node  $pn_i$  in the path which utilized the packet  $rrep_i$  gathers the particulars of its antecedent node  $pn_{i-1}$  in pathway, descendant node  $pn_{i+1}$  and communicating nodes of main path node  $pn_i$  and descendant path node  $pn_{i+1}$
6. Main path node  $pn_i$  revises its routing table by the particulars attained in earlier step.
7. The methods 6 and 7 frequently continue until acknowledgement packet is delivered to origin node  $n_s$
8. Origin node  $n_s$  derives the desired path which includes zones with crowded nodes.
9. For every pathway node 1 to n of the path chosen,  $n_s$  replies  $ack(pn)_i$  for  $i = 1..n$ .
10. On gaining the  $ack(pn)_i$ ,  $pn_i$  begins deriving the substitute path among  $pn_i$  and  $pn_{i+2}$ , so that the substitute path can utilize communicating nodes of the  $pn_i$  with  $pn_{i+1}$  merely.
11.  $pn_i$  then records substitute path among the nodes  $pn_i$  and  $pn_{i+2}$  at routing collection.

### C. Managing Congestion

When the packet is crashed and that is determined that it is crashed at the node  $pn_i$  then MAC layer checks the conflict position near  $pn_i$ , if that point is found then it makes the antecedent node  $pn_{i-1}$  of main node  $pn_i$  aware regarding the need of the retransferring in the given span  $\tau$  as conflict alert  $con_+$ . If the span id maximizing the delay near  $pn_{i-1}$  so that the packet is crashing at the node  $pn_{i-1}$  and its values is higher than the tolerable threshold value, then the node depends on the substitute path among the nodes  $pn_{i-1}$  and  $pn_{i+1}$  which is present in the routing collection. This substitute path will be on use until the MAC layer sends the acknowledgement  $con_-$  of conflict removed at the main path node  $pn_i$  by the node  $pn_{i-1}$ . When the node  $pn_{i-1}$  receives the acknowledgement  $mac_-$  sent by the MAC layer then it returns the path back to the  $pn_{i+1}$ . The MAC layer again validates and if it derives that the congestion is not because of the conflict then MAC checks the buffer during the inward rush at the main node and if it is full

then delivers  $bof_+$  regarding the crowd in the buffer. When the node  $pn_{i-1}$  takes delivery of  $bof_+$ , then it tries to reduce the inward rush so that the delay that is incrementing may not make the packet get crashed at the main node  $pn_{i-1}$ . If this process fails to reduce the inward rush at the node  $pn_{i-1}$ , then the network layer makes the all the remaining nodes of the zone  $C_c$  in which the node  $pn_{i-1}$  is present aware, so that the rest will reduce their inward rush because of which the increment in the delay may not make the packet get crashed near their own man nodes. Even if this case fails than the network layer makes the descendant zone of the present zone  $C_c$  aware of this situation. This procedure will be continued frequently until the congestion that is caused due to the rush in the buffer gets prohibited or it is delivered to the zone  $C_s$  in which origin node  $n_s$  is present. If the result is failed to come then in order to continue the information transfer among the nodes  $pn_{i-1}$  and  $pn_{i+1}$ , that was troubled because of the congestion bear the main node  $pn_i$ , the node  $pn_{i-1}$  depends on the substitute path that is accessible in the routing collection. If the MAC determines that the congestion is occurred due to the link collapse among the node  $n_i$  and its descendant  $n_{i+1}$  then the main node  $pn_i$  chooses the substitute path in order bond up with the  $pn_{i+2}$  that is stored in the routing collection of the main node  $pn_i$ .

### Algorithm for congestion management and working information transport in opposition to congestion

1. Let us assume a case of packet crashing at  $pn_i$
2. MAC checks the position of the conflict:
3. If congestion arouse because of conflict near  $pn_i$ 
  - a. then MAC recognizes the conflict near  $pn_i$  and make  $pn_{i-1}$  aware by sending a information in  $con_+$ ,
  - b. then  $pn_{i-1}$  functions on the congestion caused by the conflict: move to step 6.
4. else if congestion is caused because of the rush in buffer near  $pn_i$ 
  - a. then MAC recognizes the rush in buffer near  $pn_i$  and make  $pn_{i-1}$  aware by sending a information in  $bof_+$
  - b. then  $pn_{i-1}$  functions on the congestion caused by the rush in buffer: move to step 7
5. else if congestion is caused because of the link

collapse among  $pn_i$  and  $pn_{i+1}$  near  $pn_i$

- a. then MAC recognizes the link collapse among  $pn_i$  and  $pn_{i+1}$ , and make aware by sending a link collapse information in  $LF_+$ .
- b. then path node  $pn_i$  functions on the congestion caused by the link collapse: move to step 8

#### 6. Managing Congestion caused by conflict:

- i. When  $con_+$  is taken the delivery from MAC, path node  $pn_{i-1}$  functions
  - a. Evaluate the  $con_+$ , that includes a particulars regarding whether retransfer is needed and span  $\tau$  for retransfer.
  - b. Checks the weight of the  $\tau$  on inward rush delay time  $\Delta$ 
    - i. If  $\Delta \geq \delta$  (inward rush delay threshold) [consequences are packet termination because of surpassed delay] For span  $\tau$ , choosing to substitute path among path node  $pn_{i-1}$  and  $pn_{i+1}$  to avoid the affected node  $pn_i$ , which was caused by congestion by conflict.
    - ii. Past the span  $\tau$  path node  $pn_{i-1}$  is taken the delivery of either  $con_+$  or  $con_-$  from MAC. MAC delivers  $mac_+$  if conflict is still id present in the affected node  $pn_i$  else intimates to  $pn_{i-1}$  regarding the situation of no conflict at affected node  $pn_i$  through  $con_-$ .
    - iii. If  $con_+$  is delivered from MAC then  $pn_{i-1}$  executes steps 1 and 2.
    - iv. else if  $con_-$  is taken delivery by  $pn_{i-1}$  then it re-establishes the original path among  $pn_{i-1}$  and  $pn_{i+1}$

#### 7. Managing Congestion caused by the rush in the Buffer

- v. When  $bof_+$  is taken the delivery from MAC, path node  $pn_{i-1}$  functions  
Evaluate the  $bof_+$ , that includes a particulars regarding congestion because of rush in the buffer near  $pn_i$ .
- vi. Executes the procedure of inward rush reducing so that delay  $\Delta$  does not cross delay threshold  $\delta$  limit.
- vii. If inward rush not reasonable as needed to manage the congestion near  $pn_i$  then

- a. Network layer makes every path node that is located in the similar zone  $c_c$  to which  $pn_{i-1}$  is part of, aware regarding congestion position near  $pn_i$ .
  - b. As a result every path node of zone  $c_c$  tries to reduce their inward rush so that that delay  $\Delta$  does not cross delay threshold  $\delta$  limit of individual path nodes.
- viii. If inward rush near individual nodes not reasonable as needed to manage the congestion near  $pn_i$  then
- a. Network layer makes path nodes in the zone  $c_p$  aware, that is antecedent to the  $c_c$ .
  - b. As a result every path node of zone  $c_c$  tries to reduce their inward rush so that that delay  $\Delta$  does not cross delay threshold  $\delta$  limit of individual path nodes.
  - c. If  $n_s \notin c_p$  then  $c_p \rightarrow c_c$ : move to step viii.
  - d. Else if inward rush at individual not reasonable as needed to manage the congestion near  $pn_i$  then  $pn_{i-1}$  chooses the substitute path that bonds  $pn_{n-1}$  and  $pn_{n+1}$  to make the information transport, which avoids the congestion affected node  $pn_i$ .

#### 8. Managing congestion caused by link collapse

- ix. When  $LF_+$  is taken the delivery from MAC then path node  $pn_i$  chooses the substitute path  $alp$  that bonds  $n_i$  and  $n_{i+2}$  to make the information transport.  
In view of the fact that the  $alp$  is being utilized the path node  $pn_i$  tries to derive a desired path among  $pn_i$  and  $pn_{i+2}$  and this substitute path gets constructed by considering communicating nodes of  $pn_i$  and  $pn_{i+1}$ .

#### IV. SIMULATIONS AND RESULTS DISCUSSION

The tool that was utilized in accomplishing the test was NS 2. Considering the mobility and amount ranging from 20 to 200, a simulation network simulation network has been constructed. The attributes and the values of the simulation are explained in the below table 1. If the packet that was sent is legal then it confirms that buffer is assigned successfully. The main goal of this model is to contrast the congestion and contention control protocol [18] and OCC. The functionality test for the two protocols by using the metrics given as follows:

TABLE I. SIMULATION ATTRIBUTES TAKEN FOR THE TEST

Amount of nodes Range	50 to 200
Dimensions of space	1500 m × 300 m
Nominal radio range	250 m
Source-destination pairs	20
Source data pattern (each)	4 packets/second
Application data payload size	512 bytes/packet
Total application data load range	128 to 512 kbps
Raw physical link bandwidth	2 Mbps
Initial PATH REQUEST timeout	2 seconds
Maximum PATH REQUEST timeout	40 seconds
Cache size	32 Paths
Cache replacement policy	FIFO
Hash length	80 bits
certificate life time	2 sec

There are few metrics in order to examine the working of the approached methodology. They are as follows:

- **DATA PACKET DELIVERY RATIO:** The ratio is derived by computing the division between the amount of information packets delivered from source and the amount of the information packets acknowledged by sink.
- **PACKET DELIVERY FRACTION:** The ratio between the information packets that are carried to target area and the packets that were produced from the origin. This paper gives the information on the working of the methodology showing the effectiveness in carrying the packets to the target. As the rate of working increases it produces the more accurate outputs.
- **AVERAGE END TO END DELAY:** This is defined as the common peer and peer delay of the information packets. Some of the reasons for this problem are loading at the time of path identification, LIFO near the interface queue, resending delays storing at the MAC and transport period. By this the differentiation of the time periods when the packet was sent and reached is determined. After this time period is derived, separating the whole time period differentiated value on the overall amount of CBR packets reached delivers the end-to-end delay for the packets that were reached. As the delay decreases the functioning, the working of the methodology is enhanced when the delay period is less.
- **PACKET LOSS:** This ratio is derived by subtracting the amount of packets that were delivered at the origin and the amount that reached to the sink. There were failure packets in the output received by us at Network and the MAC layers. This method sends the packet to the target until the path is derived, or else it searches unless a path is figured out. There are also situations when the buffer leaves the packet, couple of them are: Packet is ready for the search of the path, but the buffer is not empty. The second one is the search of the path crossed the time limit. From this, it is derived that as much less is the loosing of the packets, more will be the functioning of the approach.
- **ROUTING OVERHEAD:** This is termed as the ratio of overall amount of the routing packets and the

information packets. This ratio is determined at the MAC layer.

Figure 2(a) illustrates Packet Delivery Ratio (PDR) for Congestion and Contention Control Protocol [18] and OCC. By considering this output it is enough to prove that OCC manages maximum failure of PDR than that of [18] in case of DSR. Fairly accurate failure amount of PDR that is restored by the OCC than [18] is 1.5%.

This is balanced amount among the pauses. The least amount of restoring examined is 0.18% and the highest id 2.5%. The next Figure 3(b) specifies OCC benefit than that of [18] in case of Path optimality. [18] utilized nearly 0.019 hops more when compared to OCC as the reason of dual distribution of the [18].

The derivation for the packet delivery fraction (PDF) is:

$$P' = \sum_{f=1}^e \frac{R_f}{N_f}$$

$$P = \frac{1}{c} * P'$$

- $P$  is the division of effectively reached packets,
- $c$  is the overall amount of flow or associations,
- $f$  is the distinctive flow id allocated as index,
- $R_f$  is the amount of packets acknowledged from flow  $f$
- $N_f$  is the amount of packets transferred to flow  $f$

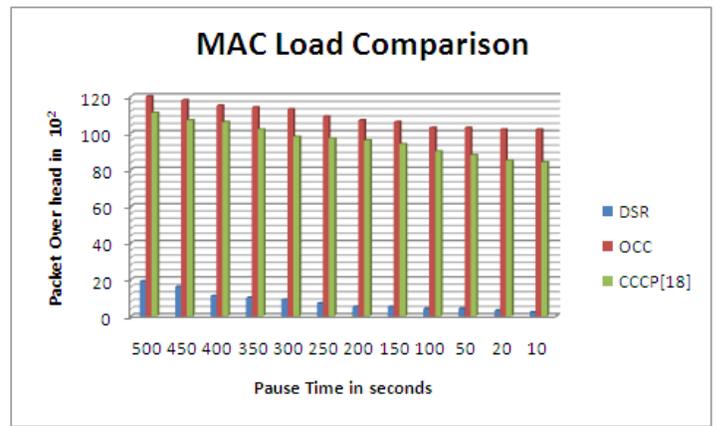
Figure 2(c) proves that OCC is has less packets than that of [18]. This benefit of the NCTS could be feasible as a reason of availability of constant paths without negotiation or offended nodes and having cross-layer congestion control and effective routing procedure. The Packet transparency derived in [18] is nearly 5.29% larger than packet transparency derived in OCC. The least and highest packet transparency in [18] than OCC derived is 3.61% and 7.29% correspondingly.

MAC load transparency is high in OCC than [18] to some extent. This is viewed in figure 2(d). This is occurred due to the control packet swap in OCC. The common MAC load transparency in OCC than [18] 1.64%. The least and highest MAC load transparency derived is 0.81 and 3.24% correspondingly.

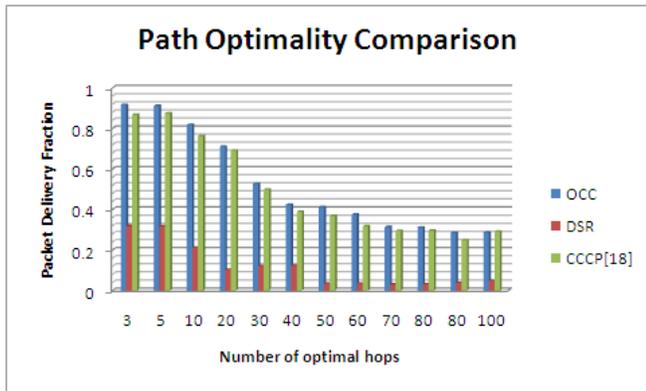
Appealing outputs have been determined for DSR when all the assessment procedures are considered. Apart from path optimality DSR executed fine as a result of not taking security concern into account as a routing attribute, and it is producing enhanced QOS without risk in routing hypothesis. But factually it is false in actual. In path optimality verification DSR place at end as a reason of not taking security restraints into account, amongst three measured procedures, eventually this made to recognize uneven paths.



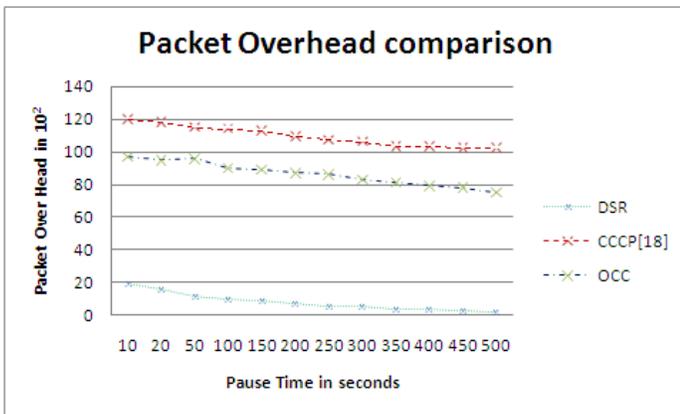
(a) Packet delivery ratio assessment utilizing line chart



(d) Mac load assessment illustrated in bar chart layout



(b) Bar chart illustration for Path optimality



(c) A line chart illustration of Packet transparency assessment details

Figure 2. Assessment details for OCC functioning than CCCP [18]

### V. CONCLUSION

This article talked about the routing algorithm named as “Stratified cross layer congestion control and endurance routing protocol”. This proposed procedure derivate two algorithms for Path discovery and congestion management correspondingly. Conventional proactive routing protocol DSR is utilized to derivate Path discovery algorithm. The congestion managing procedure has been separated into three units. Primary one manages the congestion occurred because of the conflicts, secondary unit is to manage the congestion occurring because of rush in the buffer and the final unit is to manage the congestion because of link collapse.

In the type of the congestion because of the rush in the buffer, our procedure manages it near the antecedent path node stage and error in this situation solves it by considering first to the zone stage and next to the network stage. This chronological procedure reduces the effort and cost for the consumption. The path recovering at the node stage that was chosen in managing the congestion facilitated the possibility of information transport opposing the rigorous congestion caused because of conflict and link collapse.

The experimental outputs that were obtained were efficient and noteworthy, such that we can widen the boundaries of the application in reducing the delay and improving the cross layer mechanism for effortless competence in the future course of time.

REFERENCES

- [1] [1] Michael Gerharz, Christian de Waal, and Matthias Frank, "A Practical View on Quality-of-Service Support in Wireless Ad Hoc Networks", BMBF
- [2] Xiaoqin Chen, Haley M. Jones, A .D .S. Jayalath, "Congestion-Aware Routing Protocol for Mobile Ad Hoc Networks", IEEE, 2007
- [3] Hongqiang Zhai, Xiang Chen, and Yuguang Fang, "Improving Transport Layer Performance in Multihop Ad Hoc Networks by Exploiting MAC Layer Information", IEEE, 2007
- [4] Yung Yi, and Sanjay Shakkottai, "Hop-by-Hop Congestion Control Over a Wireless Multi-Hop Network", IEEE, 2007
- [5] Tom Goff, Nael B. Abu-Ghazaleh, Dhananjay S. Phatak and Ridvan Kahvecioglu, "Preemptive Routing in Ad Hoc Networks", ACM, 2001
- [6] Xuyang Wang and Dmitri Perkins, "Cross-layer Hop-by-hop Congestion Control in Mobile Ad Hoc Networks", IEEE, 2008
- [7] Dzmityr Kliazovich, Fabrizio Granelli, "Cross-layer Congestion Control in Ad hoc Wireless Networks," Elsevier, 2005
- [8] Duc A. Tran and Harish Raghavendra, "Congestion Adaptive Routing in Mobile Ad Hoc Networks", 2006
- [9] Nishant Gupta, Samir R. Das. Energy-Aware On-Demand Routing for Mobile Ad Hoc Networks, OPNET Technologies, Inc. 7255 Woodmont Avenue Bethesda, MD 20814 U.S.A., Computer Science Department SUNY at Stony Brook Stony Brook, NY 11794-4400 U.S.A.
- [10] Laura, Energy Consumption Model for performance analysis of routing protocols in MANET, Journal of mobile networks and application 2000.
- [11] LIXin MIAO Jian –song, A new traffic allocation algorithm in AD hoc networks, "The Journal of ChinaUniversity of Post and Telecommunication", Volume 13. Issue3. September 2006.
- [12] Chun-Yuan Chiu; Wu, E.H.-K.; Gen-Huey Chen; "A Reliable and Efficient MAC Layer Broadcast Protocol for Mobile Ad Hoc Networks," Vehicular Technology, IEEE Transactions on , vol.56, no.4, pp.2296-2305, July 2007
- [13] Giovanidis, A. Stanczak, S., Fraunhofer Inst. for Telecommun., Heinrich Hertz Inst., Berlin, Germany This paper appears in: 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009
- [14] Outay, F.; Vèque, V.; Bouallègue, R.; Inst. of Fundamental Electron., Univ. Paris-Sud 11, Orsay, France This paper appears in: 2010 IEEE 29th International Performance Computing and Communications Conference (IPCCC)
- [15] [Yingqun Yu; Giannakis, G.B.; , "Cross-layer congestion and contention control for wireless ad hoc networks," Wireless Communications, IEEE Transactions on , vol.7, no.1, pp.37-42, Jan. 2008
- [16] <http://www-lih.univ-lehavre.fr/~hogie/madhoc/>
- [17] Prof.K.Srinivas and Prof.A.A.Chari. Article: Cross Layer Congestion Control in MANETs and Current State of Art. International Journal of Computer Applications 29(6):28-35, September 2011. Published by Foundation of Computer Science, New York, USA
- [18] Yingqun Yu; Giannakis, G.B.; , "Cross-layer congestion and contention control for wireless ad hoc networks," Wireless Communications, IEEE Transactions on , vol.7, no.1, pp.37-42, Jan. 2008 doi: 10.1109/TWC.2008.060514.