A REVIEW ON TCP CONGESTION CONTROL ALGORITHMS AND RECEIVER SIDE FEEDBACK SCHEMES OVER MANETS

Priya * , Kamal Gupta #

* Dept. of Computer Science and Engg.
GNIT, Mullana(Ambala), India .
Asst. Professor, Dept. of Computer Science and Engg.
GNIT, Mullana(Ambala), India

ABSTRACT

A Mobile Ad hoc Network (MANET) is a dynamic multi-hop wireless network that is established by a group of mobile stations without necessarily using pre-existing infrastructure or centralized administration. Traditionally, first-generation wireless networks were targeted primarily at voice and data communications occurring at low data rates. A mobile Ad hoc network is an autonomous system of mobile hosts which are free to move around randomly and organize themselves arbitrarily. *Ad hoc networks need to possess self-organizing characteristics, and they must perform routing and packet-forwarding functions. This paper* is focused on *transmission control protocol (TCP) is one of the most popular and widely used end-to-end protocols for the Internet today. As TCP was designed for wire d networks it considers that all packet loss in the network is due to congestion. Wireless medium is more exposed to transmission errors and sudden topological changes.*

Keyword : *- MANET, QoS, TCP.*

I. INTRODUCTION

Multiple access techniques are used to provide access to a large number of users within same bandwidth. Of all Wireless communications have become very pervasive. The number of mobile phones and wireless Internet users has increased significantly in recent years. The topology of an ad hoc wireless network is dynamically changing since devices are not tied down to specific locations over time. The fact that nodes are not static implies that centralized media access is not entirely applicable. Routing protocols in ad hoc networks need to deal with the mobility of nodes and constraints in power and bandwidth. Ad hoc devices rely on batteries to operate; hence, any inefficiency in communication protocols can drastically shorten the uptime of these devices. As the popularity of mobile devices and wireless networks significantly increased, wireless mobile networks has become popular and active field of communication and networks over the years. MANET is the new advance innovation which permits clients to communicate without any physical infrastructure regardless of their position, that's why it is sometime stated as an "infrastructure-less" network. A MANET comprises of various mobile nodes which are connected through wireless links and each movable node acts not only as a host but also as a router to establish a route. The route between the nodes in the network can communicate with several different paths. An ad-hoc network is a self-configuring and adaptive network. It allows the nodes/devices to maintain path by adding and removing the nodes to and from the network. Due to node mobility, the network topology changes rapidly. Due to the major characteristic of MANETs i.e. vigorous topology and lack of centralized management security, MANETs are vulnerable to attacks.

With the increase of mobile devices as well as development in wireless communication, adhoc networking is gaining importance with the growing number of well-known applications in the commercial, Military and private sectors. Mobile Ad-Hoc Networks permit users to access and interchange information regardless of their geographic position or proximity to infrastructure. In comparison to the infrastructure networks, all the nodes in MANETs are moveable and their connections are more dynamic. Unlike other mobile network, MANETs do not require a static infrastructure.

All members at these networks acts as both hosts and routers forming an autonomous network heavily depended on the belief that all participants give and take resources in a legitimate manner. The nodes are generally devices such as laptops, PDAs and other mobile devices. The features can be broadly classified in terms of connectivity, bandwidth and battery lifetime etc.

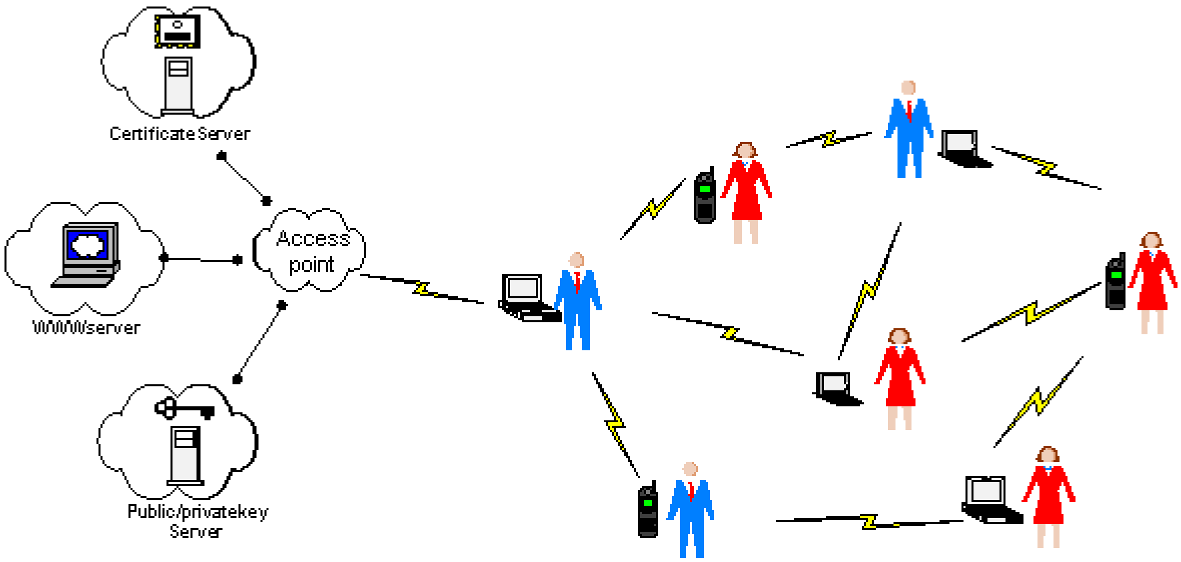

Figure 1.1: Mobile Ad hoc Network

A. Routing

Routing is the process of selecting paths in a network through which data is to be send. Routing is performed by many kinds of networks, including telephone network, internet and transport networks. Each Routing directs forwarding the passing of logically addressed packets from their source toward their destination through intermediate nodes which are hardware devices called routers, bridges, firewalls. Routing process directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus constructing routing tables which are held in routers memory becomes very important for efficient routing. A routing metric is a value used by a routing algo*rithm to determine whether one route should perform better than other. Metrics can cover information like bandwidth, delay, hop count, path cost, reliability etc.

A routing metric is a value used by a routing algorithm to determine whether one route should perform better than other. Metrics can cover information like bandwidth, delay, hop count, path cost, reliability etc.

Ad hoc routing has following goals:

- Route computation must be distributed because centralized routing in a dynamic network is impossible even for small network.
- Each host must care only about the routes to its destination and must not be involved in frequent topology updates for the portions of the network that have no traffic.
- Stale route must be avoided or detected and eliminated quickly.
- If the topology stabilzes then routes must converge to the optimal routes.
- As few hosts as possible must be involved in route computation and state propagation as this involve monitoring and updating at least some states in the network.
- Give the hosts the best response time and throughput.
- Provide the maximum possible reliability by selecting alternative routes if hosts connectivity fails due to mobility of the host.

- The no packet collisions must be kept minimal by limiting the no of broadcasts made by each other.
- It must use scarce resources such as bandwidth, computing power, memory and battery power.
- It is desirable to have a backup route when the primary route has become stale and is to be recomputed.

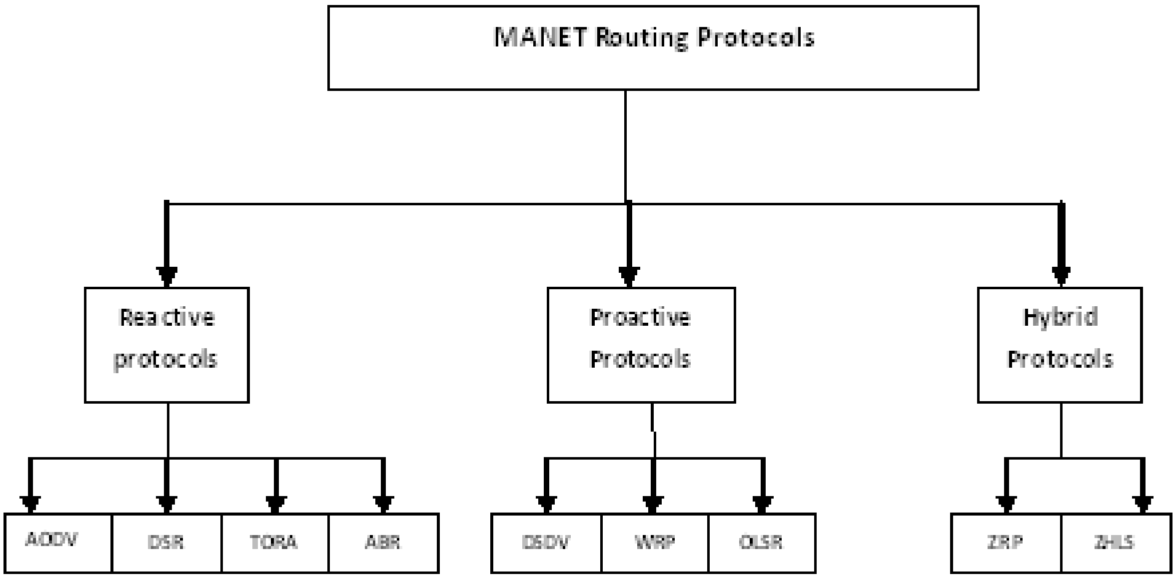

Figure 2. Classification of Ad hoc Network Routing Protocols

Ad hoc routing has following goals:

- Route computation must be distributed because centralized routing in a dynamic network is impossible even for small network.
- Each node must care only about the routes to its destination and must not be involved in frequent topology updates for the portions of the network that have no traffic.
- Stale route must be avoided or detected and eliminated quickly.
- If the topology stabilizes then routes must converge to the optimal routes.
- As few nodes as possible must be involved in route computation and state propagation as this involve monitoring and updating at least some states in the network.
- Give the nodes the best response time and throughput.
- Provide the maximum possible reliability by selecting alternative routes if nodes connectivity fails due to mobility of the node.
- The no packet collisions must be kept minimal by limiting the no of broadcasts made by each other.
- It must use scarce resources such as bandwidth, computing power, memory and battery power.

It is desirable to have a backup route when the primary route has become stale and is to be recomputed.

B. Transmission Control Protocol (TCP)

TCP is a connection oriented point-to-point protocol. It is a means for building a reliable communications stream on the top of the unreliable Internet Protocol (IP). TCP is the protocol that supports nearly all Internet applications. TCP is used by a large number of IP applications, such as email, Web services, and TELNET. As a connection-oriented protocol, TCP ensures that data is transferred reliably from a source to a destination. Reliability in transmission involves the use of some form of handshake between the sender and receiver. Also, sequence numbers can be used to ensure in-sequence delivery of segments and help to identify lost or corrupted segments. Retransmission can be used to resend lost or corrupted segments. Hence, a retransmission timer is needed to determine when to initiate a resend. For TCP, an adaptive retransmission mechanism is employed to accommodate the varying delays encountered in the Internet environment. When the load offered to the network is more than its capacity to handle, congestion builds up. Congestion can be dealt with by employing a principle borrowed from physics - the law of conservation of packets. The idea is to refrain from injecting a new packet into the network until an old one leaves. TCP attempts to achieve this goal by dynamically manipulating the window size. Figure 1.6, show how TCP manage network congestion.

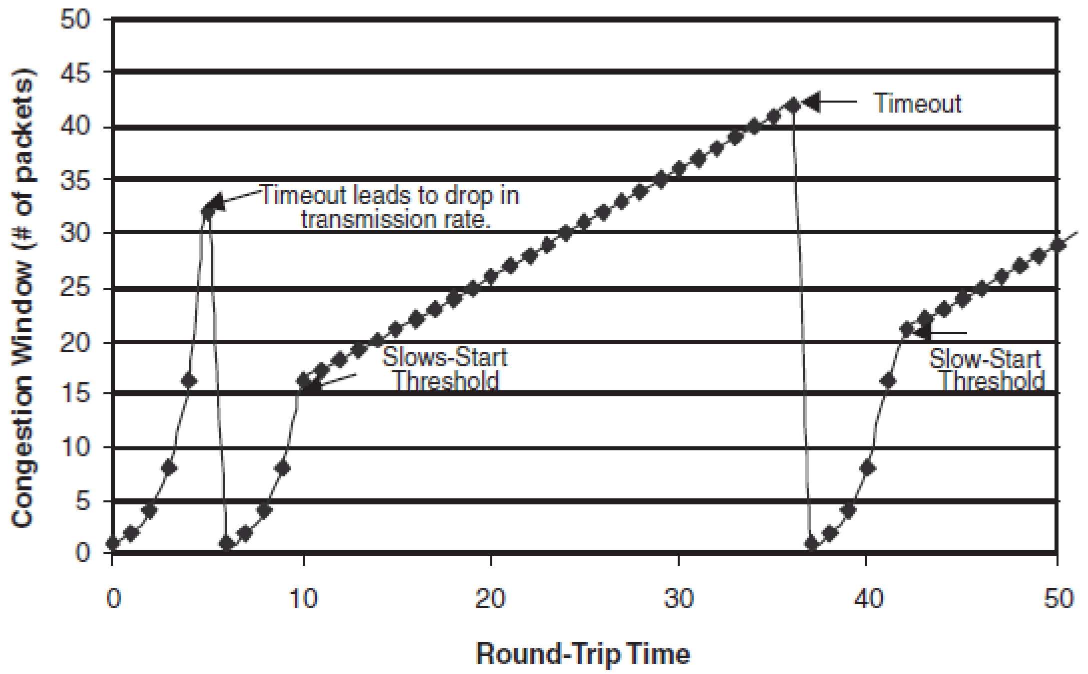

Figure3. TCP congestion control [2].

C. Versions of TCP

TCP primary purpose is to provide a connection oriented reliable data transfer service between different applications to be able to provide these services on top of an unreliable communication system. TCP needs to consider data transfer, reliability flow control, multiplexing, TCP segment, and congestion control and connection management. TCP does not depend on the underlying network layers and, hence, design of various TCP versions is based on the properties of wired networks. However, TCP congestion control algorithms may not perform well in heterogeneous networks. The TCP protocol has been extensively tuned to give good performance at the transport layer in the traditional wired network environment. However, TCP in its present form is not well suited for ad hoc networks where packet loss due to broken routes can result in the counterproductive invocation of TCP‘s congestion control mechanisms [11].

- **TCP Reno**

TCP Reno employs the basic principle of Tahoe, such as slow starts and the congestion avoidance. However it adds some intelligence over it so that lost packets are detected earlier and the pipeline is not emptied every time a packet is lost. Reno requires that we receive immediate acknowledgement whenever a segment is received [9, 14].

The logic behind this is that whenever we receive a duplicate acknowledgment, then his duplicate acknowledgment could have been received if the next segment in sequence expected, has been delayed in the network and the segments reached there out of order or else that the packet is lost.

If we receive a number of duplicate acknowledgements then that means that sufficient time have passed and even if the segment had taken a longer path, it should have gotten to the receiver by now. There is a very high probability that it was lost. So Reno suggests an algorithm called _Fast Re-Transmit‘. Whenever we receive 3 duplicate ACK_s we take it as a sign that the segment was lost, so we re-transmit the segment without waiting for timeout. Thus we manage to re-transmit the segment with the pipe almost full. Another modification that RENO makes is in that after a packet loss, it does not reduce the congestion window to 1. Since this empties the pipe. It enters into an algorithm which we call Fast-Re-Transmit' [9]**.**

- **TCP New Reno**

TCP New RENO [9] is a slight modification over TCP-RENO. It is able to detect multiple packet losses and thus is much more efficient that RENO in the event of multiple packet losses. Like RENO, New-RENO also enters into fast-retransmit when it receives multiple duplicate packets, however it differs from RENO in that it does not exit fast-recovery until all the data which was out standing at the time it entered fast recovery is acknowledged. The fast-recovery phase proceeds as in Reno, however when a fresh ACK is received then there are two cases:

i. If it ACK_s all the segments which were outstanding when we entered fast recovery then it exits fast recovery and sets CWD to threshold value and continues congestion avoidance like Tahoe.

ii. If the ACK is a partial ACK then it deduces that the next segment in line was lost and it re-transmits that segment and sets the number of duplicate ACKS received to zero. It exits Fast recovery when all the data in the window is acknowledged.

- **1.4.4.3 TCP SACK**

TCP-SACK (Selective Acknowledgment) [8] conserves the basic ideology of the TCP functionalities. The TCP-SACK works best when various packets got dropped from one window of data. The receiver uses the 'option' fields of TCP header (SACK option) for notifying the sender of three blocks of non-contiguous set of data received and enqueuer by the receiver. The first starting block represents the most recent packet received, and the next blocks represent the most recently reported SACK blocks.

The sender keeps a scoreboard in order to provide information about SACK blocks received so far. In this way, the sender can conclude that whether there are missing packets at the receiver. If so, and its congestion window permits, the sender retransmits the next packet from its list of missing packets. In case there are no such packets at the receiver and the congestion window allows, the sender simply transmits a new packet. As per the previous discussion, fast retransmission and fast recovery can only handle one packet loss from one window of data within one transmission time out period; TCP may experience poor performance when multiple packets are lost in one window. To overcome this limitation, recently the Selective Acknowledgement option (SACK) is suggested as an addition to the standard TCP implementation. In the event of multiple losses within a window, the sender can conclude that which packets have been lost and should be retransmitted using the information provided in the SACK blocks. A SACK-enabled sender can retransmit multiple lost packets in one RTT instead of detecting only one lost packet in each RTT.

- **TCP FACK**

FACK or Forward Acknowledgement is a special algorithm that works on top of the SACK options, and is geared at congestion controlling. FACK algorithm uses information provided by SACK to add more precise control to the injection of data into the network during recovery – this is achieved by explicitly measuring the total number of bytes of data outstanding in the network. FACK decouples congestion control from data recovery thereby attaining more precise control over the data flow in the network. The main idea of FACK algorithm is to consider the most forward selective acknowledgement sequence number as a sign that all the previous acknowledged segments were lost. This observation allows improving recovery of losses significantly [9].

1.4.4.7 TCP-Westwood

TCP Westwood makes no attempt to correct the problem of non-congestion packet loss in wireless networks solely like Veno, but rather to improve the efficiency of TCP in all heterogeneous networks. It estimates the network's bandwidth by properly low-pass filtering and averaging the rate of returning acknowledgment packets per RTT. It then uses this bandwidth estimate to adjust the ssthreshand the cwnd to a value close to it when a packet loss is experienced (adaptive decrease). In particular, when three DUPACKs are received, both the cwnd and ssthreshare set equal to the Estimated Bandwidth (BWE) times the minimum measured RTT (RTTmin); when a coarse timeout expires, the ssthreshis set as before, while the cwndis set equal to one. The improvement of Westwood is a more realistic bandwidth estimation in comparison to TCP Vegas, which significantly increases TCP throughput over wireless communication links. TCP Westwood has also been tested in against handovers in simulated [17, 18].

- **TCP-Compound**

The key idea is that if the link is under-utilized, the high-speed protocol should be aggressive in increasing sending rate to obtain available bandwidth more quickly. However, once the link is fully utilized, being aggressive is no longer good, as it will only cause problems like TCP unfairness. With the increase of the sending rate, queue is built at the bottleneck, and the delay-based flow gradually reduces its sending rate. The aggregated throughput for the communication also gradually reduces but is bound by the standard TCP flow. Compound TCP (CTCP) [29], which incorporates a scalable delay-based component into the standard TCP congestion avoidance algorithm. This scalable delay-based component has a rapid window increase rule when the network is sensed to be under-utilized and gracefully reduces the sending rate once the bottleneck queue is built. With this delay-based component as an auto-tuning knob, Compound TCP can satisfy all three requirements pretty well:

1) CTCP can efficiently use the network resource and achieve high link utilization.

2) CTCP has similar or even improved RTT fairness compared to regular TCP. This is due to the delay-based component employed in the CTCP congestion avoidance algorithm. It is known that delay-based flow.

3) CTCP has good TCP-fairness. By employing the delay based component, CTCP can gracefully reduce the sending rate when the link is fully utilized. In this way, a CTCP flow will not cause more self-induced packet losses than a standard TCP flow, and therefore maintains fairness to other competing regular TCP flows.

- **TCP-Cubic**

CUBIC is an enhanced version of BIC: it simplifies the BIC window control and improves its TCP-friendliness and RTT-fairness. The window growth function of CUBIC is governed by a cubic function in terms of the elapsed time since the last loss event. TCP-cubic function provides a good stability and scalability. Furthermore, the real-time nature of this transport protocol keeps the window growth rate independent of RTT, which keeps the protocol TCP friendly under both short and long RTT paths..[29].

II. LITERATURE REVIEW

Muhammad Aamir et al. (2013), propose a scheme of buffer management for packet queues for fixed and mobile hosts over wireless ad hoc environment. For a host, the packet queue is maintained in such a way that an equal buffer space is allocated to each neighbouring source and an allowable extension is also available to each neighbour to avoid any underutilization of resources. The allocation is made in the buffer of a centrally communicating MANET host and it is based on number of packets received in the queue at host's buffer to utilize the buffer space efficiently without any monopolization of some surrounding source. According to this scheme for achieve efficient queuing in the buffer of a centrally communicating host called *QMN* through an active queue management strategy by assigning dynamic buffer space to all neighbouring hosts in proportion to the number of packets received from neighbours and hence controlling packet drop probabilities. The authors simulated this scheme for packet loss ratios and transmission efficiencies in 50-host, 150-host, and 250-host scenarios and compared its performance with Drop Tail and PAQMAN schemes and evaluates the performance of proposed scheme in conjunction with DiffServ implementation of QoS packet markings for VoIP traffic in terms of throughput, packet end-to-end delay, and jitter statistics and found it better as compared to Drop Tail and PAQMAN schemes.

Sanjeev Patel (2013), proposed a model to calculate dropping probability and packet loss for Active Queue Management and shown a comparative analysis of the loss delay product as a new parameter of performance measure obtained from simulation on ns2 for different AQM algorithms. congestion caused due to many unavoidable events like retransmission and increased RTT due to queuing delay. There are a number of mechanisms that have been proposed for IP layer protocols to maintain high throughput and low delay in the network in the absence of feedback from the network. The author has attempted to analyse the AQM algorithm using delay, jitter, throughput, loss rate as measurement parameters. The statistical concept of Random Drop is technique in which a packet randomly selected from all traffic passing through the gateway belongs to a particular connection with a probability matching the connection's proportion to the traffic. Dropping of random packets from connections leads to reduce the total steady state traffic of the gateway. From experiment results, author concludes that RED performs better than other AQM algorithms at low bandwidth.

F.Furqan Doan et al. (2013), propose a mechanism namely WiMAX Fair Intelligent Congestion Control (WFICC) to avoid congestion at the base station. WFICC ensures that the traffic is scheduled in such a way that the base station output buffer operates at a target operating point, without violating the QoS requirements of connections. A detailed simulation study is performed in ns-2 to evaluate the effectiveness of proposed algorithm to meet the QoS requirements of different Class of Services (CoSs). The results have shown that the proposed WFICC algorithm enables the base station to avoid congestion and ensures the provision of QoS of different Class of Services (CoSs) in terms of throughput, fairness and packet delay.

S. Soundararajan et al. (2012), proposed new approach Multipath Load Balancing and Rate Based Congestion Control (MLBRBCC) based on rate control mechanism for avoiding congestion that contains an adaptive rate control based technique in which the destination host copies the estimated rate from the intermediate hosts and the feedback is forwarded to the sender through an acknowledgement packet. Here authors compare the proposed algorithm against explicit rate based congestion control (XRCC) for different performance metrics such as average end-to-end delay, average packet delivery ratio, drops and throughput. In Proposed MLBRBCC, the source host forwards the data packet to the destination through the intermediate hosts. On reception of the data packet at the intermediate host, percentage of channel utilization and queue length are estimated and host is verified for congestion status. After the reception of the data packet, the destination host checks for the rate information in the packets IP header fields. Along with other essential fields, estimated rate is copied to an acknowledgement packet and sent as a feedback to the sender. The sender performs rate control according to the estimated rate obtained from the destination. From Simulation results, the authors conclude that Proposed MLBRBCC has higher better than XRCC.

P. Arivubrakan et al. (2012), focuses on the analysis the performance of AODV and DSR routing protocols under varying range of the transmission in terms of distance and simulation time using Network Simulator (ns2). The performance of AODV & DSR has been analysed with varying transmission range with a distance of 50m, 75m, 100m,125m and 150m under CBR connection of simulation time at 3ms and 5ms using ns2. Data transmitted by a host is received by all the hosts within its communication range. The authors compare theses protocols and found that overall performance of DSR is better than AODV routing protocols at 125m range. Also, they found that the performance of the routing protocol could be enhanced in higher transmission range.

Ipsita Panda (2012), gave overview about various routing protocol for QoS parameter in MANETs. As different applications have different requirements, the services required by them and the associated QoS parameters differ from application to application. For example, in case of multimedia applications time, bandwidth requirement, power requirement, probability of packet loss, the variation in latency (jitter), Route acquisition Delay, Communication Overhead, Scalability are the key QoS parameters, whereas military applications have stringent security requirements. For applications such as emergency search and rescue operations, availability of network is the key QoS parameter.

Makoto Ikeda et al. (2012), evaluate the performance of two routing protocols namely AODV (reactive) and OLSR (proactive) using performance metrics such as CWND (congestion window) and throughput for single and multiple TCP traffic flow over Mobile adhoc network using NS-3 Simulator. TCP has built-in support for congestion control. Congestion control ensures that TCP does not pump data at a rate higher than what the network can handle. Here authors used the TCP-Newreno as TCP congestion control algorithm for congestion avoidance. The authors consider different parameters such as random waypoint mobility model with a randomly chosen speed, uniformly distributed Chosen speed , log-distance path loss model and constant speed delay model; to create scenarios for simulation. From simulation based evaluation, authors found that the number of hosts affects the performance of the network, because of the communication coverage and for AODV the flows have fairness of communication whereas for OLSR, one of the flows is aggressive towards the others.

S. Rajeswari et al. (2012), presented a simulation-based performance evaluation and comparison of three queuing techniques namely First-In-First-Out , *Random early detection* and Weighted Fair Queuing which is implemented against the AEERG protocol for different number of hosts, packet size and pause time . In FIFO queuing (known as first come-first-serve (FCFS) queuing), all packets are placed in a single queue and then processing will begin in the same order on which they arrived. *RED* also known as threshold based queuing discipline, is an active queue management algorithm. It is used for a congestion avoidance algorithm. This algorithm plays an important role by the way of not admitting full queues for processing, reducing the packet delay and loss. It monitors the average queue size and average number of dropped packets based on statistical probabilities. It statistically starts of dropping the packets from flows before it reaches its threshold value. WFQ is a combination of PQ and FQ algorithms. As in the FQ method, all queues are served so that there is no bandwidth starvation, but some queues have more weight in a sense that they receive more service. In other words, a weight is given to each queue to assign different priorities to the queues. From simulation based comparison, the authors noticed that using RED has greatly improved all the performance measures especially with FIFO. The reason is that RED monitors the average queue size and randomly drops packets when congestion is detected.

III. CONCLUSION

The transmission control protocol (TCP) is one of the most popular and widely used end-to-end protocols for the Internet today. Unlike routing, where packets are relayed hop-by-hop toward their destination, TCP actually provides reliable end to-end transmission of transport-level segments from source to receiver. A critical look at the above literature highlights *TCP is unable to distinguish losses due to route failures and network congestion, TCP suffers from frequent route failures and* design of TCP has not considered very lossy links. Different TCP versions react with different types of behavior. In addition, from the perspective of transport layer, we believe that TCP will be on top of the routing protocols for reliable data transmission.

REFERENCES

[1] Muhammad Aamir and Mustafa A. Zaidi (2013), "A Buffer Management Scheme for Packet Queues in MANET" TSINGHUA SCIENCE AND TECHNOLOGY, ISSN -1007-0214, Volume 18, Number 6, pp543-553 Dec. 2013.

[2] Sanjeev Patel (2013), "Performance Analysis and Modeling of Congestion Control Algorithms B ased on Active Queue Management" IEEE, pp. 449-454, 2013.

[3] Fatima Furqan and Doan B. Hoang (2013), " WFICC: A New Mechanism for Provision of QoS and Congestion Control in WiMAX", The 10th Annual IEEE CCNC- Wireless Networking, IEEE, 2013.

[4] S. Soundararajan and R. S. Bhuvaneswaran (2012), " Multipath Load Balancing & Rate Based Congestion Control for Mobile Ad Hoc Networks (MANET)" IEEE, Dec. 2012.

[5] P. Arivubrakan, V. R. Sarma Dhulipala (2012), "QoS Enhancement by varying Transmission Range in Wireless Ad-hoc Networks" International Journal of Computer Applications (0975 – 8887), Volume 37, No. 9, January 2012.

[6] Ipsita Panda (2012)," A Survey on Routing Protocols of MANETs by Using QoS Metrics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[7] Makoto Ikeda, Elis Kulla, Masahiro Hiyama, Leonard Barolli, Muhammad Younas and Makoto Takizawa (2012), "TCP Congestion Control in MANETs for Multiple Traffic Considering Pro active and Reactive Routing Protocols" 15th International Conference on Network-Based Information Systems, IEEE, Oct. 2012.

[8] S. Rajeswari and Y. Venkataramani (2012), "Congestion Control and QOS Improvement for AEERG protocol in MANET" International Journal on AdHoc Networking Systems (IJANS), Vol. 2, No. 1, January 2012

[9] Subir Kumar Sarkar, T G Basavaraju, and C Puttamadappa "Ad Hoc Mobile Wireless Networks – principles, protocols, and applications " AUERBACH PUBLICATIONS, Taylor & Francis Group, New York, Landon.