Proceedings of the Pakistan Academy of Sciences 52 (3): 201–214 (2015)

ISSN: 0377 - 2969 (print), 2306 - 1448 (online)

Pakistan Academy of Sciences

Research Article

QoS Assurance in Higher Mobility Mobile Ad Hoc Networks using Multipath Admission Control Protocol

Muhammad Asif[1], Sana ul Haq[1], Naveed Ahmad[2], Tariqullah Jan[3*], and Muhammad Wasimuddin[1]

[1]Department of Electronics, University of Peshawar, Peshawar, Pakistan
[2]Department of Computer Science, University of Peshawar, Peshawar, Pakistan
[3]Department of Electrical Engineering, University of Engineering and Technology, Peshawar, Pakistan

Abstract: The cheap and easy availability of wireless devices boosted the MANETs supported applications. Due to these emerging applications MANETs are not only deployed in military sector but in every walk of life. Now QoS assurance to these applications is an essential part rather than additional feature in MANETs. The routing protocols provide only data route rather than assuring any kind of guaranteed QoS to applications. The routing protocols must be equipped with additional features such as traffic scheduling, QoS awareness, admission control, and traffic priority to assure guaranteed QoS.In this article we will present our designed Flow aware admission control protocol that work with Dynamic Source Routing (DSR) to assure guaranteed QoS provisioning. The admission control assures high throughput in highly mobile scenario and volatile topology of MANETs by sustaining partially disjoint multiple paths between source and destination. The protocol injects the data traffic to the network on the basis of availability of resources. The protocol calculates the available bandwidth using channel idle time ratio (CITR) and takes the decision of accepting or rejecting the new data traffic to the network. The protocol repairs the route locally and reduces the network load and results in high performance. The protocol is compared with the state of the art admission control protocols using network simulator-2.

Keywords: Admission control, multimedia applications, MANETs, QoS, multipath

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are combination of mobile nodes, works as an end node as well as a router, communicate over a wireless channel [1]. The nodes can join or leave the network on their own will, which results in a dynamic and unpredictable topology. MANETs have no infrastructure or centralized control. Due to these characteristics of MANETs, it became very popular in military as well as every walk of life. The widely acceptance of MANETs compel the research community to support different kinds of applications over MANETs. The applications range from normal text data to video. These applications have different Quality of Service (QoS) requirements. Some of the applications just need throughput guarantee while others required guaranteed throughput, boundedend-to-end delay and jitter [1].QoS assurance in MANETs is challenging and research oriented task [2].

Research studies show that Routing Protocols only provide routes for the data without any kind of QoS assurance to the applications. Many researchers have made efforts to provide guaranteed QoS to the applications and majority of these QoS-aware routing protocols find the route on the basis of capacity availability, traffic congestions and node stability. These routing protocols provide a

Received, March 2015; Accepted, April 2015
*Corresponding author: Tariqullah Jan; Email: tariqullahjan@uetpeshawar.edu.pk

uni-path between source and destination. In case of route failures, the routing protocols have to search for another route, which causes extra delay and degraded throughput. The link failures occurs either due to congestions or nodes mobility.

The designed Flow aware admission control protocol with multipath tackles both the reasons of longer delay as well as degraded throughput. The protocol will inject the traffic load to the network according to the available capacity and will maintain multiple paths between source and destination to cope with the route failure to high mobility of nodes. The protocol works with the Dynamic Source Routing (DSR) protocol [3]. The paper presents the design, characteristics and performance of Flow Aware Admission Control-Multipath (FAAC-Multipath) protocols and comparison with the other state of the art protocols such as Contention Aware Admission Control protocol (CACP) [4], Multipath admission control protocol for MANETS (MACMAN) [5] and Flow Aware Admission Control (FAAC) protocol [6]. The protocols are evaluated in different high mobility scenarios. The remaining sections of the paper presents: the background study, designing of FAAC-Multipath protocol, comparison with other well-known admission control protocols and conclusion of the paper.

2. BACKGROUND WORK

Most of the reactive routing protocols support only best effort services without any kind of QoS guarantees. DSR and AODV are most common and well accepted protocols in this category. AODV-BR [7]is the extended version of AODV that uses intermediate route repair locally. The optimized version of AODV-BR [8] maintains the backup paths not only with the help of route reply but as well as due to the data packet as well. The data packets following the routes also help the protocol to find the data route for data sessions. The intermediate route repair or intermediate backup path did not assure the route availability at any cost, so it is not a sufficient technique for backup route availability. The application needs the guaranteed backup path so it can switch the data at the same time of primary route failure. The author [9] uses limited flood technique to solve the route failure problem, but this is not optimal solution in unpredictable and volatile topology networks like MANETs. The work presented in [8] uses multiple constraints such as delay, reliability and capacity for route selection but did not explain how routes can be updated and can remove the stale information. While in [10] the author proposed to use pre-emptive techniques to cope with route failure but this is also not feasible in MANETs like network where the topology is totally unpredictable and where route failures occurs not only due to traffic congestion but due to nodes movement as well.

Multipath routing technique can solve the problem upto some limit of route failure due to changing mobility but unable to solve the problem of route failure due to congestion or more traffic injection to the network than the its capacity. The congestion problem can be solved using admission control protocols. Multipath protocols show higher performance than the uni-path protocols in higher mobility scenarios [11, 12]. These protocols provide best effort services. Some of the QoS-aware routing protocols based on contention free MAC [13, 14]. As there is no centralized control in MANETs, so it is not feasible to use contention free MAC. The hidden node can cause collision of data packets and exposed node reduces the efficiency of channel utilization [15]. Therefore, we will consider the protocols that uses contention aware MAC for capacity calculation.

It is fairly an open research issue in research community to increase the battery life of portable or mobile devices such as PDA, smart phone etc. Although research achievement has begun to solve the problem of limited battery life, it is still a fact that portable or mobile devices have less power supply as compared to wired networks devices [16]. Therefore, the design of protocol should minimize the overhead, because it will drain energy of the device proportionally [17].

MP-DSR [18] discovers the routes on the basis of route reliability but does not assure guaranteed throughput. The protocols select the best available reliable routes but the requirement satisfying routes. Adaptive Dispersity QoS Routing (ADQR) Protocol [19] divides the traffic among the multiple routes which gives the problem of re-arranging the data traffic at the receiver. The protocol does not provide any solution to that problem. Interference aware QoS Multipath Routing (IMPR) [20] protocol proposes to find the routes on the basis of link stability and available bandwidth but did not provide any information about the mechanism of combination of these two metrics.

Scalable Multipath on Demand Routing in Mobile Ad Hoc Networks (SMORT) [21] tackles the route failure problem by providing multiple routes to intermediate nodes only. In route stability-based multipath QoS routing (SMQR) [22] protocol calculate the route capacity only considering the individual node's capacity not neighbours capacity. In wireless communication, one node transmission affects the available capacity of the neighbours' nodes as well. So only to consider the nodes capacity by itself will severely affect the performance. It will inject more traffic than the available capacity and will result in degraded throughput and high packet loss. MACMAN provides multiple routes for each data session but these multiple routes are fully disjoint. It is very difficult to find and maintain such routes in MANETs. It introduces a lot of overheads in the network while finding such routes. The admission control mechanism of MACMAN is a combination of CACP and Perceptive Admission Control (PAC) protocols [23].

3. FAAC-MULTIPATH PROTOCOL

Flow Aware Admission Control-Multipath (FAAC-Multipath) protocol incorporates both routing and admission control aspects of operation. Its purpose is to provide end-to-end guaranteed throughput services to application data sessions that have a strict constraint on the minimum level of throughput they require. FAAC-multipath protocol establishes and maintains multiple paths between source and destination on demand. The protocol assures guaranteed throughput to the application in high mobility scenarios. The protocol includes features to discover routes that nominally have adequate capacity to support admission of data sessions, as well as to admit only those new sessions that would not have a derogatory effect on the throughput of the previously-admitted sessions and finally to uphold the level of throughput that it has promised to sessions by way of admitting them. The design and implementation of the protocol is presented in this paper and performance of the protocol is compared with other well-known admission control protocols. FAAC-multipath partially utilizes the function of DSR protocol. The protocol finds and maintains partially disjoint routes between source and destination. Both the routes i.e. primary and secondary are established on capacity estimation of the said routes, means both routes must fulfil the capacity requirement of the application. The following sections give a full description of its operation as well as the design choices made. The protocol working mechanism is a combination of application layer and network layer. We have explained the behaviour and characteristics of each layer involved in our protocol.

3.1 Application Layer Model

Application layer is the 5th layer in TCP/IP suite and is basically responsible for different services. Different applications run on application layer. We have developed an application that generates constant bit rate data and the application agent defines the notion of a session. A new data session is specified by the following fields: data session ID, start time (s) of data session, minimum required throughput (bps), and data packet size (bytes). The session ID is allocated by the application agent. The throughput requirement defines how many bits, and therefore packets, are generated per second, as well as the desired end-to-end throughput. Traffic is modelled by constant bit rate sources, since this adequately demonstrates the ability of FAAC-Multipath to handle various traffic loads and to make admission decisions.

When a new session is generated by a user, a blocking timer is set to expire in 10s and a session request (SReq) message is passed to the network at the source node. The source application agent will block the session if it does not receive the session reply (SRep) in 10s. The blocking timer is set to 10s, so that the application agent can generate two SReq for each data session before blocking the data session. The SReq is passed down to the User Datagram Protocol (UDP) agent. The UDP agent encapsulates the SReq in a UDP packet, giving it a unique sequential packet ID. The SReq is carried as the application data and passed down to the routing agent, which takes over the handling of SReq.

3.2 Network Layer Model

Network layer is the 3rd layer in TCP/IP suite and routing protocol runs on this layer. As FAAC-Multipath protocol is partially coupled with DSR protocol, therefore it is implemented on network layer. Application data sessions that are requesting service from and admission to the network are assumed to specify their desired traffic characteristics to the protocol. The characteristic of the data session is modelled in the form of Session Request (SReq) packet. The SReq is passed down to the network layer to model the arrival of a session admission request at a traffic source node. The routing agent will find the route in route cache or will initiate the Route Request (RtRq). When route is found then the protocol will test the route nodes resources according to Session Request (SReq). The Novelty of the designed protocol is the method of propagating Session Request (SReq), resource checking and to find the route for throughput sensitive data session. Figure 1 shows the position of FAAC-Multipath protocol in TCP/IP suite. The protocol works on network layer and as well MAC layer, because MAC layer calculate the remaining resources for the protocol to take admission decision.

Application Layer	Session Request
Transport Layer	UDP/TCP
Network Layer	FAAC Protocol
Data Link Layer	Link Layer
Physical Layer	Physical Layer

Fig. 1. FAAC protocol in view of TCP/IP suite.

3.3 Protocol Implementations

FAAC-Multipath protocol is implemented in two phases:

- In first phase, the protocol searches the route from source to destination in route cache. If the route is available in the route cache, then the protocol checks the resources for that route in second phase of the protocol implementation. If there is no source to destination route in route cache, then the routing agent generates the route request (RtRq) and finds the routes between intended source and destination.
- In second phase of admission control, local and neighbour resources are tested before forwarding the SReq to other nodes. As in the second stage, the full route is known to the source, so protocol checks the resources with the full knowledge of contention count (C_{count}).

3.4 Route Discovery

In this process, the protocol finds the route from source to destination on the basis of application's requirements. The application agent specifies the date session requirements in a control packet called Session Request (SReq). The Network layer receives these requirements from application layer and encapsulates these SReq requirements in Route Request (RtRq) packet and store the information in the cache of source node of the data session.

The source node checks its route cache for the route to destination. If route is available then it starts the capacity testing of the route else initiate the

route discovery. The source node first conduct its own capacity estimation and after this initiate route request in case of sufficient capacity availability. The source forward the RtRq and each receiving node do the capacity estimation locally.

Every intermediate node only forwards the RtRq if it can support the new data session without affecting the quality of already admitted data sessions. The source as well as all the intermediate nodes reserves the resources for the specified data in RtRq. At this stage, the protocol partially admits the data session means not fully. The RtRq which has encapsulated the SReq propagates in this manner and reaches the destination finally if it is possible. The destination node may have received more than one RtRqs for the same data session. The destination node sends Route Reply (RRep) to the source node. On a way back of RRep to the source node, each intermediate node checks its two hops neighbours capacity using a control packet called admission request. If the two hops neighbours of the intermediate node can satisfy the request of the new data session, then it forwards the RRep to the next node on a route. In this method the primary route is established between source and destination. The secondary or backup route process is explained in a paper in a later section.

3.5 Capacity Testing

The required capacity of a node (C_{req}) can be estimated by using the following equation. The session single hop requirement is calculated as:

$$C_{req} = b_{req} * W_{req} \quad (1)$$

Both types of capacity are measured in bits per second. Where b_{req} is the required capacity by the session and W_{req} is the weighting factor means the overheads of different layers to be included with the data capacity as show in following equation 2.

$$W_{req} = \frac{(T_{DIFS} + 3T_{SIFS} + T_{RTS} + T_{CTS} + T_{DATA} + T_{ACK} + T_{backoff} + T_{MAChdr} + T_{IPhdr} + T_{UDPhdr} + T_{SRhdr} + T_{QoShdr})}{T_{DATA}} \quad (2)$$

Here T_{DIFS} and T_{SIFS} are the times taken by distributed coordinated function (DCF) inter-frame space (DIFS) and short inter-frame space (SIFS) employed by the direct sequence spread spectrum (DSSS) physical layer (PHY) specification in IEEE 802.11 standard [24], T_{RTS}, T_{CTS}, T_{DATA} and T_{ACK} are the times taken to transmit request-to-send (RTS),clear-to-send (CTS), Data and ACK frames (along with the physical layer preambles) respectively, $T_{backoff}$ represents the time for which a node backs off before each packet transmission and T_{MAChdr}, T_{IPhdr}, T_{SRhdr}, $T_{UDPhdr,}$ T_{QoShdr} are the times taken to transmit the fixed size MAC, IP, source route, UDP and QoS-specification (SReq contents) headers on each data frame. So for any node to forward the SReq should satisfy the following equation.

$$(T_{idle} - T_{resv})\beta > C_{req} * C_{count}$$
$$where \ \text{resv} \in 1,2,3,4,,,,, \quad (3)$$

Where T_{idle} is the fraction of channel idle time, T_{resv} is the session reserved fraction of the channel time, which is not yet being used, but which has been reserved by previously processed session request (SReq), and β is the node transmission rate, which specifies the raw channel capacity in bps. FAAC-Multipath protocol requires that the 802.11 MAC protocol monitors the status of the channel reported by the virtual and physical carrier-sensing mechanisms. The basic unit of time in the 802.11 MAC specifications is the time slot, the duration of which is between 9μs and 20μs depending on the type of PHY assumed. In our model, the MAC protocol simply checks the channel status once per time slot, since this is a computationally cheap operation, and records the number of slots for which it is deemed idle. This number is aggregated for one second before being reported to the higher layer protocol. This avoids responding to momentary fluctuations in the CITR.

Fig. 2 represents the testing of local and neighbours' node resources. Small circle represent mobile nodes, middle and large circles represent the transmission and carrier sensing range of node 'B' respectively. Node 'S' is the source and node 'D' is the destination of the data session. Solid

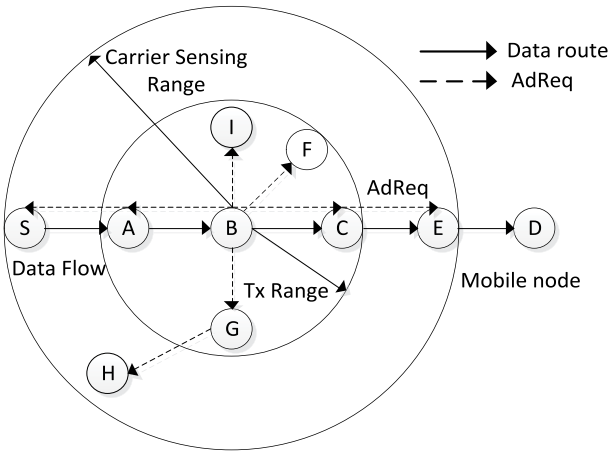

Fig. 2. Capacity test at local and neighbour nodes.

arrows represent the intended data route from 'S' to 'D' and dotted arrows represent the transmission of Admission Request (AdReq) control packets from node 'B' to its two hops neighbours to check their capacity.

3.5.1 Processing of Session Request (SReq)

The receiving node of SReq tests its local resources according to equation (3). If it can satisfy the requirement of the new session then it tests the resources of its two hops neighbour by transmitting admission request (AdReq) packet. If the SReq node did not receive the Admission Denial (AD) packet within the specified time, then it considers that its neighbours can accommodate the new data session. The node forwards the SReq to other node on the intended route of the data and reserves the required resources of the data session. Each node will continue the process of checking local and neighbours' resources and forwarding the SReq till destination node. After receiving SReq by destination, it generates Session Reply (SRep) and transmits back to source of the data session on same route followed by SReq. FAAC-Multipath protocol checks the node resources during the session request phase with full knowledge of contention count (C_{count}). Contention count of the node can be calculated by the following formula [4].

$$C_{count} = (CSN \cap R) \setminus D \quad (4)$$

Here Contention Count (C_{count}) is the combination of Carrier Sensing Neighbours (CSN) and tentative route (R) of the data traffic excluding the destination node (D). The destination node does not transmit the data further therefore, it is not considered in Ccount. The following algorithm explains the processing of SReq by each individual node.

```
# Received SReq
If (Bavail>= Breq) then
        -Broadcast AdReq
Note:   If (AD) then
                -Drop SReq
                -Inform Source Node
        Else
  If (time>=SReqtime) then
                -Reserve resources
                -Propagate SReq
          Else
                        -Goto Note:
                End if
        End if
Else
        -Drop SReq
        -Inform Source Node
End if
```

3.5.2 Processing of Admission Request (AdReq)

The receiving node of AdReq also tests their local capacity using equation (3). If it can satisfy the requirements, then it stores the session and route information, otherwise will send the admission denied (AD) packet to the AdReq source node. The following algorithm explains the processing of AdReq by each node. AdReq time to live (TTL) represents the number of nodes to which AdReq packet has to be forward.

3.6 Selection of Backup/Secondary Route

The protocol establishes and maintains a backup route for all data sessions. These routes must be partially disjoint. For the backup routes, the protocol checks for route in a source node cache, if it is available then the protocol starts the testing

and partially disjoint-ness of the backup route to the primary route. The backup route request (BRReq) carries the primary route information and checks the disjoint-ness with the primary route. At any stage, when both the routes are found sharing the maximum 50% of nodes in common, the secondary route is rejected.

In backup route selection, every node starting from source to destination, tests its local as well as two hops neighbour's capacity in a similar way to primary route. But capacity test of local and neighbours are conducted during BRReq forwarding, not at a time back up route reply (BRRep) as in primary route selection. In backup capacity estimation, contention difference is used instead of contention count, because contention count may underestimate the capacity of the backup route. The contention difference can be easily calculated using the following formula.

$$CD = \langle |C_{count}| - |CSN \cap R_{curr} \backslash \{D\}| \rangle \quad (5)$$

CD is contention Difference, C_{count} is contention count, CSN represent Carrier sensing range of the node, whose capacity is being estimated, R_{curr} represent the current data route and D represent the destination of the data session. Figure 3shows the explanation of Contention Difference.

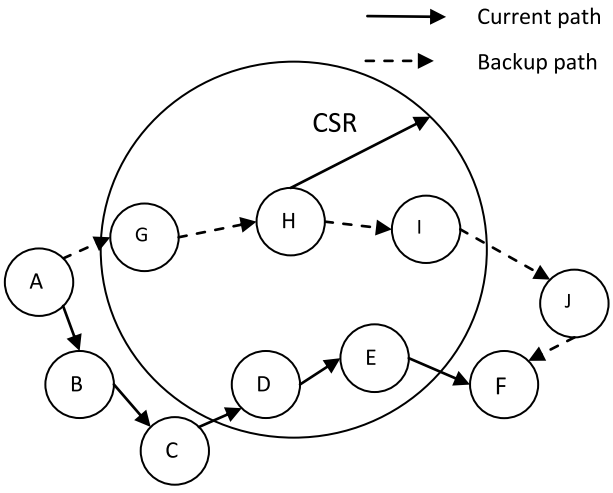

Fig. 3. Calculation of contention difference.

Small circle are mobile nodes and large circle represents the node's CSR. The primary route for the data session is represented by solid line between source and destination while backup route is represented by dotted line. The contention count of node H is 3, while CD of the node H is 1. Two of the neighbour nodes of node H is already in primary route, so it will not be included in capacity estimation, i.e., CD, because the data traffic will divert to secondary route only when primary route fails. In a similar fashion, the CD of all nodes can be find easily.

3.7 Reliability of Backup Route

In Mobile Ad hoc Networks, it is very difficult to maintain fully disjoint routes particularly in high mobility scenarios. So instead of fully disjoint routes, FAAC-Multipath protocol will establish partially disjoint routes. It means that both the routes can share the nodes 50%. This disjoint-ness improves the reliability of the backup route and reduces the chances of both routes failure simultaneously. The following equation finds the reliability of the backup route.

$$B_{avail} - B_{resr} = CD.B_{req} \quad (6)$$

B_{avail} is the available bandwidth of the node, B_{resr} is the reserved bandwidth for some session but not yet utilizing, CD is contention difference and B_{req} is the required bandwidth of the data session.

3.8 Switching Mechanism

The switching mechanism is one of the most important aspects of FAAC-Multipath protocol. It actually avoids the route failure, avoids the collision and tries to uphold the guaranteed throughput in low as well as high mobility scenarios. The fast switching mechanism benefited the protocol to avoid the session pausing mechanism, which increases end-to-end delay and results in collision and route failure. Switching mechanism is implemented in the following three different scenarios:

- The protocol switches the data session from primary to secondary route, when the primary route is not satisfying the requirements of the data session. The failure to satisfy the requirement can be due to node mobility or collision. When

a route node of other data session moves into the interference range of the earlier stated data session's route nodes, it affects the throughput of the session and also increases PLR which in turn increases end-to-end delay.

- The FAAC-MM protocol switches the data session from primary to secondary route when primary route fails either due to mobility or due to failure of excessive re-transmission at the MAC layer. When a route nodes move out of the transmission range of the data sending node then failure detecting node informs the source node and the source node switches the data session from primary route to secondary route.
- The protocol also switches the data session from primary to secondary route when it finds that the secondary route offers higher throughput. The protocol admits the data session when it finds a route from source to destination that satisfies the session requirements. As the protocol does not wait for secondary route discovery to initiate the data session, so when source node become aware that secondary route is offering higher throughput, then the protocol switches the data session from primary to secondary route. One thing must be noted in this scenario that the primary route is still satisfying the requirements of the data session. It upholds the guaranteed throughput and bounded end to end delay.

4. SIMULATION ENVIRONMENT

FAAC-Multipath protocol is tested using extensive simulation with other well-known admission control protocols under different simulation environment and network traffic load. The simulation results show the comparison of the performance of the protocols. The paper presents the comparison of FAAC-Multipath protocol, CACP, MACMAN and FAAC. FAAC and CACP maintain uni-path between source and destination. CACP is a well-known and leading admission control protocol for MANETs. MACMAN maintains multiple paths between source and destination. MACMAN utilizes the functionality of CACP and Passive Admission Control (PAC) protocol. The simulation results show the performance under different node mobility and also the capability of the protocols admission control techniques.

4.1 Simulation Setup

The simulation of the protocols carried out using well accepted network simulator NS-2. The data files of the simulations are further processed by text based programming language, AWK. Table 1 show the simulation parameters, which are used during simulation of the protocols. The number of nodes, simulated area size and the average transmission range were selected using the guidelines in [25] for rigorously evaluating a multi-hop routing protocol.

Table 1. Simulation parameters.

S. No.	Parameters	Values
1	Total mobile nodes	100
2	Total traffic sources	50
3	Per source sessions	20
5	Data packet Size	512 bytes
6	Mobility model	Random WayPoint
7	Routing protocol	DSR
8	Node speed	2,4, 8, 16, 32
9	Tx rage	250m
10	CSR	500m
11	Channel bandwidth	2Mbps
11	Simulation area	1500m * 1500m
12	Pause time	801sec
13	Simulation time	800 sec
14	Results averaged over	10 runs

4.2 Mobility Model

Number of mobility models is available to check the performance of the protocols in MANETs. These mobility models are used to generate node position and movements' pattern of the nodes during simulation. Literature survey shows 64% of the researcher's research papers used Random Waypoint Mobility (RWP) model to test the

protocols in MANETs [26]. RWP model excellently exhibit the movement pattern of the mobile nodes, but the initial velocity of nodes must not be zero. Zero initial velocity of mobile nodes creates concentration of the nodes in the middle of the simulation area. We have used RWP mobility model to test our protocol performance and the designed protocol also work with any other mobility model as well.

4.3 Communication Model

IEEE 802.11b, Distributed Coordination Function (DCF) is used in our simulation as a communication model [24]. DCF uses CSMA/CA technique for channel contention among mobile nodes. Channel capacity is shared among mobile nodes within their Carrier Sensing Range (CSR).

4.4 Performance Evaluation Metrics

Different metrics can be used to evaluate the performance of the protocols. The careful selection of metrics helps in fair analysis of the protocols. The protocols performance and efficiency are evaluated using traffic admission and completion of session with routing load, etc.

5. SIMULATION RESULTS ANALYSIS

This section of the paper presents the analysis of the simulation results on basis of performance evaluation metrics. Each protocol is analysed deeply according to their performance and results.

5.1 Session Admission Ratio

Figure 4 shows the Session Admission Ratio (SAR) of the studied protocols at different node speed. Node speed affects the performance of the protocols due to frequent topology changes. Node movement causes collision and frequent route failures. As the node speed increases, the SAR of the protocols decreases because the protocol generates more control overheads to find or recover the data route.

The CACP protocol admits more sessions than FAAC protocol because CACP does not consider

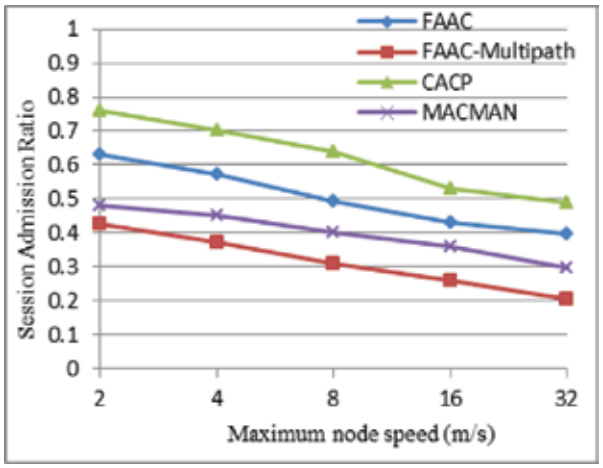

Fig. 4. Session admission ratio.

the effect of new data session on the existing data session in the network. The CACP protocol drops session and then uses this free capacity for the admission of other new sessions. Data session admission ratio in FAAC decreases as the node maximum speed increases because the provisioning of guaranteed throughput in such mobile scenario becomes difficult. The main task of FAAC protocol is to assure the guaranteed throughput to the admitted session and complete the session that have been admitted.

SAR of FAAC-Multipath is low and it decreases from 42.6% to 20.5% when speed increases from 2 to 32 m/s. Higher speed of nodes causes frequent route failures, more re-routing, local route repair, increases Packet Loss Ratio(PLR) and average end-to-end delay that results in consumption of network capacity and decrease the SAR. SAR of MACMAN is higher than FAAC-Multipath because FAAC-Multipath test the resources very thoroughly during the admission control and consider the effect on previously admitted sessions, because the main objective is to complete the data session not only to admit the data session.

5.2 Session Completion Ratio

Figure 5 represents the Session Completion Ratio (SCR) of the studied protocols and their behaviour at different node speed. Higher node speed decreases the SCR of the protocols because it changes topology frequently and results in collision

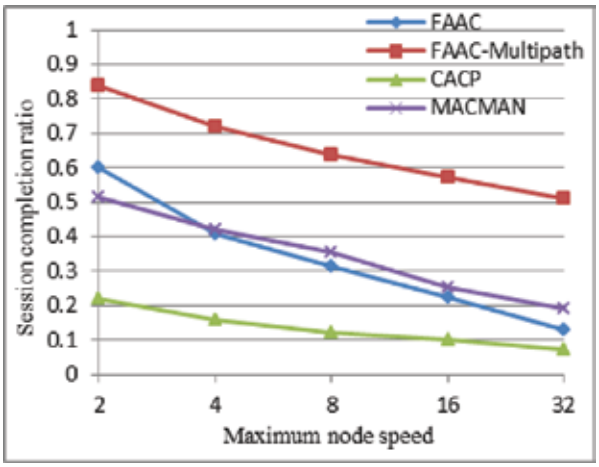

Fig. 5. Session completion ratio.

at MAC layer. The excessive re-transmission at the MAC layer causes the route failure, which either results in switching the data session to another route or initiate new route discovery. The switching mechanism or initiating the route discovery increases the overheads and results in degraded throughput. The session drops if its requirements are not fulfilled. It is clear from the figure that the data session completion ratio of FAAC is higher than CACP protocols. The completion ratio of FAAC protocol varies from 60.3 % to 12.8% by increasing speed from 2 to 32m/s while the completion ratio of CACP decreases from 21.9% to 7.4%, respectively. CACP admits more data sessions and then drops the sessions due to failure of providing the guaranteed throughput to data sessions.

SCR of MACMAN protocol is higher than FAAC protocol at higher node speed because higher speed cause frequent route failure and MACMAN takes an advantage of back up route availability. The SCR of the MACMAN is decreases from 51.4% to 19.2% when node speed rises from 2 to 32m/s. FAAC-Multipath performs better at different node speed among all the studied protocols. It's fast re-routing mechanism and local route repair mechanism helps to maintain the agreed throughput to the data session. Moreover the thoroughly controlled admission of data session also helps to achieve high SCR. Its SCR decreases from 83.7% to 51.1%, when node speed changes from 2 to 32m/s.

5.3 Packet Loss Ratio

Node speed has a great effect on the Packet Loss Ratio of the studied protocols. Figure 6 shows the Packet Loss Ratio of the four studied protocols i.e., CACP, FAAC, FAAC-Multipath and MACMAN. Nodes mobility make the data route stale and also causes route failure, which results in data packet loss. CACP protocol is severely affected by higher node speed, which increases the collision and as a result the protocol drops the data packets. FAAC protocol PLR is lower than CACP due to thorough admission control and efficient utilization of resources. FAAC finds alternate routes for the data session faster than CACP protocol, which results in low PLR. However, the PLR of FAAC protocol is higher than MACMAN and FAAC-Multipath protocols because it initiates route discovery or start the testing of available routes in source cache for the session. The PLR has great impact on session completion ratio of the protocols.

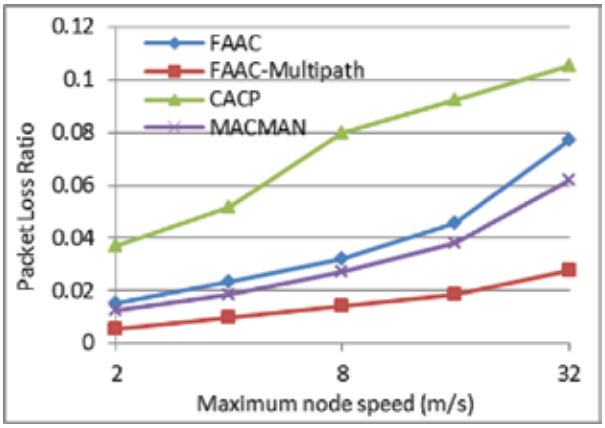

Fig. 6. Packet loss ratio.

PLR of MACMAN is higher than FAAC-Multipath at different node speed and its PLR are increasing as the node speed increases. The increase in node speed changes the topology very frequently and the node movement may affect the capacity of each other and as a result either decreases the session throughput or fails the data route. The node movement not only causes collision at the MAC layer, but also causes the buffer overflow. The MACMAN protocol session pausing mechanism although reduces the PLR that is due to collision,

but on the other hand, session pausing mechanism increases the average end-to-end delay which in turn increases the PLR that is due to the buffer overflow. Its PLR increases from 1.2% to 6.2% when node maximum speed changes from 2 to 32m/s.

FAAC-Multipath protocol has lowest PLR due to thorough admission control, fast re-routing and local route repair of routes. The reserved capacity plays a vital role in frequent topology changes and switches the data session from primary to secondary route. Its PLR increases from 0.57% to 2.7% when node speed changes from 2 and 32m/s.

5.4 Average End-to-End Delay

The average end-to-end delay is the second most important metric for evaluation of network layer protocols. It shows the efficiency of the protocols to deal with congestion, mobility, PLR and utilization of available capacity. Excessive dropping of packets either due to route failure or due to collision increase the average end to end delay of the data packets. Figure 7 shows the effect of nodes mobility over different protocols. Higher node speed causes frequent route failures and protocols initiate route discovery frequently that introduces more overheads to the network. Higher speed increases the interference that results in high PLR and longer end-to-end delays. FAAC protocol has smaller average end-to-end delay than MACMAN protocol at lower node speed because lower node speed causes less number of route failures. At higher node speed, route failure occurs more frequently and MACMAN protocol takes an advantage of backup routes and attains smaller average end-to-end delay.

MACMAN protocol has a longer average end-to-end delay than FAAC-Multipath protocol, due to its session pausing mechanism and slow re-route mechanism. MACMAN protocol pauses the session, when its achieved throughput is less than the requested. Session pausing mechanism of the MACMAN protocol results in longer average end-to-end delay which in turn also increases the PLR. MACMAN protocol maintains fully disjoint routes, which is very difficult to achieve in such frequent changing topology. FAAC-Multipath uses fast re-routing strategy instead of session pausing mechanism. The fast re-routing mechanism avoids the collision and keeps the average end-to-end delay minimum, which results in higher SCR and lower PLR among the studied protocols. SAR and reserved capacity also contribute to maintain minimum average end-to-end delay at different node speed.

5.5 Aggregate Throughput

The Aggregate throughput is related to the successful transmission of data packets. Route failure, PLR and average end-to-end delay affects the aggregate throughput of the network. Figure 8 shows the aggregate throughput of the FAAC, CACP, FAAC-Multipath and MACMAN protocols. Aggregate throughput of the protocols reduces with the rising node speed. MACMAN protocol achieves

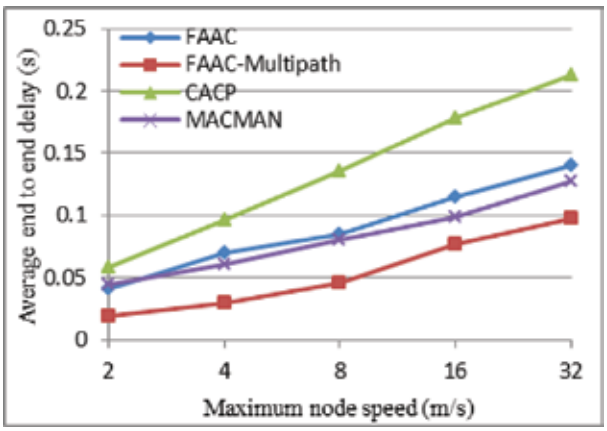

Fig.7. Average end-to-end Delay.

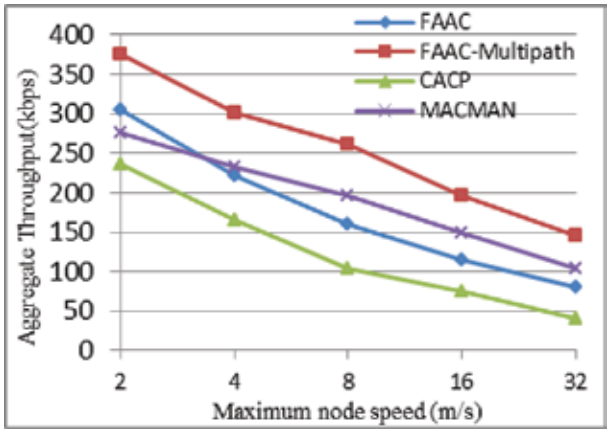

Fig. 8. Aggregate throughput.

higher aggregate throughput than FAAC protocol at higher node speed. The simulation results show that multi-path protocols works better in fast changing topology environment.

MACMAN protocol aggregate throughput is mainly affected by increasing average end-to-end delay with increase in node speed. Although MACMAN protocol uses backup route to achieve higher aggregate throughput, its session pausing mechanism increases the average end-to-end delay, which in turn decreases the throughput. MACMAN protocol attains lower aggregated throughput than FAAC-Multipath protocol.

The main objective of FAAC-Multipath protocol is to assure and uphold the throughput of each session which has been guaranteed at the time of session admission. The thorough admission control, tested backup route, fast re-routing and the absence of session pausing mechanism upholds the highest aggregate throughput of the protocol. It maintains minimum average end-to-end delay among all the studied protocol, which also contribute to the highest aggregate throughput. The SCR of the Figure 4-25 also confirms the result shown in Figure 4-28. Although the aggregate throughput of the FAAC-Multipath decreases with the increase in node maximum speed but still it maintains the guaranteed throughput of a higher ratio of the admitted session into the network.

5.6 Useful Aggregate Throughput

This metric shows only the average aggregate throughput of the completed sessions in Figure 9. The aggregate throughput of sessions, which drops in the middle, may not be useful to the application. Node mobility or speed create challenging environment for the protocols to uphold the guaranteed throughput till session completion. It shows the protocols' behaviour dealing with frequent route failure and unpredictable topology. Useful aggregate throughput is calculated by multiplying the aggregate throughput with the session completion ratio of the protocol. Due to higher aggregate throughput and session

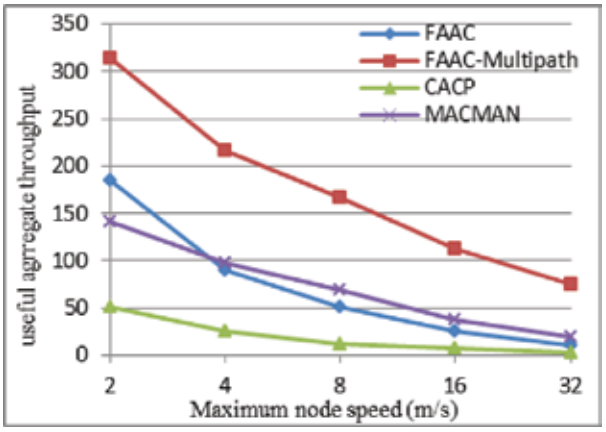

Fig. 9. Useful aggregate throughput.

completion ratio of FAAC protocol, the useful throughput of FAAC is higher than the CACP protocols. The useful aggregate throughput of all the protocols degrades as the node speed increases because higher node speed causes frequent route failure and increases PLR. The figure shows that FAAC-Multipath has maintained its highest useful aggregate throughput due to its highest SCR and aggregated throughput.

5.7 Normalized Routing Load

Normalized Routing Load of the stated protocol increases with the increase in node speed as represented in Figure 10. Here, mobile speed is the main cause of route failure and this failure occurs very frequently. Due to frequent changes in topology, single path AC protocols do not achieve

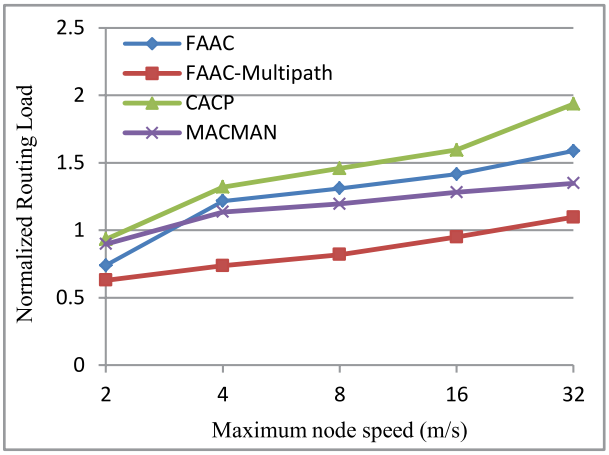

Fig. 10. Normalized routing load.

higher aggregate throughput because most of the session drop in the middle of session duration. CACP and FAAC initiates and test the capacity of route for each route failure. In high mobile scenario, MACMAN achieves higher aggregate throughput and SCR than FAAC protocol, which compensates the higher overhead of multiple routes and maintains lower NRL than FAAC protocol. FAAC-Multipath has lowest NRL among the studied protocols. The partial disjoint multiple routes and fast re-routing mechanism helps to assure aggregate throughput throughout the session duration that results in higher SCR. Higher SCR and aggregate throughput helps the protocol to compensate the routing overheads and maintain lower NRL.

6. CONCLUSIONS

Flow Aware Admission Control (FAAC)-Multipath protocol is designed with the characteristics of tested multipath and local route repair functionality. Both these characteristics and functionality enhances the throughput and session completion ratio enormously of the protocol. The simulation results establish the fact that Session Completion Ratio has improved by 60% and Throughput by 10%. FAAC-Multipath is compared with the state of the art Admission Control Protocols, which are single as well as multipath capabilities.

7. REFERENCES

1. Asif, M., Z. Sun & H. Cruickshank. Admission control protocols in mobile ad hoc networks provisioning QoS. In: *Proceedings of 7th International Conference on Frontiers of Information Technology,* Abbottabad, Pakistan, p. 1-4 (2009).
2. Stefano, B., M. Conti, S. Giordano & I. Stojmenovic. *Mobile ad Hoc Networking: The Cutting Edge Directions,* 2nd ed., Wiley-IEEE (2013).
3. Johson, D., Y. Hu & D. Maltz. *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks*. IETF MANET Working Group Experimental RFC 4782 (2007).
4. Yang, Y. & R. Kravets. Contention-aware admission control for ad hoc networks. *IEEE Transaction on Mobile Computing* 4(4): 363-377 (2005).
5. Lindgren, A. & M. Elizabeth. Multipath admission control protocol for MANETs. *ACM SIGMOBILE Mobile Computing and Communications Review* 8(4): 68-71 (2004).
6. Asif, M., Z. Sun, H. Cruickshank & N. Ahmad. QoS provisioning in contention aware MANETs using Flow Aware Admission Control protocol. In: *Proceedings of IADIS International Conference on Telecommunications, Networks and Systems*, Rome, Italy, p. 99-106 (2011).
7. Lee, S., & M. Gelra. AODV-BR: Backup Routing in Ad Hoc Networks. In: *Proceedings of IEEE Conference on Wireless Communications and Networking Conference*, Chicago, USA, p. 1311-1316 (2000).
8. Wu, S.L., S. Y. Ni., J.P. Sheu & Y.C. Tseng. Route Maintenance in a Wireless Mobile Ad Hoc Network. *Telecommunications Systems*18(1-3): 61–84 (2001).
9. Castenada, R., S.R. Das & M.K. Maria. Query localization techniques for on-demand routing protocols for mobile ad hoc networks. *Wireless Networks* 8(2-3): 137-151 (2002).
10. Goff, T., N. Abu-Ghazaleh., D. Phatak & R. Kahvecioglu. Pre-emptive routing in ad hoc networks. *Journal of Parallel and Distributed Computing* 63(2):123-140 (2003).
11. Marina, K.M & S.R. Das. Ad hoc on-demand multipath distance vector routing. *Wireless Communications and Mobile Computing* 6: 969-988 (2006).
12. Li, X. & L. Cuthbert. Multipath QoS routing of supporting Diffserv in Mobile Ad hoc Networks. In: *Proceedings of IEEE Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing,* Towson, Maryland, USA, p. 308-313 (2005).
13. Lin, C.R. On-Demand QoS Routing in Multihop Mobile Networks. In: *Proceedings of IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, Anchorage, Alaska, USA, p. 1735-1744 (2001).
14. Liao, W.H., S.L. Wang, J.P. Sheu & Y.C. Tseng. A Multi-Path QoS Routing Protocol in a Wireless Mobile Ad Hoc Network. *Telecommunications Systems* 19(3-4): 329-347 (2002).
15. Yu, W., Z. Mi, D. Niu & R. Xu. Algorithm of exposed terminals concurrent transmission based on reverse path in MANET. In: *Proceedings of 2nd IEEE International Conference on Mechanic Automation and Control Engineering,* Hohhot, China, p. 3819-3822 (2011).
16. Wannawilai, P. & C. Sathitwiriyawong. AOMDV with Sufficient Bandwidth Aware. In: *Proceedings of 10thIEEE International Conference on Computer and Information Technology,* Bradford, UK, p. 305-312 (2010).

17. Senthilkumar, M. & S. Somasundaram. Energy Aware Multiple Constraints Intelligent Multipath QoS Routing Protocol with Dynamic Mobility Prediction for MANET. In: *Proceedings of International on Process Automation, Control and Computing,* Coimbatore, India, p.1-8 (2011).
18. Leung, R., J. Liu, E. Poon, A. Chan & L. Baochun. MP-DSR: a QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks. In: *Proceedings of 26th Annual IEEE Conference on Local Computer Networks, Tampa, Florida,* USA, p. 132-141 (2001).
19. Hwang, Y. & P. Varshney. An adaptive QoS routing protocol with dispersity for ad-hoc networks. In: *Proceedings of 36th Annual Hawaii International Conference on System Sciences,* Big Island, HI, USA, p. 6-9 (2003).
20. Wang, Y.H., C.H. Tsai, H.Z. Lin & C.A. Wang. Interference aware QoS Multipath Routing for Ad Hoc Wireless Networks. *International Journal of Computers and Applications* 29(4): 372-378 (2007).
21. Reddy, R.L. & V.S. Raghavan. SMORT: Scalable Multipath on Demand Routing in Mobile Ad Hoc Networks. *Ad Hoc Networks* 5(2): 162-188 (2007).
22. Sarma, N. & S. Nanda. A multipath QoS routing with route stability for mobile ad hoc networks. *IETE Technical Review* 27(5): 380-397 (2010).
23. Chakeres, I.D, E.M. Belding-Royer & J.P. Macker. Perceptive admission control for wireless network quality of service. *Ad Hoc Networks* 5 (7): 1129-1148 (2007).
24. IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std. 802.11* (2007).
25. Kurkowski, S., T. Camp & W. Navidi. Two Standards for Rigorous MANET Routing Protocol Evaluation. In: *Proceedings of 3rd IEEE Conference on Mobile Ad hoc and Sensor Systems,*Vancouver, British Columbia, Canada, p. 256-266 (2006).
26. Navidi, W. & T. Camp. Stationary distributions for the random waypoint mobility model. *IEEE Transaction on Mobile Computing* 3(1): 99-108 (2004).