

Novel Strategies Practicing Quality of Service in MANETs

Ajay Koul
School of CSE
SMVD University
Katra-182320

Mamta Bucha
School of CSE
SMVD University
Katra-182320

ABSTRACT

Researchers are working on securing MANETs by implementing more and more complex techniques like cryptography, digital signatures, hashing etc. These empirical techniques are highly effective in providing security but also have major influences over throughput, excellences of the system, sustain high cost and thereby degrade the Quality of Service (QoS). To improve the performance of MANETs in terms of end-to-end delay, throughput, least resource exploitation, least information loss etc. a different approach of deploying security in MANETs is required without sacrificing the QoS. In this paper, we have investigated the Quality of Service methods and protocols that various researchers have proposed and found protocols that provide good Quality of Service. The idea is to investigate further those protocols to provide security with less impact on QoS in near future

Keywords

Bandwidth estimation, Fault tolerance, Issues in MANET, QoS Metrics, Multipath routing

1. INTRODUCTION

Quality of service (QoS) is the check maintained by the established network to assure best quality producing results to its users as per their requirements. This check is satisfied by setting some quality parameters (minimum throughput, minimum/maximum packet delay, minimum/maximum packet loss, minimum/maximum hop counts etc. according to the application's requirements). E.g. for multimedia delay sensitive applications, network must satisfy the minimum delay and minimum bandwidth requirements. But due to shared wireless medium and dynamic network topology of MANETs, it is very problematic to satisfy all quality bounds at one time. Though there are many ways of attaining QoS in MANETs by implementing it on all layers of OSI. Like in medium access control (MAC) layer, it is determined that which next node among the competing nodes should broadcast its packets on the shared wireless channel. Lately, much effort has also been focused on designing MAC protocols for the efficient utilization and allocation of resources on MAC layer. INSIGNIA [1] is one of the QoS frameworks which creates, reestablishes and terminates end-to-end reservations. It is developed in accordance with the management of amount of bandwidth used by the network and it is transparent to any underlying MAC protocol. On network layer, it is the network routing protocol that decides the most feasible routes that satisfy the QoS checks and are efficient in utilization of resources. Based on that collected data, route gets selected. For this QoS routing protocols are used which only efforts to establish the best feasible routes by initiating discovery of those nodes that can serve the requirements of application. It also reestablishes routes from source to destination during route failures by keeping up-to-date state

information about whole network. In application layer, dynamic connections, failures and reconnections in the network can be checked. Packet dropping, collisions, bandwidth consumption, errors in received packets bits can be checked on different layers respectively [2], [3], [4], and [5].

After getting through many research papers which have discussed about MANET's deployment, routing, security, QoS features and issues etc. It is clear that infrastructure-less networks, MANETs are only established when some specific application needs to perform for solving some kind of problem. So, before raising an infrastructure-less network, we need to confine and find out what are our needs and what do we actually want from the network. After giving a clear perspective of the application's requirements and its goals, we can categorize it into the QoS provisioning approaches that are discussed in section IV. For example, if an application needs certain bandwidth over some specific time schedule and cannot share it with anyone then it can be at least realized that the application needs a hard QoS approach. Likewise applications that have more concern over security of its data with delay constraints need to work on MAC layer and network layer. It requires following coupled and dependent QoS approaches. This distinct approach can minimize the overhead of optimizing all layers of OSI and the consequent costs too. Therefore, a QoS model for a specific application can be proposed with or without being transparent to underlying protocols. One can work on managing the intake of flow of admissions in application and session layers which can positively reduce the overload on other layers. Priorities can also be set for admissions of flows. An existing routing protocol can be modified or extended while preserving its basic features. Like flooding protocol is best known for its assured end-to-end packet delivery but its main issue is redundancy of packets in the network which can cause congestion. The basic feature of this protocol can be implemented into the QoS scheme with some modifications in its routing procedure so that least resources get consumed for end-to-end packet delivery. Choosing an appropriate routing protocol is another task for fulfilling the application's needs and QoS constraints in network. Remember that there is a big difference between choosing shortest path and QoS path. It is because shortest path may lead to the destination earlier but might be it is using the scarce resources in higher rate. Whereas QoS path may not be the shortest path but it can be the most feasible path in terms of bandwidth, power and other limited resources usage. Several routing protocols are available which can provide the shortest routes but this does not mean that they also provide QoS. On choosing the right routing protocol we can estimate about which QoS constraints it can satisfy, what new metrics need to add and what other methods need to implement or what existed features need to modify. Transport layer protocols can also be considered because on that layer it is important to know if there is any

packet loss and if yes, then is there any errors or packets are dropping due to congestion. Similarly, MAC protocols should also be carefully chosen so that hidden and exposed nodes problem can be avoided. On physical layer, the most considerable part is to reduce the effects of fading, shadowing, noise and other distortions; minimizing and maximizing the use of power resource etc. After development of whole view of the QoS scheme, more improvements can be done by executing it in the worst environment and making it vulnerable to scarcity of resources, power etc. because it may help in finding out the pros and cons of our scheme before anyone criticized it. So on further steps can be taken accordingly. One more thing is assumptions should be made as less as possible because it generates the doubtful possibilities. As all models, protocols are first developed on simulation grounds. Assumptions made first may not set the goal to its right path in its real time implementation. Thus, we need a strong pragmatic approach in framing MANETs in the real environment so that we can predict the issues that may arise after deploying the network.

In this paper, we have discussed the most common aspects of MANETs in section II that need to be foreseen before implementing QoS techniques. Then various generalized metrics through which quality of the network services and protocol can be measured have been outlined in section III. After an extensive study of various research papers, we have tried to approach a different trend of promising good QoS in MANETs in section IV which stresses upon satisfying more QoS constraints other than only throughput and delay. It is because protocols that are considering only quality of service may be unfeasible or unrealistic due to inadequate resources and overhead of excessive computations. A protocol which is focusing particularly on one layer may not be well-suited for the functioning or utilization of limited resources on the other layer. A well-designed protocol must be able to react dynamically with respect to the network size, topology, computations and storage overhead. It must be scalable to accomplish the essential quality requirements of the applications. But it is also tough to assure QoS promises initially to a session which has peculiar QoS requirements, due to node mobility, frequently link failures and frequently changing states information in order to update the network. Recently, much attention has been directed on providing better QoS in the routing protocols to make them more scalable and proficient in every manner [6], [7], [8], [9].

2. HIGHLIGHTS ON VARIOUS ASPECTS OF MANETS WHILE PROMISING QOS

MANETs accentuates certain characteristics that can raise several complications in the provisioning of QoS. These characteristics are very significant according to the different requirements of user's applications. Various characteristics and problems that can be foreseen before and after deploying MANETs are discussed below:

2.1 Reliability of Wireless Channel

While propagating through wireless medium, radio waves may deviate from their path and undergo multi-path propagation. They may experience attenuation and noise interference. Due to this characteristic, information exchange is susceptible to attacks like eavesdropping, impersonation, spoofing, routing information disorders, denial of service etc. Hence wireless medium is highly uncertain and insecure without the provision of sophisticated security mechanisms. Many protocols are aimed on providing security first [10].

2.2 No Centralized Control

MANETs lack centralized access to coordinate the node activities. Nodes at their own take control decisions. They become self-routers and self-forwarders which are significant in some manner but it also complicates the methods of QoS provisions with so much unpredictability in the environment. Distributed control of the network is helpful but it generates additional overheads [11].

2.3 Changing Network Topology due to Mobile Nodes

Mobility is another major concern that needs extensive attention as it is the base of MANETs. Links between MANET nodes frequently break and reestablish when nodes move which sometimes leads to unpredictable topology. Running QoS sessions may get delayed or ends up due to frequent route breaks. This requires reestablishment of new QoS sessions for new routes which incurs further delays. There is another problem of the existence of stale routing information if the rate of change of topology is higher than the rate of updating of routing tables. It must be updated quickly on node's movement or change in topology in order to reestablish the QoS paths and it requires extensively efficient QoS methods to cope with congestion problem due to the presence of extra routing information [12], [13].

2.4 No. of Multi Hops

Due to arbitrary location of nodes in the mobile ad hoc network, data may be required to transfer either through single hop or multiple hops via intermediate nodes. So routing protocol for such type of network must be able to maintain paths between intermediate and neighbor nodes. By maintaining different paths for the destination, the paths which become invalid due to link failures can again be reestablished by choosing another optimized path. Many conventional routing protocols [14], [15], [16] have been designed to minimize the level of data traffic and the number of hops in the network.

2.5 Network Scalability

It must be scalable as per network requirements. If the network needs to increase its size by adding thousands more nodes then it must stand by the additional number of nodes. Addition of more nodes should not affect the performance of the network. It must be capable of generating the same output instead better results consistently. Therefore, QoS providing methods must sustain the network scalability [9].

2.6 Limited Bandwidth and Other Resources

QoS provisioning methods must consider the rate of utilization of critical resources such as battery and bandwidth along with other resources like proficiency, buffer size etc. because resource availability and its accessibility have significant effects on their performances. It must be equally distributed among the nodes. Some QoS oriented protocol's [12] main concern is saving power because it may not be possible to replace or recharge the battery of nodes placed in the remote and harsh areas.

2.7 Tradeoff between Redundancy and Latency

If data delivery is the main requirement of the user then redundancy would be sure in the network. It is because user wants to receive data anyhow by single path or by multipath, by secured medium or by insecure medium. Packets arrive in

destination through different paths by utilizing maximum bandwidth and the most critical resource i.e. energy. These reserved resources are consumed unnecessarily for sending same packets at the destination. But here is one issue with minimizing redundancy that if it is minimized then latency increases because it requires the evaluation of most recent packet and rejection of old redundant packets. So an efficient QoS mechanism should be designed by considering both factors [17], [18].

2.8 Heterogeneous Nature and Variant Traffic Rate

MANETs are known for their heterogeneous nature. There can be different types of elements present in the network. One may be capturing weather data; another may be observing only movements of other mobile nodes. It means that different nodes may be performing different activities at the same time. Therefore all nodes may be exchanging information which depends upon the respond of each other. It further requires synchronization between the varying rates of traffic generated by various nodes. This MANET's nature makes the design of QoS provisioning methods more challenging.

2.9 Shadowing and Multipath Fading

Multipath fading and shadowing [19] needs to be considering while designing the network. It arises in any multipath propagation environment where the elements of the network are mobile. Signals may arrive at the destination directly or via reflecting objects such as buildings, furniture in the offices, ground etc. at different times. These obstacles may attenuate signal's strength through absorption or reflection and therefore weaken it. Due to the mobile nature of nodes in MANETs, the signal strength may vary. Signals may completely fade away or the signal may fall below an operating strength. QoS provisioning methods must incorporate some mechanisms to lower fading effects caused by the topology and node's surroundings. Many probabilistic models [20] have been proposed to eliminate these effects.

2.10 Hidden and Exposed Node Problems

Hidden node problem arises in MAC layer when packets are originated from two nodes which are not in each other's communication ranges but are connected to one intermediate node. On that intermediate node, the packets get collide and this collision remains unidentified by the source nodes. In exposed terminal problem, if two nodes (say B and C) are communicating with each other but node A and B lies in each other's communication range. Node A defers its transmission even if it is not interfering with node C. So a node use the resources extensively to resend packets and reestablish routes therefore it necessitates the provision of good QoS methods to avoid these problems [10].

2.11 Physical Security of Nodes

Generally security is provided to mitigate problems like spoofing, impersonation, tampering of data etc. but what about the physical security of nodes which are placed in far enemies areas. Without physical security, provision of QoS to the network is of no use. It is because if full resources are utilized efficiently with the help of QoS provisioning methods but someone tampers the hardware in absence of the others then what would be the use of QoS provisions. All would go waste.

3. GENERAL QoS METRICS

Quality of Service of a protocol is said to be effective for the network when its predetermined attributes met the user's requirements. These attributes may be taken as end-to-end delay, performance, minimum/maximum bandwidth consumption, acceptable jitter, tolerable packet loss, maximum power consumption and minimum/maximum rate of power consumption etc. QoS protocols may take only one attribute as their constraint or more than one attribute as multiple constraints to optimize the network. These constraints can be applied on different layers of the network. However it complicates the QoS provisioning methods but it also ensures the promising quality results. Table 1 provides a list of metrics which are usually considered for checking quality of the established network or for measuring performances of different QoS provisioning methods.

4. EFFICIENT STRATEGIES IN PRACTICE FOR QoS

QoS promising not only requires confronting for reservation and distribution of critical resources but also requires an efficient management of admitted QoS sessions so that no session utilizes the whole resources and also no session remain starved of resources. Approaches for QoS provisioning have been classified into many categories [21]. First approach is based on the guarantee of meeting QoS requirements. It is hard QoS provisioning and soft QoS provisioning. In hard approach, QoS requirements of an admitted session are guaranteed to be met.

Table 1 QoS Metrics

Metrics	Used in different QoS provisioning methods
Available bandwidth	QoS Routing in Ad Hoc Wireless Networks [13]
Maximum acceptable jitter	Generalized Quality-of-Service Routing with Resource Allocation [37]
Energy consumed per packet	Power-Aware Routing in MANETs [2]
Buffer space	Routing Protocol with QoS Guarantees for Ad-Hoc Network [14]
Distribution of routing load	Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks [8]
Minimum/maximum throughput	QoS Routing in Ad Hoc Wireless Networks [13]
Maximum acceptable packet loss	A Position-Based QoS Routing Scheme for UWB MANETs [3]
Maximum acceptable end-to-end delay	Distributed Quality-of-Service Routing in Ad Hoc Networks [38]
Stability of link	Link Stability Models for QoS Ad Hoc Routing Algorithms [7]
Delay in channel contention	QoS Routing Using Lower Layer Information in Ad hoc Networks [39]
Trusted links for path selection	MRPC: Maximizing Network Life-time for Reliable Routing in Wireless Environments [6], A QoS Routing Method for Ad Hoc

	Networks Based on Genetic Algorithm [40]
Node's stability with its relative neighbors	Hybrid Ad Hoc Routing Protocol — HARP [9]
Ratio of Signal-to-interference in a link	On-Demand SIR and Bandwidth Guaranteed Routing with Transmit Power Assignment in Ad Hoc Mobile Networks [4]
No. of retransmissions required over a link	QoS Provisioning using BER-Based Routing in Ad Hoc Wireless Networks [5]
Residual battery on a node/ average life of a node	Power-Aware Routing in MANETs [2], MRPC: Maximizing Network Life-time for Reliable Routing in Wireless Environments [6]

There is an end-to-end path between source and destination node and resources are kept reserved until the acquired QoS session ends. Problem in this approach is that resources once allocated cannot be shared with other flows until the session ends and may get wasted if not fully utilized by the application. Best example of this approach is ATM (Asynchronous Transfer Mode) network. In soft approach, resources are not guaranteed for the whole session instead they are reserved only for short time intervals. When an application needs resources, it is been allocated and when the resources are not in use then they get allocated to any other application. It chooses the data traffic based on their priority. Best example of this approach is VoIP, video sharing etc. Second approach is based on mechanisms that are maintaining route information. It is proactive, reactive or hybrid mechanisms approach. Proactive mechanisms are based on storing and updating the route information in routing tables. Reactive mechanisms are used for on demand route requests. Therefore no routing tables are maintained and in hybrid approach it depends upon the requirements whether it needs the information to be maintained on each node or it wants to generate the route on request. The third approach is stateful and stateless approach. In stateful approach, each node is already configured by a unique address and a global address table which stores all network nodes' addresses. In stateless

approach, there is no global address table is maintained. Each node is assigned an address on its own. But it does a verification process to check the duplicate addresses present in the network. Stateful approach is difficult to implement in real time environment because it needs extra overhead in maintaining all the addresses. In case a node fails or a node moves in or out to the network, it requires to update all paths related to that node's address. This becomes more complex in large network whereas stateless approach is more feasible as compared to stateful approach. It has less overhead. The fourth approach is based on interaction between QoS provisioning mechanisms, network and MAC layer protocol. When interaction goes between network routing protocol and a QoS provisioning mechanism for finding feasible routes in the network, it is called as coupled approach. When interaction is done between network layer and MAC layer to exploit the acute reserved resources on founded feasible routes, then it is called as decoupled approach. The fifth approach is dependent and independent approach. When a QoS provisioning method is dependent on the underlying routing or MAC protocols then it is called as dependent approach and when it is transparent to any underlying protocol, then it is called as independent approach. In this section, we have highlighted the methodologies used in some novel protocols that have tried to meet multiple QoS constrains and solved many other problems too like hidden node problems, redundancies in the networks, link failures etc. Table 2 shows the methods we have surveyed with their special features, requirements and assumptions and at the end of this section, table 3 is given which shows the metrics used in the surveyed methods for measuring their performances and for route discovery.

4.1 QoS-Aware Routing based on Bandwidth Estimation for Mobile Ad hoc Networks

In [22], L. Chen et al proposed a QoS routing protocol based on AODV routing protocol. It integrates an admission control mechanism with a feedback mechanism. This mechanism includes current network state as feedback to the application to appropriately adjust the amount of data they transmit. The unique part of this protocol is that it uses bandwidth estimation to react to network traffic.

Table 2 Requirements And Assumptions In The Surveyed Methods

Surveyed methods	Special features	Requirements and assumptions
QoS-Aware Routing Based on Bandwidth Estimation for MANETs [22]	Two new schemes Hello-Listen bandwidth estimation are added and Immediate hello packet for releasing resources.	This protocol is for nodes running IEEE 802.11 medium access control. From source to destination, it requires knowledge of available end-to-end bandwidth along the route.
QoS-enabled ant colony-based multipath routing for MANETs [23]	Forward ants and Backward ants to select high valued route from multiple routes and avoid loops.	Path would be selected based on node's stability and path preference probability.
Gateway Discovery Algorithm Based on Multiple QoS Path Parameters Between Mobile Node and Gateway Node [24]	Stressed upon communication between infrastructure and infrastructure-less networks.	It assumes that all gateway nodes are equipped with 802.11b interface and are accessible to all network nodes which are having route to gateway node.
Bandwidth-Satisfied Multicast Trees in MANETs [25]	Generates bandwidth satisfied multicast trees to estimate shortest routes and solves hidden route and hidden multicast route problems.	IEEE 802.11 DCF (distribution coordination function) is used as the MAC-layer protocol. Unslotted CSMA/CA method is used to send

		packets.
Distributed Fault-Tolerant Quality of Wireless Networks [28]	Fault tolerance, allocation/deallocation of resources to/from nodes/failure nodes, link repairs at the site	<p>Each node has a unique identifier.</p> <p>If Euclidean distance of two nodes is ≤ 30 m (as in 802.11g), then they can be the members of same cluster.</p> <p>It is assumed that CFSR has converged with the relevant features of EFDCB.</p> <p>It is assumed that applications having soft QoS constraints use adaptive techniques to reduce QoS disruptions.</p> <p>Combinatorial stability is also assumed.</p>

To find the available residual bandwidth at each node, it uses two bandwidth estimation methods to maintain new flows. One method (“Listen” Bandwidth Estimation) is for hosts to listen to the channel and estimate the available bandwidth based on the ratio of free and busy times. In this scheme, IEEE 802.11 MAC utilizes both physical and a virtual carrier sense through network allocation vector (NAV), to determine free and busy times. If NAV’s value is less than the current time and receive/send state is also idle then it means channel is free. MAC sets the channel busy when NAV sets a new value and receive/send state also changes from idle to any other state. The other method (“Hello” Bandwidth Estimation) is used to re-allocate the available bandwidth when routes break. In this scheme, the sender’s and its one-hop neighbor’s current bandwidth usage is piggybacked in the “Hello”

message. Then each host calculates its available bandwidth based on the piggybacked information received via “Hello” messages and knowledge of the frequency reuse pattern. Hence, each host estimates its residual bandwidth based on information from hosts within two-hops. They have modified the “Hello” message to include two fields. First field includes host address, consumed bandwidth, timestamp and second field includes neighbor’s addresses, consumed bandwidth and timestamp. The residual bandwidth is estimated by subtracting overall consumed bandwidth from the raw channel bandwidth, divided by a weight factor. The design of this protocol and its routing features supports two kinds of applications. First is where the minimal bandwidth must be guaranteed and the second is where the application can adjust its coding rate according to feedback received from the network.

Table 3 Metrics Used In The Surveyed Methods

QoS Metrics		Surveyed methods				
		[22]	[23]	[24]	[25]	[28]
Metrics used in measuring protocol’s performances	End-to-end delay	•	•	•		
	Packet delivery ratio	•	•			
	Power consumption per hop	•		•		
	Minimal residual bandwidth	•	•		•	
	Overall end-to-end throughput	•		•	•	•
	Hop count		•	•		
	Path success ratio		•	•		
	Routing overhead with mobility		•			
	Packet delivery ratio with mobility/ varying no. of nodes		•			
	Data packets receiving ratio				•	
	Admission ratio				•	
	No. of control bytes generated per second				•	
	Connection/Failure recovery time					•
	No. of dropped packets		•			•

	Amount of sustainable flow bandwidth					•
Metrics used for route discovery/setup	Residual bandwidth estimation	•			•	
	Stability of nodes		•			
	Path preference probability		•			
	Next hop availability		•			
	Node availability		•			
	Link availability		•			
	Path availability time period				•	
	Available load capacity				•	
	latency				•	
	Minimum hop count				•	
	Power consumption		•			

Route discovery phase:

To initiate route discovery, the source node sends a route request (RREQ) packet whose header is modified to model-flag. This model-flag shows whether the source is using admission scheme or adaptive feedback scheme. When an intermediate node gets RREQ packet, it first calculates its residual bandwidth and checks the model-flag. If it shows admission scheme, the node compares its residual bandwidth with the requested bandwidth. If its residual bandwidth is greater than the requested bandwidth, it forwards the received RREQ; otherwise discards. If model-flag shows adaptive feedback scheme, the node compares its residual bandwidth with the min-bandwidth field in RREQ packet. If its residual bandwidth is greater than the min-bandwidth, it forwards the RREQ packet; otherwise, it updates the min-bandwidth value using its residual bandwidth. Finally, the destination node sends modified RREP (route reply) packet which is further updated by the intermediate nodes in between when they receive this RREP along the route to source node.

Route maintenance phase:

A forced cache update scheme is included for releasing the bandwidth used by the broken path. In this scheme, two separate packets (Immediate Hello packet and Error packet) are used to release the bandwidth from all neighboring nodes. But it cannot be done by broadcasting an “Error” message because it is a unicast packet. “Error” packet is used to stimulate updation of bandwidth consumption registers and the propagation of “Immediate Hello” packets. When a node gets an “Immediate Hello” packet, it sends its regular “Hello” packet immediately and when node gets an “Error” packet, it subtracts the amount of bandwidth that the broken route consumes from its bandwidth consumption register to reflect the bandwidth allocation changes. The route discovery process is reinitiated after the source node receives the “Error” packet.

4.2 Quality-of-Service-enabled ant Colony-based Multipath Routing for Mobile ad hoc Networks

In [23], P. V. Krishna et al proposed a QoS enabled ant colony based multipath routing (QAMR) algorithm to solve bandwidth allocation problem in MANETs. In this approach, foraging behavior of ant colony is applied to select path based on the stability of nodes and path preference probability (probability to select a particular path of higher preference value from all the available paths). Authors have used ant-like agents called forward ants or reactive FANT that are generated by source node for finding multiple routes to destination node and backward ants (BANT) that return to set up the paths. These agents are used to measure several parameters like next hop availability (NHA), delay and bandwidth for satisfying QoS constraints. NHA calculates path preference probability to find the availability of next node and link for transmitting data where next node’s availability is calculated in terms of its remaining battery time. Nodes with the longest remaining battery time are selected for the construction of long live path from source to destination. Pheromone tables are used to represent paths with their preference values.

Route discovery phase:

In this phase, source node checks its trusted neighbors and selects the nodes having NHA higher than the predetermined threshold value. This is done to broadcast FANT only to the trusted neighbors and to reduce the routing overhead. When FANT agent is received by an intermediate node, it first checks whether its own address is already present in agent’s path field. If its address is present, it immediately discards the FANT to avoid loops. If not, it attaches its address to FANT and broadcasts further to all of its trusted neighbors until it reaches to destination node. FANT maintains a stack in its path field where it stores all the visiting nodes. At each intermediate node, it collects information about processing delay, transmission delay of each link and its available capacity and the number of hops visited. The destination node

waits for FANT for time interval $T_w = CT_d$, where T_d is end-to-end time delay for the first FANT received and C is an integer constant to receive all the FANTs. On reaching destination, based on the calculations of path preference values by popping up the visiting nodes in the stack, the destination node generates BANT only for the paths that satisfy QoS constraints and unicast it to the source node. All intermediate nodes who receive BANT, update their pheromone tables by using path preference probability which is based on the calculations of NHA, bandwidth and delay values received from FANT at the destination node. BANT gets discarded on the intermediate node if it does not find the same node along its route to source due to node's movement. If source node receives multiple BANTs then it selects node with higher pheromone value for data transmission and if nodes have no neighborhood relationship or link is lost then the pheromone value on that link becomes zero. For establishing relationship between nodes, hello messages are periodically broadcasted between them and when relationship establishes; an initial pheromone value 0.1 gets deposited on that link. Pheromone value also gets decay by a Factor ρ on that link if data is not transmitted for a finite time interval T_{decay} .

Route maintenance phase:

Routing load on the nodes having high pheromone value in the selected route may increase due to the repeatedly use of that path. It may cause depletion of node's resources and addition of more delay. To avoid this, the path preference probability of that path calculated by NHA is checked periodically and then automatically reduced. If NHA value of a node drops below threshold value, then that node sends a message to its predecessor node that it has become off. This message is notified to the predecessor node so that it can choose another alternate route without depleting its resources on that node. To maintain these alternate routes, whether they are in use or not, a check is maintained at regular time intervals to validate them.

4.3 Gateway Discovery Algorithm based on Multiple QoS Path Parameters between Mobile Node and Gateway Node

In [24], S. H. Bouk et al proposes a gateway selection scheme in which some gateway nodes equipped with multiple interfaces are used to provide communication between the infrastructure network and the infrastructure less network. If a MANET node wants to send data to node in the infrastructure network, it computes the overall QoS value of each path (δ_i) from its routing table and chooses the potential gateway that has a path with maximum QoS value, δ_i . A feedback scheme is also introduced to update the route dynamics. In this scheme, gateway nodes are selected and accessed from the route having maximum available load capacity. The residual load capacity of a route is the minimum available load capacity of a node along the route from source to destination.

Selection of path to the gateway node:

The overall QoS value (δ_i) of a route i between a MANET node and a gateway node, is calculated as $(L_i/L_{max}) + (C_i/C_{max}) + (Y_{min}/Y_i)$ where L_i/L_{max} represents minimum/maximum path availability period, C_i/C_{max} represents overall residual path load capacity/maximum residual path load capacity, and Y_{min}/Y_i represents the minimum path latency/ additive measurement of latency on each link between the gateway and mobile. After computing the overall QoS, for every route to the gateway node, a gateway node is selected by the MANET node. Route with

maximum QoS value, δ_i is selected by the MANET node.

Initially each gateway node periodically broadcasts a message Gateway Advertisement (GW_ADV) within a proactive region of k -hops which includes its current parameters and available capacity. When a MANET node i in proactive region receives this message, it computes minimum path availability period, L_i and overall residual path load capacity, C_i , then it updates its routing table and modifies GW_ADV and further forwards this message into the network.

In the reactive region, MANET node j sends GW_DISC message to discover the gateway node. This message is processed at every hop and forwarded until it is received by any node in the proactive area or a gateway node. If a node k in the proactive area receives gateway discovery message GW_DISC, it sends a unicast gateway advertisement message GW_ADV to the sender of the GW_DISC. Before sending GW_ADV to the sender of the GW_DISC, node k of proactive region compares L_i and C_i parameters in its routing table with the parameters of received GW_DISC message and adds the GW_ADV message with minimum of both parameters L_i and C_i along with the additive path latency, Y_i and the latency of GW_DISC message. On receiving GW_ADV, the MANET node updates its routing table and intermediate nodes on active route also unicast these route update messages to the source nodes when a new link is trying to create through this active route or an old connection is terminated. All this is done to discover the best available path to the potential gateway node.

4.4 Bandwidth-Satisfied Multicast Trees in MANETs

In [25], C. C. Hu et al proposed a bandwidth-aware multicasting protocol to minimize the number of forwarders in MANETs so that the consumption of node's battery and the bandwidth can be minimized. It also solves two bandwidth violation problems namely, hidden route problem (HRP) and hidden multicast route problem (HMRP) that are found in MCDAR [26]. It generates a bandwidth-satisfied multicast tree to admit new flows with the requested bandwidths and assembles all information from the network to determine bandwidth-satisfied multicast routes. Each node in the network maintains its two neighbor tables for residual bandwidth estimation that are one hop neighbor table and two hop neighbor table. Every two neighbor nodes periodically exchange their one-hop neighbor tables via hello packets in order to maintain their relationship and the two neighbor tables. When a node i receives hello packet from node j , node i uses node j 's one hop neighbor table to update its (node i) two hop neighbor table.

Discovery of bandwidth satisfied multicast tree:

This protocol uses a procedure, named Shortest Routes to establish route to the destination node with minimum no. of hops. If violation of bandwidth occurs, the Shortest Route procedure invokes another procedure B_Violation. A node i violates the bandwidth if the bandwidth increment induced by the forwarders exceeds node i 's residual bandwidth. Hidden route problem can be avoided in ongoing flows that pass via one-hop neighbors of the forwarders who have passed B_Violation check. The Shortest Route procedure chooses the node that was not selected before and that is closest to the destination of the new flow. There may be multiple shortest routes generated for the destination. If the new flow is supported with a single route, then the bandwidth requirement can be satisfied. But if the new flow is carried with multiple routes simultaneously then it may violates the bandwidth.

This may cause hidden multicast route problem. To remove this problem, authors proposed a new procedure, named *B_Satisfied_MulticastTree*. It is a heuristic approach which set three parameters for the new flow, namely, *vs* (source/server of new flow), *D* (set of destinations/clients of the new flow), and *b_req* (bandwidth requirement of new flow). This tree is established by executing repeat-until loop iteratively till set of destinations i.e. *D* gets empty. In each of iteration, a client (say node *x*) which was not selected before and has minimum number of hops to the server, is chosen to establish connection with server (*vs*). Thus, all links gets established between the server and clients. Then the procedure *Shortest_Route* is invoked to determine bandwidth satisfied shortest routes from all the established links. This procedure uses related concepts of *ODMRP* [27] in generating multicast trees and integrates some new features. The authors have used *b_join_query* and *b_join_reply* as two new routing control packets to discover bandwidth satisfied multicast trees. *b_join_query* includes hop count from server (*vs*) and it is initially set as zero and broadcasted by the server when it wants to start a new flow with certain bandwidth Requirement (*b_req*) to the clients. When a client node (say node *y*) receives this query, it checks whether hop count in the query is less than the maximum hop count (*maxhopcount*) – 1 and if it is less, then it increments the hop count by 1 and further transmits the query to its neighbor nodes and waits for *b_join_reply* for a certain time period. If hop count is equal to the *maxhopcount* – 1 then it does not further transmit the query, it replies to the server with *b_join_reply*. In case it has further transmitted the *b_join_query* and if time outs, then client node *y* replies *b_join_reply* back to the server which initially broadcasted the *b_join_query*. Now this reply query contains all the neighbors of client node *y*. This procedure runs till *D* (set of destinations/clients of the new flow) gets empty and the server *vs* discovers a bandwidth-satisfied multicast tree.

Recovery of Bandwidth-Satisfied Multicast Trees:

Links connection-disconnection due to node's movement form inadequate multicast trees. To recuperate from them, authors proposed a distributed algorithm in which the client node maintains a check whether the packet receiving ratio is bandwidth satisfied or not. If it is not satisfied with the route to server, it executes the distributed algorithm and finds a new route which satisfies bandwidth requirements. In this case, a new control packet is used, named *b_recovery_query* which is broadcasted by the client to search a new route to its neighbors. This query consists of set of forwarders *F* that are found in the route. When a neighbor node receives the recovery query, it checks whether the requested bandwidth in this packet is causing bandwidth violation or not. If it is causing violation, it discards the query. Otherwise, it swaps the set of forwarders in the query with its own set and further forwards the query. When another client node along the

existing multicast tree collects *b_recovery_query*, it sends *b_recovery_reply* as a reply to the client who broadcasted the *b_recovery_query*. This recovery query traverses in reverse route. The client node receives multiple copies of this message but it selects that *b_recovery_reply* which is traversed from the shortest route (i.e. minimum no. of hops) and reconnects to the server.

4.5 Distributed Fault-Tolerant Quality of Wireless Networks

In [28], L.C. Llewellyn et al, proposed an Extended fault distributed cluster based algorithm (EFDCB) that provides fault tolerant QoS in MANETs by addressing two main problems i.e. QoS link failure recovery which is done near the failure point and links stability. Authors have used and modified existing algorithms [29], [30], [31], [32] to remove some of their limitations and to achieve more fault tolerance, scalability, minimized redundancy in control messages and efficiency by adding some more QoS techniques like negotiating paths before choosing feasible path, resource allocation-deallocation from the failure nodes. There are two techniques for failure recovery. One is to reroute the traffic from neighbor of the failed node instead of rerouting from source node again. Also it does not require the precursor node of a failed node to be capable of reaching failed node's successor. Second is multilevel path redundancy which uses multiple paths for routing the same traffic according to the critical need of QoS

Initialization of clusters and repair of links:

When a node joins the cluster, it executes the initialization procedure to determine its role in the cluster and seeks whether there is a cluster head with higher weight than it. If a cluster head is already present with higher weight, then the node joins it and sends a message to the cluster head about its associated connections, all available resources so that the cluster head update its cluster table. If it sees no other node present with higher weight then it becomes cluster head. The new cluster head checks the no. of already present cluster heads in the cluster. If they are greater than $K=0$, which is used to control the spatial density of cluster heads, then it sends a RESIGN message for the cluster head having lowest weight who violates the *K*-neighborhood condition. When $K=0$, the node having largest weight replaces all cluster heads in the range having lower weight than the node now become cluster head. In this algorithm, cluster head of each cluster stores information regarding all supported QoS connections and available resources of its cluster and shares this information with all its members. If an intermediate node becomes defunct node *D* (node having fault), then before the occurrence of fault in it, the cluster head again calculates the new feasible routes in the cluster and selects those routes that satisfy its QoS constraints.

Table 4 What QoS Constraints Met And Where They Lag?

Surveyed methods	Compare d with	QoS constraints met	Weaknesses
QoS-Aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks	AODV [16]	<ol style="list-style-type: none"> 1. Its hello bandwidth estimation scheme avoids generating extra control messages. 2. Frequency can be used again outside of the second neighbouring node's range. 3. Improvement in packet delivery ratio for high requested loads. 4. Overcomes hidden node problem. 5. Packet delivery ratio rises with increasing weight factor. 	<ol style="list-style-type: none"> 1. Its listen bandwidth estimation scheme counts only the used bandwidth. It doesn't differentiate the corresponding bandwidth cost for each flow. When a route breaks, accuracy of bandwidth estimation gets affected. 2. Listen scheme uses large weight factor to avoid congestion and the overheads caused by RTS and data packet retransmissions due to fading errors which may alter the required weight factor's value. 4. Doesn't perform well for fast changing networks. It is designed and tested for low mobility networks. 5. No predictive scheme is applied to find a new path before the old one gets fail. 6. Shadowing affects node's transmission range and causes variations in it.
QoS-enabled ant colony-based multipath routing for MANETs	AODV, ARMAN [33]	<ol style="list-style-type: none"> 1. QoS success rate, packet delivery ratio, throughput is higher. 2. Network lifetime is increased. 	<ol style="list-style-type: none"> 1. More number of control packets is required during route discovery and during continuous monitoring/searching of existing/new routes. 2. Routing overhead is slightly higher.
Gateway Discovery Algorithm Based on Multiple QoS Path Parameters Between Mobile Node and Gateway Node	QoS-aware adaptive Internet gateway selection in AWIAN[34], LLR[35]	<ol style="list-style-type: none"> 1. Selects more stable, real time and less congested path with minimum load and latency. 2. Improves network throughput. 3. Reduces packet loss. 4. Improves end-to-end delay performance. 5. Reduces energy consumption and control overhead. 6. Improves success rate. 	<ol style="list-style-type: none"> 1. Weighting factors applied for computing overall weight are application specific. 2. In feedback mechanism, a source node has to remain intact with the status of the route which may waste the resources.
Bandwidth-Satisfied Multicast Trees in MANETs	Heu, Opt and MCEDAR [36], [26]	<ol style="list-style-type: none"> 1. Improves network throughput. 2. Network performance increases when admission ratio goes up. 3. Admission ratios are higher. 4. Reduces the no. of forwarders. 5. Avoids hidden route problem and hidden multi-route problem. 6. Generates fewer control bytes per second in mobile nodes. 	<ol style="list-style-type: none"> 1. Receiving ratio drops drastically on bandwidth violation. 2. Slightly increase in no. of control packets per second when the group size increases. 3. When multicast groups exceed 5, admission ratio becomes lower as a result of few extra control packets produced.
Distributed Fault-Tolerant Quality of Wireless Networks	FDCB [29]	<ol style="list-style-type: none"> 1. Provides scalability, efficiency, and fault tolerance. 2. Reduces routing control messages redundancy and packet drops. 3. Reduces the effect of a connection failure. 4. Traffic is expected to be serviced at a higher rate. 5. Connection reestablishment is faster. 6. It continues to function properly up to 100 failures per second. 7. Resistant to variations in distance between the cluster-head of a failed node and the sources using resources on that failed node. 8. It is tested on all failure rates and claimed to be more than two times faster than the global rerouting alternative. 9. Negotiates only few links for finding feasible QoS paths. 	<ol style="list-style-type: none"> 1. It is not discussed how failures are handled. 2. Problem of alleviating the impact of an unpredicted node failure on QoS is not considered. 3. Does not employ feedback implosion avoidance. 4. Does not execute updates fast enough to have a precise view of the network state.

In case of gateway node, before it becomes defunct node (DGWN), the cluster head selects a potential gateway node (P-GWN) having next highest weight in descending order that can satisfy the QoS constraints which the DGWN used to satisfy when it was in good condition. After selecting P-GWN, cluster head allocates it with required resources and the precursor node to DGWN restores its route by shifting its traffic through this P-GWN when it does not receive a beacon from DGWN for a specific time period. Cluster head then directs all its cluster nodes to support QoS connections via message REPAIR. If the available resources cannot satisfy QoS connections, then the cluster head sends a message FAILED_CONNEX (i.e. failed connection for that QoS path cannot be repaired) to all nodes which were consuming resources on that failed node and no route changes are executed in that cluster. In case cluster head fails, then the cluster node with next higher weight in descending order becomes new cluster head and tries to repair connections of previously failed cluster head. Otherwise if this cluster node does not support QoS connections of the failed cluster head, it waits for a specific time for other cluster node (to become cluster head) which has next higher weight in descending order from failed cluster head.

De-allocation of resources:

When the source node 'a' is to route new traffic from the node 'b', it checks its cluster members table to confirm if node 'b' is present in the set. If yes, then its (node b) available resources are obtained from cluster QoS table and they get reserved till the session ends. If the destination node is present in another cluster, then source node 'a' forwards the message PATH (a.rsrcs, dst) to the gateway nodes to request resources from each node (say node c) along the new established potential QoS connection to destination node. On receiving this message, node 'c' (if it is a destination node) checks its availability table to see if it has the required resources to allocate. If yes, then it responds with message CTS (a) which navigates back to the source node 'a'. Otherwise, simply drops the message PATH. After sending CTS (a), it waits for a specific time interval to receive data packet. If time outs and no data packet is received then it de-allocates the allocated resources. If node 'c' is an intermediary node, then it starts its countdown timer for receiving the associated message CTS (a) from the destination node. If counter expires and no CTS (a) is received, then it de-allocates the resources.

5. SUMMARY

In [22], we studied two bandwidth estimation schemes which outperform each other in different scenarios. "Hello" bandwidth estimation scheme is better than "Listen" scheme in mobile topologies and has better end-to-end throughput because if route breaks by losing "Hello" messages, then the other flows used the underestimated bandwidth. But in "Listen" scheme, when the route breaks, the node has no knowledge of the bandwidth consumed by each node in the broken link. Therefore it is unable to release the occupied bandwidth immediately which eventually affects the accurate bandwidth estimation. Therefore it slightly drops the end-to-end throughput. In static topologies, both of these schemes perform likewise by using large weight factors which reduces the accidental loss of "Hello" messages that incorrectly signals a broken route and cause congestion. But "Hello" scheme has slightly extra overhead than the "Listen" scheme because it appends "Hello" messages with the information of bandwidth consumed by neighbor node. This method also obscures hidden nodes effect by leaving extra bandwidth for them. It has some more flaws that the overhead caused by the

retransmission of RTS, CTS, and ACK packets due to fading errors affect differently on different size of packets. Therefore, different weight factors are used for different size of packets.

In [23], routes are selected based on path preference probability metric which is computed by next hop availability (NHA) metric. NHA is further computed by taking other metrics that are node availability, link availability, battery life etc. Hop count is another key metric considered for path computations. This protocol incurs additional overhead of control packets for periodically updating the paths and for searching new paths using FANT and BANT messages. So, it has slightly higher overhead as compared to AODV. But it has higher packet delivery ratio than AODV because it also considers other metrics like node stability and link stability. The advantage of using multiple paths and path preference probability is that when source node receives active route failure message due to node mobility, then it at once invalidates that failure link in its routing table and chooses another best valid route from its routing table. This protocol also shows increase in the network's lifetime because nodes with the longest remaining battery time are selected for the construction of long live path from source to destination.

Algorithm [24], has considered path availability time period as an important metric to select a potential gateway between two networks. This metric specifies the total time a MANET node takes to access the gateway node and it is computed by evaluating the minimum link availability period between intermediate nodes along the path between a MANET node and a gateway node. The other metrics used are path latency and residual path load capacity on which different weighting factors are applied for computing overall weight. These weighting factors are application specific and it is claimed that this algorithm even increases throughput in case low weight is assigned to one of the three metrics. Another good approach of this scheme is that it also incorporates feedback mechanism which allows source node to remain intact with the status of the route which makes it more practical and therefore reduces end-to-end delay and congestion.

In [25], there is a slight overhead of generating and recovering bandwidth-satisfied multicast tree because it needs additional control information especially in case the number of nodes increases. Authors have evaluated in their results that admission ratio goes lower when multicast groups exceed 5 because it also increases the number of forwarders and therefore extra control packets need to be produced. But as compared to MCEDAR [26], it performs still better. Moreover, the main strength of this approach is that it removes hidden route and hidden multicast route problems.

In [28], the gateway node connecting the two clusters has all information about the routes to the destination node present in one cluster and the source node present in the other cluster. So, redundancy of routing control messages in the network and connection failures also gets reduced. Thus, it reduces the overhead of rerouting from the source node on connection failures. So, it is efficient in connection reestablishments. One more unique feature of this protocol is that when a node allocates its resources, it waits for a certain time period and if it does not get response within that time limit, it de-allocates its resources. Thus, it helps in reserving resources for another flow. Authors have shown in their result that this extended version of FDCB performs better as compared to FDCB [29] by comparing total failures per second. It has shown less packet drop and increased throughput. But the flaw of this approach is that unexpected node failures are not considered,

in that case, there is only one option of rerouting from the source node. Moreover, if routing load is higher and there are frequently high rate of link failures, then its performance goes slightly down.

6. CONCLUSION

In this paper, we have explored those methods that are not only satisfying throughput and delay constraints but also have dealt with other worthwhile constraints like removing hidden node problems, multipath problems, improving scalability, distribution of acutely critical resources that is distribution of bandwidth according to the application's needs and consumption of battery power according to the work load of the application or it's another status (either node is idle or utilizing the resources unnecessarily). In section II, we have highlighted various common aspects in MANETs that are really needed to be discussed before thinking of QoS metrics and applying constraints. Table 1 in section III has listed the general QoS metrics that are commonly stressed upon in every QoS provisioning technique. In section IV, we have discussed in detail the surveyed methods that have tried to meet more than one or two QoS constraints. Special features of the surveyed methods, their requirements/assumptions and metrics are mentioned in table 2 and table 3. In section V, we have summarized with the surveyed method's constraints that are met and also listed some of their weaknesses and the other protocols that are compared to these surveyed ones in the Table 4. Lastly, it may conclude that a distinct strategy is required for pragmatic QoS approaches and to redistribute the different resources/services so that changes may not affect the other parameters and services on different layers. It is because if our application has no stringent constraints like time delays, cost etc. and it wants only throughput then what is the need of providing QoS in all layers. Providing QoS in all layers may make an approach more expensive and more complex. But if a user is bounded with all constraints especially cost, delay, bandwidth, throughput and others that we have discussed then all the implemented schemes may need to be redefined on every layer to get the desired results. Furthermore, a clear perspective of the application's requirements and its goals need to be set first in solving two main questions that what are our needs and what do we actually want from the network.

7. ACKNOWLEDGEMENTS

The Authors would like to thank the University Grants commission for funding the project titled Secure & QoS oriented Routing Protocol for MANETs. This work is the initial study of existing various QoS routing protocols & models proposed by various researchers in the area of ad hoc networks.

8. REFERENCES

- [1] S. Lee, G. Ahn, X. Zhang, and A. Campbell, "INSIGNIA: An IP-Based Quality of Service Framework for Mobile ad Hoc Networks," Proc. JPDC, 2000, pp. 374–406.
- [2] S. Singh, M. Woo, and C. S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," Proc. MobiCom, 1998, pp. 181–90.
- [3] Abdrabou and W. Zhuang, "A Position-Based QoS Routing Scheme for UWB Mobile Ad Hoc Networks," IEEE JSAC, 2006, pp. 850–56.
- [4] D. Kim, C.-H. Min, and S. Kim, "On-Demand SIR and Bandwidth Guaranteed Routing with Transmit Power Assignment in Ad Hoc Mobile Networks," IEEE Trans. Veh. Tech., 2004, pp. 1215–23.
- [5] N. Wisitpongphan et al., "QoS Provisioning using BER-Based Routing in Ad Hoc Wireless Networks," Proc. Vehic. Tech. Conf., 2005, pp. 2483–87.
- [6] Misra and S. Banerjee, "MRPC: Maximising Network Life-time for Reliable Routing in Wireless Environments," Proc. IEEE WCN, 2002.
- [7] Rubin and Y.-C. Liu, "Link Stability Models for QoS Ad Hoc Routing Algorithms," Proc. IEEE Vehic. Tech. Conf., 2003, pp. 3084–88.
- [8] E. Perkins et al., "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," IEEE Pers. Commun. Mag., 2001, pp. 16–28.
- [9] N. Nikaein, C. Bonnet, and N. Nikaein, "Hybrid Ad Hoc Routing Protocol — HARP," Proc. Int'l. Symp. Telecommun., 2001.
- [10] D. Shukla, L. Chandran-Wadia, and S. Iyer, "Mitigating the Exposed Node Problem in IEEE 802.11 Ad Hoc Networks," Proc. ICCCN, 2003, pp. 157–62.
- [11] C.E. Perkins, Ed., Ad Hoc Networking, Ch. 3, Addison Wesley 2001.
- [12] C.-K. Toh, "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks," IEEE Trans. Commun., 2001, pp. 138–47.
- [13] C. R. Lin and J.-S. Liu, "QoS Routing in Ad Hoc Wireless Networks," IEEE JSAC, 1999, pp. 1426–38.
- [14] M. Sheng, J. Li, and Y. Shi, "Routing Protocol with QoS Guarantees for Ad-Hoc Network," Electronics Letters, vol. 39, 2003, pp. 143–45.
- [15] D. Johnson, D. Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multi-hop Wireless Ad Hoc Networks in Ad Hoc Networking, ch. 5, Addison-Wesley, 2001, pp. 139–72.
- [16] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing," Proc. IEEE WMCSA, 1999, pp. 90–100.
- [17] E. Neely and M.J. Modiano, "Capacity and Delay Trade-Offs for Ad Hoc Mobile Networks," IEEE Trans. Info. Theory, 2005.
- [18] G. Aggelou and R. Tafazolli, "RDMAR: A Bandwidth-Efficient Routing Protocol for Mobile Ad Hoc Networks," Proc. ACM WOWMOM, 1999, pp. 26–33.
- [19] J. Mullen and H. Huang, "Impact of multipath fading in wireless ad hoc networks," Proc. ACM PE-WASUN, 2005, pp. 181-188
- [20] T. K. Sarkar, Z. Ji, K. Kim and A. Medour, "A Survey of Various Propagation Models for Mobile Communication", IEEE Antennas and Propagation Magazine, 2003, pp. 51-82
- [21] S. Misra, I. Woungang and S. C. Misra, Guide to Wireless Ad Hoc Networks. Springer-Verlag London Limited, 2009, pp. 297–302.
- [22] L. Chen and W. B. Heinzelman, "QoS-Aware Routing Based on Bandwidth Estimation for Mobile Ad Hoc Networks", IEEE Journal on SAC, 2005, pp. 561-572.
- [23] P. V. Krishna, V. Saritha, G. Vedha, A. Bhiwal, A.S.

- Chawla, "Quality-of-service-enabled ant colony-based multipath routing for mobile ad hoc networks", *Commun, IET*, 2012, pp. 76- 83.
- [24] S. H. Bouk, I. Sasase, S. H. Ahmed, and N. Javaid, "Gateway Discovery Algorithm Based on Multiple QoS Path Parameters Between Mobile Node and Gateway Node", *IEEE JCN*, 2012, pp. 434 – 442.
- [25] C. -C. Hu, E. -H. Kuang Wu and G.-Huey Chen, "Bandwidth-Satisfied Multicast Trees in MANETs", *IEEE Transactions On Mobile Computing*, 2008, pp. 712-723.
- [26] P. Sinha, R. Sivakumar, and V. Bhanghavan, "MCEDAR: Multicast Core-Extraction Distributed Ad Hoc Routing,"*Proc. IEEE WCNC*, 1999, pp. 1313-1317.
- [27] S.J. Lee and M. Gerla, "On-Demand Multicast Routing Protocol in Multi hop Wireless Mobile Networks," *ACM/Kluwer MONET*, 2002, pp. 441-453.
- [28] L. C. Llewellyn, K. M. Hopkinson and S. R. Graham, "Distributed Fault-Tolerant Quality of Wireless Networks", *IEEE Transactions On Mobile Computing*, 2011, pp. 175-190.
- [29] A.S. Nargunam and M.P. Sebastian, "Fully Distributed Cluster Based Routing Architecture for Mobile Ad Hoc Networks,"*Proc. IEEE WiMob*, 2005, pp. 383-389.
- [30] S. Chen and K. Nahrstedt, "On Finding Multi-Constrained Paths," *Proc. ICC*, 1998, pp. 874-879.
- [31] R. Ghosh and S. Basagni, "Mitigating the Impact of Node Mobility on Ad Hoc Clustering," *WiMob*, 2008, pp. 295-308.
- [32] G. Dimitriadis and F.N. Pavlidou, "Clustered Fisheye State Routing for Ad Hoc Wireless Networks," *Proc. IEEE MWCN*, 2002, pp. 207-211.
- [33] Deepalakshmi, P., Radhakrishnan, S.: 'Ant colony based QoS routing algorithm for mobile ad hoc networks', *Proc. IJRTE*, 2009, pp. 459-462.
- [34] B. N. Park, W. Lee, C. Lee, and C. K. Shin, "QoS-aware adaptive Internet gateway selection in ad hoc wireless Internet access networks," in *Proc. IEEE BROADNETS*, 2006, pp. 1-10.
- [35] M. Wu, W. K. G. Seah, and L. W. C. Wong, "A link-connectivity-prediction-based location-aided routing protocol for hybrid wired-wireless networks," in *Proc. ICMU*, 2005.
- [36] C.C. Hu, E.H.K. Wu, and G.H. Chen, "Bandwidth-Satisfied Multicast Trees in MANETs,"*Proc. IEEE WiMob '05*, pp. 323-328, 2005.
- [37] R. Bashandy, E. K. P. Chong, and A. Ghafoor, "Generalized Quality-of-Service Routing with Resource Allocation," *Proc. IEEE JSAC*, 2005, pp. 450-63.
- [38] S. Chen and K. Nahrstedt, "Distributed Quality-of-Service Routing in Ad Hoc Networks," *IEEE JSAC*, 1999, pp. 1488-505.
- [39] Z. Fan, "QoS Routing Using Lower Layer Information in Ad Hoc Networks," *Proc. PIMRC.*, 2004, pp. 135-39.
- [40] L. Barolli, A. Koyama, and N. Shiratori, "A QoS Routing Method for Ad Hoc Networks Based on Genetic Algorithm," *Proc. Database and Expert Systems Applications*, 2003, pp. 175-79.