MULTI-OBJECTIVE OPTIMIZATION ASSISTED NETWORK CONDITION AWARE QOS-ROUTING PROTOCOL FOR MANETS: MNCQM

Shashi Raj K[1] and Siddesh G K[2]

[1]Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru, India
[2]Department of Electronics and Communication, JSS Academy of Technical Education, Bengaluru, India

ABSTRACT

The exponential rise in wireless communication systems and allied applications has revitalized academia-industries to achieve more efficient data transmission system to meet Quality-of-Service (QoS) demands. Amongst major wireless communication techniques, Mobile Ad-hoc Network (MANET) is found potential to provide decentralized and infrastructure less communication among multiple distributed nodes across network region. However, dynamic network conditions such as changing topology, congestion, packet drop, intrusion possibilities etc often make MANET's routing a tedious task. On the other hand, mobile network feature broadens the horizon for intruders to penetrate the network and causes performance degradation. Unlike classical MANET protocols where major efforts have been made on single network parameter based routing decision, this research paper proposes a novel Elitist Genetic Algorithm (EGA) Multi-Objective Optimization assisted Network Condition Aware QoS-Routing Protocol for Mobile Ad-hoc Networks (MNCQM). Our proposed MNCQM protocol exhibits two phase implementation where at first it performs node-profiling under dynamic network topology for which three factors; irregular MAC information exchange, queuing overflow and topological variations have been considered. Towards this objective node features like Packet Forwarding Probability (PFP) at the MAC layer, Success Probability of Data Transmission (SPDT) of a neighboring node, and Probability of Successful Data Delivery (PSDD) have been obtained to estimate Node-Trustworthiness Index (NTI), which is further used to eliminate untrustworthy nodes. In the second phase of implementation, a novel Evolutionary Computing assisted non-disjoint best forwarding path selection model is developed that exploits node's and allied link's connectivity and availability features to identify the quasi-sub-optimal forwarding paths. EGA algorithm intends to reduce hop-counts, connectivity-loss and node or link unavailability to estimate best forwarding node. One key feature of the proposed model is dual-supplementary forwarding path selection that enables alternate path formation in case of link outage and thus avoids any iterative network discovery phase.

KEYWORDS

MANET, QoS communication, Node-trustworthiness, Network awareness, Evolutionary computing based routing decision.

1. INTRODUCTION

The exponential rise in communication system demands, especially wireless communication systems have revitalized academia-industries to achieve more efficient and Quality of Service (QoS) centric data transmission. On the other hand, the high pace increase in application and

DOI: 10.5121/ijcnc.2019.11401

allied complexities of the operating conditions has been making classical transmission protocols confined [1]. Static nature of Wireless Sensor Networks (WSNs) has given rise to a more effective and mobile network solution named Mobile-Adhoc Network (MANET). Amongst numerous wireless communication paradigms, MANET has been found more potential to enable infrastructure-less and decentralized data transmission to serve major communication demands. The infrastructure-less and decentralized nature of MANET enable it to be used under mobile network conditions and (Ad-hoc) network restoration purposes during certain natural calamity [1]. It can be formed by deploying multiple nodes working cooperatively under mobile topology without imposing need of sophisticated and complex network infrastructure. In addition, the nodes of MANET can function as routers as well to perform communication between two hosts by incorporating multi-hop routing scheme. Being a decentralized and infrastructure less network MANET undergoes significantly high topological changes and network condition's variation such as congestion, packet drop, retransmission, link outage, eavesdropping and packet loss caused due to certain malicious node. Such adversaries often results into QoS compromise. Noticeably, QoS compromise can be reflected in terms of reduced data transmission rate, higher latency, increased retransmission, bandwidth and energy exhaustion etc. On contrary, up surging wireless communication systems demand QoS and Quality of Experience (QoE) provision under dynamic network conditions [4]. Typically, MANET being a dynamic network topology often undergoes adversaries like link quality, link outage probability, data drop probability, resource unavailability etc [40]. The classical reactive routing models employ constrained node parameters to perform (best) routing decision; however dynamic nature of MANET and allied topological variations give rise to the probability of varying network (and/or node) condition. Furthermore, MANET has always been the victim of major network intrusion efforts where malicious nodes try to intrude the predefined network to cause either data-loss or QoS degradation [2-4]. Exploring in depth it can be found that in multi-hop transmission in addition to the malicious node, even the native (predefined and approved) nodes might behave haphazardly impacting overall network performance [1][4]. These nodes can behave irregularly casing link-outage, data drop, congestion or queuing delay or overflow etc, which eventually degrades QoS delivery [7]. In this case exploiting dynamic network and/or node condition for (optimal) best forwarding node (BFN) selection can be of utmost significance. BFN with suitable routing strategy can reduce link-outage probability [4], malicious caused premature link-outage, data drop, and retransmission. With this motive, in this research paper we have focused on developing a robust Dynamic Network (node) Profiling assisted BFN selection model for QoS delivery over MANETs. Though, a few efforts have been made to augment routing protocols for MANETs; however majority of the existing model either employ congestion probability [5] or link quality [41] to perform routing decision. In practice, there can be the condition where a malicious node with available bandwidth and network vicinity (i.e., within radio range) can be a part of the existing network and could cause attack or packet loss in later phase of data transmission. It signifies the need of a robust (node) trustworthiness estimation model of node-profiling strategy. The node-profiling of a node can help transmitter identifying optimal BFN to achieve and retain QoS delivery in MANETs. Such robustness can help a routing decision model to avoid false positive that can preserve QoS delivery in terms of reliable data transmission and minimum bandwidth exhaustion.

In this research paper the emphasis is made on monitoring and exploiting node characteristics over simulation period and identifying non-cooperative misbehaving nodes to isolate it for preserving or augmenting network QoS delivery. Unlike major classical MANET protocols where it is hypothesized that packet loss occurs due to malicious nodes alone, we have examined different other factors impacting packet loss. Furthermore, the focus is made on developing a node-trustworthiness model in conjunction with dynamic network topology to perform node-profiling that helps in achieving optimal routing decision. To perform node profiling or

trustworthiness estimation, it is vital to understand key factors signifying a node as malicious or suitable BFN. With this motive, in this paper we have exploited three key factors; irregularity at the MAC layer or improper information exchange at IEEE 802.11 MAC, queuing overflow and topological variations to perform node-profiling. Exploiting multiple dynamic node parameters such as Packet Forwarding Probability (PFP) at the MAC layer, Success Probability of Data Transmission (SPDT) of a neighboring node, and Probability of Successful Data Delivery (PSDD), we have estimated a factor called Node-Trustworthiness Index (NTI) that helps avoiding untrustworthy nodes. Furthermore, in this paper evolutionary computing assisted routing model is developed that performs dual disjoint best forwarding path selection by exploiting node or link connectivity as well as dynamic availability. In addition, it intends to maintain minimum hop while assuring best (dual) forwarding path with no shared (network) elements. This as a result intends to maintain network reliability as well as topological optimization assisted reliable routing so as to retain higher network performance.

The other sections of the paper are divided as follows. Section II discusses some of the key related works, while problem formulation for the current study is discussed in Section III. The detailed discussion of the proposed MNCQM routing protocol is given in Section IV. Section V presents the simulation results and its inferences, while the references used are presented at the end of the manuscript.

2. RELATED WORK

This section primarily discusses some of the key literatures pertaining to MANET routing protocols.

The dynamic nature of MANET requires a well defined and cross-information schematic across the IEEE 802.11 protocol stack [7]. Authors [7-9] have recommended using network (and/or node) information from the different layers of the protocol stack to make suitable routing decision. However, they [7-9] focused mainly on achieving QoS delivery by enabling timely and reliable data transmission. To assure reliability for data transmission over MANET the authors [10] applied retransmission and replication schemes. Unfortunately, such approaches increase delay, bandwidth and energy exhaustion that eventually degrades QoS delivery. Authors [11] applied multi-path transmission concept to achieve higher reliability; however it increased computational and signaling overheads depleting energy of the nodes. As an augmented solution, authors [11] developed Sequential Assignment Routing (SAR) that forms multipath in between source to the destination by forming multiple trees in which the root of the individual tree is a one-hop neighbor. Authors [11] applied residual energy of each node to perform routing decision, where the route with maximum energy was considered as Best Forwarding Link (BFL). In addition to energy, end-to-end delay of each path was considered for routing decision [12][39]. In [13] authors exploited link quality and number of hops as routing decision parameter to perform multipath transmission over sensor network. However, authors could not address the issue of mobility and dynamic routing decision under dynamic network topology which is common in MANETs. In [14][15], authors estimated cost of each path to assess its suitability as BFL in sensor network. Noticeably, these all approaches focus mainly on link based decision, while in practice a malicious node too can have sufficient node feature to become a part of route [6]. Interestingly, such malicious nodes could cause major QoS degradation and link outage in later phase of communication. An improved model was suggested in [14] where node-entropy was applied to identify best forwarding node (BFN); however its suitability with MANETs can't be assured.

MANETs with fixed buffer size was considered in [16], where authors applied Markov chain concept to exploit input rate-dependent throughput and packet loss ratio even under dynamic transmission scenario for route decision. Authors [16] employed queuing concept, end-to-end delay to assess the impact of deadline time (packet's end-to-end delay) and buffer size on network throughput, delay and packet loss. A multicast routing protocol for MANET was developed in [17] that constituted multiple multicast trees where each multicast tree meets a predefined bandwidth demands to support bandwidth efficient routing. To achieve reliable transmission network coding (NC) scheme was taken into consideration. In [18] kNN query concept was applied to perform query classification under dynamic network topology for better performance. Authors [18] applied Filling Area (FA) model to process kNN queries that resulted minimum overhead and search space. Authors [19] applied delay and bandwidth occupancy feature to perform routing decision in MANET. Residual energy was used as a objective function to perform routing decision in Ad-hoc On Demand Multipath Distance Vector (AOMDV) routing in MANET. The path with minimum energy was considered as BFL to perform multipath data transmission. A few efforts [20] have exploited clustering concept to perform routing decision where Genetic Algorithm (GA) was applied for Cluster Head (CH) selection. Clustering with node trustworthiness concept was applied in [21] to achieve reliable data transmission over MANETs. Weight based clustering was suggested in [22] to perform routing decision. Authors [22] applied node parameters like inter-node distance, radio range of the node and residual energy to perform routing decision. Cross layer concept was applied in [23] to augment routing decision where approached like enhanced Rate Monotonic Algorithm (RMA) and Earliest Deadline First (EDF) were applied at the network layer of IEEE 802.11 protocol stack. Authors in [24] recommended cross layer architecture where they considered node density, mobility and MAC queuing scheme to assist QoS delivery. Similarly in [25] cross layer model was recommended where optimization measure was incorporated at the network layer by reducing flooding overhead.

In addition to the network condition awareness based routing decision; authors have made effort to employ trust based routing in MANETs [26]. In a few efforts [26] watchdog and path rating models were applied so as to reduce the adverse affect of malicious nodes on network performance. However, this approach considered each packet drop as misbehaving node which can't be generalized in dynamic network conditions where there can be drop due to numerous reasons as discussed above. Further in [27-29] authors applied acknowledgment-based routing schemes. However, it [27] suffered signalling overhead due to iterative beaconing and acknowledgement by each consecutive node in path to the sender as well as receiver for each packet of data transmission. Though, being a better solution than [27], the model recommended in [28] could not address the issue of false malicious node detection and route changes that adversely affected fair-QoS delivery to each participating node. As an optimised solution authors [29] proposed an Enhanced Adaptive ACKnowledgement (EAACK) protocol to detect misbehaviour nodes in MANETs by applying DSA and RSA digital signatures. To assess packet loss rate in MANETs, authors [30] recommended using the Expected Packet Count (EPC) at the receiving node. Though, this approach was efficient for estimating packet delivery condition and allied loss rate, it could not rectify the loss problem in the network. In [31] authors applied received signal strength indicator (RSSI), the link quality indicator (LQI), and the packet reception rate (PRR) to perform routing decision in WSNs. However, this approach could not deal with dynamic topology and varying network condition. Authors [32] exploited inter-node cooperation features to detect malicious nodes in MANETs; however it suffered excessively due to conflicting node-status update and trustworthiness of the updates provided by neighbouring nodes. A defence trust model was developed in [33] that focussed on filtering second hand information by exploiting information like node-confidentiality, deviation and distance. Authors

[34] performed node's overhearing monitoring for intrusion identification. They found that overhearing results into reduced throughput and high latency. Node collaborative reputation based routing decision was suggested in [35]. In [36], authors recommended the use of node statistics such as the number of received forwarded packets etc to assess packet drop probability at a node in MANET.

3. PROBLEM FORMULATION

To ensure QoS provision and reliable data communication over MANETs enabling optimal route decision or forwarding path selection is of vital significance. Primarily, under mobile network condition where there is significantly high topological variation estimating the BFN is highly tedious task. However, to perform BFN selection under mobility maintaining efficient node table, network and node parameter state information is must. In addition, applying key node information to characterize suitability of a node to become BFN can also play vital role in QoS centric communication. In majority of the existing routing protocols authors have applied node parameters such as residual energy, packet drop per node, link quality, congestion probability etc as distinct node-parameters to perform routing decision. However, in practice even an interrupting node can have sufficient node parameters as stated above, but its inclusion in forwarding path formation can lead premature link-outage, data drop and hence reduced performance. To alleviate such kind of problems, authors have applied security model where predominant focus has been made on data security of node security; however to achieve QoS delivery with reliable data transmission exploiting both network dynamic conditions as well as node's trustworthiness is inevitable. Majority of the classical watchdog schemes often undergo issues like overhearing caused energy exhaustion. The use of network condition aware and trust based model can be of utmost significance to avoid any improper node consideration during forwarding path selection. This approach in addition could avoid immature link outage, intentional packet drop caused due to untrustworthy nodes. As an optimal solution, this research intends to incorporate a distributed time division-based node and allied link monitoring strategy so as to enable reliable transmission decision as well as premature link outage avoidance. In this paper both dynamic network conditions as well as node-trustworthiness have been taken into consideration. In this paper, at first Micro-Level Network Assessment has been performed that helps in identifying the key factors causing packet loss and QoS degradation in MANETs. Employing network condition as well as node-trustworthiness factor, BFN selection has been performed that not only assures optimal selection of the forwarding node but also avoids the malicious node that strongly augments QoS delivery and reliable data transmission over MANETs. Key decisive network condition parameters, factors such as MAC layer information, queue information such as flooding condition, and rate of link changes etc have been exploited to perform profiling for each node. In this research three key factors; irregular or improper information exchange at IEEE 802.11 MAC, queuing overflow and topological variations. Multiple node parameters such as Packet Forwarding Probability (PFP) at the MAC layer, Success Probability of Data Transmission (SPDT) of a neighboring node, and Probability of Successful Data Delivery (PSDD) have been estimated for each node for respective profiling that helps avoiding any untrustworthy node to become route member. In addition, to assure QoS centric communication over MANET, this paper proposes a robust evolutionary computing assisted topological optimization model that exploits node and link availability and connectivity features to achieve dual (supplementary) disjoint best forwarding paths. Here, the prime motive is to consider only those nodes or links with maximum availability and minimum connectivity loss while maintaining minimum hops and shared network component. This approach can efficiently achieve two parallel disjoint forwarding path with minimum hops (with minimum connected network elements) so as to ensure reliable

data transmission without imposing any computational overheads. Unlike classical Dijkstra minimum distance based approach, MNCQM applies the well known evolutionary computing algorithm Elitist Genetic Algorithm to perform (dual and disjoint) best forwarding path estimation. Here, the motive is to form two disjoint paths with minimum shared elements and hops while ensuring that the participating nodes have sufficient or suitable link and/or node availability and connectivity. This as a result could achieve better performance even under dynamic topology or varying network conditions.

4. PROPOSED METHOD

The overall design or implementation of the proposed MNCQM routing protocol can be presented in two consecutive phases. These are:

1. Node Profiling and Trustworthiness Estimation
2. Evolutionary Computing assisted topological optimization and dual-disjoint (best) forwarding path selection.

The detailed discussion of the proposed MNCQM routing protocol and allied implementation model is presented in the sub-sequent sections.

4.1 Node Profiling and Trustworthiness Estimation

Identifying the parameters having direct relation to the network performance (here, MANET) can be vital to design an optimistic routing model. Before designing the proposed routing model, a snippet of the key parameters influencing MANET's performance are given as follows:

Undeniably, in MANET's both dynamic topology as well as vulnerability of getting attacked due to malicious nodes are the critical factors affecting overall performance. To design a novel and robust routing protocol for MANETs, in this paper we have critically addressed the constraints influencing overall performance, especially causing data drop. These factors are:

1. IEEE 802.11e MAC information,
2. Queuing Overflow Condition, and
3. Dynamic Topology or Topological Variations.

A snippet of these key factors and allied solution is discussed in the sub-sequent sections.

4.1.1 IEEE 802.11e MAC information

In practice MANET might undergo packet drop condition at the MAC layer, especially at the forwarding node. Practically, the prime reasons behind data drop at MAC are obstacle routing entries or malicious nodes, suddenly imposed congestion, out-of-range from next hop node etc. It signifies that a well informed condition of the MAC layer of IEEE 802.11 protocol can be vital to assess data drop and make preventive measure so as to achieve QoS delivery. Observing IEEE 802.11 MAC standard, which is default protocol stack for MANET, a transmitter or forwarding node transmits targeted data packet and receives a link-layer ACK from the receiver [16]. Considering the significance of link quality towards QoS delivery, authors [16] recommending transmission of a beacon message or probe packet before transmitting the targeted actual data packet. In this process, each node required transmitting or broadcasting a probe signal or packet at

the interval of 10 seconds. However, such iterative probe packet transmission lead energy as well as bandwidth exhaustion. Unlike such classical approaches, in our previous paper [41], we designed a cross layer model where Adaptive Link Quality (ALQ) was obtained from proactive node table management scheme that enables our routing protocol to retain reliable forwarding node selection. Though, this approach was efficient to avoid selection of any link-vulnerable node selection; however could not address the characteristics and activities of a link between two nodes. Assessing link-characteristics can help performing link-profiling that eventually could enable optimal Best Forwarding Link (BFL) Selection. In our proposed model, to avoid energy and bandwidth exhaustion as occurred in [16], we focus on leveraging the beacon signal (say, HELLO signal) which is already exchanged in the routing activities. Here, each node performs node feature exchange with its neighbouring node at certain defined interval (here, 10 second). More specifically, in our proposed routing scheme, each node exchanges dynamic link information to its one-hop distant neighbour node by exploiting a preset number of beacon signals. In this process, each node maintains the retrieved beacon message (i.e., HELLO) pertaining to the on-hop distant neighbouring node. In case a node receives the expected number of beacon message from its one-hop distant neighbouring node it states that there exists suitable network-link condition and interference-less condition to make BFL decision. On contrary, in case a node finds a link behaving irregularly and dropping packets it signifies that the link and allied node is vulnerable. In addition, in case a node doesn't receive any beacon message, specifically the total expected number of HELLO messages, it signifies the presence of certain link-interference or vulnerabilities. In our proposed MNCQM protocol, addition to the one-hop distant neighbouring node, the Best Forwarding Node (BFN) too exchanges its dynamic node information to the neighbouring node that enables reliable BFL selection for QoS centric communication. Thus, employing this information, a node P can estimate the likelihood whether a node can transmit data successfully to the destination node Q. Exploring link quality and its reliability at the link layer between these two nodes can help establishing a secure and fault resilient transmission. In this paper the Packet Forwarding Probability (PFP) at the MAC layer has been estimated using (1).

$$P_M = \frac{\mu_{recv(t_{i-1},t_i)}}{\mu_{exp(t_{i-1},t_i)}} \quad (1)$$

In above equation (1), μ_{recv} signifies the total number of beacon message of HELLO packets received, while μ_{exp} states the total expected number of beacon message during transmission time (t_{i-1}, t_i). In addition to the PFP sensitive routing, we have focussed on assessing "Queuing-Overflow" to ensure reliable data delivery.

4.1.2 Queuing Overflow Conditions

In typical MANET network, data queues might undergo overflow condition because of the sudden increased payloads, multiple simultaneous activities and buffer consumption. In addition, the simultaneous node activities such as functional-as-routers for multi-hop forwarding too impose queuing overflow. When the route-traffic exceeds a suitable limit or threshold its results into limited data traffic, low data rate transmission that eventually causes QoS violation [31][32]. Practically, the node-queuing overflow can be visualized in terms of data drop by neighbouring or forwarding node, whose selection as BFN can lead unreliable path (say, BFL) selection. Such nodes can cause link-outage of data drop abruptly. Thus, identifying such misbehaviour node can help avoiding any probability of link-failure or data loss. With this motive, in this paper identifying a forwarding node with packet dropping behaviour, it has been marked as a

misbehaving node which has been further excluded to become a part of BFL. Practically, exceedingly high data traffic can cause congestion in a channel or over a link that eventually results into queuing overflow on certain node. In addition to the above stated vulnerable node identification we have examined Traffic Load Intensity (TLI) [33] of a node that signifies its ability to accommodate data traffic without imposing any significant data drop. In MNCQM routing model, we have considered CLI as the decision variable that estimates the Queue-status at the one-hop distant neighbouring node signifying its suitability to forward data without imposing data drop and retransmission. Here, the source node monitors the load traffic statistics proactively using Proactive Node Table Management (PNTM). In MNCQM, to estimate the load condition and congestion each forwarding candidate-node or neighbouring node samples its Interface Queue Length (IQL) at the MAC layer of IEEE 802.11e and transmits it to the transmitter node as a part of beacon acknowledgement or HELLO message.

Consider i be the one-hop distant neighbouring node and l_j be the value of jth sample presenting queue length at current time-instant. Let, L be the total number of queue-length samples retrieved over the expected time period. In such case, the average traffic load at a node can be estimated using (2).

$$TL_i = \frac{1}{L}\sum_{j=1}^{N} l_j \tag{2}$$

Consider, l_{max} be the maximum IQL of a node at its IEEE 802.11e MAC layer. Thus, the total Traffic Load Density (TLD) at that node can be estimated using (3).

$$TLD_i = \frac{TL_i}{l_{max}} \tag{3}$$

In our proposed MNCQM protocol we have exploited the dynamic value of TLD_i to estimate the Success Probability of Data Transmission (SPDT) at a neighbouring node i (i.e., P_{Succ_i}). Mathematically, it is obtained by (4).

$$P_{Succ\_i} = 1 - TLI_B \tag{4}$$

As stated in above section, since the probability of successful data transmission is related to TLD, it can be inferred that a significantly small value of TLD can influence packet forwarding probability. With this motive, in this paper we have focussed on selecting a neighbouring node with suitable TLD. Noticeably, relatively higher node density causes more traffic in the network as well as higher TLD for the neighbouring (forwarding) nodes. This as a result could reduce the eventual packet forwarding success probability P_{Succ_i}. In MANETs it becomes inevitable to consider security issues, especially when certain node starts behaving unexpectedly and violates the protocol. Such nodes can often cause packet drop and hence degraded network performance. In some cases, it has been found that in MANETs the malicious nodes often lies or mislead about its queuing condition or allied network status. For instance, an intruder can abruptly state its queue is completely occupied and full signifying no bandwidth available to accommodate traffic data. This issue often leads improper bandwidth utilization and QoS violation. Alleviating such malicious nodes can help retaining reliable BFL to achieve QoS transmission over MANETs. MNCQM routing model characterizes each neighbouring nodes and profiles it in above stated terms to remove such nodes becoming a part of BFL and thus achieves optimal performance even under dynamic topology and network changes.

4.1.3 Dynamic Topology

In majority of the classical trusts-based routing scheme researchers have focussed on alleviating the issue of overhearing to characterize the trustworthiness of a node. In these approaches, transmitter node forwards its data to the next hop node only after assuring that it doesn't cause overhearing and resulting re-transmission probability to the one-hop distant nodes. This feature helps in enabling reliable and resource efficient data transmission to the sink node. In case a transmitter is capable of overhearing the packet forwarding from the one-hop BFN node, it states fair and successful interaction, else identified as malicious node. The situation when a transmitter node is not able to overhear the re-transmission of its packet effectively even though it took place, or the sink node is unreachable because of the stale routing information, this forwarding node is identified as malicious node and is avoided from becoming part of the BFL formation. In addition, node mobility or resulting topological variations in MANETs could impose numerous vulnerabilities when making BFN and/or BFL selection. In such case assessing trustworthiness of the each participating node is vital to achieve QoS provision [34]. Practically, a node can assess trustworthiness of the neighbouring node based on the rate of link changes [34]. In MNCQM, we have used the Rate of Link Change (RLC) to assess node trustworthiness and its relation to achieve higher QoS provision. Here, RLC at certain node i has been estimated using equation (5).

$$\eta_i = \gamma_i + \varepsilon_i \tag{5}$$

In equation (5), the variable γ_u states the Rate of Link Arrival (RLA), while ε_u signifies Rate of Link Outage (RLO) or breakage rate by ith node [35]. Considering the suggestions [35] where the maximum RLA γ_{i_Max} is equivalent to the RLO, we have derived the maximum RLC (ε_{i_Max}) as $\gamma_{uMax} + \varepsilon_{i\_Max} = 2.\sigma_i$. Thus, the RLC can be obtained using (6).

$$\eta = \frac{\gamma_i + \varepsilon_i}{2.\sigma_i} \tag{6}$$

Now, estimating the value of the above derived equation (6), MNCQM estimates the highest Probability Of Successful Data Delivery (PSDD) (or forwarding) by a node using (7).

$$P_\eta = 1 - \eta \tag{7}$$

Observing (7), it can be found that the higher RLC signifies more dynamic neighbourhoods that could adversely affect the probability of successful data transmission (or forwarding) by a node. In such case, MNCQM considers a node with moderate or low RLC to constitute network topology.

4.2 Evolutionary Computing assisted topological optimization and dual-disjoint (best) forwarding path selection

So far in the previous sections, we focussed on assessing nodes for their reliability and trustworthiness; however in MANETs selecting best forwarding node based on network conditions awareness is must. With this motive, in this paper dual object function has been taken into consideration where the first intends to obtain the reliable node for network planning, while another focuses on achieving optimal network topology configuration and the Best Forwarding Path (BFP) formation. The previous section mainly addressed identifying the reliable or trustworthy nodes (say, node profiling) to be considered for network planning. This section

mainly discusses the second objective of this research, i.e., to perform network condition aware routing decision. To achieve it, we have intended to exploit node features so as to identify a node with minimum hop, optimal bandwidth use, minimum energy consumption and higher network availability. To assure reliable communication over dynamic-topology MANET, we have designed a novel Dual-Route Concept (DRC) that possess two parallel routes from source to destination, while retaining second route as "Standby-Solution". This second route also called Remote Front-End Concentrator (RFEC) provides alternate path in case of any fault condition using logical AND gate configuration. With this configuration the data transmission can be continued till at least one path is functional and it makes overall communication system robust and reliable.

Being a network condition aware routing model, we consider dynamic node characterization in terms of "Availability, Unavailability, Connectivity and Connectivity Loss". Here, availability signifies the time for which a node or allied link can be active and functional. On contrary, unavailability refers the duration for which link or node remains dead. Similarly, connectivity refers the time for which the node remains connected, while connectivity loss refers the time fraction during which the node remains detached to the allied RFEC. Typically, connectivity loss is defined as the likelihood of a node being detached to the RFEC at certain random period. Observing these two factors, it can be found that to achieve reliable data transmission, retaining higher connectivity and availability is must, and statistically these network parameters can be exploited to obtain probabilistic behaviour of a node for future decision. Exploring in depth it can be found that the node behaviour or characteristics in MANET often varies due to movement, relative location, changing node parameters etc. This variation is somewhere related to hop-counts and availability of the link. Considering this fact, in this paper, as second objective we have developed a network optimization model using heuristic concept that intends to maintain maximum connectivity or availability, minimum hops etc.

4.2.1 Hop-Count Optimization

Selecting nodes with the minimum number of hops can enable network reliable as well as computational efficient. Considering this fact, our proposed routing protocol intends to retain optimal connectivity while maintaining minimum hops and disjoint paths for routing decision. Unlike major exiting approaches where Dijkstra algorithm is used to perform the shortest path selection, we have developed an evolutionary computing (EC) assisted enhanced shortest path planning model. This approach enables optimal path formation from one node to another in a graph by performing pruning of the complete set of paths. Typically, to perform path formation, Dijkstra algorithm increases the selected paths (hop-counts) by supplementing a new hop to any neighboring node. This process applies all connecting (neighbouring) nodes and hence constructs multiple paths. During pruning in case multiple paths connects or meets at the same intermediate node, then the two BFPs are selected and others are removed. This approach enables selection of the single best path with better connectivity and hop counts and hence is better than classical Dijkstra algorithm. Additionally, this approach reduces the search space (i.e., the number of nodes to be searched in the next steps) that makes overall computation efficient and resource efficient. In addition to the hop-count optimization, we have focussed on achieving higher availability to ensure QoS provision. A snippet of the proposed no-disjoint availability enhancement scheme is given as follows:

4.2.2 No-Disjoint Availability Optimization

To achieve (no) disjoint availability optimization, in our proposed routing model the two paths possessing maximum availability are identified. Unlike hop-count optimization, here we focus on exploiting node and link availability information (except the joint node). Once performing shortest path planning and network (topology) optimization, the path with the minimum computational cost is identified (the lower node or components would result into lower cost). However, practically due to the stochastic nature of the availability, total path availability can not be the sum of the availability of comprising nodes or elements. In such case, a first order approximation method can be applied to obtain path/node unavailability (as the sum of unavailability of comprising node or elements), which can further be used to perform routing decision. Thus, considering these two objectives, in this paper a Multi-Objective Optimization (MOO) scheme is developed using Elitist Genetic Algorithm (EGA) that intends to identify best two disjoint paths with minimum unavailability and higher reliability. To achieve it in this paper EGA has been applied in conjunction with Monte Carlo simulation that enables inculcation of the dynamic topology and network uncertainties. The detailed discussion of the proposed MOO optimization method is given in the sub-sequent sections.

4.2.3 Bayesian Network (BN)

To model the network and its probabilistic behaviour we have applied Bayesian Network (BN) model, where a direct acyclic graph is formed. In this model each node in the graph signifies a random variable, where the direct links are selected in such manner that the (joint) cumulative probability distribution of all comprising nodes (say, variable) can be estimated as the product of the conditional likelihood of each variable in its graph. When such correspondence are satisfied between the structure of the graph and the cumulative probability, the graphical model is stated as BN [37][38].Once obtaining the key graph structure and allied conditional probability of each node the BN is formed, it becomes easy to estimate the probability (probable values) of the variables in the graph. Considering our research objective where the focus is made on developing a BFP with higher connectivity, BN avoids deriving any sophisticated mathematical formulations for node-connectivity as a function of node availability and link quality. With this motive, in our proposed routing model BN scheme has been considered as the probabilistic estimation model for network routing optimization. BN based MANET can be represented in terms of multi-layer hierarchical structure comprising node and links, branches, paths and connectivity. A snippet of these variables is given as follows:

Table 1. Snippet of the variables

Variable	Significance
Node and Links	BN node as variable 1 can be only when the node can communicate or is available. If a node is not available for communication it is labelled as 0.
Branches	BN node is 1 only when connected nodes and the links connecting the nodes are available.
Paths	In this layer of BM, each node is responsible for providing a path connecting node 0 to the RFEC.
Connectivity	It states the connectivity between the selected nodes.

Here, one assumption that the availability of a node is often independent of the availability of other node. Similarly, availability of a link can be independent of the availability of the other links. Typically in BM, the probability of the first layer is specified by availability of each node

or link, while the second and third layers assume a deterministic approach stating that any branch or path can work only when associated elements functions. In such case, it gives the allied conditional probabilities as 1 or 0. In the same way the path variables can be selected. The last or the fourth layer variable signifies the service state of node signifying 1 when the node is connected to RFEC and 0 otherwise. Considering above discussion it can be inferred that the state of all variables can be defined as the function of the variables in lower layers and hence conditional probability values can also be selected other than 0 or 1. Once constructing the BN the node connectivity and allied network conditions are obtained. Observing the state of the node or link connectivity and availability has been obtained. This information can also be applied to estimate the link-outage probability estimation. In addition, it can enable learning different rules and allied associations amongst the pattern or network data. The detailed discussion of the link and node availability/connectivity estimation is given in the sub-sequent sections. Though, BN avoids deriving any sophisticated mathematical model for link or node connectivity, however a snippet of the mathematical models involved is given as follows:

4.2.4 Optimal Path Availability Estimation

In MANET, a route $\mathcal{R}$ or path connecting source n_0 to the destination n_f can be the evolving sequence of nodes $\mathcal{N} = \{n_0 \ldots\ldots n_f\}$ which are connected with respective link (quality) order, given as $\mathcal{E} = \{e_{0,1}, \ldots\ldots e_{f-1,f}\}$.

Here, the variable $e_{i,i+1}$ states the link in between the node n_i and node n_{i+1}. As already stated, a route or path can exist (say, available) only when all connected nodes and constituting links are available, and hence it can be written as (8).

$$A_r(\mathcal{R}) = \prod_{j=0}^{f} \mathcal{A}_n\ (n_j) \prod_{k=0}^{f-1} \mathcal{A}_e\ (e_{k,k+1}) \tag{8}$$

Now, the unavailable path can be obtained as (9).

$$U_r(R) = 1 - A_r(R) = 1 - \prod_{j=0}^{f} A_n\ (n_j) \prod_{k=0}^{f-1} A_e\ (e_{k,k+1}) \tag{9}$$

Typically, in current day scenarios with advanced communication paradigm, link or node unavailability cases are less and therefore "First-Order Approximation (FOP) can be vital. Now, ignoring in (9) each product with multiple unavailability cases, node or link unavailability can be derived as (10).

$$\begin{aligned} U_r(\mathcal{R}) &= 1 - \prod_{j=0}^{f}(1 - U_n(n_j)) \prod_{k=0}^{f-1}(1 - U_e\ (e_{k,k+1})) \\ &\approx \sum_{j=0}^{f} U_n\ (n_j) + \sum_{k=0}^{f-1} U_e\ (e_{k,k+1}) \end{aligned} \tag{10}$$

Equation (10) signifies an additive unavailability paradigm in which the overall influence of incorporating additional node augments an unavailability increment that predominantly relies on the unavailability of the supplemented node or associated link. In practice, such additive paradigms can be more reliable as compared to the non-additive ones due to the issues pertaining to the finite precision terms in the form1 - I, (tentative value near 10^{-9}). Furthermore, such additive paradigm enables use of Dijkstra algorithm to identify the most available path.

4.2.4.1 Node Connectivity

It refers the likelihood that minimum one path in between source to destination is functional. Considering our proposed model, any node n_0 can be connected to the RFEC only when any of these criteria is satisfied.

1. Node n_0 is available.
2. Node C is available.
3. Minimum one of the paths from n_0 to destination is functional or available.

As already discussed to retain QoS delivery over MANET, our proposed routing protocol hypothesizes that the individual node possesses two distinct (disjoint) paths connecting to the RFEC. In case of completely disjoint paths where it doesn't share any node or link, the (node) connectivity can be obtained using following method:

Consider that the paths for a node n_0 be $\mathcal{R}_0$, …….$\mathcal{R}_{K-1}$ and $\overline{\mathcal{R}_k}$ be the nodes and links from $\mathcal{R}_k$ (excluding terminals). Then

$$C(n_0) = \mathcal{A}(n_0)\mathcal{A}\left(\bigcup_{k=0}^{K-1}\overline{\mathcal{R}_k}\right)\mathcal{A}(C) \tag{11}$$

In (11), the second component signifies the availability of the disjoint set of sub-paths. Now, considering the availability of the terminal nodes the connectivity of n_0 can be lost in case all routes $\overline{\mathcal{R}_k}$ fail. Now, hypothesizing link or allied node's failure as independent -independent, availability can be obtained using (12).

$$\mathcal{A}\left(\bigcup_{k=0}^{K-1}\overline{\mathcal{R}_k}\right) = 1 - \prod_{k=0}^{K-1} U_r\left(\overline{\mathcal{R}_k}\right) \tag{12}$$

Now, considering $\{n_{k,0}, \ldots\ldots\ldots n_k, f_k\}$ as the set of nodes and $\{e_{k,1,2} \ldots\ldots, n_k, f_{k-1}, f_k\}$ as the corresponding links from path k in such manner that $n_{k,0} = n_0$ y n_k, $f_k = C$, then applying equation (9), we can estimate the link or node unavailability as equation (13).

$$\begin{aligned} U_r\left(\overline{\mathcal{R}_k}\right) &= 1 - \mathcal{A}_r\overline{\left(\mathcal{R}_k\right)} \\ &= 1 - \prod_{i=1}^{f_{k-1}}\mathcal{A}_n\left(n_{k,i}\right)\prod_{j=0}^{f_{k-1}}\mathcal{A}_e\left(e_{k,j,j+1}\right) \end{aligned} \tag{13}$$

Now, using equations (11), (12) and (13), connectivity of a node n_0 can be obtained as (14).

$$\begin{aligned} C(n_0) &= \mathcal{A}(n_0)\mathcal{A}(C) \\ &\times \left(1 - \prod_{k=0}^{K-1}\left(1 - \prod_{i=1}^{f_{k-1}}\mathcal{A}_n\left(n_{k,i}\right)\prod_{j=0}^{f_{k-1}}\mathcal{A}_e\left(e_{k,j,j+1}\right)\right)\right) \end{aligned} \tag{14}$$

As already stated to achieve reliable and robust transmission over MANETs selecting a path with minimum shared elements can be vital. With this motive we estimate the total shared elements in each path.

4.2.4.2 Shared elements per path estimation

This is the matter of fact that connectivity of a node with two non-disjoint routes can be obtained by decoupling the role of shared elements and allied disjoints nodes or links. Consider that $\mathcal{R}_0$ and $\mathcal{R}_1$ be the two supplementary paths then the connectivity can be obtained using (15).

$$C(n_0) = \prod_{j\epsilon\Phi_n}^{f} A_n\,(n_j) \prod_{k\epsilon\Phi_e}^{f-1} A_e\,(e_{k,k+1}) \times \left(1 - \left(1 - \prod_{i\epsilon\Phi_{n,0}} A_n\,(n_{0,i}) \prod_{j\epsilon\Phi_{e,0}} A_e\,(e_{0,j,j+1})\right)\right) \times \left(1 - \prod_{i\epsilon\Phi_{n,1}} A_n\,(n_{1,i}) \prod_{j\epsilon\Phi_{e,1}} A_e\,(e_{1,j,j+1})\right)\Bigg) \tag{15}$$

In (15), the variables Φ_n and Φ_e signify the sets of shared elements (i.e., node and links, correspondingly). Similarly, the variables $\Phi_{n,i}$ and $\Phi_{e,i}$ states the sets of non-shared elements from path i. Now, substituting availability products with 1st order approximations defined in the form of respective unavailability, the connectivity loss can be estimated using (16) and (17).

$$L\,(n_0) = 1 - C(n_0) \tag{16}$$

$$L\,(n_0) \approx \sum_{j\epsilon\Phi_n}^{f} U_n\,(n_j) + \sum_{k\epsilon\Phi_e}^{f-1} U_e\,(e_{k,k+1}) + \left(\sum_{i\epsilon\Phi_{n,0}} U_n\,(n_{0,i}) + \sum_{j\epsilon\Phi_{e,0}} U_e\,(e_{0,j,j+1})\right) \times \left(\sum_{i\epsilon\Phi_{n,1}} U_n\,(n_{1,i}) + \sum_{j\epsilon\Phi_{e,1}} U_e\,(e_{1,j,j+1})\right) \tag{17}$$

Considering the fact that non-shared links don't contribute loss probability of the node significantly, it is obtained using (18)

$$L\,(n_0) \approx \sum_{j\epsilon\Phi_n}^{f} U_n\,(n_j) + \sum_{k\epsilon\Phi_e}^{f-1} U_e\,(e_{k,k+1}) \tag{18}$$

Now, observing (17) and (18) it can be found that the most reliable pair would have two distinct disjoint paths, as the shared or common nodes or links possess a first-order influence (18) exhibiting that even a single fault in any shared element can disrupt both paths or link-outage and hence QoS violation. However, the most reliable pair might possess non disjoint paths due to no supplementary non-disjoint node or link and the low presence of disjoint paths. In this case the

routes with certain common links might retain high levels of reliability and availability. Unlike classical approach, in this paper we intend to perform routing decision only with the nodes with the minimum connectivity loss probability. With this motive, we have applied a MOO model that intends to estimate the paths with minimum hop counts as well as minimum Connectivity Loss (CL).

4.2.4.3 Elitist Genetic Algorithm (EGA) based Best Forwarding Path Selection

Unlike classical analytical model, in this paper we have applied Elitist Genetic Algorithm (EGA) that performs MOO to achieve best forwarding paths for reliable and QoS centric routing over MANETs. In this method the proposed EGA model intends to reduce the connectivity loss as defined in (10). In our proposed approach EGA algorithm considers both connectivity loss and number of hops as objective function to perform the best (non-disjoint) forwarding paths estimation, and thus simulates the problem of MOO. Our proposed EGA method intends to achieve a quasi-optimal solution by retaining maximum connectivity and link reliability. EGA continues retrieving suitable forwarding paths by searching over a set of feasible paths, which are continuously constructed by supplementing a new hop and estimating respective availability and connectivity. In this method, EGA terminates when the likelihood of estimating a suitable or better paths (two non-disjoint paths) is very low.

The overall routing optimization method can be illustrated using following process-sequences:

Step-1 Network Initialization

1.1. Perform node profiling using Packet Forwarding Probability (PFP) at the MAC layer, Success Probability of Data Transmission (SPDT) of a neighboring node, and Probability of Successful Data Delivery (PSDD) criteria and isolate malicious or non-trustworthy nodes.
1.2. Form a BN with multiple nodes and allied elements.
1.3. Assign n_0 as the inception node and n_f as the RFEC. Consider $S_0 = \{n_0\}$ be the functional or active paths.

Step-2 Identify the incomplete path having not connectivity with RFEC node in S_k .

2.1. Select an incomplete path $R^* \in S_k$.
2.2. Estimate all possible paths retrieved by prolonging R* from its terminal node by appending or adding a single hop.
2.3. Estimate S_k' by substituting R* in S_k by the extended paths.
2.4. Estimate the probability of link outage of all the new path pairs by means of the proposed Bayesian Network.
2.5. Perform pruning by setting S_{k+1} as the result of eliminating all suboptimal paths in S_k .

Step-3 Use BFP to transmit data from source to destination

3.1. Form the best forwarding path from the identified two non-disjoint paths and initiate data transmission between source and destination.

The simulation results obtained and their respective inferences are presented in the sub-sequent section.

5. SIMULATION RESULTS AND DISCUSSION

In this paper an optimistic vision was made to ensure MANET secure and reliable while giving the specific focus to augment QoS delivery. Observing major existing works, it can be found that most of the at hand protocols either focus on network security or on performance enhancement; while to achive a cumulatve optimal solution maintainig balance between security as well as performance is must. This paper focusses on assessing node's reliability based routing decision as well as node or network parameter sensitive routing decision. In other words, the proposed MNCQM routing protool can be stated as a dual-optimization measure where focus was made at first to ensure that no untrustworthy node is participating or available in routing table, while in the next phase an evolutionary computing assisted network topological management scheme was developed so as to ensure reliable data transmission. In the first phase of work, the protocol exploited different node behaviour to assess its suitability to becomes topology, while in the ascending phase node connectivty and availability were considered to design a most reliable best forwarding path. In addition, the focus was made on maintainig minimum number of hops so as to reduce both vulnerability as well as computational cost. Towards this objective Elitist Genetic Algorithm (EGA) was developed which was executed over Baysian based topology to estimate dual-best forwarding paths with minimum shared components. Here, the prime objective was to construct two disjoint paths with higher connectivity and availability so that in case of any probable node or link failure the supplimentary could ensure timely data delivery without executing network discovery phase. This as a result saves computation, resource as well as reduces delay. Noticeably, in the proposed method the key significance of dual path strategy is to ensure reliable communication while maintaining minimum hops, minimum connectivity-loss and maximum link or node availability. The overall proposed routing protocol was developed using well known Network Simulator tool named NS2. The proposed MNCQM routing protocol has been implemented as enhancement of the classical AODV routing protocol with native IEEE 802.11 standard protocol stack. Noticeably, to assess efficacy of our proposed model during simulation compromising nodes as well as node death condition was applied. The predominant motive was to assess proactive routing decision by the proposed routing protocol. Some of the key network simulation parameters are given in Table 2.

Table 2. Simulation Environment

Parameter	**Value**
MAC	IEEE 802.11
PHY	802.11PHY
Antenna	Omni-directional
Radio Range	200
Number of nodes	10,20,30,40,50,60
Efficiency of RF power amplifier	0.47
Link margin	40 dB
Gain factor	30 dB
Power density of AWGN channel	-134 dBm /Hz
Noise Figure (Receiver)	10 dB
Carrier frequency	2.5 GHz
BER performance	10^{-3}
Transmitter circuit power consumption	98.2 mw
Receiver circuit power consumption	112.6 mw
Antenna gain of Transceiver	5 dB

Routing table management	Proactive
Transmission rate	10-512 kb/sec
Packet size	512 kb
Routing Protocol	Native AODV MNCQM

The overall performance analysis has been performed in reference to the proactive routing protocol AODV in terms of Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Energy Consumption, Delay and bandwidth consumption. A snippet of the results obtained and their inferences is given as follows:

Figure 1 presents the comparative performance of our proposed MNCQM routing protocol and native AODV protocol. Observing the results it can be found that the proposed routing model outperforms classical AODV. As stated above our proposed MNCQM routing protocol at first identifies compromizing nodes and dead nodes based on different node parameters or characteristics like Packet Forwarding Probability (PFP) at the MAC layer, Success Probability of Data Transmission (SPDT) of a neighboring node, and Probability of Successful Data Delivery (PSDD) which enables it to avoid such untrustworthy nodes to be a part of route or tranmission path. During communication, MNCQM assesses link or node quality including node connectivity and availability (or link connectivity and availability) to identify dual-disjoint paths between source and desitnation node. This approach enables our proposed MNCQM routing protocol to exhibit more reliable data transmission than the native AODV routing protocol. This efficacy can be observed through the results obtained (Figure 1 and Figure 2). Here, MNCQM routing protocol exhibits PDR upto 100% which is higher than the native AODV protocol (PDR-84%). Similarly, PLR performance to affirms robustness of our proposed MNCQM routing protocol over classical AODV routing approach. Observing above results, it can be found that the proposed MNCQM routing protocol exhibits better even with increase in nodes or network density. Interestingly, in Figure 1 initially it exhibits low PDR with lower number of nodes that could be caused due to lack of sufficient nodes in between source and destination with higher inter-node distance. With increase in node density MNCQM finds sufficient nodes (say, neighbouring nodes) to perform EGA based forwarding path estimation followed by data transmission.

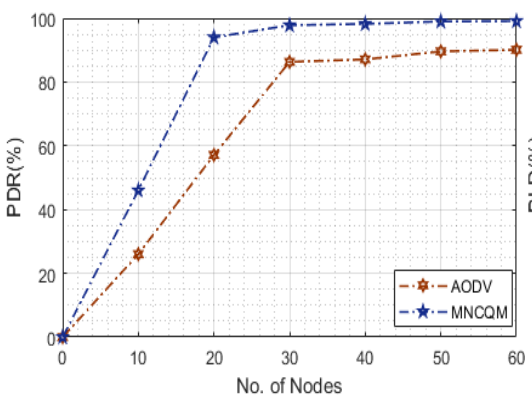

Figure 1. Packet Delivery Ratio (%)

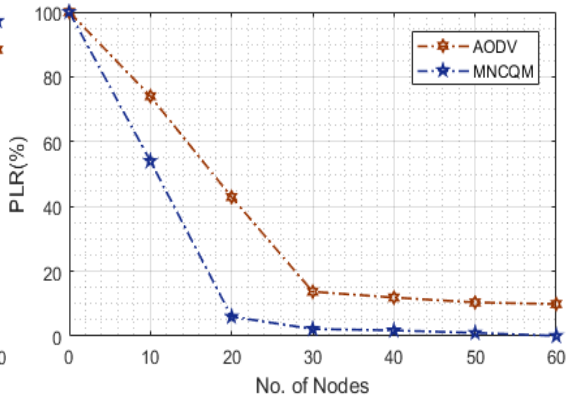

Figure 2. Packet Loss Ratio (%)

Figure 3 presents delay performance by the proposed MNCQM routing protocol, where it can be found that it outperforms classical AODV because of minimum retransmission possibility and higher PDR. In other words, MNCQM assures reliable transmission and hence avoids retransmission probability. In addition, it avoids iterative network discovery during any link

outage (due to pre-established supplementary or disjoint supplementary path) probability and therefore the delay incurred is very less.

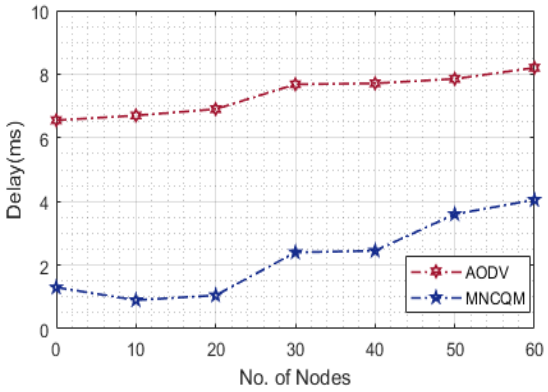

Figure 3. Delay performance (ms)

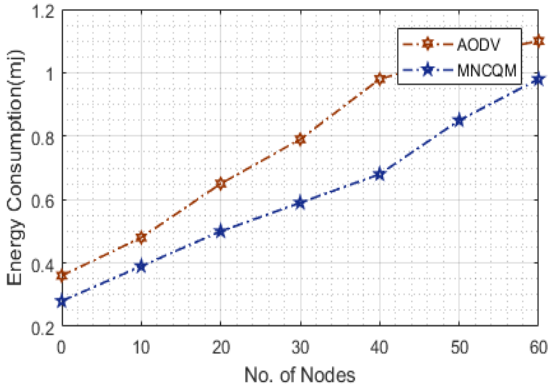

Figure 4. Energy Consumption (mJ)

The impact of such robustness can be easily visualized in Figure 4, where MNCQM has exhibited lower energy consumption as compared to native AODV protocol. Figure 5 presents the bandwidth utilization by MNCQM where it supersedes native AODV. This is because of link or network adaptive routing decision and minimum communication overheads. Typically overheads impose routing protocol to undergo resource or spectrum exhaustion, MNCQM avoids such complexity and hence preserves bandwidth significantly. Moreover, as it avoids iterative signaling cost during alternate path formation, its bandwidth efficacy can be hypothesized affirmatively.

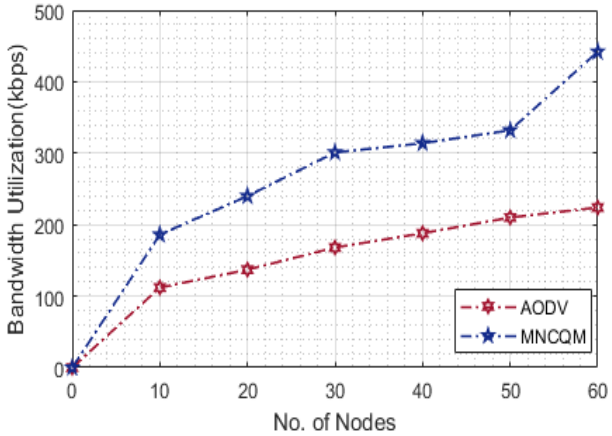

Figure 5. Bandwidth Utilization (kbps)

Finally, the overall performance analysis is summarized in table 3. It clearly indicates that there is greater improvement in above discussed parameters with MNCQM over AODV.

Table 3. Comparative Analysis

Parameter	AODV	MNCQM	Percentage of Improvement of the MNCQM
Packet Delivery Ratio	84%	100%	16
Packet Loss Ratio	15%	0%	15
Delay	8 ms	4 ms	50
Energy Consumption	1.1 mJ	1 mJ	91
Bandwidth Utilization	220 kbps	440 kbps	50

6. CONCLUSION

Considering the significance of a novel and robust routing protocol for QoS centric MANETs, in this paper multi-objective optimization with hierarchical enhancement effort was considered. To achieve it, the focus was made on ensuring topology formation only with reliable or trustworthy nodes and then constituting dual disjoint best forwarding path estimation while maintaining higher node and link connectivity as well as link availability. In addition, this research developed a novel evolutionary computing based shortest path identification scheme with higher availability and minimum connectivity loss. Such robustness can be of vital significance when considering that with classical shortest path models to constitute dual best forwarding path there can be common nodes or links (say elements) that in case of adversaries could force entire network to stop communication and hence can degrade QoS assurance. On contrary, MNCQM avoids common network elements even assuring minimum hops, high connectivity and high availability that eventually strengthened it to exhibit higher packet delivery ratio, minimum packet loss, minimum delay and minimum energy consumption. Undeniably, the use of Elitist Genetic Algorithm (EGA) for the considered multi-objective optimization could have contributed significantly to perform dual disjoint best forwarding paths for QoS centric communication over MANETs. Summarily, the proposed MNCQM routing protocol can be stated as an optimistic routing approach focused on assuring reliable as well as computational efficient topological planning to accomplish QoS centric communication over MANETs. The simulation results have exhibited that the proposed routing protocol can enable better performance in terms of packet delivery ratio, packet loss, delay, bandwidth consumption, energy exhaustion that affirms its suitability with real-time communication or routing purposes. One noticeable robustness of the proposed routing protocol is that it avoids dependency on a single BFN based routing decision that in case of node or link failure could cause QoS degradation. On contrary, MNCQM provides optimized supplementary path with no-common network elements and hence can guarantee successful data delivery. In future in addition to the link connectivity and availability, node dynamic characteristics such as packet injection rate, also called packet velocity, congestion probability etc can be used to make best forwarding decision.

REFERENCES

[1] S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, IETF WG Charter, http://www.ietf.org/html.charters/manet-charter.html, January 1999.

[2] Z. Iqbal, S. Khan, Amjad Mehmood, Jaime Lloret, and Nabil Ali Alrajeh “Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks” Hindawi Publishing Corporation Journal of Sensors Volume 2016, Article ID 5486437, 18 pages.

[3] C. T. Calafate, M. P. Malumbres, J. Oliver, J. C. Cano and P. Manzoni, "QoS Support in MANETs: a Modular Architecture Based on the IEEE 802.11e Technology," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 5, pp. 678-692, May 2009.

[4] Z. Li and X. Yang, "A Reliability-Oriented Web Service Discovery Scheme with Cross-Layer Design in MANET," 2016 IEEE International Conference on Web Services, San Francisco, CA, 2016, pp. 404-411.

[5] S. V. Sangolli and J. Thyagarajan, "An efficient congestion control scheme using cross-layered approach and comparison of TCP variants for mobile ad-hoc networks (MANETs)," 2014 First International Conference on Networks & Soft Computing, Guntur, 2014, pp. 30-34.

[6] P. Samar and S. B. Wicker, “On the behavior of communication links of a node in a multi-hop mobile environment,” in proceedings 5th ACM Intl. symposium on Mobile ad hoc networking and computing, 2004.

[7] D. Chen and P. K. Varshney, “QoS support in wireless sensor networks: a survey”, International Conference on Wireless Networks, ICWN '04, Las Vegas, USA, June 2004, pp. 227-233.

[8] F. Xia, “QoS Challenges and opportunities in wireless sensor/actuator networks”, Sensors 2008, vol.8, no.2, 2008, pp. 1099-1110.

[9] Y.J. Li, C.S. Chen, Y.Q. Song and Z. Wang, “Real-time QoS support in wireless sensor networks: a survey”, 7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems, FeT’07, Toulouse, France, 2007.

[10] H. Alwan and A. Agarwal, “A Survey on Fault Tolerant Routing Techniques in Wireless Sensor Networks”, in proceedings of the Third International Conference on Sensor Technologies and Applications, Athens/Glyfada, Greece, 2009, pp. 366-371.

[11] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, “Protocols for self organization of a wireless sensor network,” IEEE Personal Communications, vol. 7, no. 5, 2000, pp. 16–27.

[12] K. Akkaya and M. Younis, “An Energy-Aware QoS Routing Protocol for Wireless Sensor Networks”, in proceedings of the 23rd International Conf. on Distributed Computing Systems Workshops, 2003, pp. 710-715.

[13] J. Chen, R. Lin, Y. Li and Y. Sun, “LQER: A Link Quality Based Routing for Wireless Sensor Networks”, Sensors, vol. 8, 2008, pp.1025- 1038.

[14] B. C. Villaverde, S. Rea and D. Pesch, “Multi- objective Cross-Layer Algorithm for Routing over Wireless Sensor Networks”, Third International Conference on Sensor Technologies and Applications, Athens/Glyfada, Greece, 2009, pp. 568-574.

[15] P.A. Abdul Saleem, Dr. Naveen Kumar "Cross Layer Design Approach in Wireless Mobile ADHOC Network Architecture" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013.

[16] Y. Fang, Y. Zhou, X. Jiang and Y. Zhang, "Practical Performance of MANETs Under Limited Buffer and Packet Lifetime," in IEEE Systems Journal, vol. 11, no. 2, pp. 995-1005, June 2017.

[17] Y. H. Chen, E. H. K. Wu and G. H. Chen, "Bandwidth-Satisfied Multicast by Multiple Trees and Network Coding in Lossy MANETs," in IEEE Systems Journal, vol. 11, no. 2, pp. 1116-1127, June 2017.

[18] Y. Komai, Y. Sasaki, T. Hara and S. Nishio, " ${k}$ Nearest Neighbor Search for Location-Dependent Sensor Data in MANETs," in IEEE Access, vol. 3, pp. 942-954, 2015.

[19] R. Jia et al., "Optimal Capacity–Delay Tradeoff in MANETs With Correlation of Node Mobility," in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1772-1785, Feb. 2017.

[20] S. Sett, P. Kumar Guha Thakurta "Effect of optimal cluster head placement in MANET through multi objective GA", In IEEE International Conference on Advances in Computer Engineering and Applications(ICACEA), pp. 832-837, 2015.

[21] D. Barman Roy Rituparna Chaki "MCBHIDS: Modified layered cluster based algorithm for black hole IDS", In Annual IEEE India Conference (INDICON), pp.1-6, 2013.

[22] Neha Gupta, Rajeev Kumar Singh, Manish Shrivastava, "Cluster formation through improved weighted clustering algorithm (IWCA) for mobile ad-hoc networks", Tenth IEEE International Conference on Wireless and Optical Communications Networks(WOCN), pp. 1-5, 2013.

[23] M. Rath, B. Pati and B. K. Pattanayak, "Cross layer based QoS platform for multimedia transmission in MANET," In 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2017, pp. 402-407.

[24] M. A. Gawas, L. J. Gudino and K. R. Anupama, "Cross layer multi QoS metric routing for multimedia traffic in 802.11E over MANETs," 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), Vienna, 2016, pp. 582-587.

[25] Z. Li and X. Yang, "A Reliability-Oriented Web Service Discovery Scheme with Cross-Layer Design in MANET," 2016 IEEE International Conference on Web Services (ICWS), San Francisco, CA, 2016, pp. 404-411.

[26] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in proceedings of the 6th annual ACM Intl. conference on Mobile computing and networking, 2000.

[27] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transactions on Mobile Computing, 6(5):536-550, 2007.

[28] T. Sheltami, A. Basabaa, and E. Shakshuki, "A3acks: adaptive three acknowledgments intrusion detection system for MANETs," Journal of Ambient Intelligence and Humanized Computing, 5(4):611–620, 2014.

[29] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "Eaack—a secure intrusion-detection system for MANETs, " IEEE Transactions on Industrial Electronics, 60(3):1089–1098, 2013.

[30] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multihop wireless routing," Wireless Networks, 11(4):419-434, 2005.

[31] B. Shebaro, D. Midi, and E. Bertino, "Fine-grained analysis of packet losses in wireless sensor networks," in 11th IEEE Intl. Conference on Sensing, Communication, and Networking (SECON), 2014.

[32] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol," in proceedings of the 3rd ACM Intl. conference on Mobile ad hoc networking & computing, 2002.

[33] A. Shabut, K. Dahal, S. Bista, and I. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," IEEE Transactions on Mobile Computing, 14(10):2101–2115, 2015.

[34] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in IEEE Intl. Conference on Performance, Computing, and Communications, 2004.

[35] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Advanced Communications and Multimedia Security, Springer, 2002.

[36] F. Anjum and R. Talpade, "Lipad: lightweight packet drop detection for ad hoc networks," in 60th IEEE Vehicular Technology Conf., volume 2, 2004.

[37] F. V. Jensen, Bayesian Networks and Decision Graphs. New Jersey: Springer-Verlag, 2001.

[38] E. Castillo, J. M. Gutierrez, and A. S. Hadi, Expert Systems and probabilistic Network Models. New York: Springer-Verlag, 1997.

[39] T. H. Sureshbhai, M. Mahajan and M. K. Rai, "An Investigational Analysis of DSDV, AODV and DSR Routing Protocols in Mobile Ad Hoc Networks," 2018 International Conference on Intelligent Circuits and Systems (ICICS), Phagwara, pp. 281-285, 2018.

[40] Saghian, Malihe, Ravanmehr, Reza, "Efficient QoS-aware Middleware for Resource Discovery in Mobile Ad Hoc Networks", Adhoc & Sensor Wireless Networks, Vol. 43 Issue 3/4, p283-312,2019.

[41] Shashi Raj K, Siddesh G K,"QoS Oriented Cross-synch Routing Protocol for Event Driven, Mission-critical Communication Over MANET: Q-CSRPM", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.11, pp.18-30, 2018.DOI: 10.5815/ijcnis.2018.11.03.

AUTHORS

Shashi Raj K. is a research scholar in the department of Electronics and Communication Engineering at Dayananda Sagar College of Engineering, Bengaluru. He has received his B.E degree in Electronics and Communication Engineering and M.Tech degree in VLSI Design and Embedded Systems from VTU, Belgaum. He has eleven international, one national journal publications and three international conference publications to his credit. His research area and area of specialization includes Wireless Networks, VLSI and Embedded systems. He is a life member of the Indian Society for Technical Education.

Dr. Siddesh G. K. is a Professor and Head of the department of Electronics and Communication Engineering at JSS Academy of Technical Education, Bengaluru. He obtained his B chelors and Masters Degree in Electronics and Communication Engineering from Bangalore University and Manipal Academy of Higher Education, Karnataka respectively. He also obtained his doctrol degree from Visvesvaraya Technological University Belgaum, Karnataka, India. He has 20 international journal publications and 5 international conference publication to his credit. His research area and area of specialization includes Wireless communication, Computer Networks, Image and Data compression and Processing.