International Journal of Communication Networks and Information Security

*ISSN: 2073-607X, 2076-0930*

*Volume **14** Issue **03 Year 2022** Page **199:213***

# Generative Boltzmann Adversarial Network in Manet Attack Detection and QOS Enhancement with Latency

**[1] Dr. Arun Kumar Marandi, [2]Ms.Richa dogra, [3]Rahul Bhatt**
**[4] Mr. Rajesh Gupta, [5]Somashekar Reddy, [6]Dr. Amit Barve**

*[1] Associate Professor, Department of Computer Science, ARKA JAIN University, Jamshedpur, Jharkhand, India*

*[2] Assistant Professor, Department of Computer Science Engineering, Chandigarh Engineering College, Jhanjeri, India*

*[3] Assistant Professor, Department of Computer Science and Engineering, Dev Bhoomi Uttarakhand University, Dehradun, Uttarakhand, India*

*[4] Pro Chancellor, Department of Management, Sanskriti University, Mathura, Uttar Pradesh, India*

*[5] Assistant Professor, Department of Computer Science and Engineering, Jain (Deemed-to-be University), Bangalore, India*

*[6] Associate Professor, Department of Computer Science and Engineering, Parul Institute of Engineering and Technology, Parul University, Vadodara, Gujarat, India.*

*[1] dr.arun@arkajainuniversity.ac.in, [2]richa.j2004@cgc.ac.in*

*[3] socse.rahulbhatt@dbuu.ac.in, [4]prochancellor@sanskriti.edu.in*

*[5] r.somashekar@jainuniversity.ac.in, [6]amit.barve17535@paruluniversity.ac.in*

***Article History***

Received: 13 August 2022
Revised: 24 October 2022
Accepted: 12 November 2022



***Abstract***

Mobile Ad-Hoc Network (MANET) are considered as self-configured network those does not have any centralized base station for the network monitoring and control. MANET environment does not control architecture for routing for the frequent maintenance of topology. The drastic development of Internet leads to adverse effect of development in MANET for different multimedia application those are sensitive to latency. Upon the effective maintenance of the QoS routing route discovery is performed to calculate queue and contention delay. However, the MANET requirement comprises of the complex procedure to withstand the Quality of Service (QoS) with Artificial Intelligence (AI). In MANET it is necessary to compute the MANET attacks with improved QoS with the reduced latency as existing model leads to higher routing and increased latency. In this paper proposed a Generative Boltzmann Networking Weighted Graph (GBNWG) model for the QoS improvement in MANET to reduce latency. With GBNWG model the MANET model network performance are computed with the weighted graph model. The developed weighted graph computes the routes in the MANET network for the estimation of the available path in the routing metrices. The proposed GBNWG model is comparatively estimated with the conventional QOD technique. Simulation analysis stated that GBNWG scheme exhibits the improved performance in the QoS parameters. The GBNWG scheme improves the PDR value by 12%, 41% reduced control packets and 45% improved throughput value.

***Keywords- MANET, Latency, Weighted Graph, Routing, Quality of Service, Attacks***

## 1. Introduction

Wireless communication is the transmission of information or evidences without the convention of better electrical conductors or wires. The evolution of wireless technology and its utilization started in 1970s. In the past few decades, mobile wireless technologies have undergone changes in their evolution and revolution over 4 to 5 generations [1]. The cellular wireless generation (G) postulates the conversion in the fundamental nature of the service, frequency bands, and non-backwards compatible transmission technology.

A Mobile Ad hoc Network is a self-configuring network which does not require any fixed infrastructure. The network changes its topology continuously as each node in the network is set free to move. The most active research work in the past few years is said to be the movement of mobile nodes with low infrastructure in ad hoc networks providing dynamic routes [2]. The Mobile Ad hoc Network is said to be a cluster of mobile nodes which are connected through the wireless links. The basic structure of MANET. The nodes within the communication range communicate each other directly, otherwise intermediate nodes take part in the communication. Each node acts as a router and forwards the data packets to other nodes. In MANET, the centralized authority is not presented to manage the network [3]. In MANET, three networks are formed which are: Peer to peer network, Self-forming network and Self-healing network

The advantages of MANET are listed as follows: Central control authority remains independent. Flexible and scalable with increased reliability due to multiple paths, less expensive as compared to wired network, the network can be set up at any place and any time, it can be established quickly in an easy way, it is robust due to decentralized mechanism and it provides access to information and facilities regardless of geographic location [4].

The major characteristics of MANET are as follows: Autonomous behavior is shown where every node in the MANET acts as both router and host, dynamic topology is observed with the nodes in the mobile network and can run in different speed [5]. If a node wants to communicate with another node which is out of transmission range, then the packet is transmitted through one or more intermediate nodes. The network control is distributed among the mobile nodes which are connected through wireless medium and the work is equally distributed between the peers [6]. The mobile nodes have less memory size, low power storage and low Central Processing Unit (CPU) capability. Reliability, routing overhead, scalability, security, multi path routing, cross layer design quality of services and energy efficiency are the major challenges faced in MANET. MANET plays the key role in the field of Military communication, Satellite networks, Vehicular communication, Environmental monitoring, Sensing forest fires, Emergency operations like rescue, commando operations and crowd control, Personal Area Networking (PAN) and Educational services like virtual classrooms, meetings and lectures [7].

Link stability is noteworthy in many aspects for route selection method in MANET. It indicates the stability of link and establishment of communication in between two nodes. The power of the node is found out by its relative speed. Link stability between mobile nodes is determined by the distance between mobile nodes. The stability of multicast routes are determined with the help of quality of links [8]. The network reliability depends on the strength of the link. The Link State Database (LSD) is maintained by every node, which stores the link and node related information for maintaining the multicast mesh and stable path from source to multicast destinations. A multicast mesh and stable routes in a mesh are generated with various packets such as Request Phase(RP), Route Request(RR) and Route Error(RE).The multicast mesh creation involves two phases: Request phase and Reply phase. In request phase, the route is discovered in the multicast group and in reply phase it generates packet after receiving the request [9]. The route failure rate is decreased by decreasing the link failure rate and the number of links composed with the route. This research work gains the motivation from the attraction of services offered by the communication technology and to make use of them without interruption. The flooding mechanism is implemented in existing multicast routing protocols for identifying the optimal links and transferring the packets [10]. From this mechanism, more computational overhead is created and high cost is required for network maintenance and route discovery. In existing techniques, the distance among two nodes are calculated for estimating the link stability, which is not able to select the optimal node for data transmission. Hence, routing mechanism with high maintenance is required for optimal path selection. In the proposed method,

QoS parameters are considered for computing link stability. Then, the network is created and clustering is performed to choose the Cluster Head (CH). The data transmission is carried out by CH and the node information is stored in the Distributed Hash Table (DHT). The information related to speed, direction of the node movement, and success ratio of the node are also stored in DHT [11]. The optimal routing path is discovered with the help of this information. The key management scheme is proposed to improve the secure data communication. It authenticates the valid users to generate the code for transmission. A novel algorithm is introduced to enhance the link stability and security in MANET. The Dynamic on-demand clustering and Cluster member selection algorithms are considered to cluster the similar requests from the nodes and to select the highest energy node as CH. In a heterogeneous environment, offloading is applied to balance the load among nodes [12].
In this paper proposed a Generative Boltzmann Networking Weighted Graph (GBNWG) for the QoS improvement in MANET. The proposed GBNWG scheme uses the weighted graph model for the estimation of routing path in the MANET. With GBNWG model the computes the effective path for the data transmission in the network. Simulation analysis stated that proposed GBNWG routing model exhibits the improved PDR value by 12%, 41% reduced control packets and 45% improved throughput value.
This paper is organized as follows: Section 2 presented a related works for the MANET is presented. The network model for the GBNWG model is presented in Section 3. The simulation results with the proposed GBNWG is given in Section 4 with comparative results and Section 5 provides the overall conclusion of the proposed GBNWG.

## 2. Related Works

In [13] proposed a lifespan estimation algorithm called Particle Swarm Optimization (PSO) centered route retrieval algorithm that crosschecked node status before data transfer. The lifespan of link and node was evaluated on the basis of existing bandwidth, relative mobility of nodes, energy drain rate and these obtained estimations were processed to form fuzzy rules. Node status was predicted from those rules and it was sent to all other nodes in the network. Hence, every node would be aware of the environment surrounded. This route rescue methodology was applied for a node which was very feeble thus, a route with stable node could be framed. The result thus, obtained were used to segregate nodes under three categories namely weak, normal and strong. This classification was then broadcasted to all other neighbors along with HELLO messages. Route Recovery Warning (RRW) message was sent to all nodes only when the node status was marked weak. Intimation of RRW makes all neighboring nodes for hunting a strong node and include it into an active route in order to avoid link failure. Data loss was significantly diminished along with lessened routing overhead.
In [14] reviewed Residual Energy based Reliable Multicast Routing Protocol (RERMR) for a stable route establishment. Network portioning happened because of auto-configuration infrastructure in MANET. Dense overhead and inadequate packet delivery ratio were a result of flexible nature of nodes. They also inferred that remaining energy in nodes should be greater for a long-lasting network. An optimized multicast backbone was built to attain more stability in nodes with greater understanding and a hopeful loop. Data packets were forwarded only in the reliable path found on the basis of a path criterion defined.The practice of route discovery was originated only from the source node. It tended to discover all sort of existing strong nodes in the network via multicast routes.Three phase procedures were conducted in route discovery.
In [15] analyzed on Zone based Routing with Parallel Collision Guided (ZCG) broadcasting protocol along with parallel and distributed broadcasting.One hop clustering algorithm was used up in ZCG, in which networks were divided into zones. Zones separated were headed by a trustful node called zone leaders (ZL), who was almost immobile and enriched with ample lifespan. ZL node elected to initiate its role via Hello messages. The nodes surrounded by the ZL are regarded as dormant nodes which were under the coverage of a wireless medium. Member nodes of nearby zones could be differentiated with an inclusion of individual ZL addresses in their own periodic hello messages. A new ZL was elected with criteria mentioned with second greatest satisfying metrics. Thus, a single point failure could be controlled with a nomination of a new ZL.

In [16] implemented Trust Aware Adhoc Routing (T2AR) protocol so as to increase the trust level among nodes present in MANET. AODV was slightly improvised by means of conditional trust rate, energy, mobility based malicious behavior prediction in T2AR. Trust rate was defined on comparing packet sequence ID of neighbor nodes with log reports, so as to safeguard the network from malicious report generation. Trust level was enlarged with the direct and indirect trust observation scheme too.

In [17] designed a Mobility Assisted Spectrum Aware Routing (MASAR) protocol for Cognitive Radio Ad-Hoc Networks (CRAHNs). Primarily nodes were permitted to collect spectrum statistics within spectrum management interval, which was certainly continued by a data transferring time. These spectrum information collected was highly helpful for users in detecting further hops. Common Control Channel (CCC) was expected to be conserved by the proposed approach for interchanges of control messages. Moreover, CCC used to behave in a way that it was a meeting channel, even for all inactive nodes so that they will be able tomerge up themselves in the route. MASAR uses the two types of channels called Sending CHannel (SCH) and a Receiving Channel (RCH). Nodes in RCH was highly cooperative for preceding hops whilenodes were linked with next hops using SCH. A Free CHannel (FCH) was updated by a node for managing link failure in networks.

In [18] offered a novel Link-stAbility and Energy aware Routing (LAER) protocol which ensured least possible energy to leave off from the nodes and with a stable link as well. An investigative neighborhood was put on to find an immediate subsequent hop between those nodes.Actually, it was responsible for an improved joined link-stability-energy metric and huge accessibility was provided by the defined LAER algorithm. Only because of these conditions specified it is highly useful in stages of control packet communication that was transferred so as to keep up the network state acquaintance. The routing protocol suggested here was centered on a topographical prototype. Lasting link lifespan model was taken on as a firmness measure that was found to be much stronger than any of the existing suggestions. It was set free out of an error-prone metrics like communication radius measure and traversing speed of the node.

In [19] proposed a Scalable Weighted Clustering Algorithm (SWCA) for mobile ad hoc networks.The difficulty of choosing an applicable cluster head in wireless ad-hoc networks was addressed here, where the nodes tend to move in their own way.The major impact of the proposed work was towards the grouping nodes in an ad hoc network and enhancements in Weighted Clustering Algorithm (WCA). A pair of contents harmonizing methodology and modest permanency prototype was consequently defined.Grouping of nodes was highly improved by augmenting the accessibility of the nodes. Regardless of the logic of freedom for moving around the nodes were supposed to be tied together as far as viable. The immobile nature of the node was preserved for a specific time span.

In [20] investigated about protocols based on infrastructure and disaster management in MANET. Emergency response operations were measured for developing a well-formed MANET. It also examined the prevailing deploying technologies of MANET for rescue operations and search for services. It was done on the basis of infrastructure criteria, disaster scenario, and communication protocols. The challenges inferred in this investigation were security in packet transmission and routing strategies in network deployed. It also faced a crisis in managing energy utilization during the time of packet transmission. Random access channel congestion occurred in the network due to an inclusion of a vast number of users in a single time span at the time of disasters. The disadvantage obtained with this approach was the deployment of an inefficient and unreliable framework of MANET.

In [21] suggested an innovative probabilistic key management algorithm with the utilization of asymmetric cryptography. It was suited for a large-scale MANET. This developed approach completely alleviated the need for archiving an entire gathering of the key in each node instead only a minimum group of a key was possibly stored. The total number of keys was stored on the basis of a random calculation of connectivity probability done prior in accordance with a size of the network. After this, a public key was shared among those nodes which send and receive packets. Shortest path for initiating the communication between a source and sink was defined with the computation of Average Cryptographic Distance. The minimal archiving of keys with probability greater than 99.99% made the network to remain connected for an elongated time interval. Asymmetric

cryptography deployed was evidently twice the measurement of path length. A major drawback observed in this approach was no assurance for a perfect end-to-end connectivity.

## 3. Network Model

In general, MANET consists of several independent entities organized in graph like structure. Network consists of a set of mobile nodes positioned at random locations. The nodes are considered as vertices and the links are considered as the edges, in which the neighboring nodes are connected with edges. Network can be represented as the directed weighted graph. The proposed Generative Boltzman Networing Weighetd Graph (GBNWG). The nodes that lie within a particular range communicate in the direct way. Each node is responsible for receiving and transmitting the data throughout the network. All the nodes in the network have an initial distinct energy during transmission. The nodes in the network must have a high level of collaboration for a successful data transmission. At the same time the nodes have limited bandwidth and energy constraints. The nodes tend to lose their energy on data forwarding, but the energy consumption is reduced, when the transmission is within the range. The equation 1 shows the communication between two nodes n1 and n2, when they are within a certain range of transmission.

$$dis_{(n_1,n_2)} \leq r \tag{1}$$

Where, r is the transmission range and dis is distance.
MANETs have bidirectional links and they consider the QoS constraints between the source and destination pair. With GBNWG bandwidth consumption through neighborhood estimation is performed in MANET to evaluate the neighbors in the wireless medium. The amount of total energy consumed through neighborhood bandwidth $B_{iconsumed}$, computed as in equation (2)

$$B_{iconsumed}\ is\ \sum_{j\in N(i)} B_j \tag{2}$$

In above equation (2) where N(i) = {all neighbour nodes i}, and Bj stated as consumed bandwidth for the connections of node j, j ∈ N(i). With GBNWG total utilized bandwidth is defined as $B_{max}$, with the computation of available bandwidth is measured using the equation (3)

$$B_{available} = B_{max} - B_{iconsumed} \tag{3}$$

The estimated value (e) in the path can be expressed as follows in equation (4) – (6)

$$D\big(p(s,d)\big) = \sum_{c\in p(s,d)} delay(e) \tag{4}$$

$$B\big(p(s,d)\big) = \min\{bandwidth(e), e \in p(s,d)\} \tag{5}$$

$$D-J\big(p(s,d)\big) = \sum_{c\in p(s,d)} D-J(e) \tag{6}$$

Where, p(s, d) is the path between a source and a destination, D represents the delay constraint, B denotes the bandwidth constraint and DJ stands for delay jitter constraint. Measuring jitter is a critical element in determining the performance of network is computed as in equation (7)

$$Jitter = \big((Packet\ Arrival + 1) - (Packet\ Start + 1)\big)\big((Packet\ Arrival) - (Packet\ Start)\big)/(n-1) \tag{7}$$

The optimal path must satisfy the following constraints presented in equation (8) – (10)

$$delay(p(s,d)) \leq D \tag{8}$$

$$bandwidth\big(p(s,d)\big) \geq B \tag{9}$$

$$delay - jitter\ (p(s,d)) \leq DJ \quad (10)$$

**Multicast Routing in MANET with GBNWG**

The multicast routing identifies different paths between a source and a destination node. The reliability of data transmission is assured in multicast routing by selecting at least a single reliable path for successful transmission. There is a route flexibility in the case of node failures in any one of the paths, and hence termed as fault tolerant routing. The process of incorporating multicast routing in MANET is challenging due to the mobile nature of the nodes, power and bandwidth constraints. The maintenance of routing table becomes an overhead due to the frequent location changes of the mobile nodes.

Distributed Hash Table (DHT) evaluate the database through maintenance of link stability to establish the stable multicast destination environment. The DHT performs four operations including ping, lookup, fetch value and storage. The Ping function guarantees the consistency of the routing tables of each node. The look up operation identifies the nearest neighboring node in a particular location based on the key value. The fetch value function retrieves the set of nearest neighbors and the store operation stores the location information for each node. The DHT is highly scalable, fault tolerant and fully decentralized. Particularly when the energy is degraded to reach threshold value, the corresponding node transfers the DHT entries to next node which acts as source node. The DHT acts as a router in the MANET that directs the packets along the selected paths. Each node contains a DHT with routing information to forward the data to the next hop nodes.

Consider the mobile nodes $N_a$ and $N_b$ within the particular range of communication with coordinates $(i_1 - i_2)$ and $(j_1 - j_2)$ between the nodes computed as in equation (11)

$$D(N_a, N_b) = \sqrt{(i_1 - i_2)^2 + (j_1 - j_2)^2} \quad (11)$$

Suppose evaluate the node $N_a$ and $N_b$ moves in the direction $\theta_1$ and $\theta_2$ with the velicities $v_1$ and V2 in the direction of $0 \leq \theta \leq 2\pi$. The developed GBNWG computed for the time period $\tau$ for the node $N_a$ and $N_b$ in the distance $d_1$ and $d_2$ with the coordinates with estimation of distance $dist_x$ for the time period is defined as in equation (12)

$$dist_x = V_x^* \tau = \frac{(v_{xnit} + v_{iFinal})}{2} * \tau \quad (12)$$

Where, $v_{xnit}$ and $v_{iFinal}$denote the initial and final velocities of the mobile nodes. The coordinates estimation in the equation is computed based on constraints using equation (13) and (14)

$$I_{xnew} = i_x + dist_x^* cos\theta_x = i_x + \tau(v_{xnit} * cos\theta_x) \quad (13)$$

$$J_{xnew} = i_x + dist_x^* cos\theta_x = i_x + \tau(v_{xnit} * cos\theta_x) \quad (14)$$

The mobile node distance are computed using the equation (15)

$$D(N_a, N_b)_{new} = \sqrt{(i_{1new} - i_{2new})^2 + (j_{1new} - j_{2new})^2} \quad (15)$$

Mobile node network coverage with the GBNWG for the estimation of link stability between nodes $N_a$ and $N_b$ for the time period is computed as in equation (16)

$$Link\ Stability(N_a, N_b) = \frac{T_R}{D(N_a, N_b)_{new}} \quad (16)$$

In above equation (16) network transmission range is stated as TR. The distributed hash table for the node ID, power level, stability factor and distance is computed using hash table presented as follows:

1. Node ID: It stores neighboring node id
2. Power level: The stored consumed total power is transmission between sender and receiver
3. Distance: This neighboring nodes stores field value
4. Stability factor: This value is evaluated based on power level, distance and link quality using equation (17)

$$S_{N_a,N_b} = \frac{PW_{N_a,N_b} * q_{N_a,N_b}}{D_{N_a,N_b}} \quad (17)$$

In above equation (17) $PW_{N_a,N_b}$ and $q_{N_a,N_b}$ represented the signal strength between the node distance to measure the link quality for the multicast routing. The quality link between the nodes are inversely proportional to the ratio of dropped packets to the propotional constant k. The packet drop between nodes are measured based on random mobility of nodes computed as in equation (18)

$$Packet\ Drop\ Ratio = \frac{Number\ of\ dropped\ packets}{Number\ received\ packets} \quad (18)$$

| Algorithm: Route Stability estimation with GBNWG |
|---|
| Step 1: Comute the link stability between neighbouring nodes with the estimated shortest path.<br>Step 2: Repeat the setep 1 for the data transmission between source to destination.<br>Step 3: Compare and evaluate each route values.<br>Step 4: Select the link stability value of route those are higher.<br>Step 5: Transfer packet with the optimal path for data transmission. |

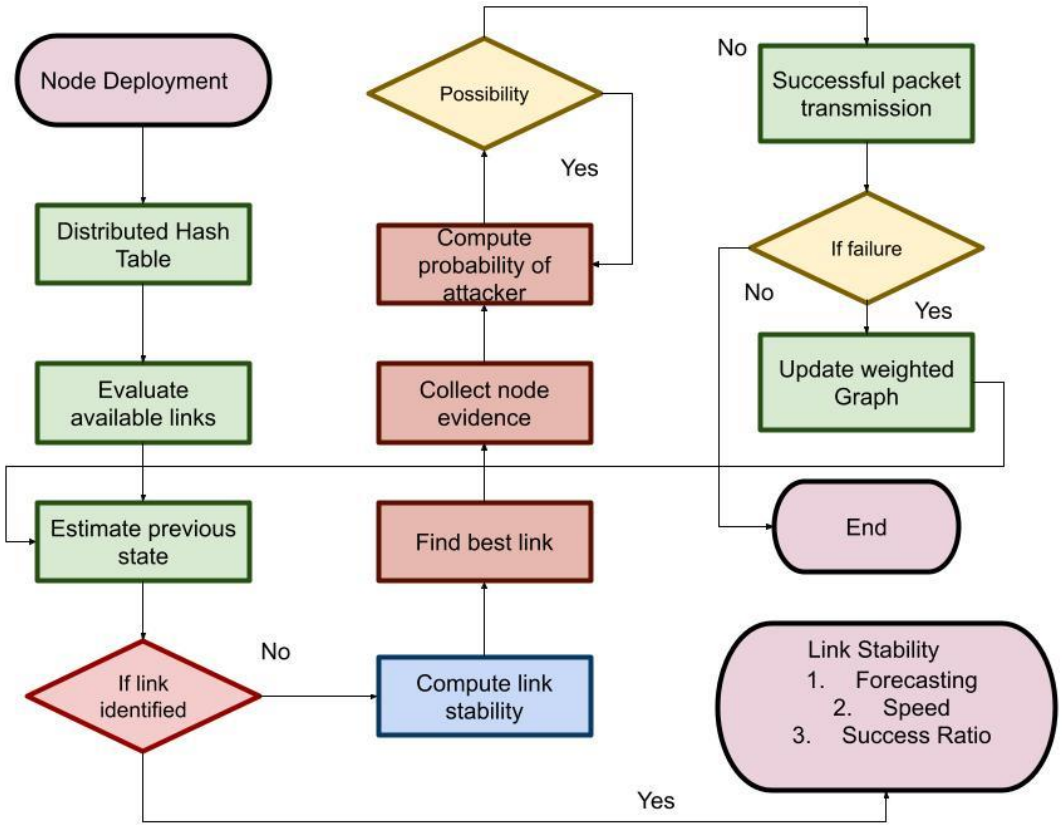


***Figure 1:*** *Flow Chart of GBNWG for the QoS improvement*

The unreliable data transmissions are due to the dynamic topology of the network for the proposed GBNWG is presented in figure 1. The link failures are due to the malfunction of the network components in the path. The links get corrupted due to the natural disasters or when a node is apart from its cluster coverage area. The power and the energy of the nodes are also a main cause of node failure. A set of nodes join together to form a link or a path. In case of over consumption of energy in some of the nodes, the battery power of those nodes gets drained that leads to node failure. The failure of a single node in a path results in path failure. The fault tolerant routing in MANET can be performed using different mechanisms. When compared to the unicast routing protocols, the

multicast routing protocols are suitable for fault tolerant routing in MANET. But, extra overhead is produced in the network due to the propagation of multiple copies of same data. As multicast routing protocol is a Non-Polynomial (NP) hard problem, it is difficult to maintain a fault tolerant data transmission in multicast routing. The process of rerouting the entire data from the source to the destination via a different path consumes more cost and time. To overcome the cost and time constraints, the traffic is shifted to the neighboring of the failed node for routing. The multilevel path redundancy is a technique that introduces several paths between two nodes. This technique varies at different scenarios based on the usage of paths. In some cases, data transmission may occur simultaneously along multiple paths. Otherwise, the paths are divided as primary and secondary paths, where the secondary paths are used on the failure of primary path. After path repair, a message will be broadcast to indicate that the repaired path is ready to use with all the necessary QoS requirements.

## 4. SIMULATION PARAMETERS

The proposed GBNWG model is implemented in Network Simulator NS-2.34 with the 50 nodes. The simulation settings incorporated for the proposed GBNWG are presented in table 1.

***Table 1:*** *Simulation Setting*

| PARAMETERS | VALUES |
|---|---|
| MANET area | 1000 M X 1000 M |
| Node Count | 50 |
| Speed of Node | 2 seconds |
| Size of Packet | 100 bytes |
| Duration of Simulation | 50 ms (millisecond) |
| Access Point Count | 1 |
| Cluster Count | 3 |
| Sink Count | 1 |
| Common Node initial energy | 10 Joules( J ) |
| Transmission Energy | 0.022 J |
| Energy level for reception | 0.032 J |
| Initial energy of cluster head | 100 J |
| Cluster head transmission energy level | 0.2 J |
| Cluster head receiving energy level | 0.4 J |

The proposed GBNWG model is evaluated based on the consideration of different parameters such as node number, Packet Delivery Ratio, throughput, redundancy, code rate and control overhead

### 4.1 Number of Nodes

With the proposed GBNWG model node count connected number is presented based on MAC address in each device through unique identification.

### 4.2 Packet Delivery Ratio (PDR)

The packet delivery ratio is stated as the ratio of delivered messages to the number of received messages as represented in equation (19)

$$PDR = \frac{Number\ of\ Packets\ Received}{Number\ of\ Packets\ Transmited} * 100 \qquad (19)$$

### 4.3 Packet transmission rate

Packet transmission rate is defined as ratio of rate of packet movement from one place to another place for the specified time.

### 4.4 Throughput

Throughput is defined as the ration of successful delivery of data over channel and measured data packets within time slot.

### 4.5 Redundancy

The communication system pathway for the additional connected links in the nodes those goes below the specified value.

### 4.6 Code rate

It is defined as the ratio of packet transmission to remaining transmitted packet count.

### 4.7 Control Packet Overhead

The packet control overhead is defined as the protocol for the RTS (Ready to send) / CTS (Clear to Send) / ACK for the simulation period.

The proposed GBNWG evaluate the routing scheme to achieve the higher code rate compared with the QOD technique presented in table 2.

***Table 2:*** *Comparison Code Rate*

| Time (ms) | Code Rate(%) | |
|---|---|---|
| | QOD based routing | GBNWG |
| 0 | 0 | 0 |
| 5 | 16 | 26 |
| 10 | 21 | 33 |
| 15 | 32 | 42 |
| 20 | 43 | 51 |
| 25 | 54 | 59 |

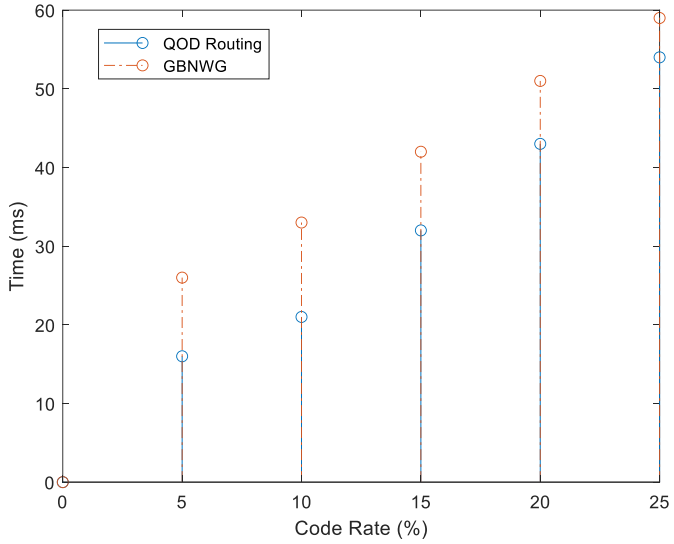


***Figure 2:*** *Comparison of Code Rate*

The figure 2 comparative examination of code rate with proposed GBNWG based routing milliseconds estimation with percentage of code rate. With existing algorithm, the proposed GBNWG model exhibits 39% improved performance. Through analysis it is stated that proposed GBNWG achieves the higher code rate compared with the existing QOD method. The proposed GBNWG routing scheme achieves the minimal control packets compared with existing QOD technique as presented in table 3.

***Table 3:*** *Comparison of Control Packets*

| Time (ms) | Control Packets | |
|---|---|---|
| | QOD based routing | GBNWG |
| 0 | 0 | 0 |
| 5 | 17 | 9 |
| 10 | 38 | 28 |
| 25 | 44 | 19 |
| 20 | 62 | 24 |
| 25 | 78 | 21 |

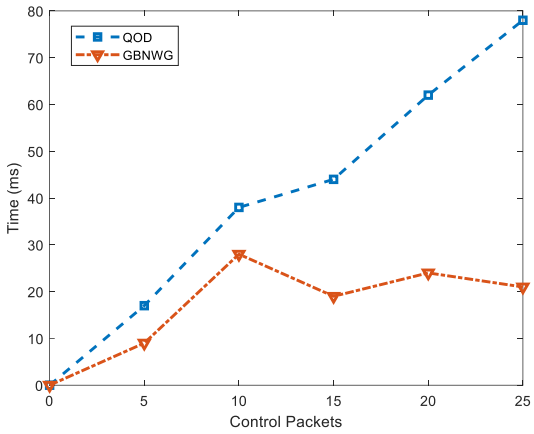


***Figure 3:*** *Comparison of Control Packets*

The figure 3 presented a comparative examination of proposed GBNWG with the existing QOD routing model. The comparative analysis expressed that data packets is achieved as 44 for the proposed GBNWG while the QOD model achieved 76. The comparative analysis of proposed GBNWG exhibits 41% improved performance compared with existing technique. It is observed that proposed GBNWG exhibits minimal control packets compared with QOD technique.

With increase in time the GBNWG exhibits higher data packet compared with QOD routing scheme. The table 4 presented a data packet considered for the comparative analysis of GBNWG and QOD routing model.

***Table 4:*** *Comparison of QOD Routing*

| **Time (ms)** | **Data Packets** | |
|---|---|---|
| | **QOD based routing** | **GBNWG** |
| 0 | 0 | 0 |
| 5 | 70 | 90 |
| 10 | 150 | 180 |
| 25 | 230 | 270 |
| 20 | 350 | 410 |
| 25 | 460 | 550 |

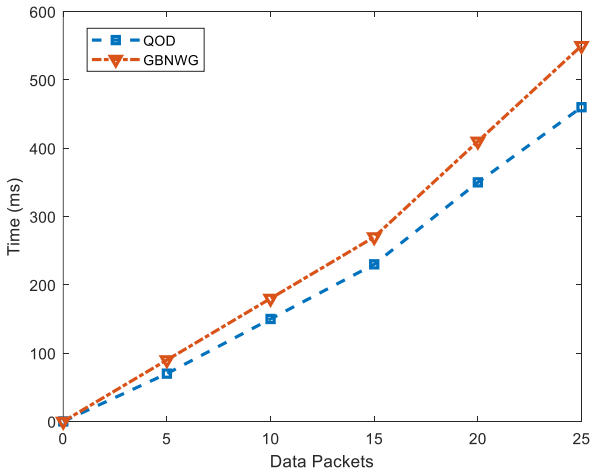


***Figure 4:*** *Comparison of Data Packets*

The network information are transmitted based on the data packets transmitted over the network based on the number of data packets. In figure 4 illustrated the data packets number is presented with the comparative analysis of proposed GBNWG with the existing QOD method. The proposed GBNWG model achieves the 18% improvement for the data packets compared with the existing method. The simulation analysis concluded that proposed GBNWG model exhibits improver

performance compared with QOD method. Through the proposed GBNWG with existing QOD scheme for the reliable received bits routing protocol presented in table 5.

***Table 5:*** *Comparison of Reliable Received bits*

| Time (ms) | Reliable Received bits | |
|---|---|---|
| | **QOD based routing** | **GBNWG** |
| 0 | 0 | 0 |
| 5 | 60 | 75 |
| 10 | 155 | 175 |
| 25 | 220 | 260 |
| 20 | 340 | 360 |
| 25 | 420 | 490 |

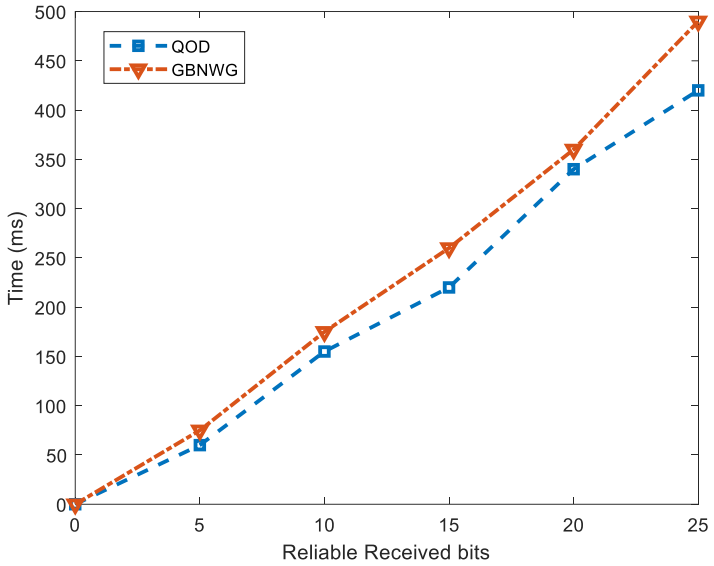


***Figure 6:*** *Comparison of Reliable Received bits*

The comparative examination of proposed GBNWG with the existing QOD scheme exhibits significant reliable received bits in figure 5. Through analysis it is observed that existing algorithm achieves the reliable received bits of 443 and proposed GBNWG scheme is achieved as 560. Simulation analysis stated that proposes GBNWG exhibits 37% improved performance than the QOD model. In table 6 the comparative analysis of proposed GBNWG with the existing QOD routing scheme.

***Table 6:*** *Comparison of Packet Delivery Ratio*

| Time (ms) | Packet Delivery Ratio | |
|---|---|---|
| | **QOD based routing** | **GBNWG** |
| 0 | 0 | 0 |
| 5 | 18 | 23 |
| 10 | 29 | 41 |
| 25 | 44 | 54 |
| 20 | 63 | 77 |
| 25 | 81 | 89 |

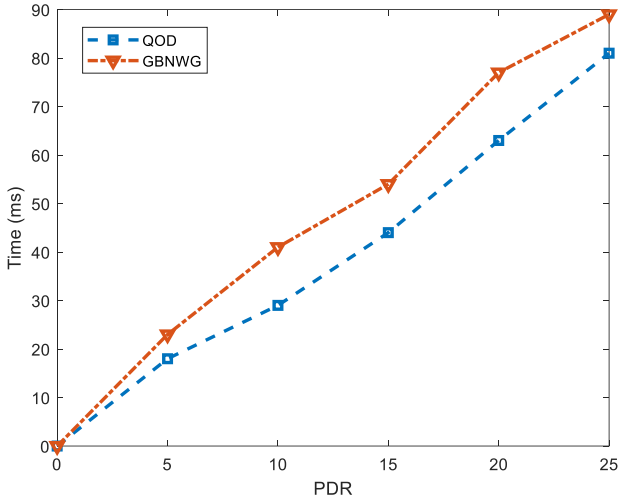


***Figure 6:*** *Comparison of PDR*

The figure 6 provides the comparative analysis of the proposed GBNWG with the QOD model. The experimental simulation analysis stated that proposed GBNWG achieves the PDR rate of 96% while the existing QOD scheme achieves the PDR value of 82%. Through comparative analysis it is observed that proposed GBNWG scheme exhibits improved PDR rate by12%. The estimated redundancy value of the proposed GBNWG presented in table 7.

***Table 7:*** *Comparison of Redundancy*

| Time (ms) | Redundancy | |
|---|---|---|
| | **QOD based routing** | **GBNWG** |
| 0 | 0 | 0 |
| 5 | 0.6 | 0 |
| 10 | 2.6 | 0 |
| 25 | 4.1 | 0.2 |
| 20 | 7.4 | 0.3 |
| 25 | 11.9 | 0.5 |

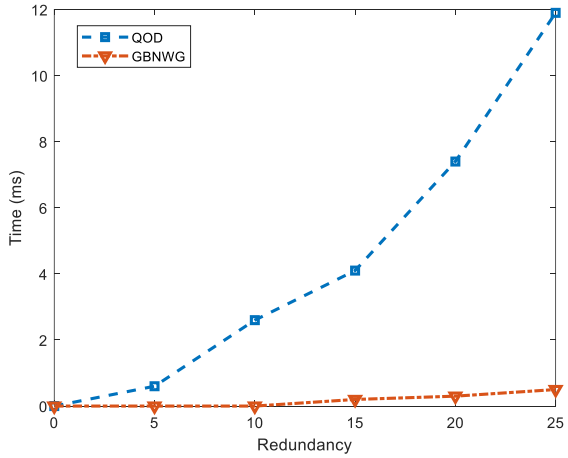


***Figure 7:*** *Comparison of Redundancy*

In figure 7 the comparative analysis of the redundancy for the proposed GBNWG with the QOD scheme. The proposed GBNWG model achieves the redundancy value of 0.2 while the existing scheme achieves the redundancy model value of 13.4. The comparative analysis expressed that proposed GBNWG scheme exhibits 45% improved performance. The effectiveness of proposed GBNWG model is examined with consideration of throughput values. In table 8 comparative examination of proposed GBNWG with QOD model is presented.

***Table 8:*** *Comparison of Throughput*

| Time (ms) | Throughput(bps) | |
|---|---|---|
| | QOD based routing | GBNWG |
| 0 | 0 | 0 |
| 6 | 320 | 360 |
| 8 | 328 | 376 |
| 10 | 339 | 384 |
| 12 | 347 | 398 |
| 14 | 358 | 409 |
| 16 | 369 | 437 |
| 18 | 374 | 468 |
| 20 | 382 | 479 |
| 22 | 393 | 483 |
| 24 | 407 | 496 |

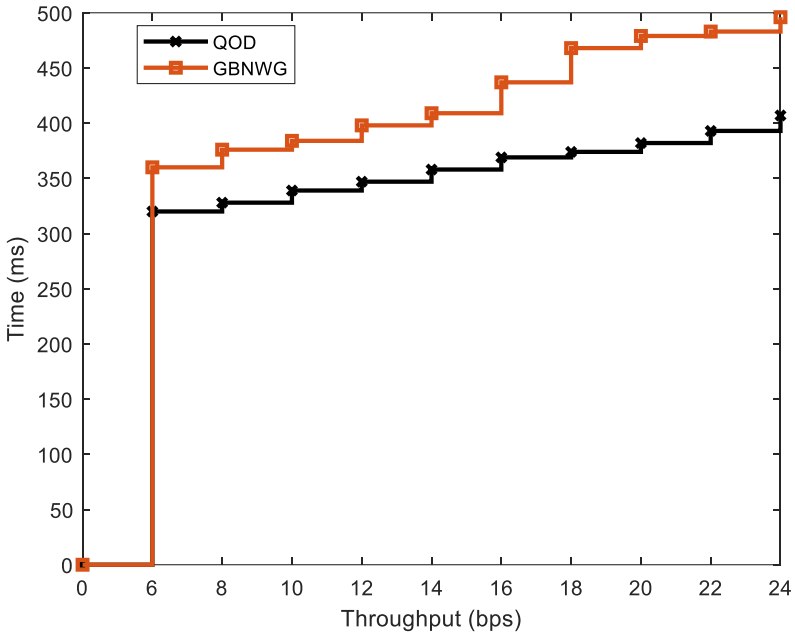


***Figure 8:*** *Comparison of Throughput*

The throughput analysis stated that proposed GBNWG model achieves the throughput value of 467 bps while the existing scheme achieves the throughput value of 378bps. The comparative analysis stated that proposed GBNWG scheme achieves the 12% improved performance compared with the QOD scheme.

## 5. Conclusion

The proposed GBNWG model exhibits effective routing path estimation scheme to evaluate the link stability. With GBNWG scheme node behaviour is estimated based on the hash table maintenance value with link node store information for multicast path establishment and maintenance. The GBNWG uses the weighted graph model for the effective routing path and fault tolerance for the prevention and failure of the system. Through GBNWG scheme effectively manages the maintenance of the hash table in the MANET network. The proposed GBNWG model performance is comparatively examined with existing QOD routing scheme. Simulation performance of the proposed GBNWG scheme exhibits improved performance in MANET network with reduced latency. The GBNWG model is exhibits improved routing performance for fault analysis in the MANET network with effective maintenance of routing in MANET.

## Reference


[1] Naskath, J., Sivakamasundari, G., & Begum, A. (2022). A study on different deep learning algorithms used in deep neural nets: MLP SOM and DBN. *Wireless Personal Communications*, 1-24.

[2] Mchergui, A., Moulahi, T., & Zeadally, S. (2021). Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs). *Vehicular Communications*, 100403.

[3] Laqtib, S., El Yassini, K., & Hasnaoui, M. L. (2020). A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. *International Journal of Electrical and Computer Engineering*, *10*(3), 2701.

[4] Haddaji, A., Ayed, S., & Fourati, L. C. (2022). Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey. *Computers and Electrical Engineering*, *104*, 108460.

[5] Pandey, S., & Singh, V. (2020, July). Blackhole attack detection using machine learning approach on MANET. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 797-802). IEEE.

[6] Vaseer, G. (2020, July). Multi-Attack Detection using Forensics and Neural Network based Prevention for Secure MANETs. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

[7] Rani, P., Verma, S., & Nguyen, G. N. (2020). Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. *IEEE Access*, *8*, 121755-121764.

[8] Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A. R., & Jayasankar, T. (2021). An optimized deep neural network based DoS attack detection in wireless video sensor network. *Journal of Ambient Intelligence and Humanized Computing*, 1-14.

[9] Ponnusamy, V., Kottursamy, K., Karthick, T., Mukeshkrishnan, M. B., Malathi, D., & Ahanger, T. A. (2020). Primary user emulation attack mitigation using neural network. *Computers & Electrical Engineering*, *88*, 106849.

[10] Mughaid, A., AlZu'bi, S., Alnajjar, A., AbuElsoud, E., Salhi, S. E., Igried, B., & Abualigah, L. (2022). Improved dropping attacks detecting system in 5g networks using machine learning and deep learning approaches. *Multimedia Tools and Applications*, 1-23.

[11] Rani, P., Verma, S., Rawat, D. B., & Dash, S. (2022). Mitigation of black hole attacks using firefly and artificial neural network. *Neural Computing and Applications*, 1-11.

[12] Abdan, M., & Seno, S. A. H. (2022). Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad Hoc Network (MANET). *Wireless Communications and Mobile Computing*, *2022*.

[13] Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., & Li, Y. (2020). Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. *IEEE Transactions on Network Science and Engineering*, *7*(4), 2219-2230

[14] Fotohi, R., & Firoozi Bari, S. (2020). A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. *The Journal of Supercomputing*, *76*(9), 6860-6886.

[15] Safara, F., Souri, A., & Serrizadeh, M. (2020). Improved intrusion detection method for communication networks using association rule mining and artificial neural networks. *IET Communications*, *14*(7), 1192-1197.

[16] Islabudeen, M., & Kavitha Devi, M. K. (2020). A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. *Wireless Personal Communications*, *112*(1), 193-224.

[17] Laqtib, S., El Yassini, K., & Hasnaoui, M. L. (2020). A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET. *International Journal of Electrical and Computer Engineering*, *10*(3), 2701.

[18] Zhang, L., Jiang, S., Shen, X., Gupta, B. B., & Tian, Z. (2021). PWG-IDS: An Intrusion Detection Model for Solving Class Imbalance in IIoT Networks Using Generative Adversarial Networks. *arXiv preprint arXiv:2110.03445*.

[19] Yu, J., Ye, X., & Li, H. (2022). A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. *Future Generation Computer Systems*, *129*, 399-406.

[20] Laqtib, S., El Yassini, K., & Hasnaoui, M. L. (2020). Evaluation of deep learning approaches for intrusion detection system in manet. In *The Proceedings of the Third International Conference on Smart City Applications* (pp. 986-998). Springer, Cham.

[21] Ezhilarasi, M., Gnanaprasanambikai, L., Kousalya, A., & Shanmugapriya, M. (2022). A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. *Soft Computing*, 1-12.