[1]S. Mohan

[2]Dr. P. Vimala

Heuristic-Based Genetic Algorithm with Batesian Mimic Features for Secure Energy Efficient QoS Multicast Routing in Manet

Abstract: - This study intends to ensure that data is delivered reliably from the source node to the destination node. By implementing the multicast routing protocol, the MANET network's reliability may be improved significantly. Evaluation of multicast routing for quality of service (QoS) is the primary goal of this study. In multicasting, data packets from one node are transmitted to a set of receiver nodes at a time, simultaneously. First, the method discovers the list of routes between any source and destination. For each mobile node, the trustworthiness is verified by considering the location, mobility speed, energy, several transmissions involved, and their neighbour list and so on. In this method, a scheme strives to predict a stable route by selecting the most stable neighbour relative to the transmitter of the route request message with secure route support and nodes impending during the route discovery process. This minimizes the contention phase, to predict the route lifetime and the transmission time of the data packet to reduce lost data packets and route error messages. The optimal path selection algorithm is used to find the path between sources and destinations. This algorithm, suggests the methodology based on the maximum energy of the node and minimum hops between the nodes. To improve the lifetime of the networks, the research introduced Taylor Kernel Fuzzy C-means clustering and Weighted Clustering Algorithm (WCA) to elect a node by having weighted probabilities. To solve the energy efficiency problem with optimal multicast routing, the research proposed QoS Aware routing of an improved Heuristic-based Genetic algorithm with Mimicking Batesian features (HG-MBF) to improve packet transmission. Further, to tackle the security attack problem, the research proposed the Gradient Deep Belief Classifier (GDBC) to detect multiple attacks in the network. From the result and discussion, the proposed method increases the attack detection rate by 82% as compared to existing works. The memory consumption and computational time of the proposed method are reduced when compared to existing methods.

Keywords: MANET, Multicast Routing, QoS, Weighted Clustering Algorithm, Heuristic-based Genetic, Mimicking Batesian features

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are made up of tiny devices named sensor nodes that are deployed around a region to sense the environment collect data and communicate that data. Sensor nodes have low battery power, minimal processing capability, and limited storage capacity. To convey the data to the sink node in this scenario, the sensor nodes route the information they have collected through intermediary nodes linked by wireless networks. To send the data gathered by various network nodes through a multi-hop routing channel that is within its range to the sink node, an appropriate routing protocol is required. Each sensor node in a multi-hop routing system must communicate both its data and data from other nodes. Due to the minimal battery power that must be provided in the sensor nodes due to the design, power optimization in WSNs is a crucial performance metric. In numerous research studies, cluster formation is modified to increase energy efficiency. The sensor nodes in a cluster-based network are divided based on certain parameters into small clusters. Through data aggregation, cluster formation promotes energy efficiency and Quality of Service (QoS) [1-2].

One of the main areas of wireless network research and development that has the most potential is the mobile ad-hoc network (MANET). MANET is an impulsive network made up of wireless nodes that can move and reconfigure themselves automatically. In the MANET, devices are free to move around, choose their routes, and regularly alter their paths to other devices. Because MANET lacks a centralised infrastructure, it is vulnerable to many types of attacks [3]. The MANET's main features are its limited battery life, constrained bandwidth, and dynamic topology. This trait makes it challenging to generate a transmission path in the MANET. An infrastructure-free network of affiliated nodes connected by wireless links makes up MANET systems. Nodes move chaotically or more accurately, randomly. From the node level to the network level, security in MANETs is essential [4-5]. However, the QoS needs to be met in a way that ensures uninterrupted service given the growing

[1] Research Scholar, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nadu 608002, India. Email: [1*]mohann85@yahoo.co.in (Corresponding Author) .

[2]Asst. Professor, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nadu 608002, India. Email: [2]vimalakathirau@gmail.com

demand for the audio/video data transmission process. The absence of centralised management, internal errors, and external interferences all contributed to the difficulties in ensuring QoS. The link breaks, battery failures, high traffic rates, process failures, and packet retransmissions are examples of internal failures. The mobility of nodes is the main obstacle in routing [6].

Low energy consumption and imbalanced energy distribution have a significant impact on the performance of energy-constrained wireless sensor networks. To attain improved QoS, efficient and sensible routing methods are also required [7]. Using an ideal trust management strategy, a highly secure QoS-aware routing algorithm (HSQ-RA) is proposed in [8]. In HSQ-RA, the improved whale optimization technique is used for multi-hop clustering, and the trust values are used for inter-cluster routing. The trust search algorithm optimises the trust of each node based on the many limitations. To develop a secure routing protocol, a neighbour node discovery is developed for identifying the black hole nodes in the MANET. The routing path through the network is also created using the multi-detection routing protocol. The aim is to create a routing path devoid of any black hole node interruptions [9]. Energy is a difficult issue in the network during data transmission. The Taylor-based Grey Wolf Optimization technique, which combines the Taylor series with the Grey Wolf Optimization approach to identify the best hops for multi-hop routing, was presented to address the energy problem in WSN [10]. The frequent task of link breakage and link construction to move data from the source node to the destination node may exacerbate the frequent changes in network architecture. The main components of MANET routing protocols are the jobs of route discovery, route creation, and data transmission. Ant Colony Optimization (ACO) with swarm intelligence is used to enhance the QoS performance of routing protocols [11]. The Trusted Secure Geographic Routing Protocol (TSGRP), which takes into account the trust value for a node obtained by combining location-trusted information and direct-trusted information, was proposed for detecting attackers [12].

However, an attacker will find it more difficult to work on different forms of offensive moves and is more likely to decline participation due to the mutual existence of the transmission system and the shortage of resources in the MANET. However, these qualities enable the node component to exercise caution while speaking or interacting with other nodes because the nature of the node changes over time and in different environments. This further demonstrates the necessity of resolving the security issue [13-14]. Topological transformation adaptive ad hoc of On-demand Multipath Distance Vector (TA-AOMDV) routing technology was introduced for capable of adjusting to support QoS during high-speed node mobility [15]. It is highly challenging to build a routing system that supports QoS in MANET because node mobility would influence the reliability of links and resource limitations will cause congestion. Frequent link interruptions would harm QoS performance, especially in the case of high-speed node movement, hence it is essential to develop a MANET routing protocol that can adapt to changes in network topology.

2. LITERATURE SURVEY

Most networks make an effort to offer adequate performance and good security. Numerous academics have suggested parallel mechanisms in the literature to study security and QoS. A security framework that is QoS-aware in MANETs was proposed by Esiefarienrhe *et al* [16] utilising the network protocol known as optimized link state routing protocol (OLSR). Although the goals of security and quality of service may not always be the same, this framework aims to close the gap so that a MANET can operate at its best. Multicast is one of the effective strategies in MANET. Multicasting is the simultaneous transmission of data packets from one node to many reception nodes at once. Transmission expenses are decreased through multicasting. One of the difficulties in MANET is choosing the cluster heads. Therefore, Sivapriya *et al* [17] proposed Optimal Route Selection (ORS), which offers cluster head selection and backup cluster head selection to prevent cluster head failure, as well as generation of the best path between the cluster head and member node based on node energy and reliability pair factor, and the emergence of the path based on maximum energy and number of hops between the nodes.

In the investigation of WSN and MANET convergence in the Internet of Things, Quy *et al* [18] took into account a crucial issue, specifically how a converged (WSN-MANET) network delivers QoS support to rich multimedia applications. This is crucial because while multimedia applications constantly demand quality services at a particular level, WSN and MANET's network performances are extremely poor. Also, the authors examine the WSN-MANETs QoS-guaranteed routing protocols. As a result, route selection assumes a very important role because a variety of factors have an impact on how mobile nodes communicate. A lack of battery life, shifting

nodes, and an upsurge in hops and delays all contribute to frequent route modifications and quick battery depletion. As a result, Singla *et al.* [19] suggested an AHP-based Cognitive Route selection in MANETs that is QoS aware (QACRM). It is a cognitive method for choosing the best path that is based on Analytic Hierarchy Process-Simple Additive Weighing (AHP-SAW). With this method, the best communication paths between the nodes are found.

Based on a cross-layer, a quality-aware energy routing protocol (CL-QAERP) is created in [20]. The suggested routing protocols have shown better outcomes than the currently used protocols. Through some efficient routing pathways, the packet delivery rate of transmission has enhanced dramatically. The proposed approach can be simulated using the network simulator ns-2. However, routing protocols do not take into account node conditions like a node's lifespan or network congestion during transmissions. The lifespan of a node is crucial since it needs a lot of power to route or transmit data. However, QoS can lengthen network lifespan, particularly when multi-path routing information is chosen. Therefore, a multi-path routing protocol for IoT-based WSNs dubbed EHO-ETQRP, which is based on the EHO (Elephant Herding Optimization) algorithm and trust, is proposed by Lavanya [21]. The suggested protocol calculated the expenses associated with congestion and node lifetimes to determine the best route for routing.

One of the most dependable hybrid routing systems, Zone Routing Protocol (ZRP) can address the lack of both proactive and reactive routing strategies to achieve particular criteria. To alleviate network congestion, Sahu *et al* [22] tried to examine several QoS factors while using ZRP as the main routing protocol in this study. To achieve the best network performance, the hybrid genetic-bat swarm clustering algorithm (GA-BSO) is suggested in [23]. It uses genetic algorithms (GA) for base station mobility optimization and cluster head (CH) selection. This allows the base station to shift the data collection to the appropriate nodes. In [24], a Hybrid genetic - Bat swarm clustering algorithm (GA-BSO) is proposed that utilizes a Genetic algorithm (GA) for the cluster head (CH) selection and optimizes the Base-station mobility to acquire the optimal network performance. By this, the base station can able to move the data collection for corresponding nodes. Mobile nodes can move anywhere in the network and provide these services. This may result in channel fading, network failure, mobile node failure, etc. Ad-hoc on Demand Multipath Distance Vector (AODMDV) protocols can be used as an alternative to avoid all of these limitations, and performance comparisons between mobile networks can be made using performance analysis.

A QoS-aware routing with bandwidth and end-to-end delay is presented to reduce the control overhead. A QoS-CR (QoS-aware cluster-based routing) solution for WSN was presented by Reebha *et al* [25]. Clustering, routing, and maintenance are the three primary activities that make up the proposed QoS-CR. Fuzzy logic-based clustering (FBC) is used at an earlier stage to effectively group the nodes into clusters and choose the cluster heads (CHs). The best routes between two CHs or from CH to BS are then found using the firefly with levy (FF-L) algorithm. The maintenance procedure is then started to evenly distribute the load and energy usage across the network.

3. RESEARCH PROBLEM DEFINITION AND MOTIVATION

Mobile Ad hoc NETwork (MANET) comprises nodes, which are free to move randomly, yet cooperate to forward packets between source and destination over a multi-hop wireless network. Due to the absence of any fixed node, each node acts as a router, providing the routing capability for the MANET. MANET nodes are autonomous. The implementation and survival of MANETs depend upon the cooperative and trusting nature of its nodes. On the contrary, there is a common assumption in the existing routing protocols that each node participating in the network is trustworthy and cooperative. The mobility of a node can cause frequent route breaks in MANETs. Updating routes can be time-consuming, thus packets might for shorter periods be lost in bursts since they are sent on non-working routes. The network must be less prone to security attacks to achieve an acceptable QoS as security vulnerabilities reduce the QoS of MANETs.

MANETs are most useful in emergencies or military crises when there is no pre-existing infrastructure. Network security in MANETs is difficult to maintain due to its dynamic topology and limited resources. Lack of centralized identity management makes them more vulnerable to attacks. Many attacks like DoS, jamming, Sybil, black hole and grey hole happen in these networks. Sybil attacks happen when multiple identities are created by the person who is responsible Wireless networks use unique identifiers that identify the person. These addresses are used for communication with the network entity. It is easy to get the identity of a node altered or stolen by an adversary. The slight problem arises from the fact that two nodes cannot have the same identity when they are

separate. This can create a really big problem if one node is using the identity of several other nodes to steal their content. This motivates the research to present a security and QoS-aware multicast routing protocol.

4. PROPOSED RESEARCH METHODOLOGY

A Mobile Ad Hoc Network (MANET) is a group of mobile nodes that are formed dynamically by an autonomous system and communicate with each other without any supporting infrastructure. In MANETs, the mobility of nodes causes many challenges, including path preservation, battery life, safety, dependability, and unexpected connection characteristics. As a result, the network's quality of service (QoS) would be compromised (QoS). For the discovery and maintenance of pathways in MANETs, the routing protocol is critical. By implementing the multicast routing protocol, the MANET network's reliability may be improved significantly. Evaluation of multicast routing for quality of service (QoS) is the primary goal of this study. The figure illustrates the flow diagram of the proposed work.

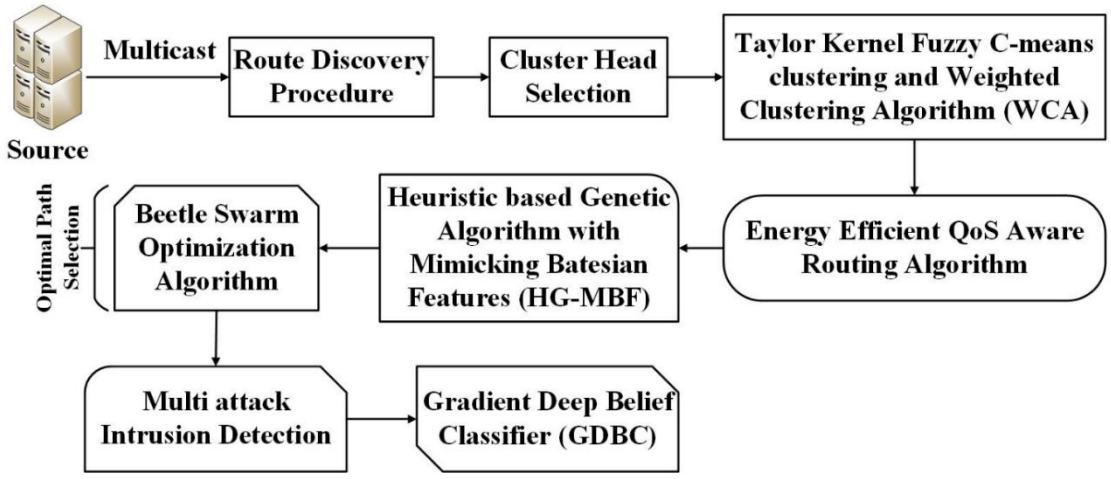

Figure 1: Flow Diagram of the Proposed Work

Figure 1 depicts the flow diagram of the proposed work. This study provides the evaluation of multicast routing for Quality of Service (QoS) with a secure routing algorithm. Initially, the method discovers the list of routes between any source and destination using route request messages and nodes impending during the route discovery process. Taylor Kernel Fuzzy C-means clustering and Weighted Clustering Algorithm (WCA) is proposed for cluster head selection. This elects a node by having weighted probabilities as a cluster Header (CH). An improved Heuristic-based Genetic algorithm with Mimics Batesian features (HG-MBF) is introduced for QoS-aware routing to improve packet transmission performance in MANETs. Beetle Swarm Optimization Algorithm with Delay Aware Energy Efficient (BSO-DAEE) to select an optimum path as well as to mitigate the delay time within the network system is proposed. Gradient Deep Belief Classifiers (GDBC) for multi-attack intrusion detection are designed with the proposed method.

(a) Route Discovery Procedure

The IoT devices are verified for their trustworthiness based on their earlier support contributed to the network. The method measures Mobile Node Secure Route Support (MSRS) for the mobile nodes whereas device support (DS) is measured for the IoT devices. This minimizes the contention phase, to predict the route lifetime and the transmission time of the data packet to reduce lost data packets and route error messages. At the reception of each packet, the route discovery is performed. In the network, the SRS-RREQ packet is broadcasted by this method to discover the routes between each source and destination. To reach different mobile nodes, the neighbours look at the routing table which contains the list of routes, upon receiving the packets. A reply is generated by the neighbour to the source node, if there exists an entry to reach the destination, otherwise forwarded the request packet to the neighbours. Similarly, to find the routes, the route request packet has been forwarded throughout the network. The nodes attach the mobility condition of the nodes, energy, number of transmissions performed, neighbour, and so on at each reply generated. The routes are identified when the source node receives the reply and the above-mentioned parameters are extracted. To the route table, the extracted routes are added. Route analysis and route selection were performed by discovered routes.

Table 1: SRS-RREQ Algorithm for Route Discovery

Algorithm 1: Route Discovery Algorithm

Input: Route Table RT, Neighbor Table Nt, Packet P.
Output: Route Table RT.
Start
Read route table Rt, neighbour table Nt and packet P, Node Table NodeT.
Generate SRS-RREQ packet
SRS-RREQ = {SourceID, DestID}
Initialize Broadcast Timer Br.
Broadcast SRS-RREQ.
While Br runs
Neighbour Receive SRS-RREQ
If SRS-RREQ.DestID ∈ $NTORSRS - RREQ \in RT$ then
Generate SRS-RREP = {NODEID, Energy,Location,NoT,NN,Speed}
Send SRS-RREP towards the source node.
Else
Forward SRS-RREQ to its neighbours
End
Receive SRS-RREP.
Extract Route $R = Route \in SRSRREP$
For each node n
Extract Energy $En = \int_{i=1}^{size\ (R)} R\ (i)\ .Energy$
Extract location $loc = \int_{i=1}^{size\ (R)} R\ (i)\ .Location$
Extract no of neighbour's $Nn = \int_{i=1}^{size\ (R)} R\ (i)\ .Neighbors$
Extract no of transmissions $NoT = \int_{i=1}^{size\ (R)} R\ (i)\ .No\ of\ Transmissions$
Extract speed $Ns = \int_{i=1}^{size\ (R)} R\ (i)\ .Speed$ Add to node table Node T.
End
End
Stop

Table 1 depicts the details of the route discovery algorithm, it represents the process of how the route between any two nodes is performed. In the identified routes, the secure route analysis is performed. Various information like mobility speed, energy, number of neighbours, number of transmissions, and location performed is attached to each intermediate node. The source extracted such information and added it to the routing table which is used to perform route selection.

(b) Cluster Head Selection

The Optimal Route Selection (ORS) provides the cluster head selection and alternate cluster head selection for avoiding the failure of the cluster head, generation of the optimal path between the cluster head and member node based on reliability pair factor and node's energy, and establishment of the path based on maximum energy and number of hops between the nodes (minimum number of hops). This research proposed an efficient algorithm for selecting Cluster Head (CH) nodes by using Taylor Kernel Fuzzy C-means clustering and Weighted Clustering Algorithm (WCA). This algorithm aims to elect a node by having weighted probabilities as a cluster Header (CH). This will be computed by all nodes individually based on the multi-objective, energy utilization, trust, degree of a node, mobility of node and distance between the CH and base stations.

(i) Taylor Kernel Fuzzy C-means Clustering Algorithm and WCA

The proposed Taylor KFCM is the modification of the standard KFCM with the Taylor series in such a way as to inherit the advantages of the Taylor series in KFCM. To handle the small variation among the clusters, the kernel FCM is the integration of kernel functions in the standard FCM. Moreover, using KFCM to map the nodes as

clusters is easy and simple. To directly compute the high dimensional space as it consumes a large time, the kernel functions perform the non-linear mapping of the input data in the dimensional space with the difficulty. On the other hand, the information of the previous iterations is not considered in the standard KFCM and the presence of the noise, the method is ineffective. The Taylor series is used to tackle the difficulty associated with the computations such that the Taylor series is integrated with the KFCM algorithm. Also, the computation of CHs makes a simple and easy phenomenon by integrating Taylor with KFCM, to compute the CH in the present iteration which considers the CHs of the previous iterations. The steps of the proposed algorithm are presented as follows.

Initialization: The randomly chosen cluster centre is initialized in the first step that is given as, S_l; $(1 \leq l \geq Q)$. Let us assume the J. Consider the f, where f varies between 1 and infinity and let us assume a factor κ, which is greater than zero.

Compute the Membership Matrix: Let us assume the membership function $J = [M_{bl}]$ given as in equation (1).

$$M_{bl} = \frac{\left(\frac{1}{1-\kappa(\omega_b, C_l)}\right)^{\frac{1}{p-1}}}{\sum_{a=1}^{N}\left(\frac{1}{1-\kappa(\omega_b, C_l)}\right)^{\frac{1}{p-1}}} \quad (1)$$

Based on the hyper tangent functions, $\kappa(\omega_b, S_l)$ is formulated. Under both the KFCM and the data-weighted clustering approach, it can be seen that M_{bl} holds the same expression. The definition of fuzzy membership degree does not change by the data-weighted fuzzy clustering approach.

Accordingly, the kernel function is given as,

$$\kappa(\omega_b, S_l) = 1 - \tanh\left(\frac{-|\omega - S|^2}{l^2}\right) \quad (2)$$

The main aim of the kernel function, $\kappa(\omega_b, S_l)$ is that it measures the similarity between the individual data point ω_b and lth cluster centre S_l and the application of the hyper tangential functions is that it is applicable for real applications. The $\kappa(\omega_b, S_l)$ is making the weighted sum of the data points to be highly robust, whenever, the ω_b lies away from the other data points. Thus, it is revealed that the proposed algorithm is capable of clustering incomplete data with greater efficiency.

Update the Cluster Centres: The cluster centres are updated following the update in the membership degree that is given as,

$$S_l\,(t+1) = \frac{\sum_{b=1}^{m} M_{bl}^{p}\kappa(\omega_b, S_l).\omega_b}{\sum_{b=1}^{m} M_{bl}^{p}\kappa(\omega_b, S_l)} \quad (3)$$

Using the standard KFCM clustering algorithm, equation (3) is the cluster centre update equation, which is modified using the Taylor series that is enumerated as follows. The Taylor series is given as,

$$S_l\,(t+1) = 0.5\,S_l(t) + 1.3591\,S_l(t-1) - 1.359\,S_l(t-2) + 0.6795\,S_l(t-3) - 0.2259\,S_l(t-4) + 0.055\,S_l(t-5) - 0.0104\,S_l(t-6) + 1.38\,e^{-5}\,S_l(t-7) - 9.92\,S_l(t-8) \quad (4)$$

$$S_l\,(t) = \frac{1}{0.5}\left\{\begin{matrix} S_l(t+1) - 1.3591\,S_l(t-1) + 1.359\,S_l(t-2) - 0.6795\,S_l(t-3) \\ +0.2259\,S_l(t-4) - 0.055\,S_l(t-5) + \\ 0.0104\,S_l(t-6) - 1.38\,e^{-5}\,S_l(t-7) + 9.92\,S_l(t-8) \end{matrix}\right\} \quad (5)$$

The Taylor series insists us simplicity and easier computation and the clustering performance is enhanced by the inclusion of the cluster centres of the previous iterations.

Best Cluster Selection: The cluster centres are subjected to the evaluation of the fit factor individually and the cluster centre with the maximal fit factor is returned as the best cluster centre. Based on the following equation, the fit factor is computed.

$$\mathrm{F} = \alpha.\mathrm{E} + \beta.\mathrm{D} + \gamma.\mathrm{T} \quad (6)$$

Terminate: The best cluster centre S_{best} returned is the best solution. The demerits associated with the existing KFCM are overcome by the clustering using the proposed Taylor KFCM.

A new constant and a new vector are introduced to the data-weighted clustering approach in contrast to the KFCM and together they affect the final clustering results. The objective functions of J_{FCM} and J_{DWF} are written as follows to clarify the differences between the KFCM and the data-weighted KFCM.

$$J_{DWF}(X,U,V,E) = \sum_{j=1}^{n} e^{t_j} \sum_{i=1}^{c} M_{bl}\, d_{i1}^2 = e^{t_1}.\sum_{i=1}^{c} M_{bl}\, d_{i1}^2 + e^{2}.\sum_{i=1}^{c} M_{bl}\, d_{i2}^2 + \cdots + e^{t_n}.\sum_{i=1}^{c} M_{bl}\, d_{in}^2 \quad (7)$$

To the optimal value of the J_{FCM}, each data point has the same contributing weight of "1" in the case of the J_{FCM}. The data weighted fuzzy clustering holds more flexibility than the FCM does as shown in the case of the J_{DWF}.

To select an optimal cluster head for a cluster, this WCA uses four parameters which are transmission power, mobility and battery power, and degree of the mobile node. For a cluster, the mobile node with the lowest combined weight will be elected as the cluster head. For mobile ad hoc networks, the cluster head selection process minimizes communication costs and computation, and the cluster head selection process is not continuing and is invoked very rarely in WCA. In case a cluster head tries to serve more nodes which are higher than the threshold value, the predefined threshold value is decided for the cluster head.

(c) Energy Efficiency with Improved QoS

Owing to nodes' mobility and networks' dynamic infrastructure, finding an ideal trustworthy routing path among source and destination in MANET is a difficult problem. Hence, the work proposed an improved Heuristic-based Genetic algorithm with Mimics Batesian features (HG-MBF) for QoS-aware routing to improve packet transmission performance in MANETs. Here, in this work, a Beetle swarm optimization algorithm with delay-aware energy efficiency (BSO-DAEE) to select an optimum path as well as to mitigate the delay time within the network system is proposed.

(i) Heuristic-Based Genetic Algorithm (HBGA)

Routing in MANETs is a complex process, satisfying intrinsic resource constraint attributes while achieving the desired QoS. For rectifying routing deficiencies in MANETs, it is hereby introduced Genetic Algorithm (GA) to achieve better QoS. By genetic operations for spawning better solutions, the conventional decision-making in the route discovery process is preceded. Inflate the gap between performance and optimization techniques, the properties of the network like infrastructure-less support, wireless communication medium, autonomous nature, etc. The QoS routing aided by a genetic algorithm governed the external node selection process. For discovering optimal routes, the genetic implication in routing requires node-level attribute monitoring.

Encoding: By permutations of integers from 1 to N, the chromosomes are formed, where N is the number of items to be packed.

Building Heuristic Decoding: In the First-Fit algorithm, the packing is performed, which decodes the solution represented in the permutation mapped on the chromosome. The capacity filled in each bin, information used in the fitness function as well as the total of required bins are determined by this process. In a cost-based fitness function, the individual chromosome assessment is carried out. For assessing chromosome fitness, the metrics that are assessed for selecting the CH are used.

Selection: To select individuals from the current population to apply the other genetic operators and form the next generation, the ranking selection is used. Based on their fitness and cumulatively receiving a probability range proportional to their position in the ranking, chromosomes are ordered. A number is randomly generated to determine the selected individual, which indicates the position of the chosen individual.

The following equation (8) is used to evaluate a cost metric ($f[cost\ (CHRi)]$) of the ith chromosome for all $e \in E$.

$$f\ [(CHRi)] = \big(bi\ (P)\ \cup ci\ (P)\big)\ \cap\ bi\ (P) \quad (8)$$

In the genetic routing process, this cost function serves as the fitness evaluation. The mathematical representation of equation (8) is shown in the following equation.

$$f\left[(CHRi)\right] = \left(bi\ (P) + ci\ (P)\right) - \ bi\ (P) \qquad (9)$$

Both bandwidth and connectivity factors are positive factors wherein a delay is considered as a diminishing variable as concluded in equation (9). For all the available chromosomes, the derived cost values swing between 0 and 1. The chromosome with a higher cost value is portrayed as the best solution.

Swap Mutation Operator: Through a swap between two genes randomly selected on the chromosome, each individual generated by the crossover operator is submitted to a random change with probability pm. To escape from a possible stagnation of the solutions, the mutation introduces new information in the population and allows the algorithm.

Fitness Function: The well-accepted expression given the adopted fitness function. Using the number of bins as a reference, with the same number of bins instead of the simplest idea of evaluating the solution only, this objective function is capable of distinguishing the efficiency of two solutions. A refined measurement of the candidate solutions is allowed by the used function. The elimination of unfilled bins of a solution, this measure facilitates during the evolutionary process, it given the better fitness value of solutions that present a lower level of capacity utilization in some bins. For this purpose, the search is directed toward the maximization of the function depicted in (10), where, M is the number of bins obtained by the solution, F_i represents the sum of the weights of the items in the ith bin, and C is the capacity of the bins.

$$f_{BPP} = \frac{\sum_{i=1}^{M}(F_i/C)^2}{M} \qquad (10)$$

A defended model species are exploited by an undefended, and thus palatable, mimic, the predator education provided mimics Batesian features. To which quasi-Batesian mimicry has been added as a third possible category, these two kinds of mimicry were the original components of a mimicry spectrum. A seemingly Mullerian relation, in the sense, that both prey species are defended in quasi-Batesian mimicry, by retarding rather than speeding up the predator learning process, can have the Batesian feature that the least defended species of the pair is harmful to the other. However, the learning process in ways other than to promote parasitism could affect either by different defence substances (qualitative variation) or by different concentrations of the same defence substance (quantitative variation), it is also conceivable that contrast in defence between a pair of similar-looking species.

Accordingly, the higher fitness chromosome is used for the next generation offspring, until the chromosome or the CN is updated, the process is repeated. The chromosomes are descended based on their cost for ease of neighbour selection. For pursuing transmission, the first position chromosome is selected from the descended list. Until a new best-fit chromosome is discovered, the chromosome with higher fitness is recursively used.

(ii) Beetle Swarm Optimization Algorithm with Delay-Aware Energy Efficiency

The main objective of the proposed methodology is to develop an energy-efficient based path selection process. The performance of the BAS algorithm in dealing with high-dimensional functions is not very satisfactory, and the iterative result is very dependent on the initial position of the beetle is founded on the continuous deepening of the experiment. The efficiency and effectiveness of optimization are greatly affected by the choice of the initial position. By expanding an individual to a group, further improvements are made to the BAS algorithm, inspired by the swarm optimization algorithm.

Accordingly, with a path-fixed and uncontrollable Mobile node, a Delay-aware Energy-efficient Routing algorithm (DERM) for route selection. To the sink within the delay constraint (called destination region) via the shortest path, and then the packets will be collected before their deadlines when the sink arrives, DERM enables each node to transmit packets to a dynamic region accessible. A flexible balance between the data delivery delay and the energy consumption is achieved by DERM and it can be observed that, compared to the other two schemes. The design of DERM is nontrivial as it intrinsically contains three issues: (1) energy-optimal routing towards time-varying regions; (2) efficient sink location estimation; and (3) a reliable fault-tolerant routing mechanism for handling the location errors. The following summarizes the contribution of this work.

For data collection in WSNs with a path-fixed and strictly uncontrollable mobile sink, DERM is the first work concerned about both the delivery delay and energy efficiency. For energy-optimal routing towards dynamic

destination regions, a location-based greedy forwarding algorithm is designed and in this new context after being slightly modified, it demonstrates that the right-hand rule can also be used for void handling.

- Based on the mobility pattern to determine the sink location, an effective location calibration method is presented, which can be combined with the rough estimation. In this manner, the routing performance can be guaranteed with very low control overhead.
- To deal with the sink location errors caused by delayed calibration or unpredicted faults, an approach named track routing is proposed. Adopting a "greedily advance, discreetly step back" strategy, can guarantee reliable and on-time delivery in an energy-efficient manner.
- Through extensive experiments and comprehensive performance comparisons, the effectiveness of the proposed method is verified. Additionally, a delay-constrained rendezvous-based routing is presented, providing a supplementary baseline.

To the optimization problem, each beetle represents a potential solution in this algorithm and the fitness function determines each beetle corresponds to a fitness value. The beetles also share information similar to the particle swarm algorithm but based on their speed and the intensity of the information to be detected by their long antennae, the direction and distance of the beetles are determined.

The idea of the particle swarm algorithm is borrowed in mathematical form. In an S-dimensional search space, there is a population of n beetles represented as $X = (X_1, X_2, \dots\dots, X_n)$, where the i th beetle represents an S-dimensional vector $X_i = (X_1, X_2, \dots\dots, X_n)^T$. The fitness value of each beetle position can be calculated according to the target function. The speed of the i th beetle is expressed as $V_i = (V_{i1}, V_{i2}, \dots\dots, V_{iS})^T$. The group extreme value of the population is represented as $P_g = \left(P_{g1}, P_{g2}, \dots\dots, P_{gS}\right)^T$, and the individual extremity of the beetle is represented as $P_i = (P_{i1}, P_{i2}, \dots\dots, P_{iS})^T$. The mathematical model for simulating its behaviour is as follows:

$$X_{is}^{k+1} = X_{is}^{k} + \lambda V_{is}^{k} + (1-\lambda)\xi_{is}^{k} \qquad (11)$$

Where, $s = 1,2, \dots, S$; i= $1,2, \dots, n$; k is the current number of iterations. The speed of beetles is represented as V_{is}, ξ_{is} represents the increase in beetle position movement, and λ is a positive constant. Then the speed formula is written as

$$V_{is}^{k+1} = \omega V_{is}^{k} + c_1 r_1 \left(P_{is}^{k} - X_{is}^{k}\right) + c_2 r_2 \left(P_{gs}^{k} - X_{gs}^{k}\right) \qquad (12)$$

Where, r_1 and r_2 are two random functions in the range [0,1], c_1 andc_2 are two positive constants, and ω is the inertia weight. ω is a fixed constant, but with the gradual improvement of the algorithm in the standard PSO algorithm.

The search behaviours of the right antenna and the left antenna are respectively expressed as:

$$\left.\begin{aligned} X_{rs}^{k+1} &= X_{rs}^{k} + V_{is}^{k} * d/2 \\ X_{is}^{k+1} &= X_{ls}^{k} + V_{is}^{k} * d/2 \end{aligned}\right\} \qquad (13)$$

A set of random solutions are first initialized by the BSO algorithm. Based on its search mechanism, the search agent updates its location at each iteration and the best solution currently available. The population's iteration speed is cannot only accelerated by the combination of these two parts but also reduce the probability of the population falling into the local optimum, which is more stable when dealing with high-dimensional problems. The pseudo-code of the BSO algorithm is presented in table 2.

Table 2: Beetle Swarm Optimization Algorithm

Algorithm 2: Beetle Swarm Optimization Algorithm
Initialize the swarm X_i $(i = 1,2, \dots, n)$
Initialize population speed v
Set step size δ, speed boundary v_{max} and v_{min}, population size $sizepop$ and maximum number of iterations K
Calculate the fitness of each search agent
While $(k < K)$
Set inertia weight ω using equation (14)

$$\omega = \omega_{max} - \frac{\omega_{max} - \omega_{min}}{K} * k \quad (14)$$

Update d using equation (15)

$$d^t = \delta^t / c_2 \quad (15)$$

for each search agent

Calculate $f(X_{rs})$ and $f(X_{ls})$using equation (13)

Update the incremental function ξ by the equation (16)

$$\xi_{is}^{k+1} = \delta^k * V_{is}^k * sign\left(f\left(X_{rs}^k\right) - f\left(X_{rs}^k\right)\right) \quad (16)$$

Update the speed formula V by the equation (12)

Update the position of the current search agent by the equation (11)

end for

Calculate the fitness of each search agent $f(x)$

Record and store the location of each search agent

for each search agent

if $f(x) < f_{pbest}$

$f_{pbest} = f(x)$

end if

if $f(x) < f_{gbest}$

$f_{gbest} = f(x)$

end if

end for

Update x^*if there is a better solution

Update step factor δ by the equation (17)

$$\delta^t = c_1 \delta^{t-1} + \delta^0 = eta^* \delta^{t-1} \quad (17)$$

end while

Return x_{best} , f_{best}

In theory, the BSO algorithm includes exploration and exploitation ability, so it belongs to global optimization. Furthermore, the rapidity and accuracy of population optimization are enhanced by the linear combination of speed and beetle search and it makes the algorithm more stable. Subsequently, the overhead of location calibration is effectively reduced by delay-aware routing.

(d) Intrusion Detection in MANET

Security is a fundamental prerequisite in a self-evaluability network and providing that in any situation is the most problematic task as the network is highly dynamic with no trusted centralized monitoring. In comparison with networks, MANETs are highly susceptible to intruders. To secure a mobile ad hoc network (MANET) in adversarial environments, a particularly challenging problem is how to feasibly detect and defend against possible attacks on routing protocols. Design of intrusion detection, and MANET prevention mechanism, with scrutinized detection rate, and memory consumption with minimal overhead are crucial research concerns. Consequently, Gradient Deep Belief Classifier (GDBC) for multi-attack intrusion detection is designed with the proposed method.

(i) Gradient Deep Belief Network Classifier

Gradient Deep Belief Network Classifier (G-DBNC) Multi-attack Intrusion Detection model is applied to make multi-attack intrusion detection in this work. DoS and Zero-day attacks are the two types of intrusions of multi-attack intrusion detection, by applying the G-DBNC model, it is detected at an early stage. To identify the attack, a zero-day attack usually refers to the time or number of days taken for a developer. To analyse the zero-day attack, packet drop rate, packet forwarding from other nodes, and packet delivery ratio against the comparison with the corresponding threshold, these three different factors are used. With Gradient Deep Belief Network Classifier (G-DBNC), the performance is analyzed.

An energy-based model with a set of visible units v_i and hidden units h_j, i and j representing a node in the visible and invisible layer respectively are formulated. Using visible units and features (data packet sent, the data packet

received directly, the data packet received via forwarding nodes, cluster head nodes) are represented via hidden units, and the values (both values given as input and initialized) are represented. An integrated formulation with energy as a constraint is then formulated as given below.

$$E(v,h) = -\sum_i b_i v_i - \sum_j b_j h_j \sum_i \sum_j v_i h_j w_{ij} \quad (18)$$

From the above equation (18), v_i, h_j refers to the bipartite states of visible unit i and hidden unit j with biases represented by b_i, b_j, w_{ij} represents the weight between them and is formulated as given below.

$$w_{ij} = E\left(v_i h_{jdata} - v_i h_{jmodel}\right) \quad (19)$$

From equation (19), E indicates the energy formulation, and a probability is assigned to visible and hidden vectors, as given below.

$$Prob\ (v,h) = \frac{1}{Z}\ e^{-E(v,h)} \quad (20)$$

Therefore, via the attention-based gradient function, the weights in the hidden units are reconstructed in this work. This is mathematically formulated as given below.

$$w_{ij} = \sum_{i,j=1}^{n} \beta_{ij} h_j \quad (21)$$

From the above equation (21), β_{ij} refers to the amount of attention the ith output should pay to the jth input, with h_j representing the reconstruction state for the jth information. For the ith output, a of the inputs (i.e., clusters formed and initialized visible units) described the attention outcomes by obtaining a softmax atop, β_{ij} is evaluated. This is mathematically formulated as given below.

$$\beta_{ij} = Softmax\left(a_{ij}\right) = \frac{Exp(a_{ij})}{Exp(a_{ik})} \quad (22)$$

$$a_{ij} = P\left(S_{i-1}, h_j\right) = RP\left(a_{ij}|v_i\right) \quad (23)$$

From the above equation (23), P refers to the positioning model that scores how well the inputs around position i and the output at position i complement each other, and h_j refers to the hidden state from the antecedent time. Finally, for position weight update and visible units for intrusion detection, relative probing RP is performed.

Using re-constructing the weight in deep belief via attention-based gradient function and positioning function, multi-attack intrusion detection is performed. First, to improve the attack detection rate, re-construction of weight is performed with the aid of an attention-based gradient function that performs relevance sorting, without concentrating on all the nodes in the clusters by applying these two functions. Finally, with the positioning function, multi-attack intrusion detection is achieved, therefore serving for both zero-day attacks and DoS attacks.

5. EXPERIMENTATION AND RESULT DISCUSSION

To simulate the routing protocol for MANET with the secured route, to provide composite services for a particular user according to their requirement, the article utilized Matlab. The required simulation parameters and their values are provided in Table 3. The proposed system is implemented in MATLAB under the windows operating system with 4 GB of RAM. The study simulated 53 intermediate nodes and 35 mobile nodes moving into an area of 1000 m × 1000 m according to the random-mobility model.

Table 3: Simulation Parameters

Parameters	Values
Number of nodes	1000
Number of mobile nodes	350
Number of packets	8
Area Size	1000×1000 (m^2)
Routing Protocol	AODV
Bandwidth	1000 kHz

The main concern of this section is to test the efficiency of MOEAQ in providing multicast users with QoS and satisfying the service requirements of multimedia applications. The article focus on quantitative aspects of efficiency such as throughput, delivery delay, jitter, and packet loss ratio. The performance evaluation metrics such as throughput, end-to-end delay, delivery ratio, average path lifetime, and routing control overhead are used to measure the performance of the algorithms. The results of the proposed QoS-based algorithm are compared with existing algorithms such as the energy-efficient routing based on the MAODV-LAMP, EPOA-MAODV, and HAPM. Further, the intrusion performance is analysed with existing methods of ANN, SAE-IDS, and BRSC respectively.

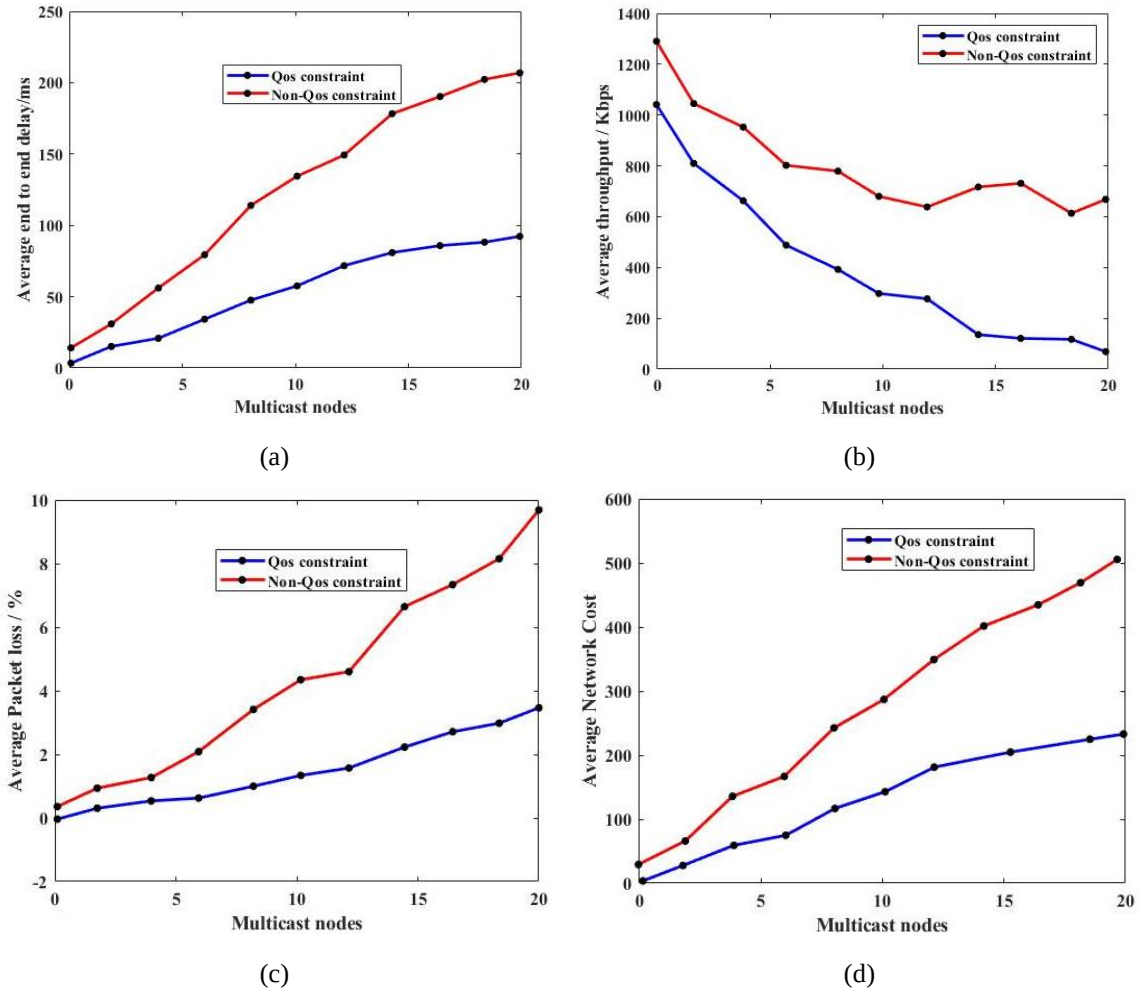

Figure 2: Multicast Node Performance Analysis

Figure 2 is the changing mode of the average end-to-end delay. The multicast route with QoS constraint can lower the cost of the delay. Figure 2(a) described the relationship between the nodes of multicast and average throughput; the multicast route with a constraint can support a much better throughput. Figure 2 (b) described the relationship between the multicast nodes and the average packet-loss rate. This can view that the multicast routing protocol with QoS reduces the packet-loss rate, and improve the transmit rate of the packet. Figure 2(c) shows the changing relationship between the multicast nodes with a node average of 3 m/s and network cost, the network cost of multicast routing of QoS constraint is much lower than that of routing without constraint. In Figure 2(d), the multicast nodes are 10, the changing relationship between the multicasts movement rate and the average price of the network, the multicast node's average movement rate of the multicast route of QoS has superior performance, while for the multicast route without QoS constraint.

a. QoS Measures Performance Analysis

The QoS measures used to ensure that quality is optimized in the network are throughput, delay, and jitter.

i. Throughput: It represents the number of bits forwarded from the MAC to higher layers in all nodes in the network; it is measured in bits per second. The throughput may also be referred to as the average number of packets successfully transmitted or received per second. This work focused on the application throughput which is the total user data sent to the intended destination per second. The formula to calculate throughput is given as:

$$Throughput = {}^{Pd}/_{T} \tag{24}$$

Where, Pd is the number of packets delivered and T is the time in seconds.

ii. Delay: This is normally the time taken for one packet to be transmitted from the source node to the destination node. This performance metric evaluates the routing protocol's effectiveness in the use of network resources. Delay may be caused by several obstacles including transfer time, buffering during discovery latency, interference queue, and propagation. The formula to calculate delay is given as:

$$Delay = Trx - Tst \tag{25}$$

Where, Trx is the time the packet is received and Tst denotes the time taken for the packet sent.

iii. Jitter: This is the variation in time between route changes and data packets arriving. The variation may be caused by internal sources, such as data transmission errors, the presence of a malicious node, and network congestion. The formula to calculate jitter is given as

$$Jitter = Dt - Dp \tag{26}$$

Where, Dt is the transmission delay of the current packet and Dp is the transmission delay of the previous packet.

iv. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the ratio of the number of data packets received by the destination, to the number of data packets sent by the source. The PDR is calculated as follows:

$$PDR = \frac{\sum packets\ Received}{\sum packets\ sent} \tag{27}$$

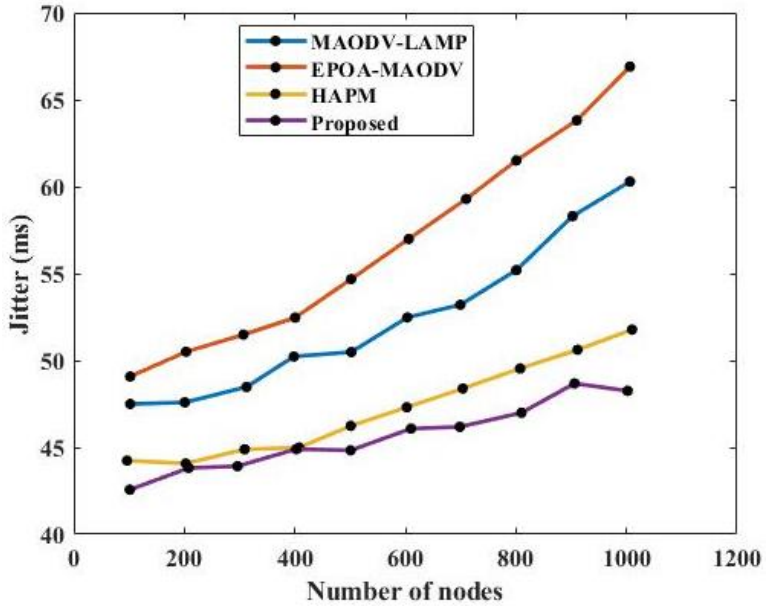

Figure 3: Jitter Performance Analysis

The proposed QoS framework outperformed the malicious scenario again in terms of jitter recording an average of about 6500 microseconds as compared to the malicious scenario which had margins of about 35,000 microseconds. In the sinkhole scenario, the first node had a delay of 26,543.9 microseconds. Nodes 2-5 showed a constant jitter of 26,468.72 microseconds but node 6 and node 12 both had 26,400.87 microseconds. This was an expected margin based on the malicious activity within this broadcast session. As shown in Figure 3, the

framework significantly lowered the levels of jitter among all the nodes. The framework proved to be effective in low-density node scenarios.

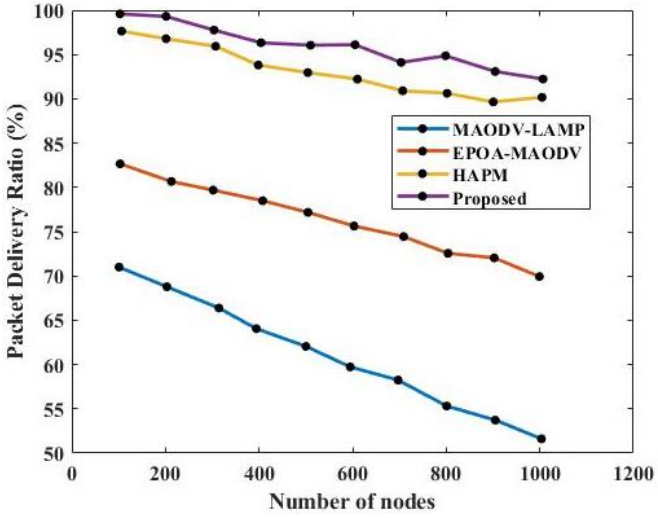

Figure 4: Packet Delivery Ratio Vs Number of Nodes

The performance of the four protocols MAODV-LAMP, EPOA-MAODV, and HAPM is shown in Figure 4. It is observed that the packet delivery ratio PDR increases relatively with the number of nodes in the network. It can be seen that there is a greater chance of having a more stable routing with a network that contains more nodes compared to a network with fewer nodes.

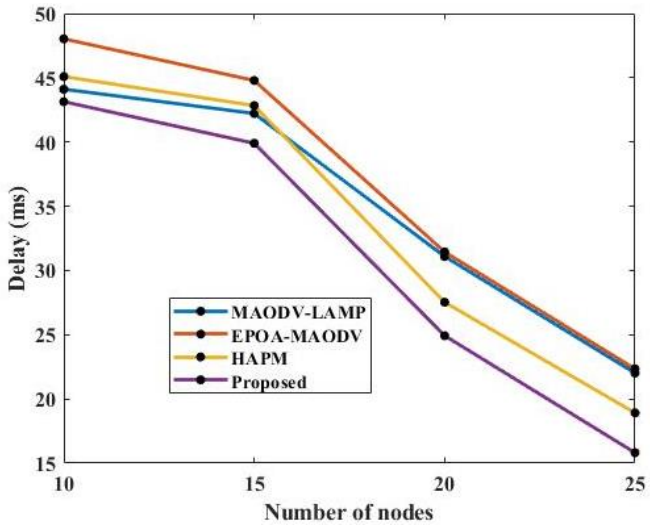

Figure 5: Delay vs Number of Nodes

The proposed QoS framework had the lowest recorded value in terms of network delay, and as expected, the malicious scenario produced the highest level of delay for any 16-node scenario as shown in Figure 5. The delay in the MANET scenario was caused by the time the attack exceeds the failure threshold value before forwarding the packets to the rest of the network when compared to the existing techniques. The framework significantly reversed this action by a significant margin meaning that the intrusion was identified, blacklisted, and alternative routes that guarantee an acceptable level of QoS were chosen. In the framework scenario, the first node had a delay of 12,251.96 microseconds. Node 20 has an elevated delay value of 13,632.94 microseconds

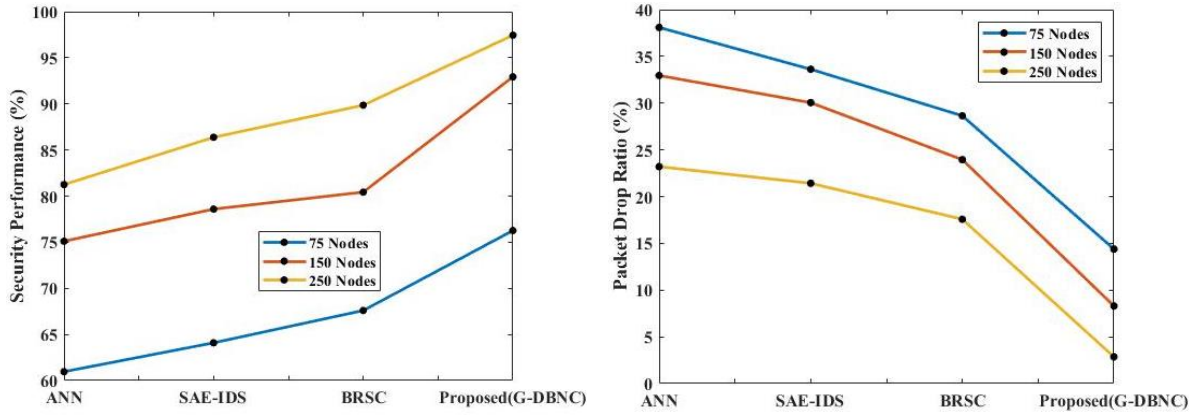

Figure 6: Performance Analysis of Intrusion Detection

The accuracy in secure routing produced by different algorithms at different nodes (75 nodes, 150 nodes, 250 nodes) is analyzed and presented in Figure 6. The proposed algorithm has produced higher accuracy than other methods ANN, SAE-IDS, and BRSC. The ratio of packet drop generated by various methods is measured and presented in Figure. In comparison to the existing techniques, the proposed G-DBNC algorithm has produced fewer packet drops than other methods.

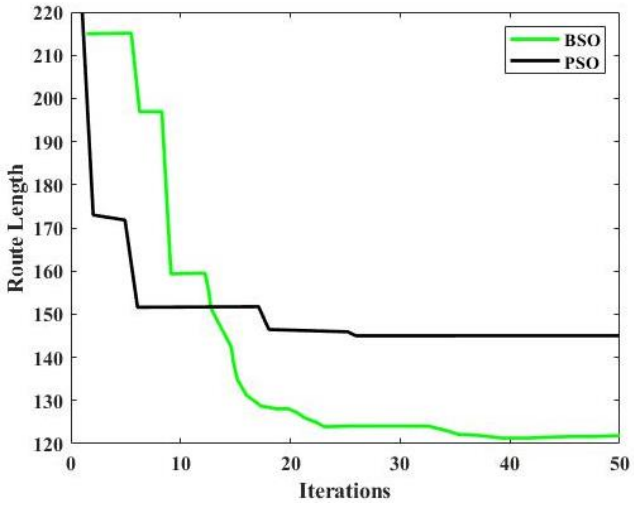

Figure 7: Iteration Time Performance analysis

Figure 7 depicts the comparison of iteration times with the route length of the optimization algorithm. The computation time increases with the increasing number of iterations when compared to the PSO technique results. The length of route planning based on the BSO algorithm is about 90% of that of the route planning based on the PSO algorithm. The three-dimensional route planning based on the BSO algorithm has a higher convergence rate compared with that based on the PSO algorithm. Given the same number of iterations, the optimization results of the BSO algorithm are generally better than those of the basic PSO algorithm. Moreover, the probability of trapping in the local optimal solution during the optimization process is decreased, which is attributed to the position updating strategy of the beetle. In the late iteration, the optimal route based on the BSO algorithm is generally better than that based on the basic PSO algorithm.

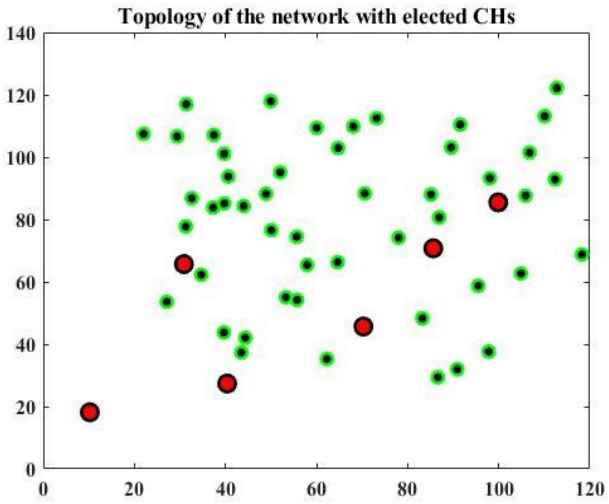

Figure 8: Cluster Head Election Using Taylor Kernel Fuzzy C-means Approach

A sample MANET with 50 nodes considered for simulation and cluster head elected using Taylor Kernel Fuzzy C-means Clustering Algorithm and weighted clustering algorithm based cluster head election is shown in Figure 8. The circled red colour indicates the elected cluster head in the topology of the networks.

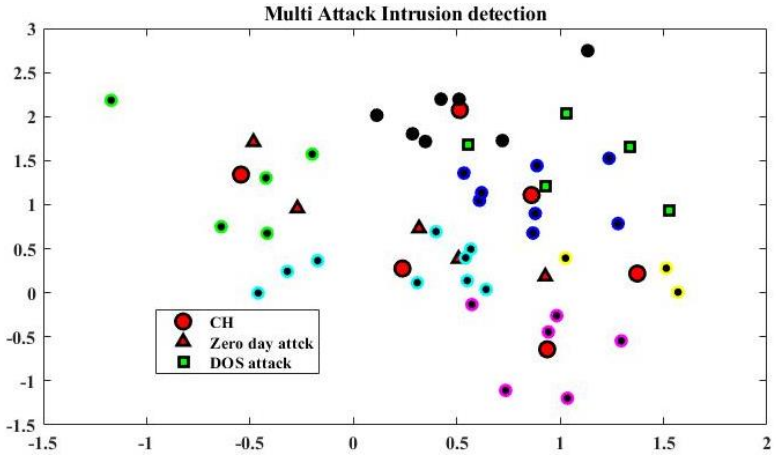

Figure 9: Multi Attack Intrusion Detection

From the above figure 9, the BSO-DAEE method exactly identifies the DOS attack and zero-day attack. This is due to the application of the Gradient Deep Belief Network Classifier in the BSO-DAEE method for multi-attack intrusion detection via re-constructing weight with attention-based gradient function and positioning function. With these functions, improve the attack detection rate, and re-construction of weight is performed for relevance sorting, without concentrating on each node in clusters. From that, efficient attack detection in the BSO-DAEE method is achieved.

i. Attack Detection Rate

The first metric to be analyzed for intrusion detection is the attack detection rate. This metric is more significant in detecting intrusion because the higher the detection rate more effective the method is. The attack detection rate is measured as given below

$$ADR = \sum_{i=1}^{n} \frac{mIDS}{m_i} * 100 \qquad (28)$$

From the above Equation (38), the attack detection rate 'ADR' is measured based on the mobile nodes provided as a sample for simulation and the mobile intruder nodes correctly identified as intrusions. It is measured in terms of percentage (%).

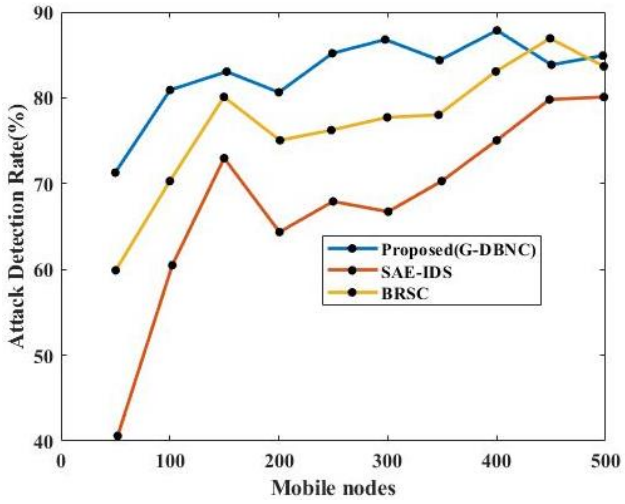

Figure 10: Attack Detection Rate Comparison Analysis

Figure 10, depicts the attack detection rate measured for 500 different mobile nodes. The figure shows that the attack detection rate is directly proportional to the mobile nodes considered for simulation. Also, it is found to be higher using the proposed BSO-DAEE method. This is because the BSO-DAEE method utilizes Gradient Deep Belief Network Classifier (G-DBNC) for multi-attack intrusion detection via re-constructing weight via attention-based gradient function and positioning function. With these functions, enhancing the attack detection rate, re-construction of weight is performed that performs relevance sorting, without concentrating on each node in clusters.

ii. Memory Consumption

The metric analyzed for intrusion detection and prevention is the memory consumed in detecting the intrusion in MANET. This metric is of paramount use because the detection rate should be improved, but the memory consumed in detecting the intrusion should also be improved. The memory consumption is formulated as given below

$$MC = \sum_{i=1}^{n} m_i * MEM[AD] \quad (29)$$

From the above Equation (39), memory consumption 'MC' is measured according to the samples concern 'mi' and the memory incurred during the detection of intrusion 'MEM [AD]' or attack. It is measured in terms of kilobytes (KB).

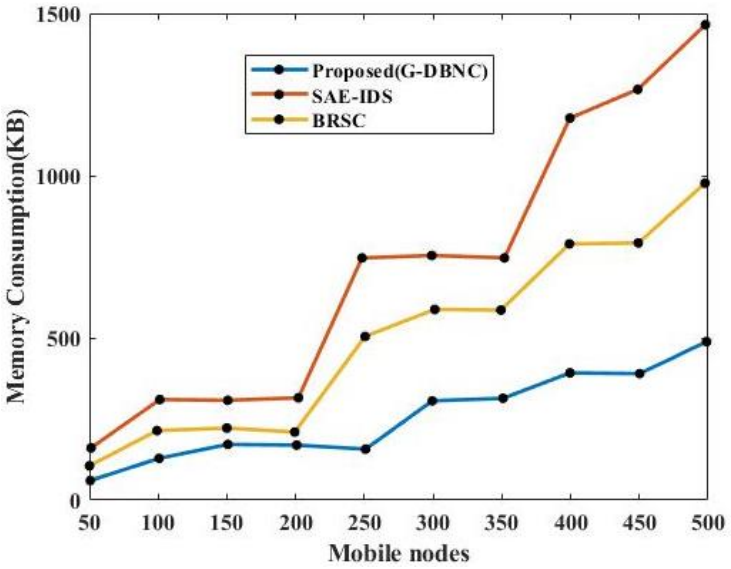

Figure 11: Memory Consumption Performance Analysis

Figure 11 depicts the memory consumption concerning 500 different mobile nodes observed at different periods. As shown in the above figure, the memory consumption is neither directly proportional nor inversely proportional to the mobile nodes. This is due to the topological changes observed in the network. In MANET, the G-DBNC method considers attack nodes in the network and it removes all the attack nodes. Thus, the memory consumption using the BSO-DAEE method is lower.

iii. Computational Time

The third metric analyzed is the computational time involved in detecting the intrusion is measured and mathematically formulated as given below.

$$CT = \sum_{i=1}^{n} m_i * Time\ [AD] \tag{30}$$

From the above Equation (40), the computational time 'CT,' is measured based on the mobile nodes considered for simulation 'mi' and the time involved in detecting the attack or intrusion 'Time[AD]'.

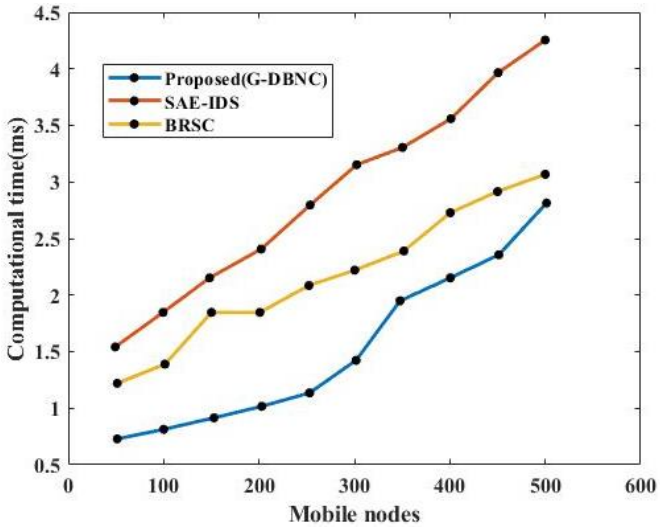

Figure 12: Computation Time Performance Analysis

Figure 12 illustrates the computational time involved in detecting the intrusion. From the figure, it is inferred that the computational time is directly proportional to the mobile nodes. This is because increasing the number of mobile nodes causes an increase in electing the cluster head and, therefore, increases cluster formation. The computational time using BSO-DAEE is minimal because of the utilization of the Gradient Deep Belief Network classifier for intrusion detection. BSO-DAEE performs relevance sorting, without concentrating on all the nodes in the clusters. Therefore, the computational time for detecting intrusion also increases linearly

5. RESEARCH CONCLUSION

Mobile Ad Hoc Networks (MANETs) are collections of mobile nodes that self-organize in networks with dynamic topologies. Base stations and access points are not necessary as part of the infrastructure for MANETs in advance. In general, the consumption of battery energy has not always been taken into account while designing a QoS multicast routing protocol with multi-constrained metrics. Multicasting is the simultaneous transmission of data packets from one node to many reception nodes at once. The process starts by identifying all possible paths between any source and destination. The location, mobility speed, energy, and amount of transmissions involved for each mobile node, as well as their neighbour list, among other factors, are used to determine whether a node is trustworthy. By choosing the most stable neighbour in relation to the transmitter of the route request message and the nodes approaching throughout the route discovery process, this method attempts to forecast a stable path. To reduce lost data packets and route error messages, this minimizes the contention phase, predicts the route lifespan, and speeds up data packet transmission. An optimal path selection algorithm is used to find the path between sources and destinations. Consequently, the article studied Taylor Kernel Fuzzy C-means clustering and Weighted Clustering Algorithm (WCA) to elect a node by having weighted probabilities as a cluster Header (CH). Further, a Heuristic-based Genetic algorithm Mimicking Batesian features (HG-MBF) for QoS-aware routing to

improve packet transmission performance in MANETs. The results of the experiments show that the proposed framework can counter the different types of threats and achieves better performance as compared to the state of art techniques. The packet delivery rate of transmission has increased significantly through multiple routing paths selected based on efficiency. Simulation can be done with MATLAB for the proposed approach. The findings have been analyzed for node parameters such as energy, reliability, bandwidth, throughput, delay, and packet delivery ratio. Simulation findings demonstrate that the suggested solution maintains a high attack detection rate with no computational overhead while substantially reducing IDS traffic and overall memory consumption. According to the findings, the suggested method outperforms existing methods in terms of attack detection rate, memory usage, and computing time respectively.

REFERENCES

[1] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G. and Kannan, A., 2020. QoS aware trust based routing algorithm for wireless sensor networks. Wireless Personal Communications, 110(4), pp.1637-1658.

[2] Sujanthi, S. and Nithya Kalyani, S., 2020. SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT. Wireless Personal Communications, 114(3), pp.2135-2169.

[3] Malik, N.A. and Rai, M., 2020. A Novel Enhanced Energy Efficient and Secure Routing Protocol for MANET. International Journal on Emerging Technologies, 11(3), pp.765-770.

[4] Phakathi, T., Lugayizi, F. and Esiefarienrhe, M., 2020. Quality of Service-aware Security Framework for Mobile Ad hoc Networks using Optimized Link State Routing Protocol. arXiv preprint arXiv:2010.01852.

[5] Yitayih, K.A. and Libsie, M., 2020. Towards developing enhanced cluster-based QoS- aware routing in MANET. Journal of Computer Networks and Communications, 2020.

[6] Ghaleb, S.A.M. and Varadharajan, V., 2020. Convergence Factor and Position Updating Improved Grey Wolf Optimization for Multi-constraint and Multipath QoS Aware Routing in Mobile Adhoc Networks. International Journal of Intelligent Engineering and Systems, 13(4).

[7] Tang, L., Lu, Z. and Fan, B., 2020. Energy efficient and reliable routing algorithm for wireless sensors networks. Applied Sciences, 10(5), p.1885.

[8] Ahmed, S., Ramesh, N.V.K. and Reddy, B., 2020. A highly secured QoS aware routing algorithm for software defined vehicle ad-hoc networks using optimal trust management scheme. Wireless Personal Communications, 113(4), pp.1807-1821.

[9] Kumar, T.S. and Benakop, D.P.G., 2020. A secure routing protocol for MANET using neighbor node discovery and multi detection routing protocol. Int. J. Eng. Trends Technol., 68(7), pp.50-55.

[10] Rahim, R., Murugan, S., Priya, S., Magesh, S. and Manikandan, R., 2020. Taylor based grey wolf optimization algorithm (TGWOA) for energy aware secure routing protocol. International Journal of Computer Networks and Applications (IJCNA), 7(4), pp.93-102.

[11] Junnarkar, A.A., Singh, Y.P. and Deshpande, V.S., 2020. Qmaa: Qos and mobility aware aco based opportunistic routing protocol for manet. In Computational intelligence in data mining (pp. 63-72). Springer, Singapore.

[12] Shajin, F.H. and Rajesh, P., 2020. Trusted secure geographic routing protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol. International Journal of Pervasive Computing and Communications.

[13] Usman, M., Jan, M.A., He, X. and Nanda, P., 2020. QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems, 109, pp.604-610.

[14] Bairwa, A.K. and Joshi, S., 2020. MLA-RPM: A Machine Learning Approach to enhance trust for secure Routing Protocol in Mobile Ad hoc networks. Int J Adv Sci Technol, 29(04), pp.11265-11274.

[15] Chen, Z., Zhou, W., Wu, S. and Cheng, L., 2020. An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. IEEE Access, 8, pp.44760- 44773.

[15] Arumugam, S. and Thangavel, R., 2022. IRDFPR-CMDNN: An energy efficient and reliable routing protocol for improved data transmission in MANET. 22(2), pp.364-375.

[16] Esiefarienrhe, B.M., Phakathi, T. and Lugayizi, F., 2022, September. Node-Based QoS-Aware Security Framework for Sinkhole Attacks in Mobile Ad-Hoc Networks. In Telecom (Vol. 3, No. 3, pp. 407-432). Multidisciplinary Digital Publishing Institute.

[17] Sivapriya, N. and Mohandas, R., 2022. Optimal Route Selection for Mobile Ad-hoc Networks based on Cluster Head Selection and Energy Efficient Multicast Routing Protocol. JOURNAL OF ALGEBRAIC STATISTICS, 13(2), pp.595-607.

[18] Quy, V.K., Nam, V.H., Linh, D.M., Ban, N.T. and Han, N.D., 2021. A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wireless Personal Communications, 120(1), pp.49-62.

[19] Singla, G., Gupta, S. and Kaur, L., 2022. QACRM: QoS Aware AHP Based Cognitive Route Selection in MANETs. Wireless Personal Communications, 123(3), pp.2089-2105.

[20] Jayaprada, S., Srikanth, B., Anuradha, C., Kranthi Kumar, K., Khasim, S. and Grandhe, P., 2022. An Efficient Cross-Layered Approach Quality-Aware Energy-Efficient Routing Protocol for QoS in MANET. In Mobile Computing and Sustainable Informatics (pp. 319-331). Springer, Singapore.

[21] Lavanyaa, R., 2021. Energy Efficient with Trust and Qos-Aware Optimal Multipath Routing Protocol Based on Elephant Herding Optimization for Iot Based Wireless Sensor Networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), pp.979-990.

[22] Sahu, P.K., Acharya, B.M. and Panda, N., 2021. QoS-Aware Unicasting Hybrid Routing Protocol for MANETs. In Intelligent and Cloud Computing (pp. 631-640). Springer, Singapore.

[23] Wilson, A.J., Radhamani, A.S. and Nishanth, R., HYBRID GA-BSO PROTOCOL FOR QoS AWARE CLUSTERING PROTOCOL IN WIRELESS SENSOR NETWORKS.

[24] Kalpana, V., Saravanan, G., Julaiha, A.N. and Balamanigandan, R., AN INTENSIFY MANET BASED CHANNEL AND QOS CONSCIOUS ROUTING USING AOMDV. Turkish Journal of Physiotherapy and Rehabilitation, 32, p.3.

[25] Reebha, S.A.B., 2021. Fuzzy Logic Based Clustering With Firefly Optimized Routing Protocol For Qos Aware Wireless Sensor Networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), pp.2693-2714.