An energy efficient multipath routing protocol for manet

DOI : 10.36909/jer.13771

Neenavath Veeraiah *, Dr.B.T.Krishna **

** Research Scholar, Department of ECE, JNTU Kakinada, Andhra Pradesh, India.*
*** Professor, Department of ECE, JNTU Kakinada, Andhra Pradesh, India.*
** Corresponding Author: neenavathveeru@gmail.com*

ABSTRACT

Energy consumption is a critical consideration in mobile ad hoc networks because the majority of mobile nodes run on low battery resources. A hectic problem was the minimization of energy, which was solved by the use of multipath routing protocols. This article proposes an energy-efficient multi-path routing protocol supported by the MANET optimization algorithm. The energy efficiency within the MANET is efficiently achieved by the use of cluster head selection with fuzzy clustering and fuzz NB. Multipath routing can be achieved by integrating the bird swarm optimization algorithm (BSA) with the whale optimization algorithm (WOA), which is called the Bird Swarm-Whale Optimization Algorithm (BSWOA). Optimal route selection is predicated on fitness variables like connectivity between the nodes, energy consumption, the maximum trust value of the route, and throughput. In comparison to existing methods, the suggested BSWOA obtained a minimum energy consumption of 8.72 J, a minimum delay of 0.00333 msec, and a maximum throughput of 0.912 bps.

Keywords: MANET, Trust, Fitness Functions, Multipath Routing, Cluster Head (CH)

INTRODUCTION

Nodes in a Mobile Ad Hoc Network (MANET) may freely move across the network without the need for any central infrastructure. The nodes engage in multi-hop communication with other nodes as well as other nodes and link directly with other nodes within their transmission range (Sajal Sarkar & Raja Datta. 2016). Because of their ease of setup, these networks are becoming more popular. A shared wireless medium and dynamic networks, however, make these networks vulnerable to a range of issues such as unanticipated topology, increased interference or congestion, and resource limits like bandwidth or energy. As a result of their reliance on limited battery resources, the nodes in this sort of network are often power-restricted, while wireless transmissions use a significant amount of energy. Nodes drain their batteries not only by sending their own packets, but also by attending to other nodes' transmissions. This results in a shared environment in which energy is wasted. Ad-hoc networks are constructed on multi-hop communication, which

means that they use energy by retransmitting messages to other nodes within the network. This decentralized network necessitates a wide range of energy management technologies. One of the most cost-effective ways to transmit data is via MANET, which has a wide range of uses (Usha, G et al., 2016). Although the implementation of MANETs is straightforward, MANET's key drawback is regarding battery-operated nodes, which interrupt the equilibrium of the network when their stored energy is drained, contributing to the demise of the nodes. Therefore, minimizing the utilization of energy within the network is vital.

MANETs are networks in which a number of nodes are clustered together so that they may communicate with one another. When a collection of mobile nodes executes the communication process by making the best use of available bandwidth and achieving high network throughput, this is referred to as "clustering." As the number of clusters grows and the pressure on the cluster head increases, more clustering strategies will be used, but they will all need more energy. It is the number of nodes in the network that defines how well communication will function; the more nodes there are, the better communication will work. When it comes to improving the network's longevity, the most significant factor is reducing energy use. A strong routing protocol between the source and destination nodes is essential for success in this instance. The only other way to do this is via the use of cluster management. Two terms, such as "cluster head" and "cluster nodes," are commonly used interchangeably in cluster design (S. Russia & R. Anita.2017**)**. The cluster head is responsible for monitoring and regulating the overall performance of the cluster nodes. Every node may serve as a cluster head in this architecture; the function of the cluster head changes based on the environment and the node's capacity (Wenjing Lou et al.,2009). The clustering strategy not only addresses some of the scalability concerns, but it also maximizes the longevity of the network with minimum energy usage. To improve communication performance and network longevity, this paper suggested protocol which provides low energy consumption and minimum delays (Gautam M. Borkar & A. R. Mahajan. 2017).

Routing is the most important phenomenon in MANETs, and it must be capable of handling the unexpected presence of topology. These mobile networks are made possible by the detection, control, and activation of mobile nodes in their surrounding environment **S.** (Satheesh Kumar & N. Sengottaiyan.2017). Multipath routing, which provides a variety of routes from the source to the destination, effectively addresses single path difficulties like delay in transmission, more energy consumption and maximum overhead information (Rashmi Chaudhry & Shashikala Tapaswi.2018). To support the structure and nature of MANETs, a variety of efficient algorithms are necessary, with a greater focus being put on the design of multipath routing protocols in order to ensure that they are functional. As well as using the intermediate nodes, these routes are used by source nodes as replacement and main routes in order to reach their respective destinations. Discovery of multipaths with the goal of reducing the severity of solo-path problems. Multipath routing, as opposed to single-path routing, has the potential to deliver faster throughput and greater consistency in an ad hoc network(Xian-Bing Meng et al.,2015). Particularly advantageous is the ability to distribute traffic loads evenly throughout a network when many pathways are used. This is very beneficial in terms of balancing energy usage, which is extremely beneficial in terms of

extending the lifetime of the network (N. Veeraiah & B. T. Krishna.2018). Thus, the energy efficient multipath routing strategy is addressed in the paper.

A new routing protocol, BSWOA, has been developed in this paper to extend the network's lifetime. Once the MANET environment is simulated, trust values for all nodes are set to zero, and transmission begins. Fuzzy clustering is used to reduce the amount of energy required. The trust manager's maximum trust value is used to pick the CH, and the fuzzy NB is used to exclude intruder nodes from the network. There is predicted to be a rise in the number of effective nodes, which are utilized to transfer data over the network. Using the BSWOA multipath optimization method, the optimum path is selected between the nodes. Route optimization is based on fitness functions such as energy consumption, throughput, node connections, and node delay in order to find the best possible path.

The rest of the paper is structured as follows. As outlined in Section 2, background and related approaches are discussed. Section 4 presents a proposed method for an energy-efficient multipath routing protocol. Simulation results with comparative analysis are in Section 5, and Section 6 gives the conclusion of the work.

MOTIVATION

It is provided in this part that a review of literature papers is conducted in connection with the requirement to establish a protocol. The motive for the investigation into the development of an energy-efficient multipath optimization method is discussed at the end of this section.

Background & Related works

A CMBCH selection method is used to improve the clustering strategy for energy-efficient communication. A cluster manager technique is presented as a solution to this issue. CH's role is reduced because of the deployment of CM. There are certain nodes that don't participate in communication, such as those controlled and monitored by the CM node. Performance in traffic reduction and load balancing are shown by CH rejoining. The suggested technique is compared to DLC and HCAL based on the experimental findings. This method needs to focus on data security during packet transmission in the network after achieving the energy improvement (S A et al.,2021**)**.

Mobility and battery reliance are the main obstacles to enhancing network longevity. To address these issues, a mobile-aware energy-efficient clustering in MANET (FQ-MEC) technique was developed. The clustering setup step uses the node's stability deviation and energy depletion parameters to select which CHs can hold responsibility for longer. The fuzzy-based Qlearning technique of reinforcement learning has been used here to decide the behavioral patterns of nodes using Chebyshev's inequality principle to adaptively sustain the loads on CHs. This improves network longevity and minimizes re-clustering rates. This method needs to focus on the optimal solution for both the cluster head and the route

(Naghma Khatoon et al.,2021). To spot the intrusion, a new method called the Anomaly Detection System has been developed. During experiments, the level of energy consumption and intruded node identification allow the sustained stable release of the cluster energy and cluster up time for a lengthier period of time, but the approach does not operate on ADS because this method cannot be suitable for producing intelligent Manets (Vikram Narayandas et al.,2017).

An ant colony-based multipath routing (QAMR) algorithm supported the foraging actions of the ant colony to pick and transfer information that supported the existence of an administration. The choice of direction here depends on the reliability of the nodes and therefore the chance of inclination. In addition to node solidity, number of hops, and path inclination probability factors, the QoS variables considered are bandwidth power, postponement, and hop tally. The route overhead is extended regardless (P.Venkata Krishna et al.,2012).An elliptic curve cryptography system for trust management to detect muggers.This approach removes malicious nodes from the network to achieve a greater packet delivery ratio, minimal delay, lowest packet loss, throughput, and successful end-to-end delivery with elevated protection in mobile ad hoc network MANET, but it cannot identify when more attackers are possible(Opinder Singh et al.,2017).

A Network Coding-based AOMDV MANET routing algorithm (NC-AOMDV) was suggested to enhance the unwavering efficiency of data transmission or to supply load balancing.To motivate package encoding at a transfer point, network coding was connected. Anyway, the overhead and usual postponement of the parcel are extended (Fubao Yang et al.,2012). A probabilistic model that greatly increases the network lifespan by reducing energy usage at each of the nodes. The downside is that in a heterogeneous network, this model does not manage load balancing in MANET (Marchang et al.,2017).

A multipath backbone route based on subterranean ants. It selects the various courses with the highest extreme inclination probability using a swarm-based ant colony optimization (ACO) technique for the purpose of relaying information towards the target. supported next hop usability, postponement, and data transmission capability, the way inclination probability is calculated. The nodes exposed to problems are identified in the path disclosure and, therefore, the applicable direction is missed. The device load on the courses is often modified at that stage by analyzing a record by each backbone node to transmit the knowledge traffic equally on the source-to-goal connections. In any case, the utilization of delay and control is extended (P. Francis Antony Selvi and M.S.K. Manikandan.2016). The MANET IDS system is built on Bayesian game theory that minimizes energy expenditure and provides a superior detection rate along with a decreased false alarm rate over a large range of attacks. This strategy did not depend on enhancing the identification rate and reducing the false positive rate of the hybrid MANET IDS lightweight and heavyweight units (Basant Subba et al.,2016).

Energy consumption is a critical consideration in mobile ad hoc wireless networks since the vast majority of mobile nodes run on low battery resources. According to existing

methods for analyzing the energy consumption in a mobile ad hoc network, the different components of energy-related expenses include the distance travelled and the time it takes for the data to be sent. Ordinary routing protocols in particularly designated distant systems, such as AODV and DSR, are basically suggested in order to identify a single route in the distance between a source and a destination node. The process of acquiring multiple routes between a source and a destination point is referred to as energy-efficient multipath routing. The multiple methods in which source and goal node sets may communicate with one another can be used to compensate for the dynamic and irregular character of ad hoc networks. As previously stated, many methods may be used to provide load adjustment, adaptability to internal failure, and the maximum data transmission rate, among others. By considering the network energy consumption and delay issues, this paper proposes an energy-efficient multipath routing protocol for MANET.

Energy Efficient Multi-Path Routing based on (BSWOA)

MANET is a wireless mobile network. In this network, the nodes are dispersed throughout the atmosphere and the nodes are clustered below a cluster generated to avoid energy wastage by some clustering algorithm. In addition, for the determination of malicious nodes and to ensure reliable connectivity in the network, the protection factor of the nodes is determined.

Let the network consist of n number of mobile nodes, N_i indicate the i^{th} mobile node, which is shown below.

$$N = \{N_1, N_2, ..., N_i, ..., N_n\} \tag{1}$$

Here, the nodes S and D are represented as the source and destination in the network. The route table maintains the trustworthiness of each node and is revised before the network is structured. By considering the trust table, the nodes that have the maximum trust values will be selected for transmission within the network. If the table of arrogance is made based on max trust value, the cluster head will be selected by applying the fuzzy clustering method. Therefore, the finalized cluster heads, which have the maximum trust value within the mobile ad hoc network, are specified.

$$C = \{C_1, C_2, ..., C_j, ..., C_m\} \tag{2}$$

Where, m define the network's cumulative CHs. The detection of intrusion is then performed, enabling the gathering of stable nodes in MANET for further communication. Finally, multipath selection is conducted to support the stable CHs that the trail has identified, and therefore the optimization created is employed for multipath selection. The flow chart of the multipath routing proposed is represented in Figure 1.

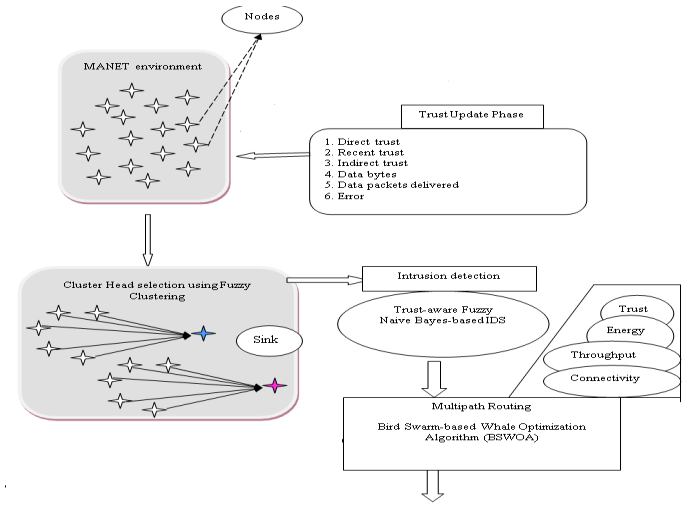

Figure 1. A pictorial representation of the proposed method

Build a trust table for the nodes of MANET

Trustworthiness may be an aspect that creates secure MANET connectivity by refusing to connect to malicious nodes within the network to avoid miscommunication. The trustworthiness of all the network nodes is then calculated and tabulated in such a manner that the degree of arrogance of the nodes is supported by the transmission and reception of the network. Six trust factors also exist, such as DT, IDT, and RT, as well as DB, fault, and DP distribution. Assume initially that all the nodes' trustworthiness value equals "1". The trust table ensures the effectiveness of the preceding multi-path communication intrusion detection in MANET. The next section deals with the formulation of the various trust models given as (Opinder Singh et al.,2017).

Direct trust (DT): Direct trust is defined as the average time at which the i^{th} node and d^{th} destination interact. To confirm the public key provided by the destination node, direct trust value is the distinction between the actual time and the expected time of the nodes. DT between i^{th} node and d^{th} destination is thus portrayed as,

$$DT_i^d(\tau) = \frac{1}{3}\left[DT_i^d(\tau - 1) - \left(\frac{\tau_{appx} - \tau_{est}}{\tau_{appx}} \right) + \omega \right] \tag{3}$$

Where, τ_{appx} corresponds to the estimated time and τ_{est} gives the public key authentication time expected. In other words, the approximate τ_{appx} and τ_{est} expected time for the destination and the node to transmit and retrieve the public key. The witness element ω of the nodes is signified.

Indirect trust (IDT): IDT, the node with the witness element is well-known to be verified based on direct trust. Nonetheless the node short of a witness value is confirmed by employing the IDT indicated below,

$$IDT_i^d(\tau) = \frac{1}{r}\sum_{i=1}^{r} DT_i^d(d) \tag{4}$$

Where, r determines the i node's absolute neighbors.

Recent trust (RT): RT, by using key validity and identification of the destination node, which is submitted depending on the time. RT is calculated using DT and IDT. It formulates the RT as,

$$RT_i^d(\tau) = \alpha * DT_i^d(\tau) + (1-\alpha) * IDT_i^d(\tau) \tag{5}$$

where, $\alpha = 0.3$.

Trust utilizing the data bytes: Depending on the data bytes, the transmission of data in bytes from the i^{th} source node to the d^{th} destination nodes calculate the trust. The trust method, which depends on the DB, is expressed as,

$$DB_i^d(\tau) = \frac{1}{2} * \left[\frac{DB^i}{\ell} + \frac{DB^d}{\ell} \right] \tag{6}$$

Where DB^i and DB^d relates to the cumulative bytes that the node i and d^{th} destination node has transmitted and received. At the sending and receiving point, let ℓ the data limits of the packet be set.

Trust Based on Error: The communication error specifies the trust using the error that is specified as,

$$\varepsilon_i^d(\tau) = \frac{1}{T} * \sum_{l=1}^{T} \varepsilon_l \tag{7}$$

Where, ε denotes the overall transactions and ε_l corresponds to the fault depending on the link error, which is either '0' or '1'.

Trust utilizing the DP delivery: Ultimately, the trust that is calculated using the delivered DPs is computed as the proportion of the total packets collected from the node to the packets sent. The DP delivery-based trust is represented as $DP_i^d(\tau)$, the number of transactions between the node and the destination is determined. Thus, i the node's trust is suggested as,

$$t^i = \left\{ DT_i^d(\tau) + IDT_i^d(\tau) + RT_i^d(\tau) + DB_i^d(\tau) + DP_i^d(\tau) + \varepsilon_i^d(\tau) \right\} \tag{8}$$

Where, t^i symbolizing the i^{th} node's trust vector.

Set the energy levels in the nodes to their initial values

At the end of each transmission, the energy values of the nodes are calculated, and the nodes' residual energy is defined as:

$$e_{i,\tau}^{remain} = e_{i,\tau-1}^{remain} - e_{i,\tau}^{trans} * s(\tau-1,\tau) - e_{i,\tau}^{receive} * s(\tau-1,\tau) \tag{9}$$

Where $e_{i,\tau}^{trans}$ and $e_{i,\tau}^{receive}$ is the required energy for a single bit of data to be transmitted. The energy in the network's initiation of contact is, however, complete. On the other hand, depending on the energy ratio measured at the initial point of contact, the balancing energy in the nodes may be varied in the range of low to high, and it is the ratio of the remaining

energy to the highest energy of the nodes at the transmission starting point. It should be noted that when the resultant energy ratio value is lower when compared to the predefined lower threshold value, then we consider the node's balancing energy not sufficient for the transmission of data in the network. If the node's balancing energy is greater than the upper threshold value, then we consider the node's balancing energy sufficient for the transmission of data in the network. Assume the upper threshold value is considered to be 0.2 (Ajay Kumar Yadav & Sachin Tripathi.2017) The balancing energy value of the node defines the transmitting energy.

The Fuzzy clustering method for cluster head selection in MANET

To ensure the efficient energy performance of the network, clustering algorithms are set up and fuzzy clustering is used for clustering the MANET nodes in this article. The goal of clustering is to pick the optimal network (Jiamin Li & Harold W. Lewis.2016). The Cluster Head is configured in such a way that the best network is created. The Cluster Head allows for more network communication. The choice of the optimum CH is founded on trust, which is the purpose component. The closely related nodes are clustered under a cluster during clustering, and the alliance is founded on the membership degree in the fuzzy clustering process. Using fuzzy clustering, the efficient handling of overlapping data is then allowed, and in addition, any node mobility relies on multiple clusters, meaning that node cluster assignment depends on the membership function of the nodes. A cluster head with a minimization function is given as,

$$Q = \sum_{i=1}^{n}\sum_{j=1}^{m} M_{ij}^{ff} \times \left\| N_i - C_j \right\|^2 ; 1 \le ff \le \infty \qquad (10)$$

Here ,the variables N_i and C_j describes the i^{th} node with j^{th} Cluster Head and $\| \|$ implies the interval among the i^{th} node with j^{th} Cluster Head in the Euclidean. Q is the Objective function and f is the fuzzifier. M_{ij}^{ff} represents the degree of membership of the individual nodes belonging to the j^{th} cluster heads. The nodes with the shortest distance from the cluster head are assumed to be clustered into a single cluster. Thus, while clustering originally, the CHs are set arbitrarily. The second step is to determine membership values with regard to their CHs for all nodes, which is followed by the calculation of the current Cluster Head based on the membership function. For a given number of iterations, the steps are repeated before the new cluster heads are derived. It is provided that the ideal cluster heads computed by applying fuzzy clustering are the same as in the equation (2).

Detection of malicious nodes by using the Fuzzy NB classifier method

Intrusion in the network is measured by using the trust-worth values of the nodes in the network. Optimal CHs are specified, and it is worth noting that the sink node recognizes the intruders using the cluster member ship information of the nodes that is sent by the sink node

to the cluster heads. An intruder node is identified, then the transmission through that node is blocked. In the sink node, a fuzzy NB classifier is installed to estimate the intruders, which is based on the probability concept. Based on the class mark chosen for the i^{th} node, decide whether the node is malicious or not based on the trust table t^i values of the node i. The primary feature of intrusion detection is to ensure stable network connectivity without any energy loss or interruption in transmission. The class's conditional probability K_x with regard to t^i trust value is given by,

$$P(K_x \mid t^i) = P(K_x) \prod_{k=1}^{9} \left(\frac{P(t_k^i | K_x)}{P(t_k^i)} \times M_k^i \right) \quad (11)$$

Here, $P(K_x)$ is the probability of x^{th} class, and here there are two-class phages. The first one is the intruder nodes, and the second one is the normal nodes, which corresponds to the class chance. $P(t_k^i | K_x)$ postulates the possibility of specific node trust values compared to the class. M_k^i is the membership degree of the i^{th} trust factor. The trust value of individual nodes can be calculated using class probability, and the class mark is calculated based on the maximum probability value. Once the intruders are identified, the mobile ad hoc network is abandoned, and the optimum multipath range is advanced until the genuine nodes are determined. The genuine nodes in the network are then defined as,

$$N = \{N_1, N_2, ..., N_i, ..., N_g\}; \; g < n \quad (12)$$

where, g defines the total normal nodes, which are less when compared to the overall nodes in the network.

Optimum multipath using the proposed BSWOA

In MANETs, multipath connectivity ensures energy-efficient network transmission for which the initial stage is to identify the interruption from which the normal nodes are selected in such a way that the route is created for communication from the source node to the destination node. However, successful communication is only ensured along the most efficient route, so a communication optimization algorithm is used. Optimal path selection depends on factors like trust values, energy consumption, throughput between the nodes, and connectivity between the nodes. Thus, initially, the route is established based on reply to messages, and the route is determined between the source node and the destination node. The optimal path selected is built on the BSWOA algorithm, which is a combination of the Whale Optimization Algorithm (WOA)(Seyedali Mirjalili & Andrew Lewis.2016) and the Bird Swarm Algorithm (BSA)(Xian-Bing Meng et al.,2015).

Solution encoding: This section illustrates the representation of the result based on the suggested BSWOA. The multipath between the S source and D destination nodes is calculated here, and the interacting multipath is determined based on the maximum value of the fitness test.

Fitness Function measurement: Path fitness is detected by the maximum trust value of the

nodes in the network, the maximum balancing energy in the nodes, the maximum throughput, and the strong connection between the nodes in the network. The fitness function value is the function of maximization, given as

$$FF = \frac{1}{4}\{t + \varepsilon + u + y\} \tag{13}$$

Here, t means trust, ε means energy, u means throughput, and y means connectivity, and they are computed using the path nodes. As in equations (8) and (9), respectively, the confidence and energy residual in the node are calculated. Measuring throughput is the ratio of the cumulative bits communicated through a path per second in the network and is prepared as

$$u = \frac{\upsilon}{\tau} \text{ bps} \tag{14}$$

There, υ implies the sum of bits sent and τ means time in measured seconds. Node connectivity [17] is defined as bidirectional connections between source and destination nodes, expressed as

$$y = \frac{1}{g}\left[\sum_{i=1}^{g} \frac{y_i}{cc} \cdot\right] \tag{15}$$

where, y_i indicates the connectivity of i^{th} node, cc represents overall contacts.

BSWOA algorithmic steps

The Bird Swarm and Whale Optimization Algorithm is led by the optimization process and is a combination of BSA and WOA. It is a swarm-based intelligence algorithm, and the steps of BSA are followed. The BSA is focused on birds' social experiences and is arranged into three activities, such as foraging, alertness, and flight. BSA's key benefits are that it restores cultural plurality and remains free from prematurity. In addition, with effective global optimum converging capacity, the effective balance between discovery and extraction is made effective. However, it is a hectic task to determine the optimization criteria, and in addition, it is important to improve the additional search functionality for an optimal result. The above problems are solved using the WOA, which improves the optimization's convergence behavior.

The Bird Swarm Algorithm is founded on a few pronouncement regulations that specify how a bird can bounce between the two behaviors of foraging and vigilance functions. At the same time, birds should maintain a map of their earlier lives in the quest for food and the best position of food in the past when foraging, which offers an accurate search for a global response. Similarly, in the vigilance process, birds migrate near the middle, which is pretentious as a cause of the swarm rivalry due to the attack. On the other hand, the birds travel to additional areas, and at this point, the birds switch between producing and scrounging. The producer has the largest reserves, while the scrounger is the one with the least reserves. But the birds choose arbitrarily between the producer and the scrounger from the highest and lowest stocks. It is important to remember that farmers are interested in their quest for food, while scroungers travel to their food producers.

Vigilance actions: In the swarm, the separate birds search for food based on their knowledge and the swarm's knowledge, which is formed as,

$$B_{b,c}^{\tau+1} = B_{b,c}^{\tau} + \left(\rho_{b,c} - B_{b,c}^{\tau}\right) \times p \times rand\,(0,1) + \left(X_c - B_{b,c}^{\tau}\right) \times q \times rand\,(0,1) \tag{16}$$

$$B_{b,c}^{\tau+1} = B_{b,c}^{\tau} + \rho_{b,c} \times p \times rand\,(0,1) - B_{b,c}^{\tau} \times p \times rand\,(0,1) + X_c \times q \times rand\,(0,1) - B_{b,c}^{\tau} \times q \times rand\,(0,1) \tag{17}$$

$$B_{b,c}^{\tau+1} = B_{b,c}^{\tau}\left[1 - p \times rand\,(0,1) - q \times rand\,(0,1)\right] + \rho_{b,c} \times p \times rand\,(0,1) + X_c \times q \times rand\,(0,1) \tag{18}$$

The above equation (18) for regular BSA for vigilance characteristics is updated by means of the WOA update equation. The Whale Optimization Algorithm is based on the humpback whales' foraging process, and the combination of the Whale Optimization Algorithm with the Bird Swarm Algorithm allows successful alignment to the optimum global result. The WOA's basic equation is given as,

$$B_{b,c}^{\tau+1} = B^{*}(\tau) - E.F \tag{19}$$

Among the three WOA phases, the encircling process is considered for the alteration of the BSA upgrade regulation. The position of the whale is modified in the encircling process based on the best target position $B^{*}(\tau)$ with optimization parameters of the coefficient vector represented as E and the space between the whale and prey represented as F. We will get there later when replacing the distance with the equation $F = H.B^{*}(\tau) - B_{b,c}^{\tau}$,

$$B_{b,c}^{\tau+1} = B^{*}(\tau) - E.\left|H.B^{*}(\tau) - B_{b,c}^{\tau}\right| \tag{20}$$

$$B_{b,c}^{\tau+1} = B^{*}(\tau)\left[1 - E.H\right] + E.B_{b,c}^{\tau} \tag{21}$$

$$B_{b,c}^{\tau} = \frac{1}{E}\left\{B_{b,c}^{\tau+1} - B^{*}(\tau)\left[1 - E.H\right]\right\} \tag{22}$$

Substituting equation (22) in equation (18), we get,

$$B_{b,c}^{\tau+1} = \frac{1}{E}\left\{B_{b,c}^{\tau+1} - B^{*}(\tau)\left[1 - E.H\right]\right\}\left[1 - p \times rand\,(0,1) - q \times rand\,(0,1)\right] + \rho_{b,c} \times p \times rand\,(0,1) + X_c \times q \times rand\,(0,1) \tag{23}$$

$$B_{b,c}^{\tau+1} = \frac{E}{\left[1 - p \times rand\,(0,1) - q \times rand\,(0,1)\right]}\left\{\begin{matrix}\left\{-B^{*}(\tau)\left[1 - E.H\right]\right\}\left[\begin{matrix}1 - p \times rand\,(0,1)\\ - q \times rand\,(0,1)\end{matrix}\right] + \\ \rho_{b,c} \times p \times rand\,(0,1) + X_c \times q \times rand\,(0,1)\end{matrix}\right\} \tag{24}$$

Here, c and $rand\,(0,1)$ represents the dimension and the numbers delivered equally, p and q numbers are positive. The bird and swarm's best location in the earlier iteration is implied as, p and X_c . In the prior iteration, the location of the b^{th} bird is denoted as, $B_{b,c}^{\tau}$. H Signifies the vector with a coefficient.

Vigilance actions: The birds travel into the middle, where the birds compete, and the behavior of the birds' vigilance is modelled as,

$$B_{b,c}^{\tau+1} = B_{b,c}^{\tau} + V_1 \left(\mu_c - B_{b,c}^{\tau}\right) \times rand\,(0,1) + V_1 \left(\rho_{h,c} - B_{b,c}^{\tau}\right) \times rand\,(-1,1) \quad (25)$$

$$V_1 = v_1 \times \exp\left(-\frac{\rho\, Fit_b}{\sum Fit + \vartheta} \times R\right) \quad (26)$$

$$V_2 = v_2 \times \exp\left(\left(\frac{\rho Fit_b - \rho Fit_h}{\left|\rho Fit_h - \rho Fit_b\right| + \vartheta}\right)\frac{R \times \rho Fit_h}{\sum Fit + \vartheta}\right) \quad (27)$$

Where, corresponds to the randomly selected positive integer between 1 and ϑ . The value of the positive constants is between h 0 and 2, and is denoted as, v_1 and v_2 . ρFit_b symbolizes the highest bird fitness metric which means the sum of the swarm's best fitness. Likewise, μ_c it implies the average of the location of the swarms.

Flight behaviour: In the condition of foraging, the birds migrate to other regions or other threats. Once the birds reach a new area, the behavior of foraging takes place in which a small number of birds behave like producers and the remaining additional birds behave like scroungers. The behaviors are represented as

$$B_{b,c}^{\tau+1} = B_{b,c}^{\tau} + randn\,(0,1) \times B_{b,c}^{\tau} \quad (28)$$

$$B_{b,c}^{\tau+1} = B_{b,c}^{\tau} + \left(B_{h,c}^{\tau} - B_{b,c}^{\tau}\right) \times fl \times \mathrm{randn}(0,1) \quad (29)$$

Where, $randn\,(0,1)$ corresponds to the distribution number of the Gaussian. As follows, the procedure stages of the recommended Bird Swarm Whale Optimization Algorithm are given: Initialisation: The first step is the population beginning that is denoted as,

$$B_{b,c}^{\tau+1};\ (1 \le b \le \vartheta);\ (1 \le c \le \hbar) \quad (30)$$

Here, ϑ defines the total no of population of the c^{th} dimensional space.

Process of this algorithm follow how fitness of the results is evaluated founded on the equation (13) to declare the best result. For all the results, the vigilance behavior or foraging behavior are determined by the state $rand\,(0,1) < P$. Two requirements of $(\tau \% \lambda \neq 0)$ plus $rand\,(0,1) < P$ are met, the solution is modified founded on foraging behavior in number (28) equation or else location is revised founded on the behavior of vigilance.

If the state $(\tau \% \lambda \neq 0)$ flops, then the swarm will be separated into scroungers and producers. The revising is performed continuously on the basis of the equations (28) and (29). If the current answer is found to be better than the finest result in the preceding repetition, either substitute the resolution with the new best result, or maintain the finest result in the previous iteration, then the viability of the solutions is tested. Repeat the steps until the global optimum best solutions are calculated for the full iterations. As the condition

collapses, the swarm is split into scroungers and developers, and the revise is carried out based on the equations (28) and (29). If it is shown that the current solution is the best effective result when compared to prior iterations, then the obtained result is replaced by the best new result, or that the best result is retained in the prior iteration, then the feasibility of the solutions is evaluated. Repeat the steps until the optimal global solutions for the complete iterations are determined. The optimization algorithm discussed in this section is therefore intended to decide the optimum multipath (best solution) for allowing safe network communication.

Proposed BSWOA algorithmic steps

Input: ϑ-total birds in a population
Output: Best solution
Population initialization
τ_{max} -maximal iterations
λ -frequency of the flight behaviour of the birds'
P -Foraging probability
p, q, v_1, v_2, fl -constants
Evaluate the fitness of ϑ individuals
While $(\tau < \tau_{max})$
If $(\tau \% \lambda \neq 0)$
For $b = 1:\vartheta$
If $rand(0,1) < P$
Foraging based on equation (24)
Else
Vigilance based on equation (25)
End If
End For
Else
Split the swarm as: scroungers and producers
For $b = 1:\vartheta$
If b is a producer
Involves in producing as in equation (28)
Else
Involves in scrounging as in equation (29)
End if
End for
End if
Evaluate the new solutions
Check the feasibility of the solutions
Declare the best solution
$\tau = \tau + 1$
End while
End

COMPARATIVE ANALYSIS WITH SIMULATION RESULTS

As mentioned in Section 1, thermoplastic composite pipes according to their characteristics For the experiments, we make use of the NS2 simulator by using simulation parameters.

Table 1. Simulation parameters

Simulation parameters	
Radio-propagation model	Propagation/Two Ray Ground
MAC type	Mac/802_11
Network interface type	Phy/WirelessPhy
Interface queue type	Queue/Drop Tail/ PriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Routing protocol	AODV
Max packet in ifq	500
Packet Size	512
Rate	250kb
Initial Energy	15.1 J
X axis	1000
Y axis	1000
Number of Nodes	100
Simulation Time	50

Performance Parameters

The Bird Swarm-Whale optimization algorithm (BSWOA) is compared to existing techniques such as Kmeans NB (Basant Subba et al.,2016), Naive Bayes (Marchang et al.,2017), and NB trust (Opinder Singh et al.,2017), and fuzzy NB optimization algorithms (Agarwal Mohan Madan et al.,2020). The performance parameters of delay, throughput, and energy consumption are considered for the analysis.

Results and discussion

Delay

Dependent on delay, Figure 2 indicates the comparative analysis. When the duration is 40 seconds, the delay for fuzzy Naive Bayes is 0.00456, K means Naive Bayes is 0.00538, naive bayes is 0.00572, Nave Bayes Trust is 0.00639, and 0.00333 m see for the suggested Bird Swarm Whale Optimization Algorithm. Results show that the proposed method offers less delay in data transmission in the network.

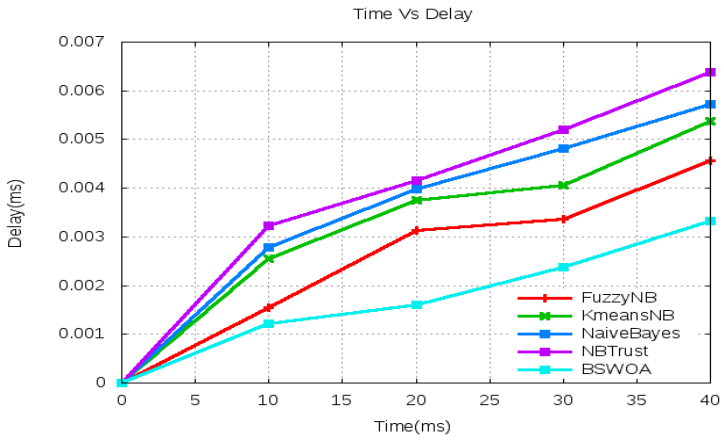

Figure 2. Delay

Energy Consumption

The comparative comparison focused on energy consumption can be seen in Figure 3. The energy expenditure of the processes for fuzzy Nave Bayes is 8.75, K means Nave Bayes is 9.04, nave bayes is 9.02, Nave Bayes Trust9.01, and implied BSWOA is 8.720 Joules, correspondingly, when the time is 40 secs. From the results, it shows that the BSWAO method provides the most effective and energy-efficient path for data transmission for ad hoc networks.

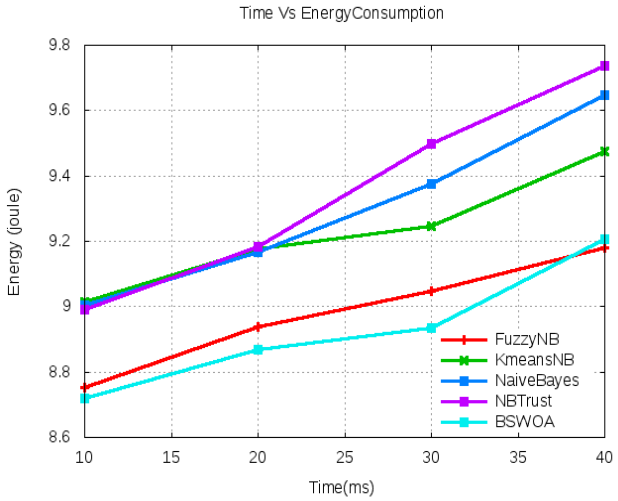

Figure 3. Energy Consumption

Throughput:

The comparative comparison as seen in Figure 4 is based on throughput. The performance of the methods are fuzzy Naive Bayes is 0.901, K means Naive Bayes is 0.893, naive bayes is 0.860, Nave Bayes Trust is 0.845, and suggested BSWOA is 0.919 bps, correspondingly, while the time is 40 secs. From simulation results, it shows the max throughput offered by the proposed method when compared to the remaining methods.

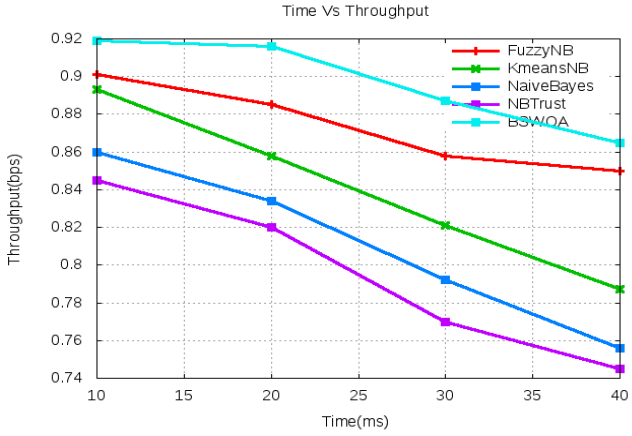

Figure 4. Throughput

Relative analysis

The relative discussion of the methods of energy-efficient multipath routing is discussed in the resultant table-2. It is observed that compared to fuzzy Naive Bayes, K means Naive Bayes, NB and Nave Bayes trust, a minimum energy consumption of 8.72 J, a minimum delay of 0.00333 msec, and a maximum throughput of 0.912 bps secs are obtained by the proposed BSWOA method.

Parameters	**Suggested**	**Fuzzy**	**K means**	**NB**	**Naive**

	BSWOA	Naive Bayes	NB		Bayes Trust
Delay (milli seconds)	0.00333	0.00456	0.00538	0.00572	0.00639
Energy utilization (Joule)	8.72	8.75	9.04	9.02	9.01
Throughput (bps)	0.912	0.901	0.893	0.860	0.845

Table 2. Comparative discussion

CONCLUSION

This work proposes BSWOA, a novel multipath routing protocol that is both energy efficient and fast. As a starting point, the network nodes are initialized with their energy and trust management in such a manner that optimization-based energy-efficient multipath routing is guaranteed. The selection of cluster heads is done based on the fuzzy clustering technique, which is used to determine which cluster head is the most trust value. Once the cluster head has been identified, the fuzzy naive bayes classifier is used to identify and avoid intruded nodes in the network, as well as to determine the most efficient path for data transmission. As a result, network communication is initiated by the secure nodes, which have low energy consumption and a long lifespan in the network. The Bird Swarm Optimization Algorithm (BSWOA) is the foundation of energy efficient routing because it is the merging of the standard Whale Optimization Algorithm into the Bird Swarm Algorithm that reaps the advantages of the Whale Optimization Algorithm into the Bird Swarm Algorithm. The best path selection is done based on the fitness functions. The simulation results of the methods shows that the suggested BSWOA obtained a minimum energy consumption of 8.72 J, a minimum delay of 0.00333 msec, and a maximum throughput of 0.912 bps

REFERENCES

Sajal Sarkar & Raja Datta. 2016. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Ad Hoc Networks 37:209-227.

Usha, G., M. Rajesh Babu & S. Saravana Kumar. 2016. Dynamic anomaly detection using cross-layer security in MANET. Computers & Electrical Engineering 59:1-11.

S. Russia & R. Anita.2017. Joint cost and secured node disjoint energy efficient multipath routing in mobile ad hoc network. Wireless Networks 23:2307–2316.

Wenjing Lou, Wei Liu, Yanchao Zhang & Yuguang Fang.2009. SPREAD: Improving network security by multipath routing in mobile ad hoc networks. Wireless Networks 15: 279–294.

Gautam M. Borkar & A. R. Mahajan. 2017. A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks 23:2455–2472.

S. Satheesh Kumar & N. Sengottaiyan.2017. Defending against jellyfish attacks using cluster based routing protocol for secured data transmission in MANET. Cluster Computing 22:1–12.

Rashmi Chaudhry & Shashikala Tapaswi.2018. Optimized power control and efficient energy conservation for topology management of MANET with an adaptive Gabriel graph.

Computers & Electrical Engineering 72:1021-1036.

Xian-Bing Meng, X.Z. Gao, Lihua Lu, Yu Liu & Hengzhen Zhang.2015. A new bio-inspired optimisation algorithm: Bird Swarm Algorithm. Journal of Experimental & Theoretical Artificial Intelligence 28:673-687.

N. Veeraiah & B. T. Krishna.2018. Selfish node detection IDSM based approach using individual master cluster node. In Proceedings of 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India.

S A, B K & J M K. 2021. Energy-efficient cluster manager-based cluster head selection technique for communication networks. International Journal of Communication Systems 34:5.

Naghma Khatoon, Prashant Pranav, Sharmistha Roy & Amritanjali.2021.FQ-MEC: Fuzzy-Based Q-Learning Approach for Mobility-Aware Energy-Efficient Clustering in MANET.Wireless Communications and Mobile Computing 5:1-12.

Vikram Narayandas, Sujanavan Tiruvayipati, Madusu Hanmandlu & Lakshmi Thimmareddy.2017. Anomaly Detection System in a Cluster-Based MANET.Proceedings in Computer Communication, Networking and Internet Security, Singapore.

P. Venkata Krishna V. Saritha G. Vedha A. Bhiwal & A.S. 2012. Quality-of-service-enabled ant colony-based multipath. IET communications 6:7683.

Opinder Singh, Jatinder Singh & Ravinder Singh.2017. Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET. Cluster Computing 21:1-13.

Fubao Yang, Shengzhi Ling, Hui Xu & Baolin Sun. 2012. Network Coding-based AOMDV Routing in MANET. Proceedings of the IEEE International Conference on Information Science and Technology, Wuhan, Nodeei,China.

Marchang, Ningrinla, Raja Datta & Sajal K. Das .2017. A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology 66:1684-1695.

Selvi, Pitchaimuthu & Manikandan, M.s.K.2016. Ant Based Multipath Backbone Routing for Load Balancing in MANET. IET Communications. 11.

Basant Subba, Santosh Biswas & Sushanta Karmakar.2016. Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal 19:782-799.

Ajay Kumar Yadav & Sachin Tripathi.2017. QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs.Peer-to-Peer Networking and Applications 10:897–909.

Jiamin Li & Harold W. Lewis.2016. Fuzzy Clustering Algorithms – Review of the Applications. In Proceedings of the IEEE International Conference on Smart Cloud, New York, NY, USA.

Seyedali Mirjalili & Andrew Lewis.2016. The Whale Optimization Algorithm. Advances in Engineering Software 95:51-67.

Agarwal Mohan Madan ,Saini Hemraj & Govil Chandra Mahesh .2020. Probabilistic and Fuzzy based Efficient Routing Protocol for Mobile Ad Hoc Networks. Recent Advances in Computer Science and Communications13:3.