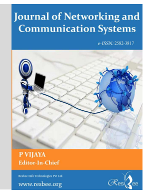
Vol.7 No.2 April 2024

Journal of Networking and Communication Systems

Received 14 February, Revised 20 March, Accepted 24 April



Advanced Message Transfer and Route Maintenance Incorporated Multipath Routing in Secure MANET

Harish goud nayenolla
University of Missouri Kansas City
nharish250@gmail.com

Abstract: A mobile ad hoc network (MANET) is a temporary network with a collection of wireless mobile nodes. The major concern in the MANET is the secure transmission of the data by preventing selfish nodes or attackers from the network. In this research, an advanced message transfer and route maintenance approach is developed for secure multipath routing in MANET. The cluster head from the nodes is selected using fuzzy clustering to address the security and energy crisis. The intrusion in the node is detected with the help of a fuzzy NB classifier (FNBC). The multipath routing is performed using the Bird Swarm-Whale Optimization Algorithm (BSWOA) for secure multipath communication between the source and the destination node. The BSWOA is developed by combining the Whale Optimization Algorithm (WOA), and Bird Swarm Algorithm (BSA). The fitness factors, such as trust, connectivity, throughput, and energy are used for the selection of optimal routes. The route maintenance is done using the dynamic quality factor based on trust and energy. The dynamic node insertion is performed using Unique Message Transfer (UMT). The performance of the developed BSWOA+UMT method is evaluated using metrics, such as delay, detection rate, energy consumption, and throughput in the absence of attack and the presence of blackhole attacks, flooding attacks, and selective path drop attacks. The developed BSWOA+UMT method obtained a minimum delay of 0.0030sec, maximum detection rate of 0.9095, minimum energy consumption of 8.7840J, and maximum throughput of 0.9005 respectively.

Keywords: Multipath Routing, Route Maintenance, Manet, Unique Message Transfer, Network.

1. Introduction

In recent years, the performance of wireless and computer technology has gained attention resulting in the widespread use of advanced mobile wireless computing applications. MANET is an efficient wireless network operation in which the functionality of routing is incorporated into the mobile nodes [8]. In MANET, the multi-hop wireless links are used for communicating between the mobile hosts, and the communication is done by relaying the messages. The transmission is performed in the MANET by developing a wireless network for setting the range of transmission between the nodes. The position of the mobile nodes can be changed at any time, which means that the nodes can leave or join the network anytime. The factors, such as resource constraint, mobility, hidden terminal problems, bandwidth, and exposed terminal problems are used for developing the routing protocol in MANET. The routing protocol provided adaptive, frequent, loop-free, fully distributed, minimum collisions, and stable topology [24] [25] [21] [22][2]. The MANET acts as both the hosts and routers besides providing equal capabilities for all the nodes. As the communication links are broken in the MANET due to the lack of infrastructure, the dynamic routing protocol is developed [13]. The changes in the available paths of the network are discovered, and the specific route is identified using the dynamic routing protocol that requires a significant amount of overhead traffic [2].

The network survivability is affected due to the limited capacity of the battery that disconnected the link. Hence, the routing protocol should provide importance to the mobile nodes for prolonging the lifetime of the network and guaranteeing the connectivity of the network [9]. The consumption of the energy in the battery is reduced by the power-aware routing protocols. The lifetime of the network is increased by forwarding the traffic through the nodes having high energy levels [8]. The traditional single-path routing algorithms are used for determining the shortest path to the destination with limited resources in the node. Some of the traditional single-path routing algorithms include Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV). It is important to note that the shortest path is not always the stable and optimal path when the node contains excessive load or resources that lead to traffic congestion in the load, thereby affecting the QoS performance. The node parameters, such

https://doi.org/10.46253/jnacs.v7i2.a3

as remaining energy, available bandwidth, and link stability are included in the selection of the path in some routing protocols [15]. For instance, the available link stability and the bandwidth are considered by the QOSAODV protocol for considering the packet type and sensor's residual energy [10] [6].

Various routing protocols, like the multipath routing protocols, are developed for increasing the network lifetime which can be improved by increasing the lifetime of the route. During the single route discovery process, the multipath routing protocols are used for the selection of the optimal route from the available routes. The number of route discovery processes is reduced during the multipath routing as there is availability of the backup routes. If one route fails then the energy consumption, end-to-end delay, and lifetime of the network are reduced [8]. After the link failure and node failure, the data transmission is restored by switching the multiple paths quickly with the help of a backup path [14]. The multipath routing provided better fault tolerance, load balancing, and bandwidth [11]. The resources, like idle queue length, available bandwidth, and battery level are available in multipath routing protocols [12]. The QoS is supported by comparing the node resources in different paths and transmitting the data for the selection of the optimal path. The path stability and the available resources of the path node are used for the selection of parameters of the path in MANET. The path stability is evaluated by the researchers through various factors. The QoS is supported rapidly by changing the adaptive link state of the routing protocol in high-speed movement scenarios of the nodes that are resource-limited. Thus, determining the appropriate criteria for the stability of the path is a challenging task in multipath routing [6].

The major intention of the research is the development of an advanced message transfer and route maintenance approach for secure multipath routing in MANET. Initially, the cluster head is selected from the nodes using fuzzy clustering. After selecting the cluster head, the intrusion node is identified with the help of FNBC. Then, the multipath route is discovered for communication between the source and the destination node using BSWOA. The multipath routing is followed by the route maintenance phase in which the dynamic quality factor is determined based on energy and trust. Finally, the dynamic node insertion and deletion phase is performed when a new node enters the network.

Proposed BSWOA+UMT for multipath routing: The major contribution of the research is the inclusion of the route maintenance phase, and dynamic node insertion and deletion phase in the multipath routing approach. The route maintenance phase in which the dynamic quality factor is defined based on energy and trust. When the new node enters the network, the UMT model is used in the Dynamic node insertion and deletion phase for adding and removing the nodes from the active node list.

The organization of the rest of the research is as follows, section 2 reviews the existing multipath routing protocol in MANET, section 3 explains the system model of the routing protocol, section 4 describes the developed advanced message transfer and route maintenance approach, section 5 illustrates the result of the proposed BSWOA+UMT method and section 5 concludes the paper.

2. Motivation

This section depicts the review of various existing multipath routing methods in MANET. These research papers are taken and reviewed according to the recently published years based on multipath routing protocols.

2.1. Literature Review

The literature review of the existing multipath routing in MANET is as follows, Kasthuribai, P. T., and Sundararajan, M.[1] developed a multipath routing in MANET using Particle Swarm Optimization And Gravitational Search Algorithm (PSOGSA). Although this method had better network lifetime and energy efficiency, it had high computational complexity. Reddy, A. P., and Satyanarayana, N.[2] designed a multipath routing technique for overcoming the issues regarding link stability and residual energy. This method used the motion parameters, like node direction and velocity for selecting the path required for the transmission of the packets of data within the nodes. This method provided high efficiency and throughput in the network. However, this method failed to consider the node's battery level. Sajal Sarkar and Raja Datta.[3] modeled a multipath routing for MANET using packet forwarding. The Markov chain was considered as a value function in the packet forwarding for the determination of the optimal routing policy. This method improved the throughput and energy consumption, reduced the delay, and balanced the load in the network. However, this method affected the performance as the load in the network increased. Ansuman Bhattacharya and KoushikSinha. [4] developed a Least Common Multiple Routing (LCMR) for the multipath routing in MANET. This method minimized the data packets using the distribution method for balancing the load by reducing the routing time. This method reduced the routing time required for transmitting the data packets. However, the major issue in the LCMR was assuring efficiency while assuring the objectives. Jabbar, W. A.*et al.*[5] developed a Multipath Battery and mobility-aware routing scheme-optimized link state routing (MBMA-OLSR) for multipath routing. The speed of the node and energy of the residual battery were evaluated using the Multi-Criteria Node Rank (MCNR) metric. The link assessment function was used for ranking the link stability. This method had high energy efficiency, but this method required more QoS metrics for determining the trade-off between the QoS and energy efficiency for the computation of the route. Chen, Z.*et al.*[6] designed a Topological change Adaptive Ad hoc On-demand Multipath Distance Vector (TA-AOMDV) for routing. This method considered the resources of the node and the probability of the link stability in the stable path selection algorithm. Depending on the estimate of periodic probability, the routing mechanism was updated in this method. This method improved the throughput and packet delivery ratio. However, this method failed to consider the protocol for scenarios with high speed. P. Francis Antony Selvi and M.S.K. Manikandan. [7] modeled a swarm-based Ant Colony Optimization (ACO) method for multipath routing. The probability of the path preference was obtained using the delay and the availability of the next hop. This method reduced the network load, but this method had high computational complexity. Aqeel Taha *et al.*[8] developed an Ad Hoc On-Demand Multipath Distance Vector with the Fitness Function (FF-AOMDV) for multipath routing. This method used the route distance and the energy level for the selection of the optimum route. This method had an extended lifetime and minimal consumption of energy. However, this method had limitations in addressing the QoS constraints. In 2023, Mamatha *et al.* [26] have implemented Optimized Link-state Routing (OLSR) and MANET. Initially, the IT2FLC-MDO algorithm was designed to solve the optimization problem. The EQ0S features were incorporated with an algorithm to formulate to enhance OLSR protocol efficiency. Multicriteria a node rank metric (MCNR) computed the features to minimize the overhead complexity. The whole process was carried out in the ns2 simulator. The simulated results improved the MANETS lifetime. In 2023, Shafi *et al.* [27] executed an Ant colony optimization-based energy-aware cross-layer routing protocol (AOERP). Initially, the nodes in the network select an adaptive relay node based on high energy factor and neighbor node ratio to avoid dead nodes. The selected relay nodes then identify a nested path in the direction of the destination using the Ant Colony Optimization (ACO) method. The routing table at each node includes additional fields like Energy Factor, NNR, Stability factor, and Pheromone values to improve the routing reliability and increase the entire network lifetime. The performance of the proposed AOERP protocol is evaluated using Network Simulator Version 2.34 (NS-2.34) and compared over existing energy-aware routing schemes. In 2023, Khudair Madhloom *et al.* [28] applied the quantum swarm intelligence technique. Initially, QACO was initialized with the parameters. Then the new GWs were inserted through the QACO algorithm. The existing GWs were tested and maintained. Furthermore, new alternative paths were tried to connect if it didn't the method tried to fix with the alternative path through QACO. In 2023, Shareef *et al.* [29] have ensembled the AODV algorithm for communication. Initially, the source node was selected. The source node then transfers the message to the adjacent node. To provide efficient routing, the delay path, the density of the router, and a minimum number of interactions were considered for the best routing routes for its destination. Finally, the Laying Chicken algorithm was used to select the effective route. The algorithm improved the effectiveness of vehicular communication. In 2022, Yamini *et al.* [30] have used ETERE to select secured routing. This paper implemented three methods they were selecting their trusted network through self-monitoring, Selecting the nodes that were already connected through coordinate monitoring, and finally, the method using the trust technique through ATA. These methods helped to transfer the information and were also used for secure routing in MSNETs. In 2021, Sundarraj, P.D. and Arulanandam, K [31] have adopted TLBO and WAFSA. Initially, Nodes were clustered based on their distance. WAFSA was used to select the optimum cluster head. This helped to transfer data securely in the clusters. ADS were used to generate a key that was secret for secure communication between the member nodes and CHs. Finally, NS-2 was used to evaluate the performance for ensuring the secure transfer of data. In 2022, Bharti *et al.* [32] have experimented with Enhanced path routing with buffer allocation (IPBA). Initially, the nodes were deployed unevenly with their restricted energy levels. Furthermore, the IPBA technique was implemented to establish strong communication. Then coupling was performed by selecting of best couple node for selection and the connection was established. If the connection was established with any error then the connection was further established through IPBA until it selects the best node. Finally, the performance was evaluated through various parameters. In 2022, Abdulrab *et al.* [33] have tried the wireless HART network for establishing multipath routing. Initially, three primary paths and a backup node were developed to ensure continuous connection in any link faults. Then through optimal network planning and deployment algorithm, the model was developed. Finally, NS2 simulators were used to compare the performance with the existing method.

2.2. Challenges

The challenges faced during the multipath routing in MANET are as follows,

- The TA-AOMDV method failed to use the routing algorithm in the scenarios with highspeed. For adapting the routing algorithm for the scenarios with high speed, the heuristic routing algorithm was developed based on the change in the parameter by letting the nodes infer the changes in the topology [6].
- The challenges in the FF-AOMDV method are the improvement of the lifetime of the network and enhancement of the energy consumption. Hence, various network resources should be considered for enhancing the QoS and lifetime of the network [8].
- The packet forwarding improved the efficiency, and the throughput of the network, but the challenge lies in improving the performance of the system for the increasing amount of load in the network [3].
- In [5], the challenge lies are deploying the MCNR metric for the assessment of the trade-off between the QoS and energy efficiency by exploiting the different layers of QoS metrics. Other challenge includes the application of the MBMA-OLSR protocol for large-scale network deployments.
- The LCMR method reduced the overall routing time, but the major concern is the improvement of energy efficiency. Hence, the challenge of the LCMR method lies in improving energy efficiency as the reduction in energy efficiency simultaneously affectsthe lifetime of the network [4].

3. System Model

This section describes the system model of MANET which is a mobile network. The nodes in the MANET are distributed in the environment and the clusters are formed during the energy crisis by grouping the nodes based on the clustering algorithm. In the MANET, the communication is secured and the malicious nodes are determined by evaluating the security factor of the nodes. Let us consider, that there are n number of nodes in the network and the nodes are given as

$$W = \{W_1, W_2, ..., W_u, ..., W_l\} \tag{1}$$

where the u^{th} node of the network is represented as, W_u. The destination and the source nodes are represented as, H and G respectively. At first, the network is initialized and then, the effective trust factors are determined for network communication by the computation of the nodes, which is followed by updating the trust table. After establishing the trust table, the CH is selected with the help of fuzzy clustering. In the network, the CHs are denoted as,

$$J = \{J_1, J_2, ..., J_v, ..., J_h\} \tag{2}$$

Where the total number of CHs is given as, h. In the MANET, the secure nodes are selected for communication through intrusion detection. Then, the CHs are used for establishing the path for the secure communication and the proposed optimization is used for the selection of multipath.

3.1. Energy Model

At the end of the communication, the energy of the MANET nodes is updated. The remaining energy of the nodes is represented as,

$$d_{u,t}^{remain} = d_{u,t-1}^{remain} - d_{u,t}^{trans} * b(t-1,t) - d_{u,t}^{receive} * b(t-1,t) \tag{3}$$

where, the energy required for communicating the information is represented as, $d_{u,t}^{trans}$ and $d_{u,t}^{receive}$. During the initiation of the network communication, the energy is considered full. The remaining energy of the nodes is evaluated based on the ratio between the remaining energy of the node, and the maximal energy during the beginning of the communication. The remaining energy lies in the high and low energy range. The remaining energy of the nodes is not necessary for transmitting the packets of data when the low range's upper threshold lies above the energy ratio, whereas the remaining energy of the nodes is sufficient for transmitting the packets of data when the upper threshold falls behind the energy ratio. The value of the upper threshold is user-defined and is set as "0.2" [23]. The link connectivity and transmission power of the channel are decided based on the remaining node energy, which means that the low values of remaining node energy describe the poor connectivity in the network.

3.2. Trust Model

The miscommunication in the network is avoided by evaluating the trust factor, which determines the trust of the nodes and rejects the malicious nodes for providing healthy communication in MANET. For the l nodes of the network, the trust degree of the nodes is calculated and tabulated to eliminate the malicious nodes. The trust factors, like direct trust, indirect trust, recent trust, trust based on data-byte, and error-based trust are evaluated in the trust model. Initially, the node is set as "1"while establishing the nodes before the communication. Further, the multi-path communication is preceded using the node's trust table to ensure the effectiveness of the intrusion detection in MANET. The trust factors are described as follows,

3.2.1. Direct TRUST (Dt)

The Direct trust is evaluated based on the communication time between the a^{th} destination and u^{th} node. The difference between the estimated time and the actual time of the u^{th} node is considered for authenticating the public key provided by the a^{th} destination indirect trust. Hence, the direct trust within the a^{th} destination and u^{th} node is given as,

$$DT_u^a(t) = \frac{1}{3}\left[DT_u^a(t-1) - \left(\frac{t_{appx} - t_{est}}{t_{appx}}\right) + \beta\right] \tag{4}$$

where, the estimated time and the actual time for the authentication of the public key is represented as, t_{est} and t_{appx}. The node's witness factor is represented as, β.

3.2.2. Indirect Trust

The Direct trust authenticated the nodes containing the witness factor, whereas the Indirect trust authenticated the nodes that did not possess the witness factor [18]. The Indirect trust is represented as,

$$IDT_u^a(t) = \frac{1}{k}\sum_{u=1}^{k} DT_u^a(a) \tag{5}$$

where the node u contains the total neighbor which is denoted as, k.

3.2.3. Trust using the Data Bytes

The trust based on the data byte is determined based on the communication of the data in bytes within the a^{th} destination and u^{th} node. The trust evaluated using the data byte is given as,

$$DB_u^a(t) = \frac{1}{2} * \left[\frac{DB^u}{\alpha} + \frac{DB^a}{\alpha}\right] \tag{6}$$

where, the total bytes that are transmitted and received at the a^{th} destination node and node u is given as, DB^a and DB^u. The packet's data limit at the sending and the receiving point is represented as, α.

3.2.4. Recent Trust (RT)

The Recent trust acknowledged the destination besides authenticating the key with the help of indirect trust and direct trust [19]. The Recent trust is determined as,

$$RT_u^a(t) = \gamma * DT_u^a(t) + (1-\gamma) * IDT_u^a(t) \tag{7}$$

where, the value of γ is given as, 0.3.

3.2.5 Error-Based Trust

The trust based on the error is used for determining the error in the communication. The error-based trust is given as,

$$\rho_u^a(t) = \frac{1}{C} * \sum_{m=1}^{C} \rho_m \tag{8}$$

where, the error and the total transactions are represented as, ρ_m and ρ. The error in the connection is denoted as either '0', or '1'.

4. Proposed Advanced Message Transfer and Route Maintenance Approach

The primary intention of this research is the development of an advanced message transfer and route maintenance approach for secure multipath routing in MANET. The developed method consists of six different phases, such as the cluster head selection phase, intrusion node identification phase, multipath route discovery phase, route maintenance phase, and the dynamic node insertion and deletion phase. The first phase is the cluster head selection phase in which fuzzy clustering is used for selecting the cluster head from the nodes. In the second phase, the intrusion node is detected with the help of the FNBC. The secure multipath communication between the source and the destination node is ensured in the multipath route discovery phase using BSWOA, which is developed by integrating BSA and WOA. The fourth phase is the route maintenance phase in which the dynamic quality factor is defined based on energy and trust. In the fifth phase, the dynamic node insertion is done to include new nodes in the active node list. The final phase is the deletion phase in which the nodes are removed from the active node list. Fig. 1 depicts the architecture of the advanced message transfer and route maintenance approach.

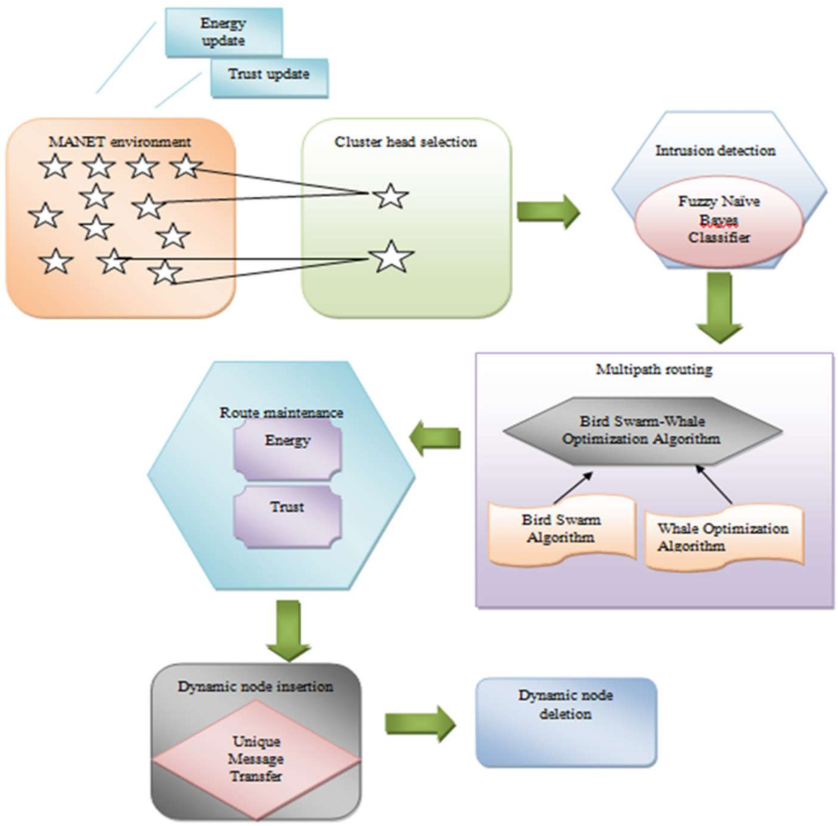


Fig. 1. *Architecture of the advanced message transfer and route maintenance approach*

4.1. Cluster Head Selection Using Fuzzy Clustering

To ensure the energy efficiency of the network, fuzzy clustering is employed for clustering the nodes in the MANET [13]. The clustering algorithm selected the optimal CH for enabling further communication in the network. The trust factors are used mainly for the selection of the optimal CH. In fuzzy clustering, similar nodes are grouped depending on the membership degree. Thus, the overlapped data is effectively managed using fuzzy clustering. Obtaining the minimization function is the major objective in the selection of CH, which is given as,

$$S = \sum_{u=1}^{g} \sum_{v=1}^{h} Q_{uv}^{rr} \times \left\| W_u - J_v \right\|^2 \; ; 1 \le rr \le \infty \tag{9}$$

where, the v^{th} CH and u^{th} node are represented as, J_v and W_u. The Euclidean distance within the v^{th} CH and u^{th} node is given as, $\| \ \|$. The fuzzifier and the objective function are defined as, r and S. At first, the CHs are randomly initialized in the fuzzy clustering mechanism. The CH with the nodes having the minimal distance is grouped under the same cluster. After the initialization, the membership value is evaluated for every node to their CHs. The new CH is selected based on the membership function, and the above steps are repeated until the new CH is determined. The fuzzy clustering computed the optimal CHs as given in equation (2).

4.2. Identification of the Intrusion Node Using FNBC

The trust factors of the nodes are used for determining the intrusion in the network. The sink node detected the intruders in the network through the information of the node, which is gathered from the communication of the node with the sink node through the CHs. Then, the intruder node is eliminated from further communicating with the other nodes. The intruder is predicted in the sink node through FNBC. The FNBC used the probability theory for determining the class label of the u^{th} node as either a normal node or an intruder node with the help of the trust table s^u. For the class R_t corresponding to the trust s^u, the conditional probability is given as,

$$P\left(R_t \middle| s^u\right) = P\left(R_t\right) \prod_{R=1}^{6} \left(\frac{P\left(s_R^u \middle| R_t\right)}{P\left(s_R^u\right)} \times Q_R^u \right) \tag{10}$$

where, the t^{th} class probability is defined as, $P(R_t)$ and the value of t is given as "2" which describes the classes, such as normal nodes and intruder nodes. The probability of the value of the individual trust for the node u in correspondence to the t^{th} class is denoted as, $P\left(s_R^u \middle| R_t\right)$. Depending on the individual node's trust factor, the probability of the class is determined and the class label of the label was evaluated depending on the maximal value of the probability. After determining the genuine nodes, the intruders are removed from communicating in the network. In the network, the genuine nodes are given as,

$$W = \{W_1, W_2, ..., W_u, ..., W_c\} \; ; \; c < n \tag{11}$$

where, the total genuine nodes are denoted as, c and n is the total nodes in the network. The optimal multipath selection is progressed after determining the genuine nodes. Thus, intrusion detection is done for performing the communication without the delay in transmission and energy degradation.

4.3. Active Node Listing Table

The active node listing table consists of the active nodes, which defines the nodes obtained by removing the malicious nodes. The new nodes are added to the active node listing table only if the nodes satisfy the UMT constraints. If any node has a low trust level, it is removed from the network.

4.4. Multipath Routing Using BSWOA

In the MANET, secure multipath communication is ensured between the source and the destination node after the detection of intrusion. The major challenge in multipath communication is the selection of the optimal path for communication. In this research, secure communication is performed using the optimization algorithm, and the optimal paths are selected based on factors, like throughput, energy, node connectivity, and trust. Initially, the multipath between the source node and the destination node is done by generating the path based on the RPL routing. The optimal paths are determined from the generated path using BSWOA. The BSWOA is developed by the integration of the BSA [16] and WOA [17]. In BSWOA, the behavior of the solution is updated based on the foraging behavior or the vigilance behavior depending on the condition, $rand(0,1) < D$. The solution is updated in the BSWOA based on the foraging behavior if it satisfied the conditions, like $rand(0,1) < D$ and $(\omega \% \eta \neq 0)$ as,

$$A_{n,o}^{\omega+1} = A_{n,o}^{\omega} + randn(0,1) \times A_{n,o}^{\omega} \tag{12}$$

where, the n^{th} bird's position in the previous iteration is denoted as, $A_{n,o}^{\omega}$, the Gaussian distribution number is represented as, $randn(0,1)$. If the condition is not satisfied, the solution is updated in the BSWOA based on the vigilance behavior as,

$$A_{n,o}^{\omega+1} = A_{n,o}^{\omega} + U_1 \left(\xi_o - A_{n,o}^{\omega} \right) \times rand(0,1) + U_1 \left(\sigma_{q,o} - A_{n,o}^{\omega} \right) \times rand(-1,1) \tag{13}$$

where, $U_1 = f_1 \times \exp\left(-\frac{\sigma Fit_n}{\sum Fit + \upsilon} \times P \right)$ and $U_2 = f_2 \times \exp\left(\left(\frac{\sigma Fit_n - \sigma Fit_q}{\left| \sigma Fit_q - \sigma Fit_n \right| + \upsilon} \right) \frac{P \times \sigma Fit_q}{\sum Fit + \upsilon} \right)$, f_1 and f_2 are the positive constants that considered the values from '0' to '2', the position integer that consists of the random value between 1 and υ is denoted as, q. The sum of the swarm's best fitness and the n^{th} bird's best fitness measure is represented as, $\sum Fit$ and σFit_n. The position of the mean of a swarm is represented as, ξ_o. If the condition $(\tau \% \lambda \neq 0)$ is not satisfied, the solution is updated based on equations (12) and (13) by dividing the swarm into producers and scroungers.

4.5. Route Maintenance

If the node is under the active nodes, and it also satisfies the dynamic quality factor that is above the threshold, the route maintenance occurs. The dynamic quality factor is evaluated by the below equation as,

$$DRF_u = \frac{1}{3}[T_u + E_u + Y_u] \tag{14}$$

where, the energy of the node and the trust of the node is given as, E_u and T_u, the connectivity of the node is represented as, Y_u.

4.6. Dynamic Node Insertion Using "UMT"

This section describes the process of addition of new nodes into the active node list. Initially, the request REQ is sent by the new node to the CH to join the active node list. The CH receives the request from the new node which is denoted as, REQ^R. After receiving the request from the new node, the acknowledgment ACK is sent by the CH to the new node which is denoted as, ACK^R. The new node receives the acknowledgement and sends the user identity U_{ID}, user password U_{pwd} to the CH. The CH saved the user identity and the user password as, U^*_{ID} and U^*_{pwd}. After that, the key to access the network P^{ID}_{key} is provided by the CH to the new node which is saved by the new node as, p^{ID}_{key}. Thus, the new node is added to the active node list with the help of p^{ID}_{key}. Fig. 2 shows the flow diagram of the Dynamic node insertion using UMT.

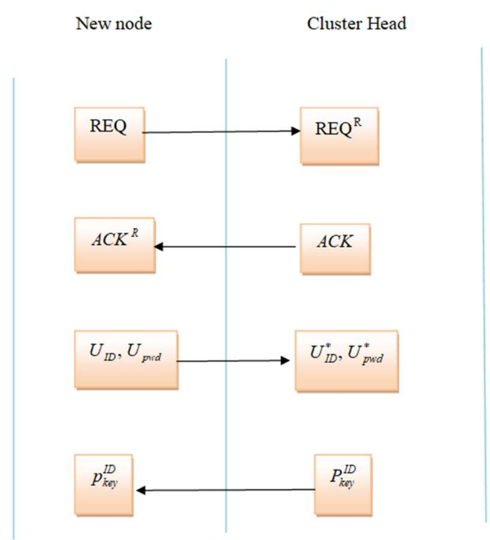


Fig. 2. *Flow diagram of Dynamic node insertion using "UMT"*

4.7. Dynamic Node Deletion

Dynamic node deletion is the process of removing the nodes from the list of active nodes. The dynamic node deletion is carried out with the help of two conditions,

i. If the node is identified as a malicious node,
ii. If the dynamic quality factor is less than the threshold.

Thus, the nodes that come under the above conditions are removed from the list of active nodes.

5. Results and Discussion

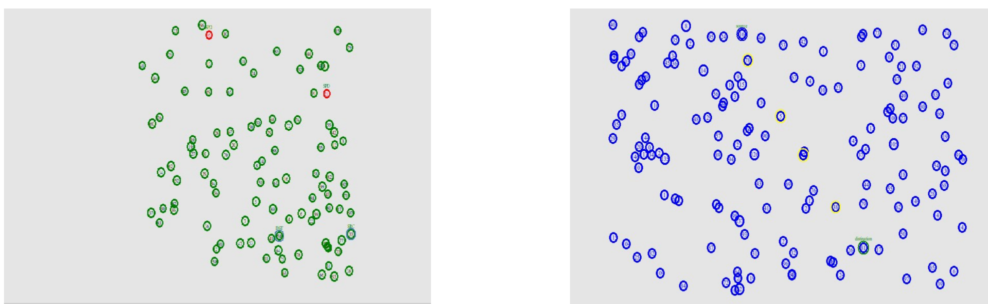
The result obtained by the proposed BSWOA+UMT method is analyzed using the metrics, such as energy, delay, detection rate, and through put by varying numbers of rounds in the presence of blackhole attacks, flooding attacks, selective path drop attacks, and in the absence of attack.

5.1. Experimental Setup

The proposed BSWOA+UMT method is implemented in NS2 software and the simulation parameters are discussed below,

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

5.2. Simulation Results



a) b)

Fig. 3. *Simulation results a) in the presence of an attack b) in the absence of an attack*

The simulation results of the developed BSWOA+UMT method are depicted in Fig. 3. Fig. 3 a) shows the environment in the network in the presence of attack and Fig. 3 b) shows the environment in the network in the absence of attack.

5.3. Evaluation Metrics

The metrics used for the evaluation of the multipath routing protocols are energy, delay, detection rate, and throughput. The detection rate is the rate of detection of malicious nodes effectively. The detection rate should be maximum for an effective routing protocol. The delay is defined as the time considered for communicating between destination and source nodes. The energy is determined using the equation (3). The throughput is the ratio of total transmitted bits in the network per second. The value of throughput and energy should be maximal for an effective method of multipath routing.

5.4. Comparative Methods

The methods, like BSWOA, Naive Bayes [20], fuzzy NB,K-means NB [19], and NBTrust [18] are compared with the developed BSWOA+UMT method for the analysis.

5.5. Comparative Analysis

The developed BSWOA+UMT method is compared with the existing fuzzy NB, K-means NB, Naive Bayes, and BSWOA method in the presence of blackhole attacks, flooding attacks, selective path drop attacks, and in the absence of attack using the evaluation metrics.

5.5.1. Comparative Analysis with Black Hole Attacks

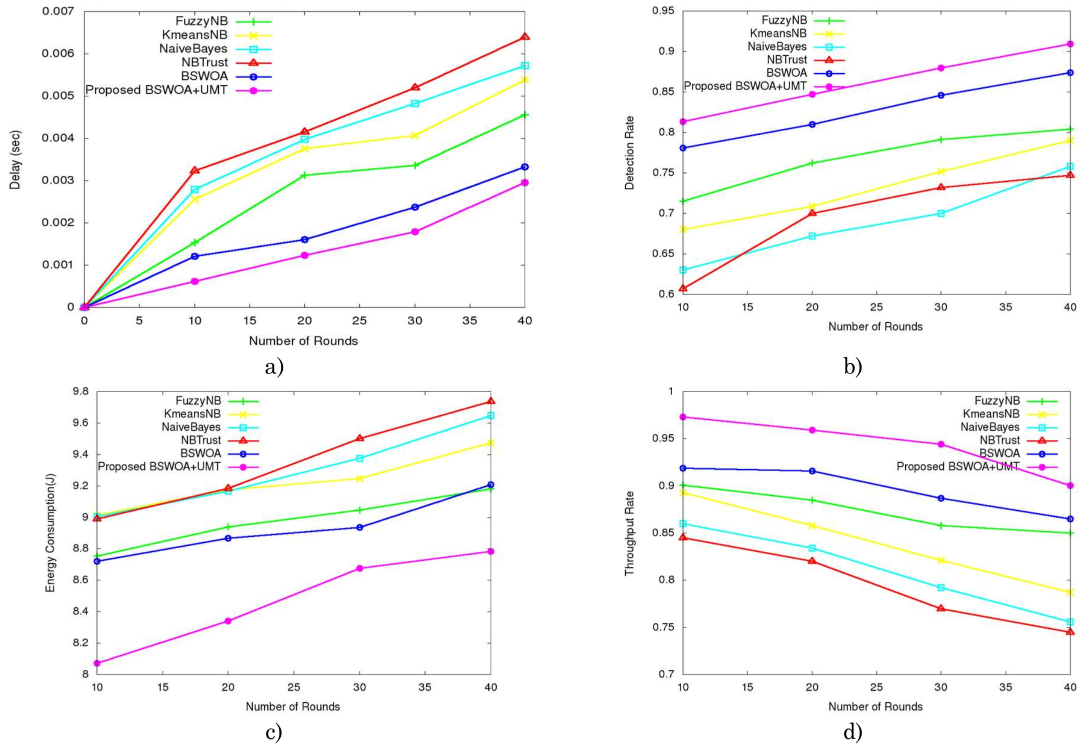


Fig. 4.*Comparative analysis using a) Delay, b) Detection rate, c) Energy consumption, d) Throughput Rate in the presence of black hole attacks*

Fig. 4 shows the comparative analysis of the multipath routing protocols using the metrics, such as energy, delay, detection rate, and throughput rate in the presence of black hole attacks. Fig. 4 a) depicts the analysis of the multipath routing protocols using delay. The delay attained by the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT for the number of rounds of 30 is 0.0031sec, 0.0038sec, 0.0040ec, 0.0042sec, 0.0016sec and 0.0012s, respectively. Fig. 4 b) explains the detection rate analysis of the multipath routing protocols. For 30 rounds, the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT obtained a detection rate of 0.791, 0.752, 0.7, 0.732, 0.846, and 0.8797, respectively. The developed BSWOA+UMT method had a percentage improvement of 10.08%, 14.52%, 20.43%, 16.79%, and 3.83% when compared with the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods, respectively.

Fig. 4 c) shows the analysis of the multipath routing protocols using the amount of energy consumed. When the number of rounds is 20, the proposed BSWOA+UMT method consumed an energy of 8.3395, whereas the existing fuzzy NB, K-means NB, Naive Bayes NBTrust, and BSWOA consumed an energy of 8.9380J, 9.1760J, 9.1660J, 9.1830J and 8.8670J, respectively. The performance improvement of the developed BSWOA+UMT method when compared to the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods is6.70%, 9.12%, 9.02%, 9.19%, and 5.95%, respectively. Fig. 4 d) illustrates the throughput analysis of the multipath routing protocols. The throughput of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT method for the number of rounds of 10 is 0.9010, 0.8930, 0.8600, 0.8450, 0.9190, and 0.9730, respectively. When compared with the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods, the developed BSWOA+UMT method obtained a performance improvement of 7.40%, 8.22%, 11.61%, 13.16%, and 5.55%, respectively.

5.5.2. Comparative Analysis with Flooding Attacks

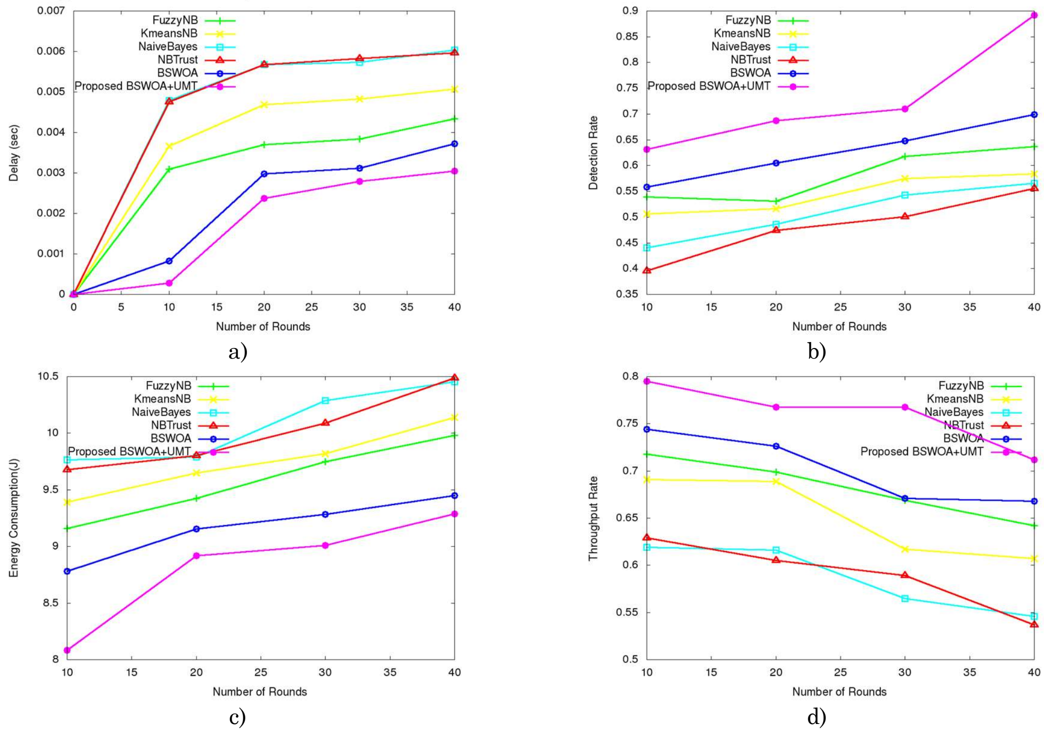


Fig. 5.*Comparative analysis using a) Delay, b) Detection rate, c) Energy consumption, d) Throughput Rate in the presence of flooding attacks*

Fig. 5 describes the comparative analysis of the multipath routing protocols in the presence of flooding attacks using the metrics, such as energy, delay, detection rate, and throughput rate.Fig. 5a) explains the delay analysis of the multipath routing protocols. For 20 number of rounds, the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT obtained a delay of 0.0037sec, 0.0047sec, 0.0057sec, 0.0057sec and 0.0030sec and 0.0024sec, respectively. Fig. 5 b) depicts the analysis of the multipath routing protocols using detection rate. The detection rate attained by the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT for the number of rounds of 30 is0.6180, 0.5750, 0.5430, 0.5010, 0.6480 and 0.7101, respectively. The performance improvement of the developed BSWOA+UMT method when compared to the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods is12.97%, 19.03%, 23.53%, 29.45%, and 8.75%, respectively.

Fig. 5 c) illustrates the energy consumption analysis of the multipath routing protocols. The energy consumed by the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT method for the number of rounds of 40 is 9.9800J, 10.1380J, 10.4560J, 10.4870J, 9.4500J and 9.2860J, respectively. When compared with the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods, the developed BSWOA+UMT method obtained a performance improvement of 6.95%, 8.40%, 11.19%, 11.45%, and 1.77%, respectively. Fig. 5 d) shows the analysis of the multipath routing protocols using throughput. When the number of rounds is 20, the proposed BSWOA+UMT method has a throughput of 0.7676, whereas the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA obtained a throughput of 0.6990, 0.6890, 0.6160, 0.6050, and 0.7260 respectively. The performance improvement of the developed BSWOA+UMT method when compared to the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust and BSWOA methods are 8.94%, 10.24%, 19.75%, 21.19%, and 5.42%, respectively.

5.5.3. Comparative Analysis with Selective Forwarding Attacks

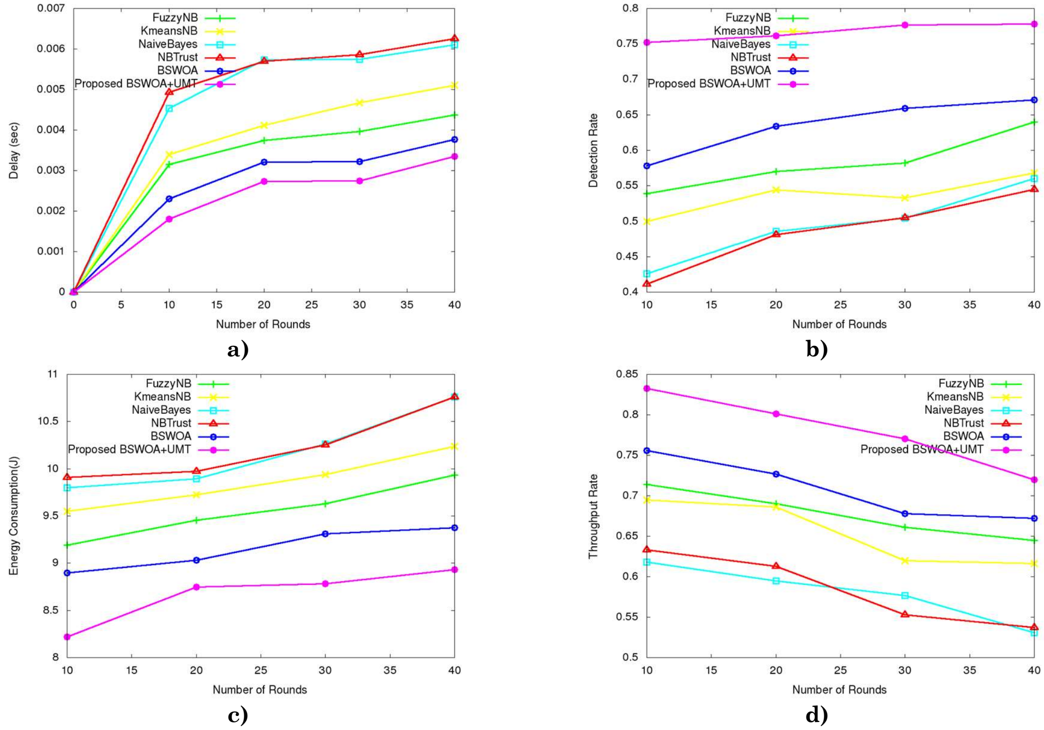


Fig. 6.*Comparative analysis using a) Delay, b) Detection rate, c) Energy consumption, d) Throughput Rate in the presence of selective forwarding attacks*

Fig. 6 shows the comparative analysis of the multipath routing protocols using the metrics, such as energy, delay, detection rate, and throughput rate in the presence of selective forwarding attacks. Fig. 6 a) illustrates the delay analysis of the multipath routing protocols. The delay of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, Pand proposed BSWOA+UMT method for the number of rounds of 20 is 0.0032sec, 0.0034sec, 0.0045sec, 0.0049sec, 0.0023sec and 0.0018 sec, respectively. Fig. 6 b) explains the detection rate analysis of the multipath routing protocols. For 40 rounds, the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT obtained a detection rate of 0.6400, 0.5680, 0.5600, 0.5450, 0.6710 and 0.7781, respectively. The developed BSWOA+UMT method had a percentage improvement of 17.74%, 27%, 28.03%, 29.95%, and 13.76% when compared with the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods, respectively.

Fig. 6 c) shows the analysis of the multipath routing protocols using the amount of energy consumed. When the number of rounds is 20, the proposed BSWOA+UMT method consumed an energy of 8.7481, whereas the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA consumed an energy of 9.4570J, 9.7230J, 9.8950J, 9.9710J and 9.0340J, respectively. The performance improvement of the developed BSWOA+UMT method when compared to the existing fuzzy NB, K-means NB, Naive Bayes, and NBTRUST, BSWOA methods are 7.50%, 10.03%, 11.59%, 12.27%, and 3.17%, respectively. Fig. 6 d) depicts the analysis of the multipath routing protocols using throughput. The throughput attained by the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT for the number of rounds of 10 is 0.7140, 0.6950, 0.6180, 0.6330, 0.7560 and 0.8324, respectively. The performance improvement of the developed BSWOA+UMT method when compared to the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods is14.22%, 16.50%, 25.75%, 23.95%, and 9.18%, respectively.

5.5.4. Comparative Analysis without Attack

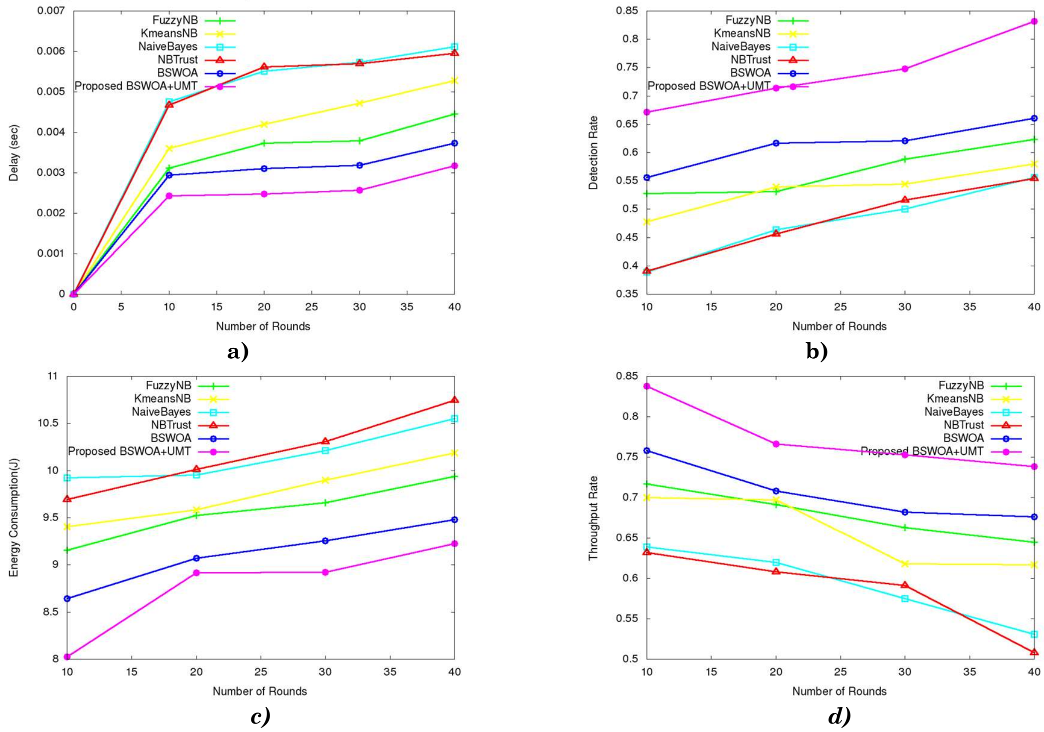


Fig. 7.*Comparative analysis using a) Delay, b) Detection rate, c) Energy consumption, d) Throughput Rate without attack*

Fig. 7 describes the comparative analysis of the multipath routing protocols in the absence of attacks using the metrics, such as energy, delay, detection rate, and throughput rate. Fig. 7 a) shows the analysis of the multipath routing protocols using the amount of delay. When the number of rounds is 20, the proposed BSWOA+UMT method obtained a delay of 0.0025s, whereas the existing fuzzy NB, K-means NB, Naive Bayes NBTrust, and BSWOA obtained a delay of 0.0037 sec, 0.0042 sec, 0.0055 sec, 0.0056 sec, and 0.0031 sec, respectively. Fig. 7 b) illustrates the detection rate analysis of the multipath routing protocols. The detection rate of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA,and proposed BSWOA+UMT method for the number of rounds of 30 is 0.5880, 0.5440, 0.5, 0.5160, 0.6210 and 0.7480, respectively. When compared with the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods, the developed BSWOA+UMT method obtained a performance improvement of 21.39%, 27.27%, 33.165, 31.02%, and 16.98%, respectively.

Fig. 7 c) depicts the analysis of the multipath routing protocols using energy consumed. The energy consumed by the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA, and proposed BSWOA+UMT for the number of rounds of 30 is 9.6580J, 9.8980J, 10.2110J, 10.3070J, 9.2570J and 8.9203J, respectively. The performance improvement of the developed BSWOA+UMT method when compared to the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods is7.64%, 9.88%, 12.64%, 13.45%, and 3.64%, respectively. Fig. 7 d) explains the throughput analysis of the multipath routing protocols. For 20 number of rounds, the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, BSWOA,and proposed BSWOA+UMT obtained a throughput of 0.6910, 0.6970, 0.6200, 0.6080, 0.7080 and 0.7661, respectively. The developed BSWOA+UMT method had a percentage improvement of 9.80%, 9.02%, 19.07%, 20.63%, and 7.58% when compared with the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods, respectively.

5.6. Comparative Discussion

Table 1 shows the comparative discussion of the multipath routing protocols using metrics, like delay, throughput, detection rate, andenergy consumption in the presence of blackhole attacks, flooding attacks, selective path drop attacks, and in the absence of attack. The developed BSWOA+UMT method obtained a minimum delay of 0.0030s when compared to the existing fuzzy NB, K-means NB, Naive Bayes NBTrust, and BSWOA with the delay of 0.0046 sec, 0.0054 sec, 0.0057 sec, 0.0064 sec and 0.0033 sec, respectively for number of rounds is 40 in the presence of blackhole attacks. The detection rate of the developed BSWOA+UMT method is 0.9095, whereas the detection rate of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 0.8040, 0.7900, 0.7580, 0.7470 and 0.8740, respectively. From the analysis, the developed BSWOA+UMT method obtained a maximum detection rate than the existing methods. In the presence of blackhole attacks, the developed BSWOA+UMT method obtained a minimum energy consumption of 8.7840J when compared to the energy consumption of the existing fuzzy NB of 9.1810J, K-means NB of 9.4750J, Naive Bayes of 9.6480J, NBTrust of 9.7360J and, BSWOA of 9.2070, respectively. When the number of rounds is 40, the developed BSWOA+UMT method obtained a maximum throughput of 0.9005, and the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods obtained a throughput of 0.8500, 0.7870, 0.7560, 0.7450, and 0.8650, respectively in the presence of blackhole attacks.

For the number of rounds is 40, the delay obtained by the developed BSWOA+UMT method is 0.0030, whereas the delay from the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 0.0043 sec, 0.0051 sec, 0.0060 sec, 0.0060 sec, and 0.0037 sec, respectively in the presence of flooding attack. The detection rate of the developed BSWOA+UMT method is 0.8915, whereas the detection rate of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 0.6370, 0.5840, 0.566, 0.5560 and 0.6990, respectively for 40 number of rounds in the presence of flooding attacks. In the presence of a flooding attack, the energy consumed by the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA and developed BSWOA+UMT method are 9.9800J, 10.1380J, 10.4560J, 10.4870J, 9.4500J, and 9.2860J, respectively. The throughput of the developed BSWOA+UMT method is 0.7119, whereas the detection rate of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 0.6420, 0.6070, 0.5460, 0.5370 and 0.6680, respectively. From the analysis, the developed BSWOA+UMT method obtained a maximum detection rate than the existing methods for 40 rounds in the presence of flooding attacks.

The developed BSWOA+UMT method obtained a minimum delay of 0.003s when compared to the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA with the delay of 0.0044 sec, 0.0051 sec, 0.0061 sec, 0.0063 sec and 0.0038 sec, respectively for number of rounds is 40 in the presence of Selective path drop Attack. In the presence of a Selective path drop Attack, the developed BSWOA+UMT method obtained a maximum detection rate of 0.7781 when compared to the detection rate of existing fuzzy NB of 0.6400, K-means NB of 0.5680, Naive Bayes of 0.5600, NBTrust of 0.5450, and BSWOA of 0.6710, respectively. The energy consumption of the developed BSWOA+UMT method is 8.9312J, whereas the energy consumption of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 9.9330J, 10.2390J, 10.7590J, 10.7590J, and 9.3730J, respectively. From the analysis, the developed BSWOA+UMT method obtained a minimum energy consumption than the existing methods. When the number of rounds is 40, the developed BSWOA+UMT method obtained a maximum throughput of 0.7196,and the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA methods obtained a throughput of 0.6450, 0.6160, 0.5310, 0.5370, and 0.6720, respectively in the presence of Selective path drop Attack.

In the absence of attacks, the developed BSWOA+UMT method obtained a minimum delay of 0.0032, whereas the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA and obtained a delay of 0.0045 sec, 0.0053 sec, 0.0061 sec, 0.0060 sec, 0.0037 sec, respectively. The detection rate of the developed BSWOA+UMT method is 0.8314, whereas the detection rate of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 0.6230, 0.5800, 0.5560, 0.5540 and 0.6610, respectively. From the analysis, the developed BSWOA+UMT method obtained a maximum detection rate than the existing methods for 40 rounds in the absence of attacks. For the number of rounds is 40, the energy consumption obtained by the developed BSWOA+UMT method is 9.2251, whereas the energy consumption of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 9.9380J, 10.1890J, 10.5520J, 10.7440J, and 9.4810J, respectively in the absence of attacks. The throughput of the developed BSWOA+UMT method is 0.7381, whereas the throughput of the existing fuzzy NB, K-means NB, Naive Bayes, NBTrust, and BSWOA is 0.6450, 0.6170, 0.5310, 0.5080, and 0.6760, respectively for 40 number of rounds in the absence of attacks.

Table 1. *Comparative discussion of the multipath routing protocols*

	Metrics	Fuzzy NB	K-means NB	Naive Bayes	NBTrust	BSWOA	BSWOA+UMT
Blackhole Attack	*Delay (sec)*	0.0046	0.0054	0.0057	0.0064	0.0033	**0.0030**
	Detection Rate	0.8040	0.7900	0.7580	0.7470	0.8740	**0.9095**
	Energy consumption (J)	9.1810	9.4750	9.6480	9.7360	9.2070	**8.7840**
	Throughput	0.8500	0.7870	0.7560	0.7450	0.8650	**0.9005**
Flooding Attack	*Delay(sec)*	0.0043	0.0051	0.0060	0.0060	0.0037	**0.0030**
	Detection Rate	0.6370	0.5840	0.566	0.5560	0.6990	**0.8915**
	Energy consumption (J)	9.9800	10.1380	10.4560	10.4870	9.4500	**9.2860**
	Throughput	0.6420	0.6070	0.5460	0.5370	0.6680	**0.7119**
Selective path drop Attack	*Delay (sec)*	0.0044	0.0051	0.0061	0.0063	0.0038	**0.0033**
	Detection Rate	0.6400	0.5680	0.5600	0.5450	0.6710	**0.7781**
	Energy consumption (J)	9.9330	10.2390	10.7590	10.7590	9.3730	**8.9312**
	Throughput	0.6450	0.6160	0.5310	0.5370	0.6720	**0.7196**
Without Attack	*Delay (sec)*	0.0045	0.0053	0.0061	0.0060	0.0037	**0.0032**
	Detection Rate	0.6230	0.5800	0.5560	0.5540	0.6610	**0.8314**
	Energy consumption (J)	9.9380	10.1890	10.5520	10.7440	9.4810	**9.2251**
	Throughput	0.6450	0.6170	0.5310	0.5080	0.6760	**0.7381**

6. Conclusion

In this research, an advanced message transfer and route maintenance approach is developed for secure multipath routing in MANET. Initially, the nodes are initialized depending on the trust and energy factor for effective multipath routing. Then, the cluster head is selected from the nodes with the help of fuzzy clustering followed by the detection of the intrusion node. During the intrusion detection, the malicious nodes are filtered out using FNBC. After that, the multipath routing is performed for secure multipath communication between the source and the destination node using BSWOA, which is the integration of BSA and WOA. The route maintenance is done through the energy and trust factors. Finally, the dynamic node insertion and deletion are performed for the inclusion and removal of nodes from the active node list. The developed BSWOA+UMT method is compared with the existing multipath routing protocol methods in the presence of blackhole attacks, flooding attacks, selective path drop attacks, and in the absence of attack using the evaluation metrics, such as delay, detection rate, energy consumption, and throughput. The developed BSWOA+UMT method obtained a minimum delay of 0.0030sec, maximum detection rate of 0.9095, minimum energy consumption of 8.7840J, and maximum throughput of 0.9005, respectively. This research can be further enhanced by implementing a more advanced optimization algorithm for multipath routing.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Kasthuribai, P. T., & Sundararajan, M., "Secured and QoS Based Energy-Aware Multipath Routing in MANET," Wireless Personal Communications, vol.101, no.4, pp.2349–2364, 2018.

[2] Reddy, A. P., & Satyanarayana, N., "Energy-efficient stable multipath routing in MANET. Wireless Networks, vol.23, no.7, pp.2083–2091, 2016.

[3] Sajal Sarkar and Raja Datta, " A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", Ad Hoc Networks, vol.37, Part 2, pp. 209-227, February 2016.

[4] Ansuman Bhattacharya and KoushikSinha, "An efficient protocol for load-balanced multipath routing in mobile ad hoc networks", Ad Hoc Networks, vol.63, pp.104-114, August 2017.

[5] Jabbar, W. A., Ismail, M., & Nordin, R., "Energy and mobility conscious multipath routing scheme for route stability and load balancing in MANETs.," Simulation Modelling Practice and Theory, vol.77, pp.245–271, 2017.

[6] Chen, Z., Zhou, W., Wu, S., & Cheng, L., "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET," IEEE Access, pp.1–1, 2020.

[7] P. Francis Antony Selvi; M.S.K.Manikandan, "Ant-based multipath backbone routing for load balancing in MANET", IET Communications, vol.11, no.1, pp.136 - 141, 2017.

[8] Aqeel Taha; Raed Alsaqour; Mueen Uddin; Maha Abdelhaq; Tanzila Saba, " Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function", IEEE Access, vol.5, pp.10369 - 10381, 24 May 2017.

[9] Perkins, C. E., "Ad hoc networking: an introduction, Ad hoc networking., May 2011.

[10] S. Hamrioui and P. Lorenz, ``EQ-AODV: Energy and QoS supported AODV for better performance in WMSNs," in Proc. IEEE Int. Conf.Commun. (ICC), pp. 435-440, May 2016.

[11] M. Aguilar Igartua andV. Carrascal Frías, "Self-configured multipath routing using path lifetime for video-streaming services over ad hoc networks," Comput. Commun., vol. 33, no. 15, pp. 1879-1891, Sep. 2010.

[12] J. Chen, Z. Li, J. Liu, and Y. Kuo, ``QoS multipath routing protocol based on cross-layer design for ad hoc networks," in Proc. Int. Conf. Internet Comput. Inf. Services, vol. 4, pp. 162-165, Sep. 2011.

[13] Mukund B. Wagh and Dr. Gomathi N, "Improved GWO-CS Algorithm-Based Optimal Routing Strategy in VANET", Journal of Networking and Communication Systems, Vol.2, no.1, pp.34-42, 2019.

[14] Moresh Madhukar Mukhedkar,Uttam Kolekar, "Hybrid PSGWO Algorithm for Trust-Based Secure Routing in MANET", Journal of Networking and Communication Systems, vol.2, no.3, pp.1-10, 2019.

[15] Deepak Rewadkar and Dharmpal Doye, "Traffic-Aware Routing in Urban VANET using PSO Model", Journal of Networking and Communication Systems, Vol.2,No.2, pp.29-36, 2019.

[16] Xian-Bing Meng, X.Z. Gao, Lihua Lu, Yu Liu, Hengzhen Zhang, "A new bio-inspired optimization algorithm: Bird Swarm Algorithm", Journal of Experimental & Theoretical Artificial Intelligence, pp. 673-687, Jun 2015.

[17] Seyedali Mirjalili and Andrew Lewis, "The Whale Optimization Algorithm," Advances in Engineering Software, vol. 95, pp. 51-67, May 2016

[18] Opinder Singh, Jatinder Singh, and Ravinder Singh, "Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET," Cluster Computing, pp. 1-13, 2017.

[19] Basant Subba, Santosh Biswas, and Sushanta Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," Engineering Science and Technology, an International Journal, vol. 19, no.2, pp. 782-799, 2016.

[20] Marchang, Ningrinla, Raja Datta, and Sajal K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1684-1695, 2017.

[21] Li, P., "CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding", In INFOCOM, pp. 100–108, 2012.

[22] Li, P., "Reliable multicast with pipelined network coding using opportunistic feeding and routing", IEEE Transactions on Parallel and Distributed Systems, vol.25, no.12, pp.3264–3273, 2014.

[23] Ajay Kumar Yadav and Sachin Tripathi, "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs", Peer-to-Peer Networking and Applications, vol.10, no.4, pp.897–909, July 2017.

[24] Youssef, M., "Routing metrics of cognitive radio networks: A survey", IEEE Communications Surveys and Tutorials, vol.16, no.1, pp.92–109, 2014.

[25] Attar, A., "A survey of security challenges in cognitive radio networks: Solutions and future research directions", Proceedings of the IEEE, vol.100, no.12, pp.3172–3186, 2012.

[26] Mamatha, C.R. and Ramakrishna, M., "An Energy Efficient Model for Node Ranking and Routing path Computation using Optimal Type-2 Fuzzy Logic Controller", 2023.

[27] Shafi, S. and Ratnam, D.V., "Ant-colony Optimization Based Energy Aware Cross Layer Routing Protocol to Improve Route Reliability in MANETs", Wireless Personal Communications, Vol. 129(3), pp.1865-1879, 2023.

[28] Khudair Madhloom, J., Abd Ali, H.N., Hasan, H.A., Hassen, O.A. and Darwish, S.M., "A Quantum-Inspired Ant Colony Optimization Approach for Exploring Routing Gateways in Mobile Ad Hoc Networks. Electronics", Vol. 12(5), pp.1171, 2023.

[29] Shareef, S.M. and Ghafoor, K.Z., "Optimized Routing algorithm for Vehicular Ad hoc networks based on NS3 Simulator".

[30] Yamini, K.A.P., Stephy, J., Suthendran, K. and Ravi, V., "Improving routing disruption attack detection in MANETs using efficient trust establishment", Transactions on Emerging Telecommunications Technologies, Vol. 33(5), pp. e4446, 2022.

[31] Sundarraj, P.D. and Arulanandam, K., "SECURE AND ENERGY-AWARE ROUTING FOR RELIABLE DATA TRANSMISSION IN MOBILE AD HOC NETWORKS".

[32] Bharti, R.K., Sumant, S.V., Durai, C., Kumar, R.A., Singh, K., Palivela, H., Kumar, B.R. and Debtera, B., "Enhanced Path Routing with Buffer Allocation Method Using Coupling Node Selection Algorithm in MANET", Wireless Communications and Mobile Computing, 2022.

[33] Abdulrab, H., Hussin, F.A., Abd Aziz, A., Awang, A., Ismail, I. and Devan, P.A.M., "Reliable fault tolerant-based multipath routing model for industrial wireless control systems", Applied Sciences, Vol. 12(2), pp.544, 2022.