IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 4, 2022, accepted January 16, 2022, date of publication January 19, 2022, date of current version February 8, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3144679

A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks

UPPALAPATI SRILAKSHMI[1], (Member, IEEE), SALEH AHMED ALGHAMDI[2], VEERA ANKALU VUYYURU[3], NEENAVATH VEERAIAH[4], AND YOUSEEF ALOTAIBI[5]

[1]Department of Computer Science and Engineering, VFSTR Deemed to be University, Vadlamudi, Guntur, Andhra Pradesh 522213, India
[2]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[3]Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Secunderabad, Telangana 500100, India
[4]Department of Electronics and Communications, DVR and DHS MIC Engineering College, Kanchikacharla, Vijayawada, Andhra Pradesh 521180, India
[5]Department of Computer Science, College of Computers and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia

Corresponding author: Neenavath Veeraiah (neenavathveeru@gmail.com)

This work was supported by the Taif University Researchers Supporting Project, Taif University, Taif, Saudi Arabia, under Grant TURSP-2020/313.

ABSTRACT Mobile ad hoc networks (MANET) are self-organizing, rapidly deployable wireless networks excellent for outdoor events, communications in places lacking radio infrastructure, disasters, and military activities. Because network topologies are flexible and dynamic, security may be the most vulnerable point in the network, open to attacks including eavesdropping, routing, and application changes. MANET has more security flaws than quality of service (QoS). It is thus recommended to use intrusion detection, which regulates system to detect further security problems. Monitoring for intrusions is crucial for prevention and additional security against unwanted access. The loss of a mobile node's power source may affect the node's ability to forward packets, which is reliant on the system's overall life. In this paper, the Bacteria for Aging Optimization Algorithm (BFOA), which finds the ideal hops in advancing the routing, is utilized to offer a trust-based protected and energy-efficient navigation in MANETs using a trust-based protected and energy-efficient navigation algorithm. The fuzzy clustering algorithm is activated first, and the Cluster Heads (CHs) are selected depending on the value of indirect, direct, and recent trust that each CH has. In addition, value nodes were discovered based on trust levels. Moreover, the CHs are engaged in multi hop routing, and the selection of the ideal route is based on the projected protocol, which selects the best routes based on latency, throughput, and connection within the course's boundaries. Even without an attack, compared to the exiting methods EA-DRP & EE-OHRA the proposed secure optimization routing (BFOA) algorithm produced a minimum energy of 0.10 m joules, a minimal latency of 0.0035 m sec, a maximum throughput of 0.70 bps, and an 83 percent detection rate, with enhanced results obtained by using a selective packet dropping attack

INDEX TERMS MANETs, energy efficiency, cluster head, trust values, bacteria for aging optimization algorithm, selective packet dropping attack.

I. INTRODUCTION

In a Mobile Ad-hoc Network (MANET) [1], each node is outfitted with a radio transmitter and a receiver, which allows them to connect with the system through wireless bidirectional communication. The most important reasons why MANETs allow data transmission with comparable characteristics while maintaining their active approach [2], [3] are as follows: It is surprising to find out that the transmission scope of this transmission is more confined than the previous transmission scope, making data swapping throughout the system impossible for any number of nodes [4]. A major difficulty with wi-fi Ad-Hoc networks is the fact that portable nodes rely on batteries, which tend to be underpowered in most locations, and it takes a considerable amount of time to recharge or replace them.

A significant hurdle to the widespread use of battery-powered devices has persisted, despite advancements in battery life technology. More study on effective protocol, platform, and technology design is required to overcome this obstacle. Power for nodes in an ad hoc system is often supplied by batteries or large electrical power sources, depending

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Elhoseny.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

on the situation. The ad hoc system's performance is severely hampered by its inability to obtain power supplies given their short lifespans. One of the most prevalent ways in which power is abused is via conversation [5].

More research is needed to attain the objective of extracting much more efficiency from their already enormous battery life resources, which has slowed to a crawl in recent years and there have been no notable achievements in this sector. When a cell node's wireless port is turned off, which occurs when the device is inactive or sleeping, energy consumption has been shown to be reliant on packet delivery. This has led to concerns about how much energy is wasted. Devices used in cellular ad hoc systems need mobility since they are portable. However, they have weight and size restrictions, as well as resource constraints in terms of capacity and bandwidth. In order to enhance the battery capacity, the nodes must become more bulky and less mobile. As a consequence, the vitality efficacy of MANETs continues to be a crucial design characteristic [6].

MANETs, like other radio-based communication systems, are vulnerable to a variety of threats. Outside attackers, as well as misbehaving objects on the inside, are among the hazards. Because of this, a variety of information assurance solutions, including data protection, access control and identity management will need to be implemented to defend these systems against cyberattacks [7], [8]. The use of wireless connections and the flexibility of different devices in such networks has a number of significant implications, and many well-known intrusion-detection processes and implementations do not instantaneously become invisible from infrastructure-based internet protocol (IP) address networks. Man-in-the-Middle attacks are becoming more common as the demand for smart and internet gadgets develops [9]. The potential of misleading warnings and incorrect allegations of nodes from networks is relatively high as a consequence of the possibility of inefficient protocol pack transfer. These potential increases when the user moves about in the system, which disrupts broadcasts and creates a multitude of pathways. There are no crucial sections of the system, such as switches, routers, and firewalls in wired IP networks, where all appropriate visitors may be detected and analyzed in order to identify criminal behavior [10].

The primary purpose of this research is to develop a secure optimization routing algorithm for MANET. It is based on a Bacteria for Aging Optimization Algorithm (BFOA). The secure iterative routing technique depends on CH selection and intrude node detection. The CH selection depends on the maximum trust of indirect, direct, and recent trust values. The threshold value concept is used to detect the intruded node for efficient and detectable routing. It is necessary to begin by selecting the CHs from the MANETS natural environment that have the greatest value of indirect, direct, and recent hope in order to proceed. This is closely followed by an intrusion detection procedure for detecting intruded nodes and ensuring that their packets are reliably transmitted from origin to destination, as well as all productive routing, which is accessed by the BFOA. It is given the capabilities, capacity, and connectivity of the trail, the defined purpose function is reliant on those attributes. A positive balance may be made between mining and manipulation phases of the algorithm, despite the fact that the proposed technique takes use of the advantages of the BFOA. Following the discovery of a packet dropping attack, the simulated results will be compared to the actual results.

The remainder of this work is arranged as follows: The related works are shown in Section II. The suggested BFOA is explained in Section III. The outputs of the suggested technique, as well as an explanation, are presented in Section IV. Section V provides a conclusion.

II. RELATED WORKS

Because of its benefit in swiftly building networks, MANET is used in a variety of areas. If mobile nodes trust one other and cooperate together, the network will function well. However, because of the dynamic topology and frequent connection failures caused by node mobility, routing is challenging, and vulnerabilities are frequently revealed. As a result, the MANET's routing should include security elements that may mitigate the effects of different assaults.

Veeraiah *et al.* [11] offer a hybrid algorithm termed the cat slap single-player algorithm (C-SSA) in MANETs for safe, energy-efficient navigation based on trust relationships between players while yet maintaining high levels of performance. Initial cluster heads (CHs) are picked using a fuzzy approach that takes into account indirect, direct, and recent trust levels for each CH. Trust levels were used to identify value nodes. According to a suggested hybrid protocol, the CHs are involved in multi-hop routing, whereby the optimal route is selected by evaluating the latency, throughput, and connectivity within this course as well as other factors. The focus of this technique should be on throughput rather than on efficiency.

To strengthen security against selfish nodes in the Adhoc On Demand Vector protocol, Anantapur and Patil [12] proposes a hash function with a location update technique that may be used in conjunction with a location update method. For the purpose of transferring data packets from one location to another, the Ad-hoc On-demand Distance Vector (AODV) routing protocol is used. As a result, to minimize packet loss throughout the whole network, the Prevention of Selfish Node Using Hash Function with location update strategy is highly recommended.

For effective data transfer, a novel Protected multipath routing based on Quality-of-Service method is provided, combined with an encryption approach Rajashanthi and Valarmathi [13]. In addition, there is the AODV-BR protocol, which uses optimal fuzzy logic for multipath routing. Optimizing Adaptive Formation is done with Grey Wolf Optimization Adaptive Formation. Homomorphic Encryption is used to choose an ideal path from the known pathways for securing data key management methods. End-to-end latency, packet distribution ratio, and other metrics are used to evaluate the efficiency of the intended strategy. By implementing the trust-aware routing protocol, which is proposed by Suresh *et al.*, [14], they are able to provide a trust-based safe routing system based on atom whale optimization algorithm. The atom whale optimization algorithm that was developed is used to choose the optimum route based on trust characteristics such as the average encounter rate, successful cooperation frequency (SCF), integrity factor, and forwarding rate, among others.

Moreover, the proposed atom whale optimization algorithm utilized to enable safe routing between the nodes, as previously stated. This method is a mixture of the atom search optimization and the whale optimization algorithm, and it benefits from the faster global convergence that the ASO and WOA provide. The fitness feature has been redesigned to take into consideration mobility and trust in the user.

In MANETs, Nithya *et al.* [15] offer a technique for ant colony routing optimization that takes security into account but is still hazy. The goal of a MANET routing protocol is to provide a constant packet transfer ratio, decreased connection overhead, and low end-to-end latency in typical standard scenarios and attack states. With its routing organization built utilizing the Optimized Fuzzy based Ant colony optimization (ACO) Algorithm for 5G, MANET surpasses other current state-of-the-the-art MANET routing protocols, such as AODV. In order to play a substantial role in 5G, millimeter-wavelengths are necessary. The goal of this study was to see how efficient a MANET with just mmWave User Equipment might be. With mmWave, MANET decreased Use equipment packet transmission loss, implying that a higher Signal to Noise Ratio leads to a higher packet delivery ratio.

A trust-based, energy-efficient Multipath Routing approach is proposed by Alappatt and Prathap [16] for use in MANET. This research investigates the direct and indirect trust of nodes and routes, and then selects the secure multipath. The vulnerable nodes are also identified and isolated using the trust values. The data packets are subsequently encrypted against data transmission assaults using SH2E, which stands for Secret key-centered Hybrid Honey Encryption. The Levy Flight Centered Shuffled Shepherd Optimization (LF-SSO) Algorithm must be used to find the best route from the multipath chosen. This technique helps extend the network's lifespan by using a route chosen by path trust, residual node energy, and path distance. Decrypted data packets must be sent from the source node to the destination node using the best path selected before transmitting to the base station (BS).

As a point of attention, Panda and Pattanayak [17] addressed security challenges. Again, numerous algorithms may be used to solve security vulnerabilities, and evolutionary technique-based algorithms tend to be the most successful. One of the most often used evolutionary techniques for optimization is ant colony optimization (ACO). We conducted a comprehensive study of ant colony optimization (ACO)-based safe MANET routing protocols, and the contents of this work may assist MANET researchers in developing secure routing protocols, particularly when employing the ACO technique to solve security challenges in a MANET.

Abdali *et al.* [18] Location-Aided Routing (LAR) approach uses an upgraded conventional PSO to reduce the needed energy usage. The simulation results show that the proposed Optimized Particle Swarm Optimization (OPSO-LAR) can achieve good performance in a comparable network environment to the state of the art. The PSO technique was used to optimize the parameter in the computing function. It was also used to pick between two or more network flooding and node coverage variables.

Energy and Congestion Aware Simple Ant Routing Algorithm (ECSARA) is a suggested method by Dsouza and Manjaiah [19], the transfer of data is accompanied by leftover energy and congestion. It picks nodes with low congestion and high residual energy. According to simulations, Energy and Congestion Aware Simple Ant Routing Algorithm (ECSARA) improves throughput and reduces latency in congested networks. It also cuts down on power use and improves packet delivery ratios. As a result, in a denser environment, ECSARA may be efficiently employed to maintain a channel for longer periods of time and deliver improved throughput.

A complex multipath routing protocol based on an optimization approach is proposed by Veeraiah and Krishna [20]. In order to handle the MANET energy and protection problem, technologies such as fuzzy clustering and fuzzy Naive Bayes, as well as the cluster head's (CH) data collecting and intrusion mitigation techniques, are successful (fuzzy NB). The Bird swarm-whale optimization algorithm (BSWOA) method is then utilized to improve multipath routing. Based on the routing protocol, this solution incorporates BSA into the whale optimization algorithm (WOA), which subsequently advances multipath routing. Table 1 compares all existing approached.

III. THE PROPOSED SECURE OPTIMIZATION ROUTING ALGORITHM

Efficient routing in MANETs ensures that data is efficiently transported from source to destination and reduces the amount of information lost during the transmission process. Furthermore, the BFOA is developed, which reduces energy loss during transmission while concurrently enhancing the system's lifetime [21], [22]. In the first stage, fuzzy clustering and CH selection are performed using the maximum direct, indirect, and recent confidence values; in the second step, intruded node identification is performed using a specified threshold value of 0.5J. Nodes with trust values more than a preset threshold are deemed normal; those with trust values lower than that are considered intruded. The goal of this strategy is to safeguard the intruded node while also ensuring secure data transmission from source to destination. The optimum pathways are then chosen using the BFOA, which is based on the intended goal feature

TABLE 1. Comparing the existing approaches.

Reference no	Published year	Approach name	Advantages	Disadvantages
[11]	2021	A hybrid algorithm termed the cat slap single-player algorithm (C-SSA)	Provides secure energy-efficient routing for source to destination.	Delay will occur in cluster head selection process and needs to focus on energy issues.
[12]	2021	The Prevention of Selfish Node using Hash Function (PSNHF) with position update algorithm	Provides reliable and secure data transmission under selfish nodes	This method needs to focus on energy issues.
[13]	2020	The AODV-BR (Adhoc on-Demand Distance Vector-Backward Routing) protocol with Optimal Fuzzy Logic is designed for multipath routing. Grey Wolf Optimization's adaptive formation technique anticipates the best path.	A key benefit of using secure routing is that it ensures data integrity, confidentiality, and non-denial of service.	This method needs to focus delay and energy issues.
[14]	2021	The atom whale optimization (AWOA)method is used to create a trust-based safe routing system. The created atom whale optimization is used to choose the best route based on trust variables such as average encounter rate, successful cooperation frequency (SCF), integrity factor, and forwarding rate.	Provides reliable and secure routing	This method needs to focus on energy issues.
[15]	2022	A enhanced fuzzy ant colony routing optimization technique used to provide security for the MANET.	Establish low end-to-end latency in conventional assault situations while maintaining a high packet transfer ratio.	Need to focus on accurate intruded node detection and energy issues.
[16]	2021	A trust-centered energy-efficient Multi path Routing scheme for MANET. Levy Flight centered Shuffled Shepherd Optimization Algorithm is applied to discover an optimal path as of the multipath selected	Provide an extremely effective and secured routing.	This method needs to focus on energy issues.
[17]	2020	Ant colony optimization (ACO)-based secure MANET routing protocol	Addressing the security issues	This method needs to focus on energy issues.
[18]	2020	The optimized conventional PSO was applied and integrated into the LAR protocol to minimize the required energy consumption	Provide better packet delivery ratio, energy consumption, overhead, and end-to-end delay.	More delay and energy consumption
[19]	2020	The Simple Ant Routing Protocol (SARA) is an ant colony routing (ACR) protocol that finds the best route between communication nodes.	Improve the network's throughput and packet delivery performance.	This method needs to focus on energy and security issues.
[20]	2020	The MANET's energy and security crises are efficiently solved utilizing fuzzy clustering and fuzzy Naive Bayes (fuzzy NB). Bird swarm-whale optimization algorithm (BSWOA) is a multipath routing system that combines bird swarm optimization (BSA) with whale optimization algorithm (WOA)	Provides secure t routing for source to destination.	Delay will occur in cluster head selection process and needs to focus on energy issues.

and considers the path's capacity, throughput, and communication. Figure 1 shows the secure optimization routing algorithm for MANETs. For adjusting the ideal hops, the BFOA is used, which leads in a global optimal solution with quicker convergence times [23], [24].

A. TRUST MANAGEMENT SYSTEM

1) DIRECT TRUST (DT)

The duration of time is based on the estimated time it takes to communicate between i^{th} node and d^{th} destination. DT is measured as the difference between the list of actual and predicted periods of time for the i^{th} node to authenticate the public key that was generated by the d^{th} destination. In this case, the data transfer between i^{th} node and d^{th} destination has been represented as,

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

where, τ_{appx} describes the estimated time and τ_{est} determines how long it will take for the public key to be authenticated. To put it differently, τ_{appx} and τ_{est} are the estimated period for receiving and sending the public key by the destination and the node. ω Signifies the opinion variable of these nodes.

2) INDIRECT DIRECT TRUST (IDT)

The node containing the opinion variable is shown in accordance with DT. However, the IDT provided by is used to authenticate the node that does not have a witness variable

$$IDT_i^d(\tau) = \frac{1}{r}\sum_{i=1}^{r} DT_i^d(d) \quad (2)$$

where, r specifies the node's overall neighbours. i.

3) RECENT TRUST (RT)

When the DT and IDT are taken into consideration, together with the important validity and accepting the destination or sink, which will be offered in part of their moment, the RT is determined. The RT is designed in the following way:

$$RT_i^d(\tau) = \alpha * DT_i^d(\tau) + (1-\alpha) * IDT_i^d(\tau) \quad (3)$$

where, $\alpha = 0.3$.

RT^d indicates the recent trust, DT^d and IDT^d represents the direct and indirect trust values.

B. CH CHOICE USING A FUZZY CLUSTERING METHOD

Associating with It is possible to assign each member of a cluster to one of many different degrees of "fuzziness" when using the fuzzy clustering approach. Cluster heads are chosen based on the greatest degree of node trust among the nodes in a fuzzy clustering algorithm. To reward this mutual trust, the node receiving the best cluster head returns it to the other node. Due to its reliance on overlapping numbers, Fuzzy Clustering Theory can only be applied to a limited number of patients' records, resulting in the patient data point being assigned to a single of many cluster centers. Fuzzy clustering is a data reduction technique. This is expressed as,

$$\mathrm{J_f} = \sum_{\mathrm{i=1}}^{\mathrm{r}}\sum_{\mathrm{j=1}}^{\mathrm{p}} \mathrm{u_{ij}^f} \times \|\mathrm{n_i} - \mathrm{H_j}\|^2 \quad 1 \le f \le \infty \quad (4)$$

where, $\mathrm{n_i}$ proposes $\mathrm{i^{th}}$ node from the MANET, $\mathrm{H_j}$ denotes that the $\mathrm{j^{th}}$ cluster head, p indicates the total no of CHs and denotes the Euclidean distance between $\mathrm{i^{th}}$ node and the $\mathrm{j^{th}}$ cluster head, respectively. The fuzziness indication is denoted by the $\{\mathrm{f} | \mathrm{f} \in \mathrm{Q} > 1\}$. The f fuzzifier is defined by the purpose function, which is denoted by the symbol $\mathrm{J_f}$. Cluster heads are delegated under the nodes in the cluster that have the shortest Euclidean distance to the cluster head in relation to the cluster head.

In order for a node to become a CH, the maximizing function(M), which is stated as follows, must be met:

$$\mathrm{M} = \frac{1}{3}\{D + I + R\} \quad (5)$$

The values of D, I, and R are the levels of direct, indirect, and recent trust, respectively. These three equations (1),(2) and (3) are used to calculate the D, I, and R values.

C. COMPARISON OF THRESHOLD VALUES FOR IDENTIFYING INTRUDED NODES

To put it another way, intruders are identified by a sink node based on information sent to it by other nodes through the CHs, and this information is based on network trust factors. Once the intruder node has been identified, it is blocked from attempting to communicate with the rest of the network by the network [25], [26]. Intruders in the sink node are anticipated by employing a specified threshold value in the sink node (0.5J). Intrusion detection's main purpose is to provide safe network connection with the least amount of energy consumption and transmission delay possible [27].

D. PROPOSED SECURE OPTIMIZATION ROUTING (BFOA) ALGORITHM

The optimal hops for MANET routing advancement are determined using the proposed BFOA method. The goal function is used to identify the ideal hops for efficient routing, and the secure optimization is described in this section.

1) RESOLUTION ENCODING

The demand for direct response encoding will serve as the answer to this optimization algorithm, and the solution is nothing more than the pathways selected for its routing in MANETs as a result of this optimization method. To ensure minimal data loss during transmission, the CHs in equation (5) have been selected to make routing from the device as efficient as possible. Using the least amount of energy loss reduces the routing latency.

2) THE REMAINING ENERGY FORMULATION

Energy remaining in the nodes, the path's throughput, and its accessibility are all factors in determining a route's fitness. Performance is maximised since the fitness function is a maximisation function.

$$F = \frac{1}{3}\{e + t + c\} \quad (6)$$

Nodes along the route are used to calculate e (energy), t (throughput), and c (route connection). To determine how much energy is remaining in the node, the following equations is used.

$$\mathrm{E^{remain}}(\tau) = \mathrm{E^{remain}}(\tau) - \mathrm{E^{transmit}}(\tau-1,\tau) - \mathrm{E^{recieve}}(\tau-1,\tau) \quad (7)$$

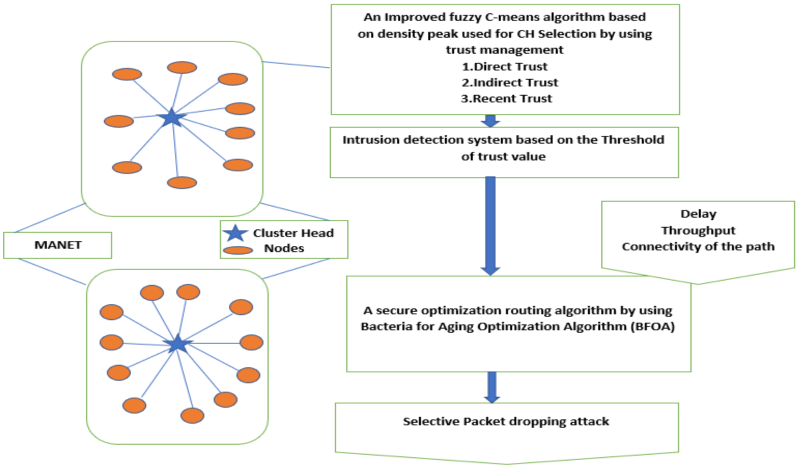

An Improved fuzzy C-means algorithm based on density peak used for CH Selection by using trust management
1.Direct Trust
2.Indirect Trust
3.Recent Trust
Intrusion detection system based on the Threshold of trust value
Delay
Throughput
Connectivity of the path
MANET
Cluster Head
Nodes
A secure optimization routing algorithm by using Bacteria for Aging Optimization Algorithm (BFOA)
Selective Packet dropping attack

FIGURE 1. **Proposed secure optimized routing.**

where, E^{remain}, $E^{transmit}$ and $E^{recieve}$ are the leftover and necessary energy for the transmission and receiving of a single bit of data. The ratio of total bits carried over a network per second through a particular route is known as the throughput, and it is expressed as

$$u = \frac{\upsilon}{\tau}\text{bps} \tag{8}$$

υ defines how many bits have been sent from source to destination, and τ defines how long has it taken Two nodes are connected by a bi-directional link, which is expressed as

$$y = \frac{1}{g}\left[\sum_{i=1}^{g}\frac{y_i}{cc}\cdot\right] \tag{9}$$

where cc the total number of connections, y_i indicates the degree of a node's connectedness, g indicates the no of nodes.

E. BACTERIA FOR AGING OPTIMIZATION ALGORITHM (BFOA)

The Bacterial Foraging Optimization Algorithm is a recent addition to the area of bio-inspired algorithms, and it pertains to the disciplines of Bacterial Optimization Algorithms and Swarm Optimization, as well as Computational Intelligence and Metaheuristics more broadly. Other swarm intelligence methods, such as Ant Colony Optimization and Particle Swarm Optimization, are connected to it. It's been employed in a variety of studies, including color picture quantization, face recognition, and engineering design issues. When BFOA is used to solve these difficulties, the outcomes are superior to those of alternative bioinspired and conventional techniques. It handles difficult numerical problems and is both computationally effective and quicker.

BFOA (bacterial foraging optimization algorithm) is a relatively recent approach in the field of biological techniques. Chemo taxis is a process in which a bacterium travels by taking little steps while hunting for nutrients. The basic notion of BFOA is to simulate the chemo-tactic movement of virtual bacteria in the issue search space, with individual bacteria communicating with one another through signals. It is global optimization method that may be used to solve a variety of optimization issues. Another source of inspiration for this method is social foraging behavior, such as ant colony and particle swarm optimization.

Phase of routing

The BFOA's major goal is sparking virtual germs chemotactic move at the hunt distance. After would be the steps from the Bacteria for Aging Optimization Algorithm:

a) Chemotaxis: Chemotaxis is the mechanism through which

bacteria migrate through tiny steps in their quest for nutrients. Flagella are used to propel the animal along. It can travel in two ways: it can tumble or swim in a certain direction for a period. It continues to do so throughout one's lifespan.

b) Swarming: This is created in E. coli cells as they traverse through the nutritional supplement gradient with one nutrient chemo-effector per matrix. With the aid of high-level succinate, the cells within formed an attractant.

c) Reproduction: Bacteria that performed well during their lifetime may lead to the next generation, but bacteria that performed poorly during their lifetime may die. To hold the swarm size stable, the good bacteria can break into two.

d) Elimination-Dispersal: adjustments in the air because bacteria being murdered or spread to some different website. To mimic this happening in BFOA couple germs are lost in addition to fresh arbitrary. Table 2 shows the symbols and definitions.

Step 1: All variables are initialized, and counters are set for the elimination-dispersal loop(l), reproduction loop(k), chemotactic loop(j) and swim counter(w) is set to zero

Step 2: Bacterium index (i) is set to zero

Step 3: Elimination-dispersal loop is started by setting $l = l + 1$

Step 4: Start the reproduction loop by setting $k = k + l$

Step 5: Start the chemotaxis loop by setting $j = j + 1$

TABLE 2. Symbols and definitions.

j	Chemotactic stage Indicator
k	Chemotactic measure indicator
i	Bacterium index
l	Elimination-dispersal Stage indicator
m	swim counter
Problem_ size	Search space's dimensions
Cells_num	Number Of germs from the populace as an entire
N_c	Quantity of chemotactic Steps
N_s	Length of swim
N_{re}	Quantity of all reproduction occasions
N_{ed}	Quantity of all Elimination-dispersal occasions
P_{ed}	Possibility of all elimination-dispersal
Step_size	In a tumble determined random path the step size is taken
d_{att}, w_{att}, h_{rep}, and w_{rep}.	The attractant-repellent coefficients are

Step 6: Start the bacterium index i = 1, *2....Cells_num*

a. Compute the fitness function using the cell-to-cell interaction from the attractant-repellent coefficient's

b. Set $J_{last} = J(i, j, k, l)$

c. Set counter $m = 0$ for swim length

d. Check m < N_s: If m < N_s is true, calculate the new fitness function and swim until fitness function is less than J_{last}. If fitness function is greater than or equal to J_{last} then tumble. If m < N_s false, go to the next bacterium index i and continue until i equals *Cells_num*

Step 7: Check $j < N_c$. If true, go to step 5

Step 8: For given *k, l* and index i = 1, 2....*Cells_num*, calculate the health of the bacterium. If any bacterium is of least health, then discard the bacterium. Rest of the bacterium will be doubled by reproduction.

Step 9: Check $k < N_{re}$. If true, go to step 4

Step 10: Eliminate and disperse for each i = 1, 2....*Cells_num* with probability P_{ed}

Step 11: Check $l < N_{ed}$. If true, go to step 3. If false, end program

IV. RESULTS

The section looks at the link between effective routing and the proposed secure optimization routing (BFOA) algorithm analysis, which is based on functionality measurements, to show how beneficial the suggested technique is

A. PERFORMANCE METRICS

All present techniques of inquiry, both with and without violence, are compared to the proposed procedure based on the following metrics: latency, energy, throughput, and detection rate. It's important to know how much energy is left in the nodes once a transmission is complete in order to determine how long a system is. The length of this device refers to the time it takes for this information to be transferred, while the output refers to the total amount of data delivered via the machine in a certain time period.

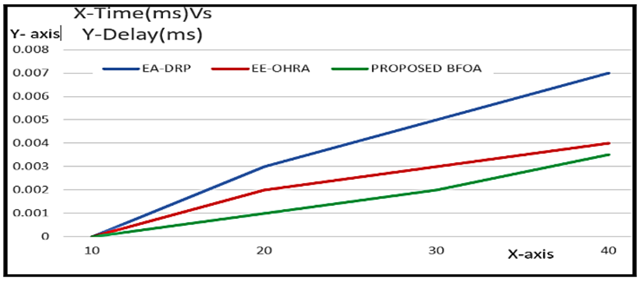


FIGURE 2. Delay in using the proposed approach.

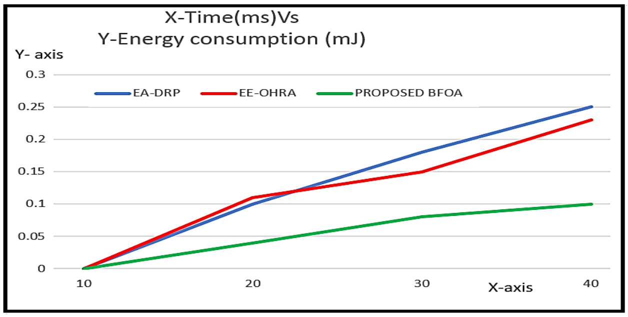


FIGURE 3. The proposed (BFOA) method's energy usage.

B. RELATIVE METHODS

EA-DRP [6] and the Energy Efficient EE-OHRA route [7] were utilized to compare the suggested secure optimization routing (BFOA) algorithm with the methodologies employed for the comparison.

1) RELATIVE EVALUATION OF THE PROPOSED SECURE OPTIMIZATION ROUTING (BFOA) ALGORITHM

a: DELAY

Comparison research on various methods led to these conclusions: Figure 2 displays the relative assessment based on the delay. The techniques EA-DRP, EE-OHRA, and the BFOA algorithm all have delays of 0.007, 0.004, and 0.0035 milliseconds for the time of 40 seconds. When compared to the current two approaches of EA-DRP and EE-OHRA methods, simulation results demonstrate that the proposed BFOA algorithm gained a minimal latency of 0.005 msec.

b: ENERGY CONSUMPTION

Figure 3 shows a comparative examination of energy expenditure. For a length of 40 seconds, the EA-DRP, the EE-OHRA and the BFOA algorithm use 0.24, 0.22 and 0.12 m Joules, respectively, of energy. In the simulations, it was discovered that the suggested secure optimization routing (BFOA) algorithm had the lowest energy usage of 0.12 milli joules when compared to the two current approaches of EA-DRP and EE-OHRA methods.

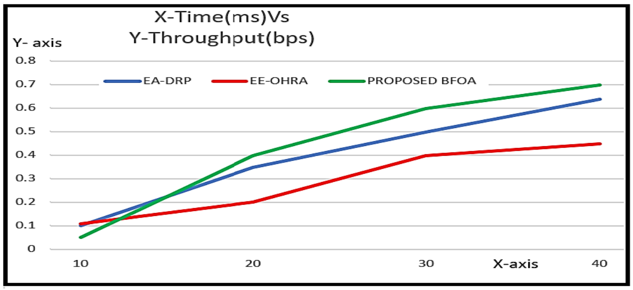


FIGURE 4. The proposed (BFOA) method's throughput.

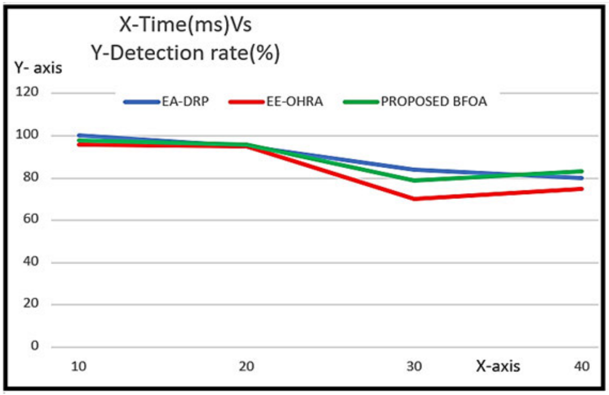


FIGURE 5. The proposed (BFOA) method's detection rate.

c: THROUGHPUT

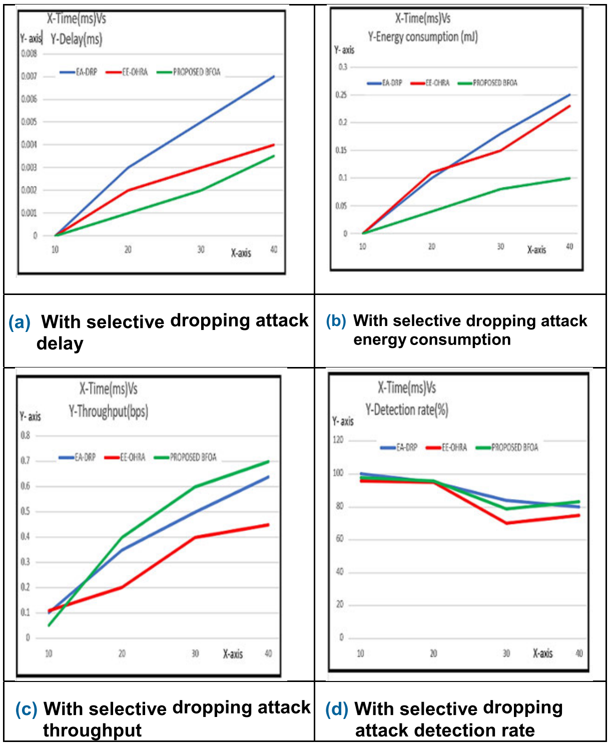
Figure 4 illustrates the development of a relative inquiry built on throughput. There were throughputs of 0.64, 0.45, and 0.70bps after a delay of 40 seconds for EA-DRP, E-OHRA, and the suggested secure optimization routing (BFOA) method.

In the simulations, the proposed recommended secure optimization routing (BFOA) algorithm achieved a maximum throughput of 0.70 bps when compared to two current methodologies, namely, the EE-OHRA method and the EA-DRP method.

d: DETECTION RATE

Figure 5 displays a comparative comparison of value based on detection rate. Delay detection rates for the techniques EA-DRP (80%), EE (75%) and suggested secure optimization routing (BFOA) algorithm is (83%), respectively, where the delay is 40 seconds.

When compared to the current two approaches of EA-DRP and EE-OHRA methodologies, simulation results demonstrate that the suggested secure optimization routing (BFOA) algorithm achieved a maximum detection rate of 83 percent. From the simulation results it shows that the proposed secure optimization routing (BFOA) method is shows better results in without attack in the performance parameters of minimum delay 0.005 m sec, minimum energy consumption 0.12 m Joules, maximum throughput of 0.70 bps and maximum detection rate of 83%.



(a) With selective dropping attack delay

(b) With selective dropping attack energy consumption

(c) With selective dropping attack throughput

(d) With selective dropping attack detection rate

FIGURE 6. With selective dropping attack delay (b) With selective dropping attack energy consumption (c) With selective dropping attack throughput (d) With selective dropping attack detection rate.

2) RELATIVE ASSESSMENT IN THE EXISTENCE OF THE SELECTIVE FORWARDING ATTACKS

The following information outlines the findings of the comparative analysis of the proposed approach. Figure 6 depicts the relative estimation depending on the delay (a). Despite the fact that the period is 40 seconds, the latency of the approaches EA-DRP, EE-OHRA, and proposed secure optimization routing (BFOA) algorithm is 0.008 0.007 and 0.0065 m sec, respectively. Figure 6 depicts the relative research based on energy expenditure (b). When the period is 40 seconds, the energy consumption of the EA-DRP, EE-OHRA, and the proposed secure optimization routing (BFOA) method are 0.25, 0.23, and 0.10 m Joules, respectively.

Figure 6 shows the relative investigation depending on throughput (c). After a 40-second delay, the throughput of the EA-DRP, EE-OHRA, and the proposed secure optimization routing (BFOA) technique are 0.65, 0.60, and 0.69 bps, respectively. Figure 6 depicts a comparison study concentrating on the detection rate (d). When the delay is 40 seconds, the methods EA-DRP, EE-OHRA, and proposed secure optimization routing (BFOA) algorithm have detection rates of 79, 74, and 80 percent, respectively.

From the simulation results it shows that the proposed secure optimization routing (BFOA) method is also shows better results with the selective packet dropping attack in the performance parameters of minimum delay 0.0065 m sec, minimum energy consumption 0.10 m Joules, maximum throughput of 0.69 bps and maximum detection rate of 80%.

V. CONCLUSION

The secure optimization routing algorithm solves both the energy issue and the communication latency between hops. Bacteria for Aging Optimization Algorithm has been used to produce an efficient routing approach (BFOA). The Fuzzy clustering approach is used in the first stage to calculate the CHs with the maximum trust values for direct, indirect, and recent trust. In the second stage, the CHs with the maximum trust values for direct, indirect, and recent trust are computed. The detection of intruded nodes is dependent on the threshold value that has been set. The CHs are in charge of routing data packets to the drain, which must go through a number of hops on their way there. In MANET, on the other hand, the most promising candidate for advanced routing is identified via the use of the Bacteria for Aging Optimization Algorithm optimization (BFOA). The suggested approach has a faster convergence rate, and it optimizes storage, throughput, and route connection limitations. The suggested technique achieved a minimum energy of 0.10 m joules, a negligible latency of 0.0035 m sec, a maximum throughput of 0.70 bps, and an 83 percent detection rate with 100 nodes. Similarly, the suggested technique showed satisfactory results for the selective packet dropping attack when compared to existing approaches.

REFERENCES

[1] S. Uppalapati, "Energy-efficient heterogeneous optimization routing protocol for wireless sensor network," *Instrum. Mesure Metrol.*, vol. 19, no. 5, pp. 391–397, Nov. 2020.

[2] S. Bharany, S. Sharma, S. Badotra, O. I. Khalaf, Y. Alotaibi, S. Alghamdi, and F. Alassery, "Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol," *Energies*, vol. 14, no. 19, p. 6016, Sep. 2021.

[3] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[4] B. Rajkumar and G. Narsimha, "Secure multipath routing and data transmission in MANET," *Int. J. Netw. Virtual Organisations*, vol. 16, no. 3, pp. 236–252, 2016.

[5] G. Anjaneyulu, V. M. Viswanatham, and B. Venkateswarlu, "Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks," *Adv. Appl. Sci. Res.*, vol. 2, no. 4, pp. 177–186, 2011.

[6] R. Prasad P and S. Shankar, "Efficient performance analysis of energy aware on demand routing protocol in mobile Ad-Hoc network," *Eng. Rep.*, vol. 2, no. 3, p. e12116, Mar. 2020.

[7] S. V. Kumar and V. AnurathaEnergy, "Efficient routing for MANET using optimized hierarchical routing algorithm (Ee-Ohra)," *Int. J. Sci. Technol. Res.*, vol. 9, no. 2, pp. 2157–2162, Feb. 2020.

[8] N.-C. Wang and Y.-L. Su, "A power-aware multicast routing protocol for mobile ad hoc networks with mobility prediction," presented at the IEEE Conf. Local Comput. Netw. 30th Anniversary (LCN)l, Sydney, NSW, Australia, Nov. 17, 2005, p. 8 and 417.

[9] R. Rout, P. Parida, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Skin lesion extraction using multiscale morphological local variance reconstruction based watershed transform and fast fuzzy C-Means clustering," *Symmetry*, vol. 13, no. 11, p. 2085, Nov. 2021.

[10] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, "A cooperative routing for MANET based on distributed trust and energy management," *Wireless Pers. Commun.*, vol. 81, no. 3, pp. 961–979, Apr. 2015.

[11] N. Veeraiah, O. I. Khalaf, C. V. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, "Trust aware secure energy efficient hybrid protocol for MANET," *IEEE Access*, vol. 9, pp. 120996–121005, 2021.

[12] A. Mallikarjuna and V. C. Patil, "PUSR: Position update secure routing protocol for MANET," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 1, pp. 93–102, Feb. 2021.

[13] M. Rajashanthi and K. Valarmathi, "A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs," *Wireless Pers. Commun.*, vol. 112, no. 1, pp. 75–90, May 2020.

[14] S. R. Halhalli, S. R. Sugave, and B. N. Jagdale, "Optimisation driven-based secure routing in MANET using atom whale optimisation algorithm," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 27, no. 1, p. 77, 2021.

[15] R. Nithya, K. Amudha, A. S. Musthafa, D. K. Sharma, E. H. Ramirez-Asis, P. Velayutham, V. Subramaniyaswamy, and S. Sengan, "An optimized fuzzy based ant colony algorithm for 5G-MANET," *CMC-Comput., Mater. Continua*, vol. 70, no. 1, pp. 1069–1087, 2022.

[16] V. Alappatt and J. P. P. M., "Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E," *Int. J. Comput. Netw. Appl.*, vol. 8, no. 4, p. 400, Aug. 2021.

[17] N. N. Panda and B. K. Pattanayak, "ACO-based secure routing protocols in MANETs," in *New Paradigm in Decision Science and Management* (Advances in Intelligent Systems and Computing), S. Patnaik, A. Ip, M. Tavana, and V. Jain, Eds. Singapore: Springer, 2019, pp. 195–206.

[18] T.-A.-N. Abdali, R. Hassan, R. C. Muniyandi, A. H. M. Aman, Q. N. Nguyen, and A. S. Al-Khaleefa, "Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in MANET," *Information*, vol. 11, no. 11, p. 529, Nov. 2020.

[19] M. B. Dsouza and D. H. Manjaiah, "Energy and congestion aware simple ant routing algorithm for MANET," in *Proc. 4th Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Coimbatore, India, Nov. 2020, pp. 744–748.

[20] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET," *Evol. Intell.*, vol. 5, pp. 1–15, Mar. 2020.

[21] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi, S. Alghamdi, and F. Alassery, "A novel approach of design and analysis of a hexagonal fractal antenna array (HFAA) for next-generation wireless communication," *Energies*, vol. 14, no. 19, p. 6204, Sep. 2021.

[22] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi, and S. Alghamdi, "Design and synthesis of multi-mode bandpass filter for wireless applications," *Electronics*, vol. 10, no. 22, p. 2853, Nov. 2021.

[23] A. F. Subahi, Y. Alotaibi, O. I. Khalaf, and F. Ajesh, "Packet drop battling mechanism for energy aware detection in wireless networks," *CMC-Comput., Mater. Continua*, vol. 66, no. 2, pp. 2077–2086, 2021.

[24] D. Chander and R. Kumar, "QoS enabled cross-layer multicast routing over mobile ad hoc networks," *Proc. Comput. Sci.*, vol. 125, pp. 215–227, Jan. 2018.

[25] P. Parthiban, G. Sundararaj, and P. Maniiarasan, "Maximizing the network life time based on energy efficient routing in ad hoc networks," *Wireless Pers. Commun.*, vol. 101, no. 2, pp. 1143–1155, Jul. 2018.

[26] V. Nithya, B. Ramachandran, and G. V. Devi, "Energy efficient tree routing protocol for topology controlled wireless sensor networks," *Int. J. Commun. Antenna Propag. (IRECAP)*, vol. 5, no. 1, pp. 1–6, 2015.

[27] P. Rajendra and P. Shankar, "Improvement of battery lifetime of mobility devices using efficient routing algorithm," *Asian J. Eng. Technol. Appl.*, vol. 1, pp. 13–20, Mar. 2017.

UPPALAPATI SRILAKSHMI (Member, IEEE) received the B.Tech. and M.Tech. degrees in computer science and engineering from JNTUH, the M.B.A. degree from SV University, and the Ph.D. degree in mobile *ad-hoc* networks from Acharya Nagarjuna University. She is currently working as an Assistant Professor at VFSTR Deemed to be University, Vadlamudi, Guntur. She is having more than 12 years of experience in academic, administration, research, and innovations. She has delivered a keynote speech in e-ICMSEM. She has published so many articles in reputed journals, like Springer, Scopus, and Web of Science. She has also participated in various international conferences organized by Springer, IEEE, and Scopus. Her research interests include mobile *ad-hoc* networks, wireless sensor networks, cloud security, information security, network security, software engineering, and software testing. She is a member of CSI and IAENG. She received the Dero Award as a Young Researcher and rewards for her accomplishments in administration, academic, and research from various professional bodies.

SALEH AHMED ALGHAMDI received the Bachelor of Education degree (Hons.) from the Department of Computer Science, Teachers College, Riyadh, Saudi Arabia, in 2004, the Master of Information Technology degree from La Trobe University, Melbourne, Australia, in 2010, and the Doctor of Philosophy degree in computer science from the Royal Melbourne Institute of Technology (RMIT) University, Melbourne, in 2014, thesis title "A Context-Aware Navigational Autonomy Aid for the Blind." He is currently an Associate Professor with the Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. His research interests include context awareness, positioning and navigation, and visually impaired assistance.

VEERA ANKALU VUYYURU received the B.Tech. degree in CSE from JNTU, Hyderabad, and the M.Tech. degree in CST from GITAM University, Visakhapatnam, India, where he is currently pursuing the Ph.D. degree in CSE. He worked at RIT, Maharashtra, India, at various levels as an Assistant Professor and a Senior Assistant Professor. He is currently working as an Associate Professor with the CSE Department, Malla Reddy Engineering College for Women (UGC-Autonomous), Telangana, India. He has one international patent, three national patents, and one design patent. One of his papers published in Springer-Free Scopus journal and three papers in reputed Scopus journals and some international conferences. His research interests include data mining, machine learning, and computer networks. He is a Lifetime Member of Indian Society for Technical Education (ISTE). He is one of the research reviewers for international journal *IJRCS*.

NEENAVATH VEERAIAH received the B.Tech. degree from the Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India, in 2007, and the M.Tech. degree from the Lakireddy Balireddy College of Engineering, Mylavaram, Andhra Pradesh, in 2011. He is currently pursuing the part-time Ph.D. degree with the ECE Department, JNTUK University, Kakinada, Andhra Pradesh. He is an Assistant Professor with the Department of Electronics and Communications, DVR and Dr. HS MIC Engineering College, Kanchikacherla, Vijayawada, Andhra Pradesh. He is an Indian Academician. He is having 12 years of teaching experience. He got an amount of seven lakhs of fund from Indian Government, one of the leading funding organizations: the Department of Science and Technology (DST). He has published 18 international research papers over the years, as well as attended a greater number of workshops and IEEE conferences. He is a member of several professional and scientific organizations.

YOUSEEF ALOTAIBI received the master's degree in information technology (computer network) from La Trobe University, Melbourne, Australia, in 2009, and the Ph.D. degree from the Department of Computer Science and Computer Engineering, La Trobe University, in 2014. He is currently an Associate Professor with the Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia. He has published several international journals and conference papers. His research interests include business process modeling, business process reengineering, information systems, security, business and IT alignment, software engineering, system analysis and design, sustainability, and smart cities development.