Received November 15, 2021, accepted December 3, 2021, date of publication December 8, 2021,
date of current version December 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3133882

An Improved Hybrid Secure Multipath Routing Protocol for MANET

UPPALAPATI SRILAKSHMI[1], (Member, IEEE), NEENAVATH VEERAIAH[2], YOUSEEF ALOTAIBI[3], SALEH AHMED ALGHAMDI[4], OSAMAH IBRAHIM KHALAF[5], AND BHIMINENI VENKATA SUBBAYAMMA[6]

[1]Department of Computer Science and Engineering, VFSTR Deemed to be University, Vadlamudi, Guntur, Andhra Pradesh 522213, India
[2]Department of Electronics and Communications, DVR & Dr. HS MIC Engineering College, Kanchikacharla, Vijayawada, Andhra Pradesh 521180, India
[3]Department of Computer Science, College of Computers and Information Systems, Umm Al-Qura University, Mecca 24382, Saudi Arabia
[4]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 26571, Saudi Arabia
[5]Al-Nahrain Nano Renewable Energy Research Center, Al-Nahrain University, Baghdad 64074, Iraq
[6]Department of ECE, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada, Andhra Pradesh 520007, India

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

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

ABSTRACT Mobile ad hoc networks (MANETs) are self-organizing nodes in a mobile network that collaborate to form dynamic network architecture to establish connections. In MANET, data must traverse several intermediary nodes before reaching its destination. There must be security in place to prevent hostile nodes from accessing this data. Multiple methods were suggested in literature for securing routing; these techniques tackle different aspects of security. In order to enhance fault tolerance, wireless network multipath routing is typically used instead of the original single path routing. The routing protocol Genetic Algorithm with Hill climbing (GAHC) described in this article shows a hybrid GA-Hill Climbing algorithm that picks the optimal route in multipath. Prior to this in the beginning, the Improved fuzzy C-means algorithm method was built on density peak, and cluster heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust. The computation is based worth nodes are at the trust threshold found in addition. Even CHs take part in the alternate paths, the blend of all the many paths from these Cluster Heads that chooses the optimal route, which is based on the predicted hybrid protocol, as well as the optimum route's aggregate features such as throughput, latency, and connection. This suggested technique requires a minimum amount of energy of 0.10 m joules and a small amount of delay time of 0.004 msec, which also yields a maximum throughput of 0.85 bits per second, a maximum detection rate of 91 percent and maximum packet delivery ratio of 89percent. The suggested approach was put through the paces with the selective packet dropping attack.

INDEX TERMS MANET, genetic algorithm (GA), cluster heads (CHs), hill climbing (HC), selective packet dropping attack.

I. INTRODUCTION

Mobile ad hoc network (MANET) is a set of mobile nodes linked by wireless connections that act as an independent system. There is no permanent infrastructure to which it is linked. Each intermediate node serves as a router in the network. Many interesting characteristics are found in MANET [1]. For instance, MANET has the capacity to be adaptive, versatile, and maintain devices connected when the node travels from one location to another. The data packets may be forwarded from the source node to the adjacent node until they reach the target node using route discovery. As is usual, they are inconsistent owing to a limited energy [2] supply for mobility in the network, like the wireless connections between nodes in the ad hoc network. Also, the lack of dynamic network topology is a restriction. Nodes in MANETs (distributed-computing networks) may dynamically join and exit the network and can move autonomously. With such a dynamic nature, MANET [3] topology is difficult to define. Unprotected network nodes may become

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

malevolent nodes and slow down the network. As a result, they are at greater risk from malicious assaults because of these fundamental characteristics, such as dynamic topology, wireless medium, and bandwidth constraints. Most of the academics are focused on determining the safest and least energy- and bandwidth-intensive path for nodes to move data in a dynamic environment.

With mobile ad hoc networks, networking is in a state of emergent evolution, particularly when it comes to security [4].

Lot of effort are going into ad hoc network research to make a network more efficient. They're working to reduce latency, increase communication capacity, and minimize packet loss. With respect to routing security, there has been a broad range of investigation into how information is transferred between the source and the destination, since there is a requirement to keep the integrity and confidentiality of the data safe while blocking any unauthenticated communications. The job is more difficult because of MANET's changing topology, infrastructural complexity, variable bandwidth needs, inadequate physical security, and multi-hop communication. Even in the face of these difficulties, MANETS have made great strides, notably in sectors like education and medicine, defense and military operations, as well as emergency and rescue management for things like earthquakes and natural disasters. Because MANETs use multi-hop communication, routing is very difficult. The literature describes many routing protocols. As either static or dynamic routing protocols, these protocols are categorized depending on the timing of their choice of the next node in the routing process. When you're describing the routing tables of routers, you may speak about them depending on the way the routing tables are modified and utilized. This kind of protocol is known as a hybrid routing protocol, which takes the best of both static and dynamic routing. In order to maintain their routing tables, they can use location-based information or geographic information of nodes.

In order to enhance fault tolerance, wireless network multipath routing [5]is typically used instead of the original single path routing. Multipath routing may decrease the packet loss rate because of many routes. Multipath routing is beneficial for mitigating the effects of packet tampering or malicious assaults during the routing process. Selecting a best route amongst various routes while finding a route happens in a single step for multipath routing protocols. As long as there is a pool of previously defined routes, multipath routing reduces the number of route discovery operations. Reduced end-to-end latency [6]and energy waste prolong network life. The concurrent multipath transfer is an effective method of routing in MANETs because of technical advances in wireless systems and portable devices. In applications like as streaming high-quality mobile movies in heterogeneous access medium, this routing method may be used.

This research is used to create an enhanced hybrid secure multipath routing protocol for MANETs. In the proposed method, the cluster heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust values of the each nodes in the network. The computation is based on trust threshold worth nodes found in addition. From the CHs, the network of interconnected hops is included, and a selection of the best routes is established using a projected hybrid protocol, and this determines the best routes. This formula determines the fitness of the route by measuring the energy left in the nodes and the overall throughput of the route., and the connectedness or accessibility of the path. At the outset, the candidate CHs are picked from the MANET natural environment based on the Improved Fuzzy C means algorithm, which depends on density peak [7] with maximum worth of indirect, direct, and recent hope. These selections will be closely followed by intrusion detection procedures for discovering intruded nodes. In this instance, the purported goal function depends on the trail's ability, throughput, and connection. By using the capabilities of the GA and HC algorithms and observing the way data is being mined and modified, this hybrid algorithm can ensure that both phases are effectively and meaningfully used. In terms of selective packet dropping attack, the simulation results will be evaluated. Creating a method is part of the literature assessment in this section. At the end of this part, there are a number of methods with their own set of challenges., which motivates research into An Improved Hybrid Secure Multipath Routing Protocol For MANET.

This paper is organized as follows: Section 2 focuses on the motivations for using current methods, including literature inspection. The proposed way of routing is shown in Section 3, as well as acknowledged in Section 4. Section 5 provides the conclusion of the work

II. RELATED WORKS

Supporting basic activities and ensuring stability are the basic requirements of MANETs in order to create a robust security architecture that can adequately address hostile behavior that attempts to breach the MANET. In such a process, communication routes are established between nodes, and data is sent from one node to another through these pathways. Many MANETs use single-path routing because of resource constraints. Thus, the network would fail if nodes along the route were to fail. This may result in data loss. Routing is a concern because if it is hacked, the whole MANET is put at risk. For a sensitive application, it is crucial to have strong dependability and availability. Multiple routes have been made available in order to improve the network's availability, resilience, and dependability. However, using numerous routes increases security issues since it provides more avenues for attackers to get access to the data. To increase the availability and dependability of the network, therefore, it is essential to protect the network from hostile activities. Most of the routing protocols in MANETs haven't been developed with security needs in mind, thus existing security problems haven't received enough attention. Researchers from Veeraiah *et al.* [8]. offer a trust-based approach to ensure energy-efficient navigation in MANETs by using the hybrid algorithm, cat slap

single-player algorithm (C-SSA), which uses an artificial intelligence (AI) system to identify the optimum paths and routes to follow. When fuzzy clustering is used, the CHs (which is just a fancy name for cluster heads) are chosen based on the overall relevance of their indirect, direct, and recent trust values. The computation is based on trust threshold worth nodes found in addition. It is the variety of routes that are projected by all the CHs that selects the best route, as well as the composite characteristics of the overall route such as throughput, latency, and connectivity.

In this approach, a minimum amount of energy is used, a brief delay is introduced, maximum throughput is achieved, and maximum packet delivery ratio is realized, with the attack included or not. In order to reduce security breaches, we need to increase our processing speed. In an effort to avoid wasted energy, the Energy Aware On-Demand Routing Protocol (EADRP) was developed by Prasad and Shankar [9]. The protocol works to keep the MANET alive for as long as possible, and it also serves as an economically efficient routing method when the routing situation varies. Setting up routes amongst the mobile nodes and protocol functions in the network as long as the energy is available is the best way to go about setting up MANET routes. When the mobile node is in idle/sleep state, the protocol will deactivate energy consumption in the transmitter and receiver. It also looks for any potential communication requests sent out over the wireless channel. In order to test the proposed energy-efficient routing protocol, it is contrasted with two additional well-known routing protocols: dynamic source routing and conditional max-min battery capacity routing. In the proposed project, we're interested in finding ways to increase the scalability of nodes, as well as finding a way to eliminate the issues that are common to two neighborhoods when the EA-DRP is performed by two distinct nodes.

According to Kumar and Anuratha [10], an Energy Efficient EE-OHRA Route Discovery was developed for MANETs to tackle the issues of curbing energy consumption and extending the life of the route. Due to the fact that the life of the course is taken into consideration when deciding on the route, routing failure is avoided. This decision eliminates one of the possible route discovery methods, while also increasing the total computational load on every node because of route discovery techniques. In order to find the longest lifespan path that's free of harmful nodes, the suggested method will have to pay attention to safety.An improved method for efficient routing in IEEE 802.11 MANETs is suggested by Bhardwaj and El-Ocla [11] Node mobility may likely cause connections to fail and therefore random data packet loss. As more data is sent back and forth, more energy will be used. We provide a fitness function that incorporates the distance between the source and destination nodes, as well as the amount of traffic, and the conservation of energy. To prevent the crowded routes, the fitness function incorporates a congestion management technique called TCP CERL. The technique can identify if the congestion loss or the random loss was the cause of the degradation. We use the AOMDV algorithm to pick the best routes that have the greatest fitness, and we integrate the new fitness function (FFn) to select such routes. When selecting the best fitness route, there are many options to consider, including a short route, maximum residual energy, and a minimal amount of data traffic even if a data packet is randomly lost. Since security is such an important issue, the effort should concentrate on it.

A routing protocol named TBSMR was suggested by Sirajuddin *et al.* [12] to improve the QoS of the MANET.

It's better suited for larger networks where several variables such as congestion, the security values of the nodes, and the battery life of the nodes are taken into consideration when performing the routing process, which helps improve speed while also reducing overhead. Additional benefits of this suggested protocol include eliminating superfluous control messages during congestion or when a node fails, which lessens the floating of routes. With this protocol, safe communication is assured, and hostile nodes are detected. To ensure the MANET network is highly secure, this effort must incorporate a diverse range of security methods, such as encryption, decryption, and the use of blockchain to implement various security algorithms.

In her paper entitled ''A Genetic Algorithm-Based Multipath Routing Technique for Wireless Sensor Networks'', Wang [13] proposes a method based on genetic algorithms for sensor network routing, which helps to enhance fault tolerance and lower energy consumption for network nodes. To get an efficient fitness function, the various distance parameters between different kinds of nodes are taken into consideration. The following characteristics are included: The number of hops from the sending device to the base station, the number of hops from the base station to the next hop, and the distance between the sending device and the base station. In addition, the method's efficacy is confirmed by a simulation study. Since security is such an important issue, the effort should concentrate on it.In an attempt to add a social metric to dynamic source routing (MMDSR), Jara *et al.* [14] suggest the use of a multipath multimedia dynamic source routing (MMDSR) protocol, which includes a social metric TS in the decision-making processes of the forwarding algorithm. To get high QoS while at the same time retain high trust of those who constitute the forwarding route, we discover a trade-off between the quality of service (QoS) and the trust of those users. This project is intended to improve trust while having no effect on QoS. This should emphasize energy and security.

Neighbor node finding is proposed by Kumar *et al.* [15] for locating black hole nodes in MANETs. Another method the multi-detection routing protocol is used for generating the routing route is that it is utilized to determine the paths in the network. The most important goal of this study is to provide the route that bypasses black hole nodes without interrupting service. This suggested method is evaluated based on how much energy is used, how long the product will last, the ratio of packets sent, throughput, and the end-to-end latency. To be more effective, it must have a greater number of assaults.

Based on blockchain, an improved version of the conventional AODV (ad hoc on-demand distance vector) protocol (AODV-MQS) is proposed by Ranno *et al.* [16]. The first step is to set up a chain of nodes in the network and store the state of all the nodes in the chain, beginning with the intermediate nodes. In addition, the smart contract has been coded to ensure that only trustworthy nodes are connected to the blockchain. In the blockchain network, the primary communication route is represented by smart contracts, while a standby way is discovered which is not connected to the main path. To be more effective, it must have a greater number of assaults. ACO acknowledge as NDLR-MP, an ACO-based node-disjoint multi-path routing system utilizing AODV protocol, as proposed by Sharma *et al.* [17] In this proposed system, a single route discovery procedure would locate all node-disjoint routes from source to destination, eliminating any routing control overhead. After the first path is found, data packet transportation is started. All other secondary routes are simultaneously detected as well. We have also proposed a route repair technique that allows traffic to flow by diverting all the existing routes away from a damaged link on the following hop's path towards the destination. If one describes the suggested route identification and maintenance techniques as performance assessment metrics, then one may consider them metrics. To prevent security assaults, this approach has to put particular emphasis on it. For performance. The new ERS parameter selects an effective, bandwidth-increased alternative route and increases network efficiency. We are consider the above methods drawbacks to design an innovative improved hybrid secure routing protocol for MANET.

III. THE PROPOSED METHOD OF EFFICIENT ROUTING

Routing is the basic process of MANETs that enables communication connections to be established among nodes, as well as the sending and delivery of packets. Data communication is the foundation for most of the security critical [18] areas such as secure data aggregation, secure localization, intrusion detection, key management, and so on. Multiple routes are vulnerable in the same way as a single route. However, there are additional security issues that must be factored in with the usage of multiple routes. It is just as essential to protect data from malicious activity in non-sensitive settings as it is to keep the network available and reliable. Furthermore, maintaining the multipath routing process is critical in order to keep the routing duties operating well. Proposed an improved hybrid secure multipath routing protocol block diagram is showing in figure 1.

In this work, a hybrid secure multipath routing protocol for MANETs is proposed. Prior to this implementation, the method was built on density peak, and cluster heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust. The computation is based on trust threshold worth nodes found in addition. From the CHs, the network of interconnected hops are included, and a selection of the best routes is established using a projected hybrid protocol, and this determines the best routes. The fitness function [19]–[23] is equal to the sum of the remaining energy in the nodes, the throughput of the route, and the path's connectedness. It can both establish the delivery of packets from their point of origin to their point of destination, as well as apply a range of routing techniques while also including a hybridization algorithm that is accessed from a hybrid routing protocol known as GAHC, which is the combination of the Genetic Algorithm (GA) and the Hill Climbing (HC) algorithm in this instance, the purported goal function depends on the trail's ability, throughput, and connection. The recommended hybrid algorithm combines the advantages of the GA and HC processes, with the added benefit of minimizing mining/manipulation times. In terms of selective packet dropping attack, the simulation results will be evaluated.

A. TRUST MANAGEMENT SYSTEM

1) DIRECT TRUST (DT)

DT is based on the estimated length of time that it takes for a link to establish from the i^{th} source node to the d^{th} end point node. It is measured as the difference between the list of real and the anticipated length of time it will take for the destination node to verify the public key that was authored by the i^{th} source node. To paraphrase, therefore, DT including the use of i^{th} node and d^{th} end point has been described 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} specifies the anticipated duration, and τ_{est} indicates the approximate time period for estimate the estimated time required to authenticate the public key. In this other way of saying it, the time it takes to τ_{appx} receive and τ_{est} transmit the public key between the destination and the node is known as well. ω Signifies the opinion variable of these nodes.

2) INDIRECT DIRECT TRUST (IDT)

A node that includes the opinion variable is shown with DT. However, without a witness variable, a node has to use the IDT, which is assigned using,

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

r specifies the neighbourhood around this node i.

3) RECENT TRUST (RT)

When computing trust, we rely on the DT and IDT, alongside the essential validity and figuring out the sink. the RT is designed to accomplish,

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

B. CH SELECTION BASED IMPROVED FUZZY C-MEANS ALGORITHM

The FCM algorithm is an unsupervised learning technique, implemented with the goal of optimizing the objective function, that uses partitioning a mobile adhoc network iteratively.

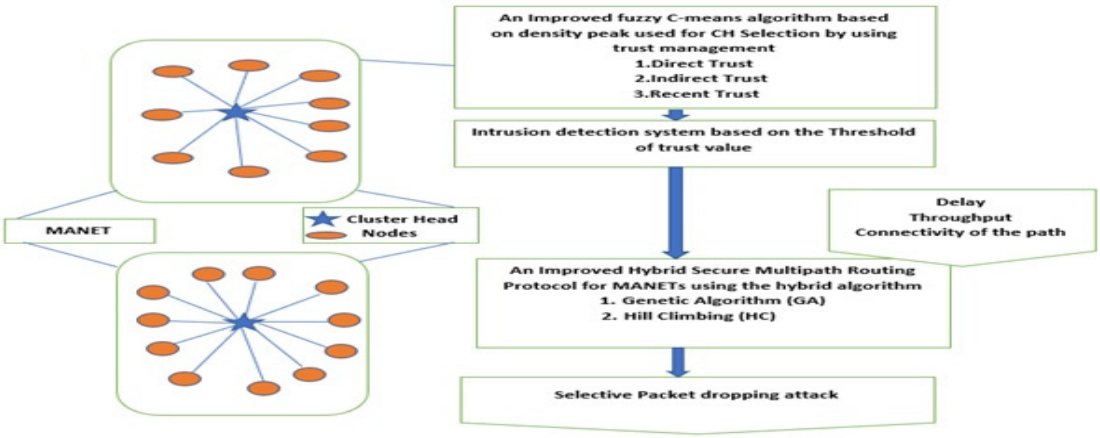

FIGURE 1. Proposed an improved hybrid secure multipath routing protocol.

To solve the clustering issue [6], [24]–[26], the FCM method incorporates fuzzy equations. The cluster result represents nodes that are individually affiliated with a certain percentage of the clustering head's total membership.

Let the entire n number of nodes be equal to $X = \{X_1, X_2, \ldots, Xn\}$. The total number of nodes is equal to X_i, where each node has a total of ρ motions. C fuzzy groups are formed and $V = \{V_1, V_2, \ldots, V_C\}$ is used as the cluster head matrix. The goal of FCM is:

$$J(U, V) = \sum_{i=1}^{c} \sum_{j=1}^{n} \left(u_{ij}\right)^m \left(d_{ij}\right)^2 \tag{4}$$

where $U = \left(u_{ij}\right)$ is an n × c dimension membership matrix, and u_{ij} represents the membership between V_i and X_j.

$d_{ij} = x_j - V_i$ is the Euclidean distance between the node j and the cluster head i. m (m > 1) is the fuzzy exponent in the algorithm. Equation (4) also needs to meet the following conditions:

where u_{ij} denotes the membership between V_i and X_j, where $U = \left(u_{ij}\right)$ which has a n x c dimensionality. $d_{ij} = X_j - V_i$ represents the Euclidean distance between the node and the cluster head i. Additionally, equation (4) must satisfy the following requirements:

$$\begin{cases} \sum_{i=1}^{c} u_{ij} = 1, & j = 1, 2, \ldots, n \\ 0 \le u_{ij} \le 1, & i = 1, 2, \ldots, C; \quad j = 1, 2, \ldots, n \\ 0 < \sum_{j=1}^{n} u_{ij} < n, & i = 1, 2, \ldots, C \end{cases} \tag{5}$$

Finally, the minimal objective function J(U,V) of FCM method was achieved via iterative optimization, and U and V may be derived as follows:

$$u_{ij} = \left\{ \frac{1}{\sum_{k-1}^{C} \frac{d_{ij}}{d_{kj}}^{1} m^{-2}} \right. \tag{6}$$

$$V_i = \frac{\sum_{j=1}^{n} \left(u_{ij}\right)^m x_j}{\sum_{j=1}^{n} \left(u_{ij}\right)^m} \tag{7}$$

FCM method requires manually assigning the cluster heads and cluster numbers and is particularly vulnerable to the first cluster heads assigned. With issues such as numerous clustering iterations, delayed convergence, local optimum solution, and poor stability, it is simple to create a myriad of other algorithms. A novel density peak-based FCM algorithm is proposed (DP-FCM). Let's find the cluster heads in DP-FCM, using the two parameters ρ_i and δ_i of total no of nodes. The density distance index φ_i is

$$\varphi_i = \rho_i \delta_i \tag{8}$$

Traverse the n no of number of nodes and discover all the δ_i values of all the nodes. Use the order in which density distance values are arranged to first get the z-coordinates. Convert the calculated density distance into an average density distance.

$$\varphi_{avg} = \frac{1}{z} \sum_{i=1}^{2} \varphi_i \tag{9}$$

From the points of the density distance value, it is clear that the points indicate a decreasing tendency. More important locations have a greater chance of becoming the clustered head. $\varphi_i > \varphi_{avg}$ Specifying that Ci at that moment is a clustering head indicates that we are at that point in time. Once the clustering head has been chosen, it will be picked based on the greatest trust value. To do the first stage of DP-FCM, a cluster head point is added to the FCM algorithm, and the clustering result is then obtained. Once a node has beyond its foundation trust values, it may be designated as a CH. The founding value of direct, indirect, and recent trust, the maximization function(M), is defined as,

$$\mathrm{M} = \frac{1}{3}\{D + I + R\} \tag{10}$$

where direct, indirect, and recent trust values are equated to D, I, and R. Are also the same as those obtained by utilizing equations (1)(2) and (3).

C. IDENTIFYING INTRUDED NODES IS MADE EASY BY THRESHOLD VALUE COMPARISON

After calculating the optimal CHs, the system's infiltration is estimated. The next step is to analyze the optimistic elements of these nodes, both from the system's perspective and the end users. Keep this in mind, since landlords have historically been connected to the sink node, which gets its flow from the CHs that connect to the system (or cluster associates). The identity of the attacker has been discovered, and the intrusion node is no longer permitted to use the network. The sink node predefined threshold (0.5J) [8]is used to estimate the presence of intruders. In the administrator's discretion, the threshold amount may be determined based on the requirements of the system.

In the majority of cases, the number is usually 0.5J. The transmission power and connection state of a channel are calculated using the remaining energy range of a particular node. When energy is low, the likelihood of finding another nearby node decreases, and as a result, the node is not part of a network's connectivity. However, if the energy of a node is greater, the transmission power of a node may be enhanced. Intrusion detection has the primary goal of maintaining a secure network connection while using less energy and delivering data as fast as feasible.

D. A HYBRID ALGORITHM FOR EFFECTIVE ROUTING

The Hybrid optimization approach, too, identifies the most useful jumps for MANET routing construction. The suggested algorithm's goal is to determine which routes have the best chances of success. Even the necessity for immediate response programming will denote the optimization algorithm's solution, and the solution is just the paths picked for its navigation in MANETs. The path's health is determined by the amount of energy left in the nodes, the path's throughput, and the path's accessibility. As a result, the fitness function is a maximizing function, represented by [8].

$$F = \frac{1}{3}\{e + t + c\} \tag{11}$$

where e stands for energy, t for throughput, and c for path connection, all of which are calculated using the path's nodes.

E. HYBRID (GA AND HC) OPTIMIZATION ALGORITHM

In considering an ad hoc network, a linked dynamic network with N nodes is being shown. The cost of the route connecting the nodes is the measure of optimization. The overall cost is equal to the sum of the individual hops' costs. To do so, look for the route with the lowest overall cost (in terms of time and money) that links your source node to your destination node.

1) REPRESENTATION OF A CHROMOSOME

Any route between the source node and the destination node is a viable solution in the GA algorithm. Optimality is achieved by settling on the solution that is the shortest. When the solution space is created from a random population of possible solutions, a solution is considered to be admissible (feasible) or inadmissible (unfeasible). Strings that cannot reach the target are inadmissible solutions. The answer to the optimization issue may be found in the chromosome. A routing path's DNA is made up of positive integers representing the IDs of nodes, and those IDs are strung together to form a path that is used to navigate to nodes. The starting point is always source node and proceeds via intermediate nodes (to nodes) and then terminates with the goal, which is the final destination. This specifies the maximum chromosomal length and defines a global maximum for chromosome length. Measuring fitness criteria

Fitness is a function that may be calculated as follows:

$$fi = \frac{1}{\sum_{j-1}^{li-1} C_{gi}(j) + g_i(j+1)} \tag{12}$$

The parameter f_i, which stands for the fitness value of the i^{th} chromosome, corresponds to the letter i and the parameter l_i is the length of the i^{th} chromosome. Gene (node) of the j^{th} locus in the i^{th} chromosome is defined as gi(j). Lastly, there is a link cost between nodes defined as C. The connection costs in the proposed method are treated as being equal to each other and equal to 1. For example, if the cost which reflects the shortest distance is hops, then the cost will be the hop count.

2) SELECTION OF BEST FIT

The process of selecting the best-fitting members of the population improves the overall quality of the group. Better-quality chromosomes are more likely to survive when the procedure is applied. In contrast to proportional selection, ordinal-based selection only uses ordered (ordinal) selections. Proportionate selection examines chromosomal characteristics relative to the general population's characteristics. This assortment includes random selection with roulette wheel selection, random selection with Stochastic Remainder Selection, and random selection with Stochastic Universal Selection. In this article, we will utilize the roulette wheel idea, and the values with the highest likelihood of being chosen are assigned greater percentages on the wheel. Those values with the best fit are assigned higher percentages, thus increasing the chance of the fit generating an offspring.

3) CROSSOVER

Operator Crossover, a process that integrates genetic material from two parent chromosomes, produces a new organism. On strings, midway crossover is used in the process of crossover. When making a midpoint crossover, each parent's chromosomes are split into two midways through. additional traits are included in the offspring's generated through crossover.

4) MUTATION

When randomly mutating genes, the mutation operator shifts the search to other areas in the solution rate. Consecutive iteration values are the same if mutation is done. Choosing the optimal path by using a hybrid optimization technique is recommended. Both the Genetic Algorithm (GA) and the Hill Climbing Algorithm are being used to the suggested hybrid optimization (HCA). Local Search-related mathematical optimization is known as hill-climbing. First, an impossible answer is proposed (known as an initial solution), and then it is modified to determine whether the modification would provide a better outcome. New solutions are often superior in terms of fitness; therefore, the new solution is implemented if the solution is better. Otherwise, the old solution is maintained. Iterative refinement of a solution using neighborhood transformations will aid progress up a hill as long as feasible. Knowledge criteria associated with hill climbing advancement include a goal, early phases, range, and a search. Increasing the available number of parameter settings stretches out the hill-climbing area of the quest room. Search space basics: The search space must include a set or a collection that is neither negated nor quantified. a perfectly symmetrical body revolution This means that when the self-assertive point revolves around a pivot point as well as an interpretation, the pivot will impact the interpretation. On one hand, relative change is asymmetrical; nevertheless, it is non-decreasing. The working flow diagram is shown in figure 2.

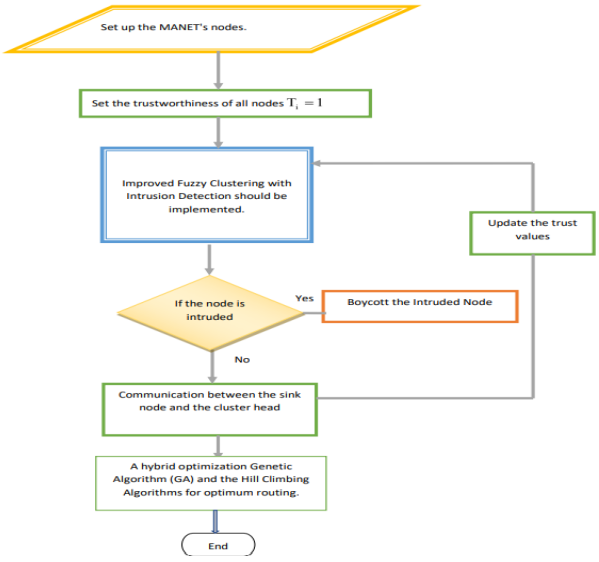

FIGURE 2. Working flow diagram.

To improve our routing unit's first ruleset, we recommend using both GA and hill climbing.

IV. RESULTS

This section focuses on the relation between the advanced routing solutions that take into consideration a combination of planned and enhanced hybrid secure multipath routing protocols and all the other comparative evaluations based on functionality measurements.

Algorithm for GA With Hill Climbing

Create a randomly generated population
for generation numbers I to 1,
as well as for the values for j between 1 and the population size.
You should use crossover and mutation operators to choose parents if the new,
solution is no longer feasible. You should then come up with a new_solution,
There is a total of N new solutions that have been found,
$N = Hill\text{-}Climbing\ (N)$
end if
end for
to start on the next level
when the halt condition is met
propose a resolution to the algorithm
end if
end for Hill-Climbing (current solution) is a method
Pick another option = continue existing strategy
if fitness of following answer > fitness of existing answer
Pick another option = continue existing strategy
end if
end while
Start the population at random.
Build a generator for I using 1 as a starting point.
j's population should be increased by one.
seek out a relative

A. INVESTIGATIONAL ARRANGEMENT

For the ad-hoc networking community, Network Simulator-2 [27] is widely used. It is open-source software that assesses the performance of existing network protocols as well as novel network protocols before they are implemented. To simulate a variety of IP networks, use the NS2 simulator. The major purpose of the NS2 simulator is to help with networking education and research. It is one of the most well-programmed in terms of comparing and inventing new routing protocols. The object-oriented form of Tool Command Language (OTCL) and the object-oriented language C++ were used to create NS2. The simulator was additionally enhanced with a hundred nodes at the simulation environment. Simulation time 40ms long. Table 1 shows the simulation parameters.

B. PERFORMANCE METRICS

The study's characteristics include delay, energy, throughput, detection rate and packet delivery ratio, and the suggested approach is compared to current methods that utilize various measurements of competence, with and without assault. This energy is that the energy that remains after all the nodes have been transferred. This should be stated as a maximum worth to assign the duration of the device. The result of this

TABLE 1. Simulation parameters.

Simulation parameters	
Model of radio-propagation	TwoRayGround
MAC	802_11
Interface	WirelessPhy
Link layer class	LL
Antenna	OmniAntenna
Protocol type	AODV
Packet Range	512
Speed	250kb
Energy Initial	15.1 J
Quantity of Nodes	100
Simulation Time	40

system is dependent on the quantity of information the system delivers within a certain time period, and the interval refers to the entire time it takes for the specified information to be sent.

C. COMPARATIVE TECHNIQUES

The methods utilized for the contrast include Energy Efficient Optimized Hierarchical Routing Algorithm (EE-OHRA) [9], Fuzzy CSO-SSA [8] to compare with the proposed an improved hybrid secure multipath routing protocol.

1) COMPARATIVE EVALUATION OF THE SUGGESTED METHOD

a: DELAY

In Figure 2, the relative assessment is shown to have a delay focus. There is a delay of about 0.004, 0.003, and 0.002 m seconds for the EE-OHRA, Fuzzy CSO-SSA, and an improved hybrid secure multipath routing protocol. The simulation results show that the proposed methods provide a minimal delay of 0.002 msec when compared to the two current existing methods.

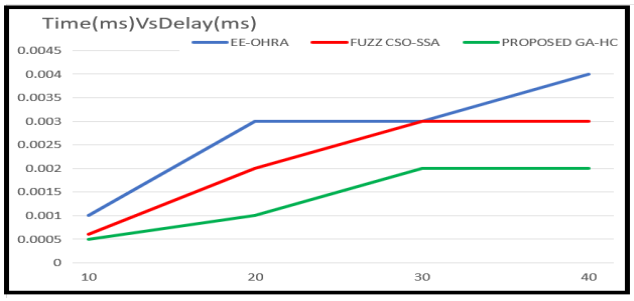

FIGURE 3. Proposed GA-HC delay.

b: ENERGY CONSUMPTION

Fig. 3 depicts the energy expenditure. When the energy consumption at 40-second intervals is about 0.22, 0.11, and 0.10 Joules, respectively EE-OHRA, Fuzzy CSO-SSA and proposed an improved hybrid secure multipath routing protocol

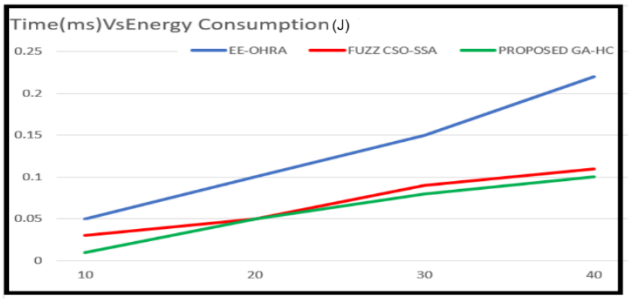

FIGURE 4. Proposed GA-HC Energy Consumption.

The simulation results suggest that proposed an improved hybrid secure multipath routing protocol get a minimal energy usage of 0.10 joules.

c: THROUGHPUT

The graph in Figure 4 demonstrates that the relative report on throughput was done. EE-OHRA, Fuzzy CSO-SSA, and proposed an improved hybrid secure multipath routing protocol all achieve throughput of 0.45, 0.74, and 0.70 bits per second.

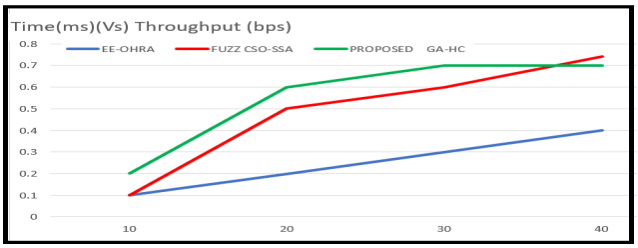

FIGURE 5. Proposed GA-HC throughput.

From the simulation results, it can be concluded that proposed an improved hybrid secure multipath routing protocol obtained the maximum throughput of 0.70 bps.

d: DETECTION RATE

The findings of the comparison in Figure 5 are shown below. EE-OHRA, Fuzzy CSO-SSA, and the proposed an improved hybrid secure multipath routing protocol detection rates are 75, 90, and 91 percent, respectively.

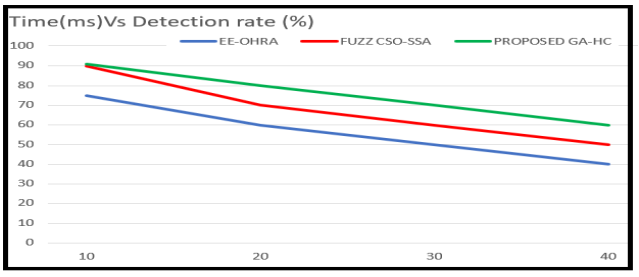

FIGURE 6. Proposed GA-HC detection rate.

TABLE 2. Comparative analysis of the proposed method with and without attack.

Without Selective Packet Dropping Attack			
Parameter	**EE-OHRA**	**FUZZ CSO-SSA**	**PROPOSED GA-HC**
Delay(ms)	0.004	0.003	0.002
Energy consumption(J)	0.22	0.11	0.10
Throughput(bps)	0.45	0.74	0.85
Detection rate (%)	75	90	91
Packet delivery ratio(%)	74	87	89
With Selective Packet Dropping Attack			
Delay(ms)	0.007	0.006	0.004
Energy consumption(J)	0.23	0.11	0.10
Throughput(bps)	0.70	0.76	0.80
Detection rate (%)	74	89	90
Packet delivery ratio (%)	70	85	88

When compared to current two approaches of EE-OHRA and Fuzzy CSO-SSA methods, the recommended method that gained a maximum detection rate of 91 percent.

e: PACKET DELIVERY RATIO

The findings of the comparison in Figure 6 are shown below. EE-OHRA, Fuzzy CSO-SSA, and the proposed an improved hybrid secure multipath routing protocol packet delivery ratio at 50 nodes are 74, 87, and 89 percent, respectively.

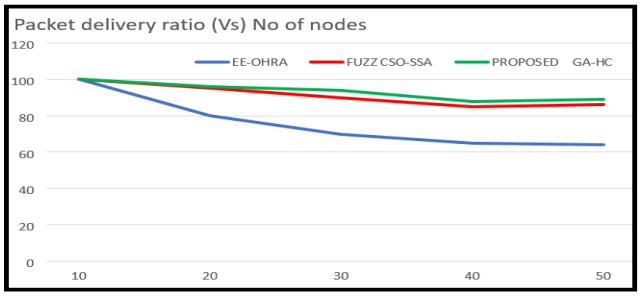

FIGURE 7. Proposed GA-HC packet delivery ratio.

From the simulation results, it can be concluded that proposed an improved hybrid secure multipath routing protocol obtained the maximum packet delivery ratio of 89 percent.

2) COMPARATIVE ANALYSIS BASED ON SELECTIVE PACKET DROPPING ATTACK

An evaluation of the process in the following data is taken into consideration. Figure 7(a) shows the estimated relative delay. The EE-OHRA, Fuzzy CSO-SSA and the proposed an improved hybrid secure multipath routing protocol, respectively, is 0.007 0.006 and 0.005 m sec, with a period of 40 seconds. The relative energy expenditure study as shown in Figure 7 (b). EE-OHRA, Fuzzy CSO-SSA and the proposed an improved hybrid secure multipath routing protocol, respectively, at 0.23, 0.11 and 0.10 m Joules, is 40 seconds in length. Throughput is presented in Figure 7 (c). The EE-OHRA, Fuzzy CSO-SSA and the proposed an improved hybrid secure multipath routing protocol is 0.70, 0.76, and 0.80 bps, respectively. The comparison with the detection rate is shown in Figure 7 (d). EE-OHRA, Fuzzy CSO-SSA and the proposed an improved hybrid secure multipath routing protocol based on trust are 74, 89 and 90 percent. correspondingly. From the findings, it is noticed that the suggested approach exhibits superior outcomes compared to current methods when it is used with the selective packet dropping attack in consideration.

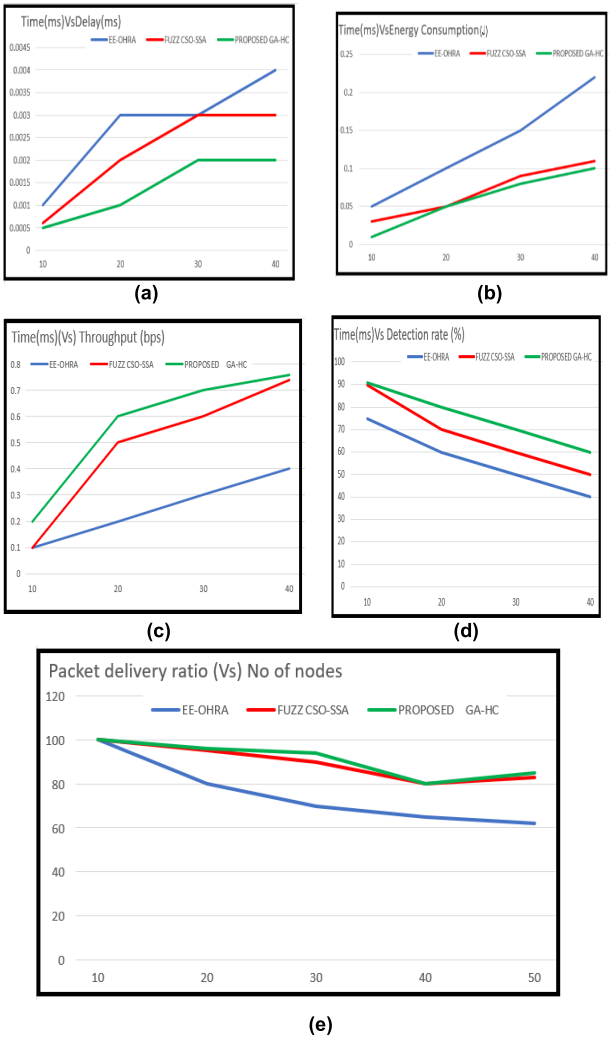

FIGURE 8. (a). Delay. (b). Energy consumption. (c). Throughput. (d). Detection rate. (e). Packet delivery ratio.

The comparison with the packet delivery ratio is shown in Figure 7 (e). EE-OHRA, Fuzzy CSO-SSA and the proposed an improved hybrid secure multipath routing protocol based on trust are 70, 85 and 88 percent. Correspondingly. Table 2 shows the comparative analysis of proposed method with and without attack.

Finally, from the simulation results the proposed method shows good results when compared to the existing methods without and with selective packet dropping attack. The proposed method offer less delay and energy consumption of 0.002 msec, 0.04 of msec and 0.10 J, with selective packet dropping attack.Maximum Throughput,detection rate and packet delivery ratio of 0.85(bps), 91% and 89 % without selective packet dropping attack.The proposed method shows good results with the attack also.

V. CONCLUSION

The MANET is a network where data is sent to many nodes that are located between the source and the destination. There must be security in place to prevent hostile nodes from accessing this data. In order to enhance fault tolerance, wireless network multipath routing is typically used instead of the original single path routing. The provided article demonstrates how a GAHC-style hybrid algorithm connects the Hill Climbing (Routing Protocol) and Genetic Algorithm (GA) in multiphase scenarios. Prior to this implementation, the method was built on density peak, and cluster heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust. The computation is based on trust threshold worth nodes found in addition. Even CHs take part in the multi-hop routing, and it is the mixture of all the routes from these CHs that chooses the optimal route, which is based on the predicted hybrid protocol, as well as the optimum route's aggregate features such as throughput, latency, and connection. The suggested approach achieved a minimum amount of energy in the form of 0.10 joules, a trivial amount of time as measured in milliseconds as well as in clock cycles, a throughput of 0.85 bits per second, a detection rate of 91 percent and packet delivery ratio 89 percent. This suggested approach was compared against the current methods when just the selective packet dropping attack was present, and to the existing techniques in the presence and absence of the selective packet dropping assault.

REFERENCES

[1] N. Veeraiah and B. T. Krishna, "Trust-aware FuzzyClus-fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule," *Wireless Netw.*, vol. 25, pp. 4021–4035, Jan. 2019, doi: 10.1007/s11276-018-01933-0.

[2] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET," in *Evolutionary Intelligence*. Berlin, Germany: Springer, Mar. 2020, pp. 1–15.

[3] M. Naseem, G. Ahamad, S. Sharma, and E. Abbasi, "EE-LB-AOMDV: An efficient energy constraints-based load-balanced multipath routing protocol for MANETs," *Int. J. Commun. Syst.*, vol. 34, no. 16, 2021, Art. no. e4946, doi: 10.1002/dac.4946.

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

[5] C. Iwendi, S. Khan, J. H. Anajemba, M. Mittal, M. Alenezi, and M. Alazab, "The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems," *Sensors*, vol. 20, no. 9, 2020, Art. no. 2559.

[6] S. Uppalapati, "Energy-efficient heterogeneous optimization routing protocol for wireless sensor network," *Instrum. Mesure Metrol.*, vol. 19, no. 5, pp. 391–397, Nov. 2020, doi: 10.18280/i2m.190510.

[7] G. M. Borkar and A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks," *Wireless Netw.*, vol. 23, no. 8, pp. 2455–2472, Nov. 2017.

[8] 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, doi: 10.1109/ACCESS.2021.3108807.

[9] R. Prasad and P. S. Shankar, "Efficient performance analysis of energy aware on demand routing protocol in mobile ad-hoc network," *Eng. Rep.*, vol. 2, no. 3, 2020, Art. no. e12116.

[10] S. V. Kumar and V. Anuratha, "Energy 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.

[11] A. Bhardwaj and H. El-Ocla, "Multipath routing protocol using genetic algorithm in mobile ad hoc networks," *IEEE Access*, vol. 8, pp. 177534–177548, 2020.

[12] M. Sirajuddin, C. H. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network," *Secur. Commun. Netw.*, vol. 2021, Apr. 2021, Art. no. 5521713.

[13] S. Wang, "Multipath routing based on genetic algorithm in wireless sensor networks," *Math. Problems Eng.*, vol. 2021, Jun. 2021, Art. no. 4815711.

[14] E. P. Jara, A. M. Mezher, M. A. Igartua, R. P. D. Redondo, and A. Fernandez-Vilas, "QSMVM: QoS-aware and social-aware multimetric routing protocol for video-streaming services over MANETS," *Sensors*, vol. 21, no. 3, p. 901, 2021.

[15] T. V. S. Kumar and D. P. G. Benakop, "A secure routing protocol for MANET using neighbor node discovery and multi detection routing protocol," *Int. J. Eng. Trends Technol.*, vol. 68, no. 7, pp. 50–55, 2020.

[16] C. Ran, S. Yan, L. Huang, and L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–16, 2021.

[17] A. Sharma and L. Tharani, "Ant colony based node disjoint local repair in multipath routing in MANET network," *Wireless Pers. Commun.*, pp. 1–28, Feb. 2021.

[18] B. S. Eddine, O. Smail, B. Meftah, M. Rebbah, and B. Cousin, "An efficient energy aware link stable multipath routing protocol for mobile ad hoc networks in urban areas," *Telfor J.*, vol. 12, no. 1, pp. 2–7, 2020, doi: 10.5937/telfor2001002E.

[19] G. Suryanarayana, K. Chandran, O. I. Khalaf, Y. Alotaibi, A. Alsufyani, and S. A. Alghamdi, "Accurate magnetic resonance image super-resolution using deep networks and Gaussian filtering in the stationary wavelet domain," *IEEE Access*, vol. 9, pp. 71406–71417, 2021.

[20] G. Li, F. Liu, A. Sharma, O. I. Khalaf, Y. Alotaibi, A. Alsufyani, and S. Alghamdi, "Research on the natural language recognition method based on cluster analysis using neural network," *Math. Problems Eng.*, vol. 2021, May 2021, Art. no. 9982305.

[21] A. Alsufyani, Y. Alotaibi, A. O. Almagrabi, S. A. Alghamdi, and N. Alsufyani, "Optimized intelligent data management framework for a cyber-physical system for computational applications," *Complex Intell. Syst.*, Aug. 2021, pp. 1–13.

[22] Y. Alotaibi, "A new database intrusion detection approach based on hybrid meta-heuristics," *Comput., Mater. Continua*, vol. 66, no. 2, pp. 1879–1895, 2021, doi: 10.32604/cmc.2020.013739.

[23] S. Uppalapati and G. Parimala, "Modified energy efficient with ACO routing protocol for MANET," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 2, pp. 1739–1745, Apr. 2021.

[24] B. Velusamy, K. Karunanithy, D. Sauveron, R. N. Akram, and J. Cho, "Multi-objective function-based node-disjoint multipath routing for mobile ad hoc networks," *Electronics*, vol. 10, no. 15, p. 1781, 2021.

[25] M. Farkhana, A. A. Hanan, H. Suhaidi, K. A. Tajudin, and Z. K. Zuhairi, "Energy conservation of content routing through wireless broadcast control in NDN based MANET: A review," *J. Netw. Comput. Appl.*, vol. 131, pp. 109–132, Apr. 2019.

[26] K. A. Darabkh, M. G. Alfawares, and S. Althunibat, "MDRMA: Multi-data rate mobility-aware AODV-based protocol for flying ad-hoc networks," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100163.

[27] J. Li and H. W. Lewis, "Fuzzy clustering algorithms review of the applications," in *Proc. IEEE Int. Conf. Smart Cloud (Smart Cloud)*, Nov.2016, pp. 282–288.

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 serving as an Assistant Professor with VFSTR Deemed to be University, Vadlamudi, Guntur. She is having more than 12 years of experience in academic, administration, research, and innovations. She has published so many articles in reputed journals, like Springer, Scopus, and Web of Science; and 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 has delivered a Keynote Speaker in e-ICMSEM. 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.

NEENAVATH VEERAIAH received the B.Tech. degree from Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh, India, in 2007, and the M.Tech. degree from 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 & Dr. HS MIC Engineering College, Kanchikacherla, Vijayawada, Andhra Pradesh. He is an Indian Academician. He has 12 years of teaching experience. He got an amount of Rs. seven lakhs from the Indian Government, one of the leading funding organizations, the Department of Science and Technology (DST). He has published 20 international research papers over the years, as well as attended a greater number of workshops and IEEE conferences. He is also a member of several professional and scientific organizations.

YOUSEEF ALOTAIBI received the master's degree in information technology (computer networks) 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.

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.

OSAMAH IBRAHIM KHALAF received the B.Sc. degree in software engineering field from Al_Rafidain University College, Iraq, the M.Sc. degree in computer engineering field from Belarussian National Technical University, and the Ph.D. degree in computer networks from the Faculty of Computer Systems and Software Engineering, University Malaysia, Pahang. He is currently a Senior Engineering and Telecommunications Lecturer at Al-Nahrain University. He has overseas work experiences in university at Binary University, Malaysia, and University Malaysia Pahang. He has hold 17 years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer science and information technology projects. He has had many published articles indexed in (ISI/Thomson Reuters) and has also participated and presented at numerous international conferences. He has a patent and has received several medals and awards due to his innovative work and research activities. He has good skills in software engineering, including experience with: Net, SQL development, database management, mobile applications design, mobile techniques, Java development, android development, and IOS mobile development, cloud system and computations, and website design. He is the editor-in-chief and main guest editor in many Scopus and SCI index journals. His brilliant personal strengths are in highly self-motivated team player who can work independently with minimum supervision, strong leadership skills, and outgoing personality.

BHIMINENI VENKATA SUBBAYAMMA received bachelor's degree from VRS Engineering College, Vijayawada, Andhra Pradesh, and the master's degree in stream of communications and radar systems from KLCE, Vaddeswaram, Guntur, Andhra Pradesh. Currently, she is working as an Assistant Professor with the Department of ECE, Prasad V. Potluri Siddhartha Institute of Technology, Kanuru, Vijayawada. Her research interests include communications and wireless networks. She is a member of IETE and ISTE.