IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 1 December 2022, accepted 17 December 2022, date of publication 21 December 2022,
date of current version 27 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3230991

RESEARCH ARTICLE

Adaptive Routing Protocol in Mobile Ad-Hoc Networks Using Genetic Algorithm

NISHIT SHAH, HOSAM EL-OCLA, (Senior Member, IEEE), AND PEARLY SHAH
Department of Computer Science, Lakehead University, Thunder Bay, ON P7B 5E1, Canada
Corresponding author: Hosam El-Ocla (hosam@lakeheadu.ca)

ABSTRACT Mobile Adhoc Network (MANET) is a wireless network in which data is transferred in a forwarding direction from the source node to the destination node via multiple intermediate nodes. Packets collision is considered one of the most crucial limitations in MANETs because the nodes in the network move in random directions at a random velocity which increases the probability of collision and this will harm the throughput, the routing overhead, and the end-to-end delay. Also, frequent node mobility leads to a topological change and link instability and this reduces the data delivery rate. Because of limited available paths to the destination node or having a high traffic load, the possibility of traffic congestion augments at the intermediate nodes which in turn affects the packet delivery, particularly with real-time applications in MANETs. In this paper, we propose an adaptive routing protocol based on a bio-inspired genetic algorithm (GA). We optimize the multiple paths returned by the AOMDV mechanism (AOMDV-FG) to select the best path to the destination. The route with the highest fitness value is considered the most optimum route. Lastly, we compare our proposed protocol with AOMDV-TA and EHO-AOMDV. We have used routing overhead, end-to-end delay, throughput, energy consumption, and packet delivery ratio as key metrics for the performance evaluation of our proposed model.

INDEX TERMS MANET, AOMDV, genetic algorithm, fitness function, queue length, collision, link stability.

I. INTRODUCTION

A group of mobile devices that dynamically construct a communication network without any centralized devices in charge of it or any pre-existing network infrastructure is known as a mobile Adhoc network (MANET). Some of the characteristics of MANETs are autonomous behavior, dynamic topology, energy-constrained operation, bandwidth-constrained, variable capacity links, and limited security [1]. The key benefit of using a mobile ad hoc network is being able to connect to the internet without the use of a wireless router. As a result, maintaining an ad hoc network is less expensive than maintaining a standard network [2]. Due to the elimination of fixed infrastructure costs and the decreased power requirements for mobile nodes, MANETs are more cost-effective. Moreover, in MANETs routing and transmission protocols are built to handle fault tolerance and it permits connection failures [3].

Despite the attractive applications, there are several disadvantages brought on by MANET's characteristics. Drawbacks of MANETs include excessive energy consumption due to the high mobility of nodes particularly as there is no external source of energy. In other words, ad hoc networks encounter significant challenges since portable nodes are powered by batteries which are typically underpowered and require a lot of time to recharge or replace [4]. More study on effective protocol, platform, and technology design is required to overcome this obstacle. Therefore to increase the network's lifespan and guarantee network connectivity, the routing protocol should take the energy of the mobile node into account [5], [6].

On the other hand, frequent topological change may result in more data collisions as connecting links among nodes continuously break. The topology changes as the node moves,

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

and this increases the risk of the established link breaking down. The original link must be replaced with other existing links or the route discovery must be restarted when using the conventional shortest path algorithm [7]. Part of the routing protocol considers the link's stability when routing is chosen to address the link failure brought on by the mobility of the nodes. These routing techniques estimate the lifespan of the link by computing the node's received signal strength or the nodes' relative mobility [8]. One of the applications where link stability plays a crucial role in business applications. For instance, in game applications where multiple users may sign in and play games, users will face lag in the game because of link instability. When links get broken frequently, users won't be able to stay signed in to the application [9]. Due to such high node mobility, the probability of collision in a network increases and this leads to packet drops. This degrades the performance of the network in various applications such as location-based services. For example, when using a geolocation application and if the data packets are not delivered on time due to collision, routes will not be calculated accurately [10]. In addition, the movement of the nodes in random directions with high velocity causes a topology change constantly and as a result, more energy is consumed to calculate a new route.

In ad hoc networks, data congestion occurs when there are too many packets transferring through a single network [11] and when the network's capacity is exceeded by these packets' load. Congestion causes delay and requires more resources for recovery and causes packet errors and bandwidth degradation [12]. When congestion occurs, it usually concentrates on a single router because it doesn't overload moveable nodes but instead impacts the entire coverage area [13]. Ad hoc networks' main problem is congestion control. It has to do with controlling how much traffic gets into a media transmission network to avoid overloading join capabilities between the prompt nodes and the network and to prevent connection failures [14]. One of the applications where congestion plays a crucial role is in the military field. One of the applications where delay plays a crucial role is in rescue operations and the healthcare industry.

In addition, scalability and lack of centralized management would degrade the performance of data transmission over MANETs. These flaws make MANET more vulnerable to malicious attacks because of limited physical security [15].

In MANETs and because the topology of an ad hoc network is dynamic, nodes are not aware of the topology of their network and must figure it out on their own. The basic guidelines state that at anytime a new node joins an ad hoc network, it must make an announcement of its presence and must also pay attention to similar announcement broadcasts received from existing mobile nodes. In this regard, there are two operations of data transmission: one is finding the best route and the other is the packet transmission. An efficient routing protocol is therefore essential to wireless communication [7]. Therefore, multi-hop routing is adapted to transport a data packet from a source node to a destination node and this requires cooperation between nodes in networks without any infrastructure [16], [17].

Multipath routing, as compared to conventional single-path routing protocols, can ease network traffic problems explained above by directing traffic to several channels, increasing network utilization, and distributing network load. The network's reliability is improved to some extent [18]. An improved version of the Ad Hoc On-demand Distance Vector Routing (AODV) routing protocol is Ad Hoc On-demand Multi-path Distance Vector Routing (AOMDV) which finds numerous paths between a given source and destination node. There are two main services provided by AOMDV; i.e route discovery and route maintenance.

Advantages of AOMDV include its ability to establish routes on demand, create loop-free nodes, maintain connectivity and fast and efficient recovery from failures [19]. Since AOMDV is a multipath routing protocol, the destination replies to multiple RREQs which results in a longer overhead in response to a single RREQ packet and this causes heavy control overhead. This is a drawback of using AOMDV because it has more message overheads during route discovery due to increased flooding.

A genetic algorithm (GA) is a search-based optimization technique based on the principles of genetics and natural selection. Fitness function and crossover techniques are the two main features of the genetic algorithm. Compared to other heuristic techniques, GA is different because it is stochastic rather than deterministic. Every member of the population of the GA represents a possible solution. Individuals are chosen depending on their fitness values [20]. Then, to produce the offspring, GA simulates the crossover genetic process found in nature by randomly exchanging part of these individuals' genetic information.

Basically in this paper, the AOMDV routing protocol is used to discover multiple routes from the source to the destination. We propose a novel fitness function (FF) as an optimization technique. Based on FF, we also propose a combination of AOMDV with a genetic algorithm (i.e AOMDV-FG). FF takes the collision of data packets, queue length, and link stability as key metrics for determining the most optimal and reliable path from source to destination. Therefore, the main contributions in this paper are:

- Proposing a new fitness function (FF) to implement a routing optimization technique. The FF includes three components as below:
  - The collision function is to evaluate data traffic in the links to avoid vulnerable routes,
  - The data congestion function at the bottleneck nodes comprising each route to reduce packet loss,
  - The links stability function to avoid routes with frequent topological change.
- Developing two multipath routing protocols based on AOMDV including AOMDV-FF and AOMDV-FG,
- Implementation of our protocols and comparing with recent protocols.

The remaining paper is organized as follows: Section II is all about the related work, Section III discusses the Proposed Protocol, Section IV presents the Methodology, Section V outlines Performance Evaluation, Section VI presents the experimental result and Section VII is about Discussion and Analysis and Section VIII gives the conclusion of the research.

II. LITERATURE REVIEW

AOMDV is a multipath routing protocol that is available on demand and supports mobile edge computing. When a node has a request to send, it first determines whether the route list contains a path to the destination node. A routing request is made if there is no path. The minimal hop count is used to choose the best path when there are multiple options for getting to the destination.

A routing protocol called Topological change Ad hoc On-demand Multipath Distance Vector (TA-AOMDV), which was suggested by authors in [21], focuses on reducing data traffic by utilizing QoS. This protocol's weakness is that it performs poorly in dynamic configurations that demand both route stability and node density. In general, this protocol only slightly improves performance whereas alternative protocols frequently perform far better.

FF-AOMDV, which provided the idea of choosing the effective route with the lowest energy consumption and the shortest distance, was proposed in [22]. Because this protocol utilized AOMDV, the transmission will use the next shortest path in the routing table in the event of any failure or link breakage. However, when compared to AOMDV, the performance of the FF-AOMDV model is not as high because it only took into account energy and shortest distance criteria, also the network lifetime improvement is fairly constrained.

Shadia et al, developed an energy-efficient steering convention in paper [23] that relied on the AOMDV directing convention and a bio-enlivened calculation known as Elephant Herding Optimization (EHO), In the creators' work, the consumed energy of hubs is streamlined by categorizing hubs into two classes. On choosing a course from the class of the fittest hubs with sufficient energy for transmission to reduce the likelihood of way disappointment and the growing number of dead hubs due to higher information loads. After each transmission round, the EHO refreshing administrator updates classes based on an isolating administrator who evaluates hubs based on energy remaining. The author's analyses demonstrate that the EHO results are better compared to other protocols. However, the delay and routing overhead are comparatively high because the node's clan needs to be updated frequently which rises the routing overhead and causes delay.

AOMDV [24] routing technology can offer a limited QoS guarantee by switching to a different path when the original one is blocked, allowing communication to proceed. However, switching to alternative paths causes a higher routing overhead as more packets will be required for route maintenance. In [25], Chen et al. proposed the QoS-AOMDV routing protocol to improve QoS support. To select high-quality pathways, this protocol collects cross-layer data on residual energy and queue length. However, the packet delivery ratio is not that high because of data collisions and this increases the delay as well.

In [26], it was proposed a routing protocol in MANETs. Random data packet loss and connection failure are likely to result from node mobility. Energy demand will increase as more data is transmitted back and forth. The authors presented a fitness function that takes into account the distance between the source and the destination nodes, the volume of traffic, and energy conservation. The fitness function uses a congestion control method called TCP CERL to avoid congested paths. The method can determine whether the degradation was brought on by random or congested loss. The optimal routes with the highest fitness are chosen using the AOMDV algorithm, which is integrated with the fitness function. When deciding on the best fitness route, there are some considerations to make, including a short route, the amount of energy, and the quantity of data traffic even if a data packet is dropped randomly. However, this method did not consider the reliability of the routes in the sense of data collision rate and link stability.

The method in [27] suggests a multipath routing protocol based on link stability. The link stability probability is calculated by the protocol using the mobility model and the length of the routing queue. This increases the link's probability of stability. The distance between nodes and the routing survival time are well-balanced. However, the energy consumption of nodes is high because frequent changes in path cause more nodes to participate in maintaining the stability of the given network.

Ad hoc On-Demand Multipath Distance Vector Routing has a congestion control strategy proposed by Vidwans et al. [28]. To enhance the network performance, the method employs a rate-based data transmission scheme and queue-based congestion control. The outcomes demonstrated improved packet delivery and reduced control overhead. However, the throughput of the system is comparatively low due to high packet loss which occurs due to collisions.

Traffic congestion and link failure are one of the most crucial problems in MANETs. The purpose of the network should be to deliver data packets from source to destination with minimal end-to-end delay. But this is difficult to achieve when we have congestion on the intermediate node, as congestion will increase the queue length and in turn cause more delay. As a result, [29] proposed an MQAM (mobility and QL aware multipath) routing technique based on the Multiple Criteria Decision Making (MCDM) measure. The results show that the suggested MQAM routing technique is superior to the traditional Multipath-Optimized Link State Routing (MP-OLSR) routing approach in terms of performance parameters like throughput, and PDR. However, the delay is comparatively high due to packet loss.

To get rid of congestion and clustering in Wireless Sensor Networks (WSN), authors of [30] presented a unique protocol called Congestion-Aware Clustering and Routing (CCR).

In [31], sender-side congestion control and model-based capacity prediction for TCP traffic over TDMA-based MANETs with no conflict were proposed. Both protocols offer effective congestion avoidance routing strategies, but they failed to account for random packet loss, which would have unduly shrunk the congestion window.

MANETs lack a central coordinator, hence wireless bandwidth distribution among mobile nodes must be organized and decentralized. Ad hoc networks frequently use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and its equivalents. However, the ''hidden terminal'' issue affects all of these CSMA/CA-based MAC schemes [32]. The foundation of ubiquitous computing is the mobile ad hoc network. Comparing an ad-hoc network to other traditional communication networks, the difficulties are far more complex. In [33], authors proposed to replace the hob count in AODV with link quality and collision count. This mechanism utilizes AODV which is a legacy protocol providing a single path. In case of links failure, the routing discovery process should be initiated and this would enlarge the latency and route overhead.

In [34], a hybrid GA-Hill Climbing method is used in the Genetic Algorithm with Hill Climbing (GAHC) routing protocol. Routes are selected based on the calculation of cluster heads (CHs) that use a projected hybrid protocol and the aggregate properties of the best path such as throughput, latency, and node connectivity. This proposed method offers a maximum throughput, detection rate, and packet delivery ratio with minimum energy and a delay time. However, this method assumes nodes with low mobility speed.

Comparison-based research on the performance improvement of routing algorithms for wireless sensor networks was presented by Muruganantham and El-Ocla [35]. There have been two main experimental cases using Djekstra Algorithm and a genetic algorithm. However, these methods assume low node mobility speed.

In [36] and based on OLSR, an artificial immune system (AIS-OLSR) protocol was proposed where the best route is selected using three criteria: hop counts, intermediate nodes energy content, and source to destination nodes distance. This protocol could increase network efficiency in terms of end-to-end latency and throughput. However, the energy consumption required for route calculation is a major concern of this protocol.

In [37], it was suggested a multipath quality of service multicast routing protocol (SR-MQMR) is stable for mobile ad-hoc networks. This mechanism considers node signal strength in the strategy to initially choose the most stable links while taking the needed bandwidth into account. The SR-MQMR protocol used fewer time slots than the MQMR protocol during the routing process and this increases the success ratio. Furthermore, reliability was significantly improved as a result of selecting stable routes. However, the frequent change in network topology and node random velocity affect the node's signal strength and reduces the network performance by affecting the packet delivery ratio.

The study in [38] presents novel link connectivity metrics (LCM) and path distribution analysis (PDA) methodologies to measure path stability when mobile nodes are traveling at a consistent speed and adopting a random trajectory. In terms of the chance that a connected link will remain connected and the likelihood that it will be recovered, the proposed method finds that the link expiry time, relative velocity, link connectedness, and link stability metrics affect surrounding nodes' LCM tactics. The effectiveness of the suggested LCM and PDA methodologies is demonstrated by analytical and simulation findings that accurately estimate path stability under topology change, consequently boosting global network connection. However, optimum values of the link expiration period cannot be identified as the length of this period causes more delay whereas the shorter of this period causes higher routing overhead in the network.

The key focus in [39] is to locate MANET neighboring nodes to build multipath routing in various mobility patterns. With minimal communication time, it also manages data forwarding and packet scheduling to balance the load. The phases of stable node prediction, stability determination, route search, and packet dissemination are explained in the proposed study. The stable nodes from the source to the destination are connected to calculate the optimum route. The route recovery procedure starts when a routing link fails. As a result, without any intervention, data packets are distributed over many pathways. An experimental study demonstrated that this method has a very low optimization performance due to inaccurate convergence. In addition, the energy consumption of every node is high as data packets are distributed through multiple pathways simultaneously and only one out of these pathways is required.

III. THE PROPOSED METHODOLOGY

A. PROBLEM STATEMENT

Data collision is one of the most common traffic problems which affect the ability of a network to transfer data and perform efficiently. In MANETs, all network nodes are constantly moving in random directions with various speeds so there is a very high possibility of data collision and this in turn affects the network performance. Additionally, because of such continuous node mobility, data packets often drop and links are broken so the route discovery process is triggered frequently. As a result, data congestion at the intermediate nodes frequently happens. This would affect negatively the performance in terms of end-to-end delay, node energy, and link stability. It is needed to probe a mechanism to select a reliable route that avoids links that possibly encounter these traffic problems.

B. PROPOSED SOLUTION

To avoid unstable links or those links with traffic problems (congested or links with high collisions rate), we propose a solution that optimizes routes using a genetic algorithm. In this regard, we introduce a new fitness function. We apply

our mechanism on the routes returned by the AOMDV protocol.

C. FITNESS FUNCTION

So the first component of our fitness function is collision avoidance and it is denoted by F_c. To find whether a route has collision or not we use CTS/RTS mechanism

- Collision Detection Using CSMA/CA with RTS/CTS Mechanism:

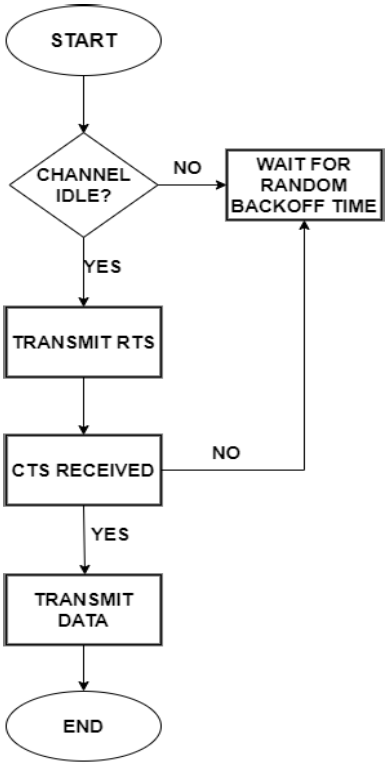


FIGURE 1. CSMA/CA using RTS/CTS mechanism.

Figure 1 explains the use of the RTC/CTS mechanism. Initially, we check whether the channel is idle or not. If it is not idle we wait for a random backoff time and after that backoff time has passed we re-check whether the channel is available or not. Once the channel is available, the sender node will send the Ready to Send (RTS) packet to the receiver node. If the receiver node is not available, we again wait for a random backoff time and re-check after being elapsed. If the receiver node is available, it will send a Clear to Send (CTS) packet back to the sender node. Once the sender node receives this packet, it will start its transmission for the data packet. This ensures that the channel is available for communication and avoids collision at any instance.

In this case, the sender node sends a hello message to the nodes of a given route returned by AOMDV. We propose that if no CTS is received, then $F_c = 0$ which means collision is detected. Otherwise, CTS is received within the round trip-time (RTT) and this means that there is no collision is detected, and the formula for that is:

$$F_c = \begin{cases} 1/RTT, & \text{CTS is received} \\ 0, & \text{No CTS is received.} \end{cases} \tag{1}$$

where F_c is the fitness function based on packets collision.

- Queue Length:

Here, we calculate the queue length for each node in a given route returned by the AOMDV mechanism using equation (2) [26], where BW is the bandwidth of the bottleneck link, T is the smallest RTT and Q is the queue length.

$$Q = (RTT - T)BW \tag{2}$$

Now, set the dynamic queue length threshold to N, where A is constant between 0 and 1 and Q_{max} is the largest value of the queue length.

$$N = A \times Q_{max} \tag{3}$$

The comparison between Q and N is made to decide the congestive status of the network.

If $Q > N$, packets may be dropped along a particular route due to predicted traffic congestion at one of the route's nodes. In this situation, it is best to avoid and remove this route from the optimum routes.

If $Q \leq N$, it means that based on the values of the other fitness function components, the evaluated route may be chosen to enter the pool of the best routes.

We provide a technique for the fitness function where the value of the congested fitness function component F_q will either have some value or reset to 0, and this is determined based on the condition $Q \leq N$.

The value is determined using equation (4), where B is the buffer size and indicates whether $Q \leq N$ is true, which implies that the route can accept packets for data transmission. If not, the route likely has congestion at one or more of its nodes, therefore we simply set the value of F_q to zero.

$$F_q = \begin{cases} 1 - \frac{Q}{B}, & Q \leq N \\ 0, & Q > N. \end{cases} \tag{4}$$

Lastly, we calculate the link stability and for this, we use the concept of Link Break Probability (LBP) and Path Stability Probability (PSP).

- Link Break Probability (LBP):

It is challenging to predict when the MANET link may break. But by comparing the recent and current signal levels, we can estimate the link's relative stability. The signal strength varies with distance, so measuring link reliability by distance is a reasonable metric. To create an analytical model, some assumptions must be made for simplicity's sake. We assume that all nodes move in a region with the same movement parameters and that the node movement model is a Random Waypoint Mobility

Model (RWMM). Within the area, all nodes are dispersed equally in their original places. The cumulative distribution function (CDF) of the probability distribution function (pdf) of the distance between two nodes, which follows the normal distribution, is as follows:

$$CDF_d = P_{(d \le r)} \cong \frac{r}{R}, 0 \le r \le R \tag{5}$$

Equation (5) [21] in the RWMM represents the probability density function of the distance between two nodes (r) exceeding the transmission range (R).

$$pdf_{2node}(r) = \frac{4}{\pi R^2}.\sqrt{R^2 - r^2}, 0 \le r \le R \tag{6}$$

$$LBP_{(r,R)} = \int_0^R P_{(d>r)}.pdr_{2node}(r)\ .dr \tag{7}$$

$$= \int_0^R (1 - CDF_d(r)).pdr_{2node}(r)\ .dr \tag{8}$$

$$\approx \int_0^R (1 - \frac{r}{R}).\frac{4}{\pi R^2}.\sqrt{R^2 - r^2}.dr, \tag{9}$$

To reduce computational overhead,

$$LBP_{(r,R)} \approx 1 - e^{(-\frac{r}{R})}, 0 \le r \le R \tag{10}$$

Path Stability Probability (PSP):
When a node gets an RREP from the destination node, the Path Stability Probability value is retrieved, and equation (10) [21] is used to calculate the Link Break Probability (LBP) value of the link between the two nodes, and hence we calculate the fitness function of the link stability F_s.

$$PSP_i = \prod_{l=1}^{L}(1 - LBP_l) \tag{11}$$

$$F_s = PSP_i \tag{12}$$

For route i, PSP is calculated for each link l contained in the set of links L. To determine the new PSP value and update the PSP, use equation (11). Finally, equation (12), will be used to select the most stable path out of the several routes returned by the AOMDV protocol.

As seen in Algorithm 1, the fitness function is the sum of the parameters i.e average of collision, the average of queue length, and the average of Link Stability. The formula for the fitness function is mentioned below:

$$FF = F_c + F_q + F_s \tag{13}$$

where F_c is fitness for collision, F_q is fitness for queue length and F_s is the fitness of link stability. We sort FFs in descending order for all routes from the source to the destination and select the route with the highest FF value.

As we see in Figure 2, we may have multiple links (e.g., $L1$, $L2$, $L3$, $L4$) from the source S to the destination D. We calculate the value of F_c, F_q, and F_s on each link and denote it with F_x. Lastly to compute the threshold value we take the average of each component. (I.e. F_{cavg}, F_{qavg} and F_{savg}) by equation (14). We set this average value as our threshold value and check whether each component has a fitness value greater than the average value in algorithm 1.

$$F_{xavg} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} F_{xij}}{n \times m} \tag{14}$$

where F_{xij} is F_c, F_q, or F_s in each j link out of m links comprising an i route of n routes.

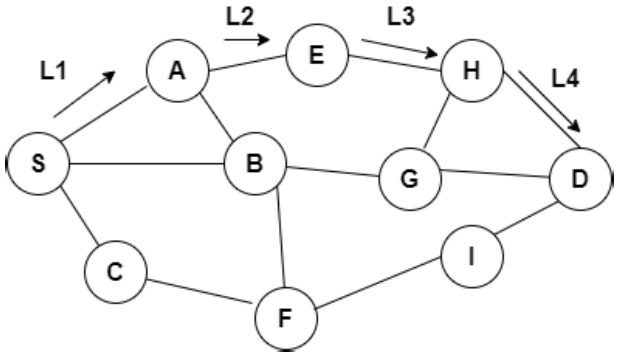


FIGURE 2. AOMDV-routing-protocol.

IV. METHODOLOGY

Firstly all nodes have unique identification numbers as well as an equal amount of energy. Afterward, source and destination nodes are selected in the network and also perform RREQ and RREP transmission between the source and the destination nodes. Let's understand the route discovery and route maintenance process.

A. ROUTE DISCOVERY PROCESS

Flooding leads to the finding of the passage. To complete the route discovery procedure, route request (RREQ) and route reply (RREP) packets are used. A node first evaluates the entries in the routing table when it has to transmit a packet to a specific destination. If the packet has an expected path to the target, it will forward it to the next hop address; otherwise, it will broadcast the route discovery process to all of its nearby nodes using an RREQ packet. Source address, broadcast ID, source sequence number, a destination address, destination sequence number, and hop count are all contained in the RREQ. By using a combination of the source address and sequence numbers (SNs), RREQ can be uniquely recognized.

The intermediate node matches the SN contained in its routing table with the sequence number contained in the RREQ packet after receiving it. If both SNs mismatch, the RREQ will be rebroadcasted to the next nearby nodes. Otherwise, the current intermediate node sets up a reverse path using the sequence number greater than RREQ's SN, and stores the reverse path entry in its routing. The reverse path entry includes the IP address of the receiving node, the source IP address, the source SN, the number of hops to the source node, and the RREQ source IP address. The backup path is then utilized to deliver an RREP to the node that received the prior RREQ. Flooding is not allowed by unicast

routing for route replies. To prevent routing loops, *SN*s are utilized to determine the most recent item in the routing table [40].

As in [41] and to update the routing table, assume the destination node D and an arbitrary node i in Figure 2. Whenever the SN of D at i is updated, the corresponding advertised hop count is set. For such SN of D, consider $hop\_count_{ik}^{D}$ denotes the hop count of kth route (for a given k) in the entry of the routing table at i for D, that is $(next\_hop_{ik}^{D}, last\_hop_{ik}^{D}, hop\_count_{ik}^{D}) \in route\_list_{i}^{D}$. When the node i initiates route advertisement for D, the hop count is updated as in equation (15), where A is the advertised hop count.

$$A_i^D = \begin{cases} \max\limits_{k}(hop\_count_{ik}^{D}), & i \neq D \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

The AOMDV route is updated whenever a node receives a route advertisement. Accordingly, AOMDV selects the best route based on the number of hops only regardless of the reliability of those routes in terms of traffic conditions and link stability. This motivates us to enhance the network performance and use the GA as explained below.

B. ROUTE MAINTENANCE PROCESS

Route maintenance is accomplished by periodically broadcasting HELLO messages to its neighbor nodes and sending Route Error (RERR) packets. The absence of HELLO messages from the receiving node indicates a link failure. If the failed route is still needed, the source node must restart the route discovery procedure. A node sends RERR to its predecessor node when it cannot transfer a packet to a certain destination [42]. As a result, whenever a node receives a RERR packet, it marks its destination table as invalid, sets the destination entry to 0, and deletes the specific route entry. As a result, the source node starts the route discovery procedure again.

In our mechanism, once multiple routes using AOMDV are received at the source node, we perform collision detection using CSMA/CA through RTS/CTS mechanism and find whether a collision is present or not using equation (1). The intermediate node estimates the queue length by equation (4) and links stability by equation (12) through the signal strength of the received RREP.

Next, we calculate the fitness value for each route as shown in Algorithm 1 and use equation (13) and select the route having the highest fitness value as the most efficient path by using the genetic algorithm (GA).

The five-step processes of the Genetic Algorithm including initialization, fitness function, selection, crossover, and mutation are elaborated in the following steps.

- Initialization:
  The genes are initialized within variable bounds. All fitness values are initialized to zero for each member of the population. Values are randomly generated between the bounds for each gene in the population based on Algorithm 2.

Algorithm 1 Fitness Calculation of Each Route

Input: For each route received from AOMDV-FG
F_c = Collision Function Component of FF
F_q = Queue Length Function Component of FF
F_s = Link Stability Function Component of FF
n = no. of possible routes
Output: Array of Fitness Function Values

foreach (i=0; i <= n; i++)
  F_c = equation (1)
  F_q = equation (4)
  F_s = equation (12)

  F_{xavg} = equation (14)

  if $(F_c \geq F_{cavg})$

    if $(F_q \geq F_{qavg})$
      if $(F_s \geq F_{savg})$

        $FF = F_c + F_q + F_s$
      end if
    end if
  end if
end foreach

In this regard, there are various parameters such as:

- ⇒ Genes: Individual nodes in a path,
- ⇒ Popsize: Popsize is the population size which means the total number of available routes between two end nodes; i.e, from source to destination,
- ⇒ C_r: It is the probability where routes may be a crossover,
- ⇒ C_m: It is the probability that a node in a route will be mutated,
- ⇒ SurvivorSel: According to the survival selection rule, a route may be accepted as an alternative depending on its fitness,
- ⇒ GensNoChange: The array of potential elite routes is sorted in descending order using the fitness values at this point in the route search process. The elite route is the route with the highest fitness value.

- Fitness Function:
  As seen in Algorithm 1, the fitness function is defined as a sum of three components that are the fitness of collision, the fitness of queue length, and the fitness of link stability. In our proposed protocol fitness function is given in equation (13).
- Crossover C:
  In this stage, every pair of routes is coupled and crossed over using the probability C_r. Nodes are switched between each couple of routes with high fitness scores and accordingly one or more offspring can be produced.

- Mutation M:
  This process is applied on the routes returned by the AOMDV and the crossover. In this phase, the order of nodes is changed in the same route using the probability C_m. New routes produced by crossover and mutation are evaluated in the survivor select stage.
- Survivor Selection:
  Here the selection function is called Selector which is defined in equation (14). This will produce the elite route's model. The routes with low fitness values are removed and new routes are created using Algorithm 2. This guarantees that the best member will always survive.

Algorithm 2 AOMDV-FG Routing Algorithm

Input: Multiple Routes
Output: Efficient Array of Routes
$C_r = 0.5$
$C_m = 0.1$
$E_r[]$ = Efficient Path
P_r = Present Route
O_r = Old Route
$N_r[]$ = New Route
FF = Fitness Function
PopSize = Population of routes
while (PopSize)
    Crossover C (P_r, O_r, C_r)
    Mutation M (P_r, O_r, C, C_m)
    Fitness (Set of N_r)

    foreach (N_{rf} set of routes)
        if (N_{rf} >= O_{rf})
            $E_r[] \leftarrow N_{rf}$
        end if
    end foreach
end while

Below we summarize the stepwise process of our proposed protocol AOMDV-FG in Algorithms 1 and 2. Figure 3 depicts the steps our routing protocol takes to build and choose routes for forwarding data packets.

1) AOMDV protocol returns an array of possible routes from the source node to the destination node. These routes are considered popsize. Here routes that have a minimum hop count will be taken into consideration.
2) We calculate the fitness value of each route using the fitness function FF in equation (13). By using the Elitism method through equation (14), we select routes with the highest fitness value and consider these routes as parents for performing crossover in the next step and all other routes are dropped.
3) Next, we perform the crossover process on parent routes to get new child routes with crossover probability C_r.

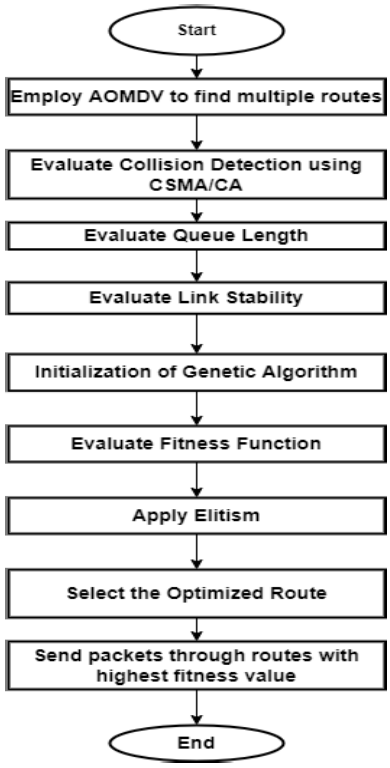


FIGURE 3. Flowchart of proposed protocol.

4) Next, we perform a mutation process on these child routes to get more routes with mutation probability C_m.
5) Here, we again use our FF to calculate fitness values for these generated routes. The routes having higher fitness values compared to parent routes are selected and the rest are dropped. This step is called survivor selection.
6) Store all potential routes from parent routes as well as child routes in an array Er.
7) Finally we sort all the entries in descending order so the route having the highest fitness value comes at the top and this is considered the most efficient route from the source to the destination.
8) Now in case there is a link breakage the route with the second-best fitness value is selected as the most optimum and so on.

To better understand our algorithm, let's take into account the network shown in Figure 2. We assume that S is the source node and D is the destination node. As shown in Figure 3 and if there is no route available, source S goes through the route discovery phase where AOMDV selects routes with the minimum hop count to D. Node S sends an RREQ to neighboring nodes A, B, and C which in turn send RREQs to their neighboring nodes E, G, F. Then again this will initiate an RREQ from G to D and other nodes will continue this process until reaching node D. The first sequence is considered as S-B-G-D. This is the shortest path and packets will be sent through this path. If any link of this path fails, packets will be sent through the second path S-A-E-H-D. If this also fails it selects the remaining possible paths through S-C-F-I-D.

Seq1: S-B-G-D
Seq2: S-A-E-H-D
Seq3: S-C-F-I-D

In the FF section, it will calculate fitness for every single path. For instance, the fitness value of Seq1, Seq2, and Seq3 are 5.6, 9.3, and 9.1, respectively. Through the "Selection" phase, the average FF is 8 so all routes with lower scores than the average will be excluded which is seq1 in this case. Based on the crossover and mutation processes, new offspring are generated i.e:

Seq4: S-B-F-I-D
Seq5: S-B-G-H-D

The offspring's FF evaluation results, which are 9.7 and 9.6 for Seq4 and Seq5, respectively, will be used to determine whether or not to include them in the population. Seq5 is the best route and will be selected because of its highest score. Seq4 will be considered next if any of Seq5 links or nodes fail during the data communication.

V. PERFORMANCE EVALUATION

A. SIMULATION MODEL AND PARAMETERS

To evaluate the effectiveness of the proposed routing protocol under various node densities, node speeds, and traffic loads various parameters and their values are utilized in Table 1.

TABLE 1. Simulation parameters.

Parameter Type	Parameter Value
Simulator	Ns-3
Number of Nodes	100
Initial Energy	100 Joules
Simulation Time	100 Seconds
Topology Dimensions	1000 m ×1000 m
Crossover Probability	0.5
Mutation Probability	0.1
Mobility Model	Random Way Point Model
Packet Loss Rate	0%
Faulty Node	0%
Mobility Speed	10 m/s
Mac Type	IEEE 802.11
Traffic Type	Constant Bit Rate (CBR)
Compared Protocols	TA-AOMDV, EHO-AOMDV

As shown in Table 1, the number of nodes taken into the consideration is 100, where all the nodes are having an equal amount of nodal energy initially assigned as 100 Joules. The simulation area where nodes move randomly is 1000 m × 1000 m with a simulation time of 100 seconds. Nodes are moving randomly in speed and direction. The MAC layer protocol is IEEE 802.11 whereas traffic type is taken as CBR i.e Constant Bit Rate. These parameters assumptions agree with those used in [7], [23], [43], and [44].

B. PERFORMANCE METRICS

The following performance metrics were used in the simulation experiments [21], [23], [26]:

1) PACKET DELIVERY RATIO (PDR)

It is the proportion of data packets that have arrived at the destination node as opposed to those that were sent from the source node. PDR provides information on how well a protocol delivers packets across the network. Following is how PDR is calculated:

$$PDR = \frac{\sum P_d}{\sum P_s} \times 100 \tag{16}$$

where P_d indicates the number of packets delivered and P_s is the number of packets sent.

2) THROUGHPUT (Th)

It measures the total amount of bits that have been successfully transmitted across the network and is stated in megabits per second (Mbps). It acts as a performance and quality indicator. Fewer packets were dropped during data transfer from the source to the destination when there was a high throughput. This is how it is calculated:

$$Th = \frac{\sum B_r \times 8}{T} \times 10^6 (Mbps) \tag{17}$$

where B_r is the total amount of received bytes, and T is the simulation time.

3) END-TO-END DELAY (E2ED)

End-to-end delay indicates the time spent for a packet to be transmitted from source to destination. E2ED is calculated as:

$$E2ED = \frac{\sum_{i=0}^{n} (t_i^{received} - t_i^{send})}{n} \tag{18}$$

where $t_i^{received}$ represents the time when the destination node received the ith packet as of the current time. t_i^{send} represents when the source node sends the ith packet in the current time, and n is the number of packets that were successfully received.

4) ENERGY CONSUMPTION (EC)

It is the total quantity of energy used by all of the network nodes throughout the simulation period. The formula is as follows.

$$EC = \sum_{i=0}^{m} I_i - E_i \tag{19}$$

where I_i is the node's initial energy of ith node out of m nodes of a given route and E_i represents the remaining energy at the end of the simulation.

5) ROUTING OVERHEAD (R)

The number of routing packets that must be broadcast to deliver data packets via route discovery and route maintenance is known as routing overhead. The network's robustness is impacted by the routing overhead in terms of node power consumption and bandwidth utilization.

$$R(\%) = \frac{RO_p}{RO_p + DT_p} \times 100 \tag{20}$$

where R is the routing overhead, RO_p indicates the number of routing packets and DT_p means the number of data packet sent.

6) COLLISION RATE (CR)

Collision Rate indicates the rate at which data packets collide or are lost in the collision. The formula for collision rate is mentioned below:

$$CR = \frac{CC}{OPkts} \tag{21}$$

where CR is the collision rate, CC is the collision count and $OPkts$ is the number of out packets.

VI. EXPERIMENTAL RESULTS

In our implementation, we normalize FF components to their averages defined in equation (14). This implies that the unity is the minimum value for each FF component in Algorithm 1.

A. PACKET DELIVERY RATIO

Packet Delivery Ratio is evaluated versus the number of nodes and simulation time in Figures 4 and 5, respectively. During the experiment, we can see that as the number of nodes or simulation time increases, more packets are required for route discovery and route maintenance. It augments the traffic in the network which leads to congestion at the intermediate nodes or collision at links. This leads to more dropping or collided packets and thus affects the network badly. Still, it can be seen that our proposed protocols AOMDV-FG and AOMDV-FF attain a higher packet delivery ratio in comparison with AOMDV-TA and EHO-AOMDV. This is because these congested nodes or collisions will result in low FF scores and accordingly their routes will be avoided while this mechanism is not considered in other protocols. Based on Table 2, AOMDV-FG improves the PDR with 4.4%, 10.28%, and 15% compared to AOMDV-FF, AOMDV-TA, and EHO-AOMDV, respectively.

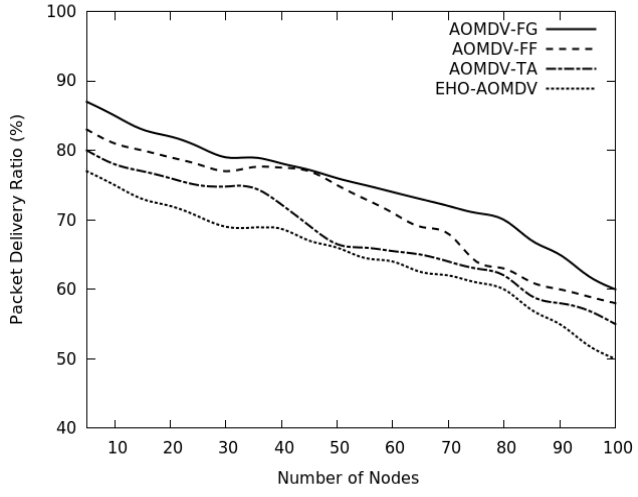


FIGURE 4. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for packet delivery ratio with the number of nodes.

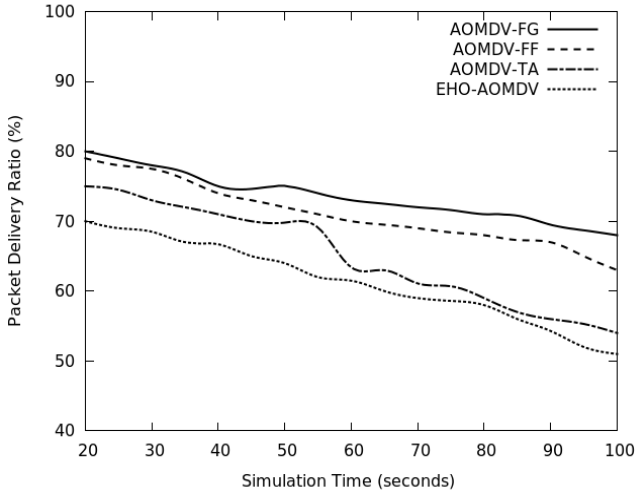


FIGURE 5. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for Packet Delivery Ratio with simulation time.

TABLE 2. Packet delivery ratio of Figure 4.

No. of nodes	AOMDV-FG	AOMDV-FF	AOMDV-TA	EHO-AOMDV
10	85	81	78	75
20	82	79	76	72
30	79	77	74.8	69
40	78.12	77.52	72.2	68.7
50	76	75	66.5	66
60	74	71	65.5	64
70	72	68	64	62
80	70	63	62	60
90	65	60	58	55
100	60	58	55	50
Sum	741.12	709.52	672	641.7
Gain %		4.4	10.28	15

B. THROUGHPUT

Throughput is evaluated through the number of nodes, faulty nodes (%), mobility speed (m/s), packet loss rate (%), and simulation time (s).

Figure 6 demonstrates how the number of nodes in a network affects the throughput. There will be more nodes accessible to transfer data packets as a network's nodes grow, which may result in higher congestion at the intermediary nodes and possibly more collisions. The throughput performance will suffer as a result. The likelihood of traffic problems including congestion and collision is decreased by our suggested protocols, AOMDV-FG and AOMDV-FF, which are centered on selecting the path with the highest connection stability and least unreliability.

Figure 7 elaborates on the throughput versus faulty nodes. Here we assume that faulty nodes may exist in the routes returned by AOMDV and we examine how each protocol will perform in various scenarios. There could be multiple reasons for faulty nodes such as battery power depletion or collision among mobile nodes. We are focusing on four different

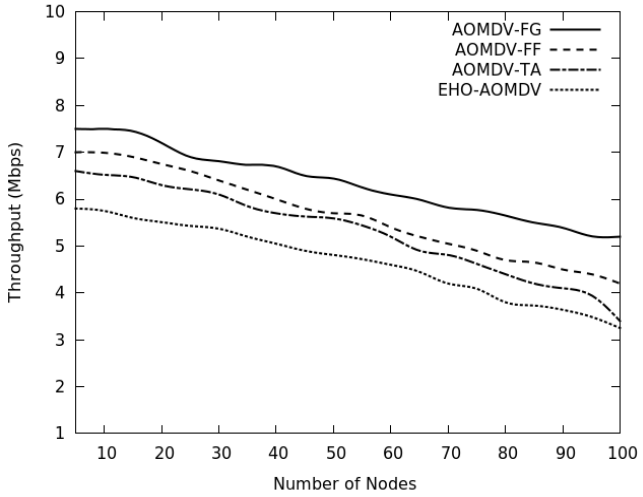


FIGURE 6. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for Throughput with the number of nodes.

possibilities (i.e. 5, 10, 20, 30%) of faulty nodes. As the number of faulty nodes increases, network performance degrades because with increasing the number of faulty nodes, fewer data packets will reach the destination and thus degrade the network throughput. However our proposed method provides a pool of alternative reliable routes that can be utilized to deliver the data efficiently compared to other protocols. This is because those routes having faulty nodes will be avoided as RTT, used in equations (1) and (2), is infinity.

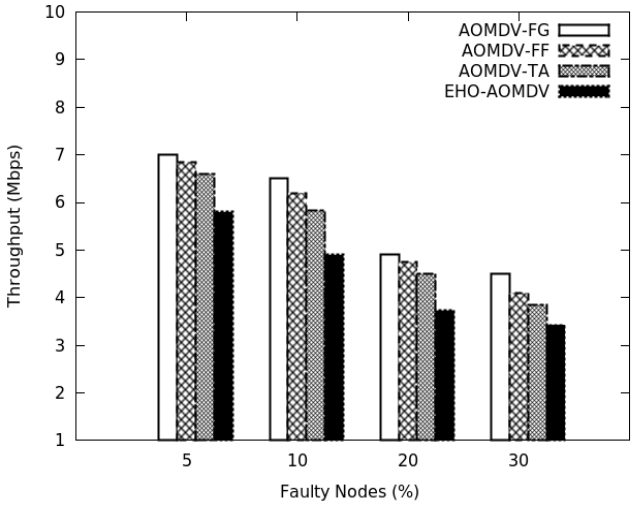


FIGURE 7. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for throughput with faulty nodes.

Figure 8 presents the throughput vs the mobility speed. Because of the frequent mobility of nodes, links usually are not stable. Our algorithm selects the most stable route where its nodes have the least mobility possibility with the lowest speeds. This performance efficiency is more obvious at the high node speed where such unstable routes are avoided in our protocols.

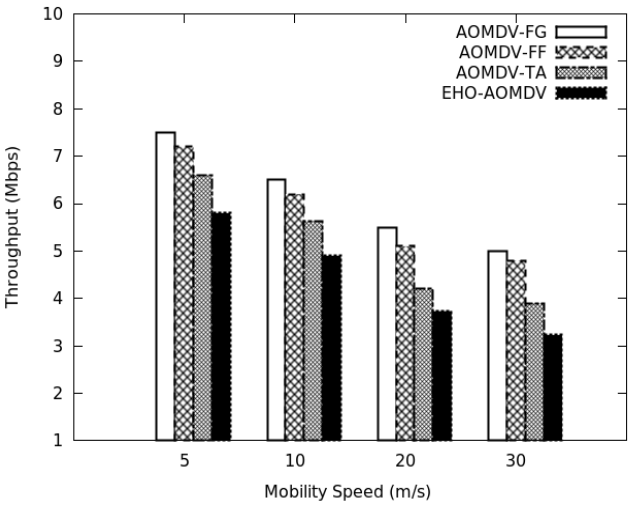


FIGURE 8. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for throughput with mobility speed.

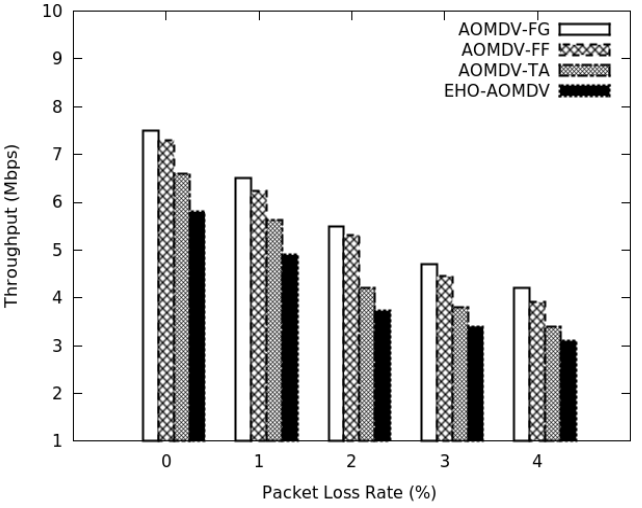


FIGURE 9. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for throughput with packet loss.

Figure 9 explains how the packet loss rate affects the throughput in a network. The packet loss rate is calculated by the total number of packets not received at the destination divided by the total number of packets sent from the source. Packet loss can be caused by data collision, less energy in the node, and high node mobility. Our proposed protocols AOMDV-FG and AOMDV-FF are performing better compared to AOMDV-TA and EHO-AOMDV because we are focusing on reducing the number of collisions in a given network. Based on Table 3, AOMDV-FG improves the throughput by 4.37%, 20.18%, and 35.69% over AOMDV-FF, AOMDV-TA, and EHO-AOMDV, respectively.

Figure 10 explains the effect of varying simulation time on the throughput in a given network. With time, the possibility

TABLE 3. Throughput vs Packet Loss of Figure 9.

Packet Loss Rate (%)	AOMDV-FG	AOMDV-FF	AOMDV-TA	EHO-AOMDV
0	7.50	7.30	6.60	5.80
1	6.50	6.24	5.63	4.90
2	5.50	5.31	4.20	3.73
3	4.70	4.45	3.80	3.40
4	4.20	3.91	3.40	3.10
Sum	28.4	27.21	23.63	20.93
Gain %		4.37	20.18	35.69

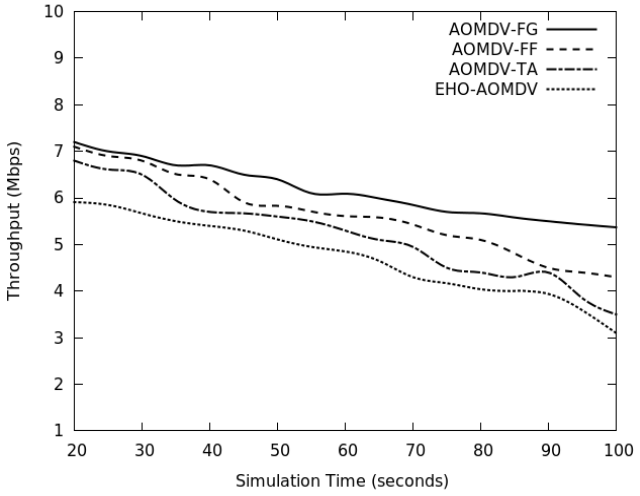


FIGURE 10. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for throughput with simulation time.

of traffic problems including data congestion and collision, due to random nodes mobility, increases and, therefore, the throughput declines. However, our protocols avoid such unreliable routes so the throughput has a better performance compared to other protocols.

C. END-TO-END DELAY

In Figure 11 and with the number of nodes, more traffic problems augment, and this in turn increases the data

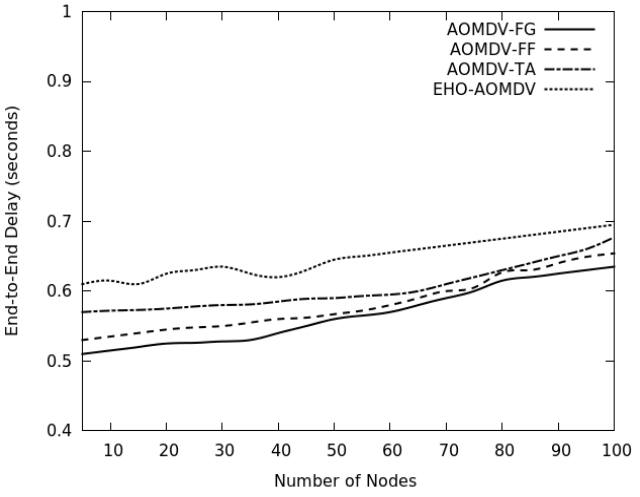


FIGURE 11. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for end-to-end delay with the number of nodes.

retransmissions. Also, this would require more nodes and processing time to find optimum routes. All these factors will be added to the end-to-end delay. Our proposed protocols require lower delay as the number of packet retransmissions reduces.

Figure 12 elaborates the effect of having faulty nodes on the end-to-end delay similarly as in Figure 7. The node may turn into being faulty before or during data transmission. If this happens during the data communication, a time delay will be consumed to inform the sender of the route disconnect, an alternative route will be explored and data retransmission is triggered. Hence this will enlarge the end-to-end delay. However, if a faulty node exists before data transmission, our protocols will avoid passing through those routes as indicated earlier.

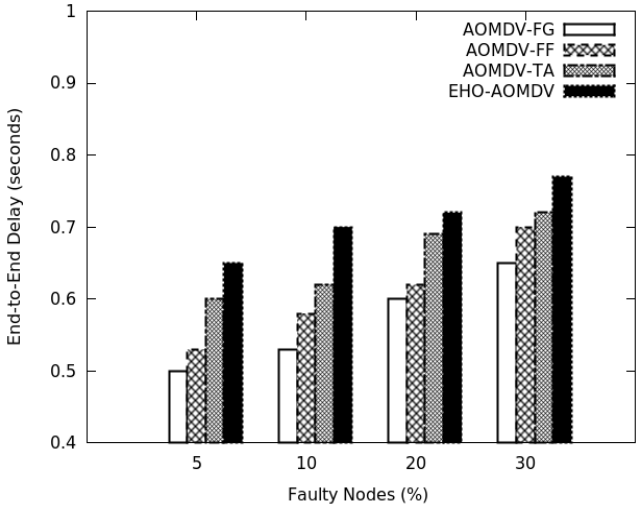


FIGURE 12. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for end-to-end delay with faulty nodes.

Because of nodes' mobility, routes would be likely lost and this may result in packets dropping. Data retransmissions would add to the end-to-end delay. Our protocols behave better than other competitors because those unstable routes are avoided as shown in Figure 13.

D. ENERGY CONSUMPTION

Our protocols reduce the energy consumption of the nodes in terms of minimizing the packet retransmissions as shown in Figures 14 and 15. With the number of nodes or time progress, a longer processing time is needed and this consumes more energy. Based on Table 4, AOMDV-FG saves energy of 10.75%, 61.96%, and 32.32% over AOMDV-FF, AOMDV-TA and EHO-AOMDV, respectively.

E. ROUTING OVERHEAD

Figures 16 and 17 show the routing overhead with various protocols. With the number of nodes or simulation time progress, the amount of RREQ messages increases flooding the network and this accordingly increases the overhead in the

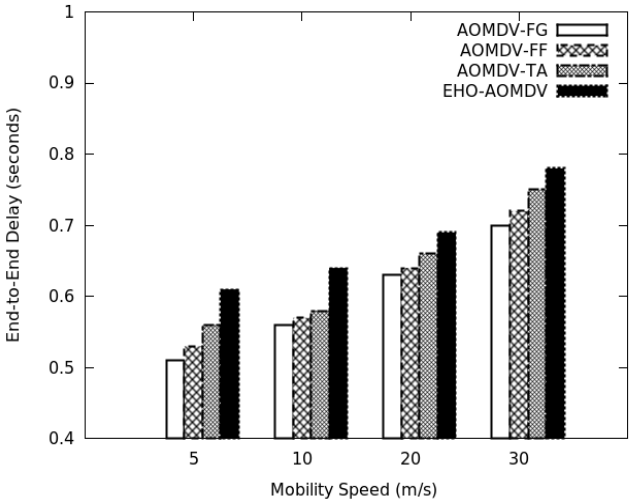


FIGURE 13. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for end-to-end delay with mobility speed.

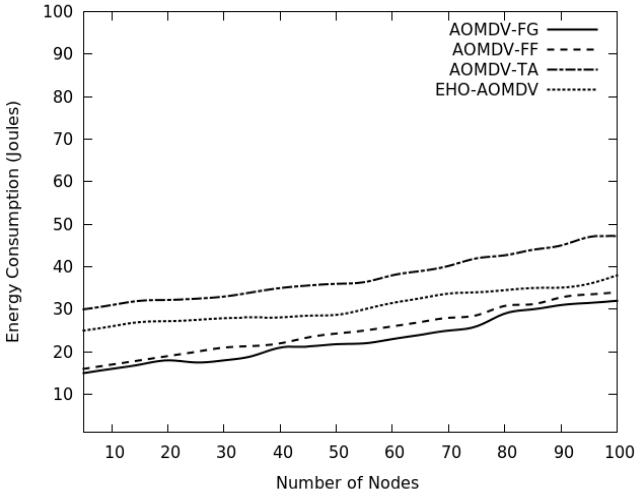


FIGURE 14. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for energy consumption with the number of nodes.

TABLE 4. Energy values of Figure 14.

No of nodes	AOMDV-FG	AOMDV-FF	AOMDV-TA	EHO-AOMDV
10	16	17	31	26
20	18	19	32.2	27.2
30	18	21	33	27.9
40	21	22	35	28.1
50	21.8	24.3	36	28.7
60	23	26	38	31.5
70	25	28	40.2	33.7
80	29	30.8	42.7	34.5
90	31	32.8	45	35.1
100	32	34	47.2	38
Sum	234.8	254.9	380.3	310.7
Savings %		10.75	61.96	32.32

network. This overhead augments when the route discovery process is triggered more frequently because of the node mobility and the instability of the routes. As already indicated earlier, our protocols optimize the routes based on the FF. As a result, the overhead with our protocols is lower than

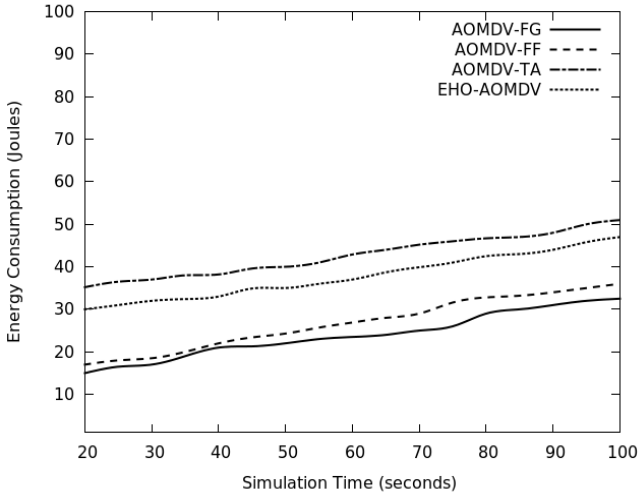


FIGURE 15. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for energy consumption with simulation time.

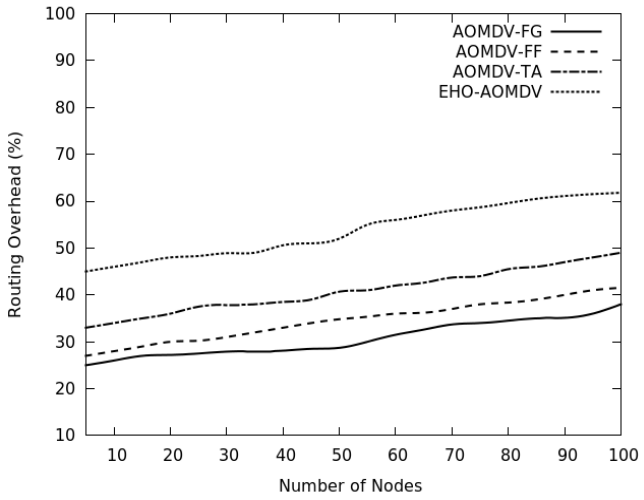


FIGURE 16. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for routing overhead with the number of nodes.

TABLE 5. Routing overhead of Figure 16.

No. of nodes	AOMDV-FG	AOMDV-FF	AOMDV-TA	EHO-AOMDV
10	26	28	34	46
20	27.2	30	36	48
30	27.9	31	37.90	48.9
40	28.1	33	38.5	50.6
50	28.7	34.81	40.7	52
60	31.5	36	42	56
70	33.7	37	43.7	58
80	34.5	38.36	45.5	59.6
90	35.1	40	47	61.1
100	38	41.53	49	61.8
Sum	310.7	349.69	414.3	542
Saving %		12.54	33.34	74.44

other algorithms. As shown in Table 5, AOMDV-FG reduces the routing overhead with 12.54%, 33.34%, and 74.44% compared to AOMDV-FF, AOMDV-TA, and EHO-AOMDV, respectively.

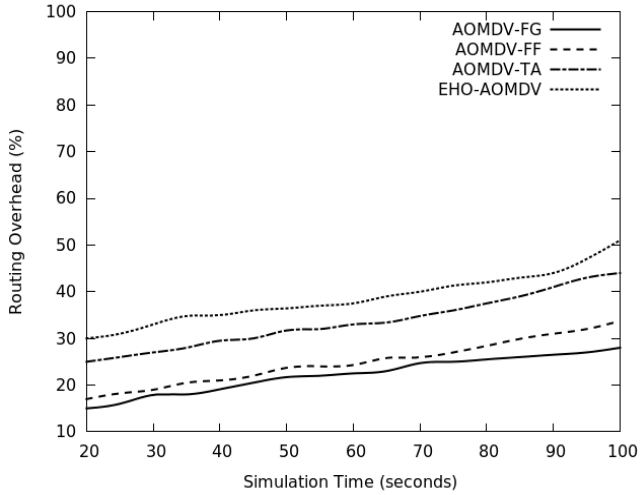


FIGURE 17. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for routing overhead with simulation time.

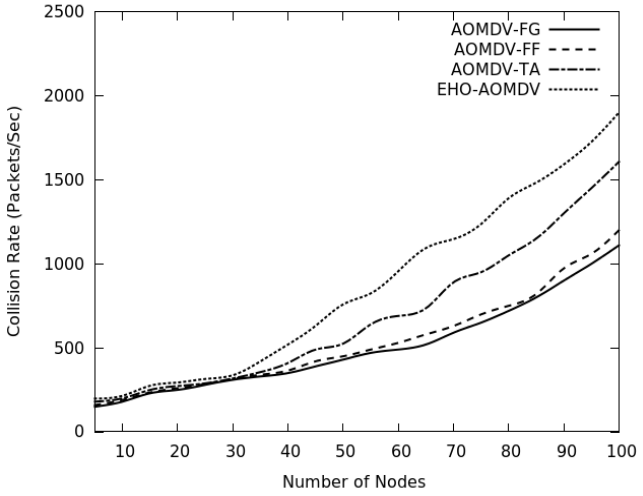


FIGURE 18. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for collision rate with the number of nodes.

F. COLLISION RATE

The collision rate in Figure 18 indicates the rate at which data packets collide or are lost in a collision. As the number of nodes increases, more data is to be communicated so collision possibility magnifies. Our protocol selects the route that has less collision possibility using the RTT mechanism in equation (1).

With the node mobility or faulty nodes' existence, routes more frequently disconnect. This increases the RREQ frames broadcast flooding the network and ergo more RTS/CTS exchange is utilized. In consequence, data collisions often occur particularly during the handshaking process as shown in Figures 19 and 20. Our protocols generate more reliable routes and hence this reduces the RREQ messages flood and RTS/CTS exchange occurs less minimizing the collisions rate.

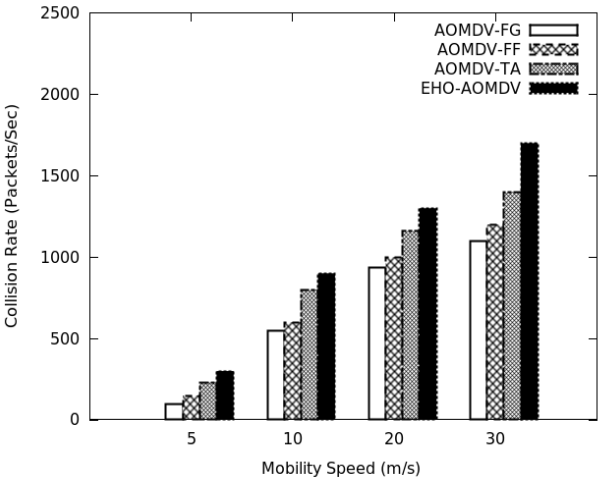


FIGURE 19. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for collision rate with mobility speed.

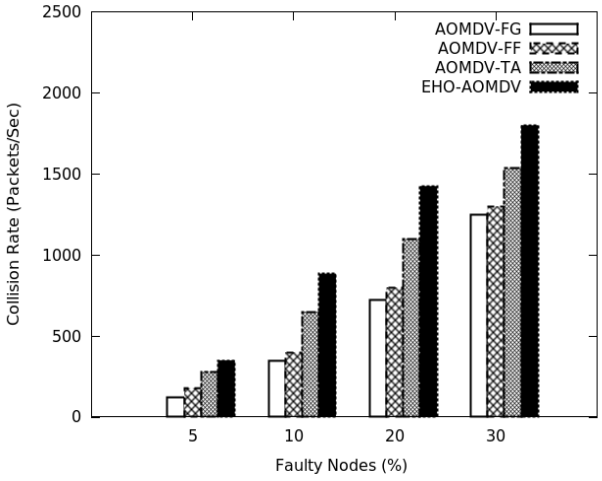


FIGURE 20. Comparison between AOMDV-TA, EHO-AOMDV with proposed protocol AOMDV-FG and AOMDV-FF for collision rate with faulty nodes.

VII. DISCUSSION AND ANALYSIS

The source node S sends an RREQ message to the neighbor nodes up the destination D if there is no route available. In Figure 21, D replies with RREP of multiple routes. Using TA-AOMDV [21], the cost of the route has been calculated as a function of node energy, links bandwidth, and queue length. The optimized route is the one with the lowest route cost and hence the lifespan of the network is extended. Returned routes are route 1 (S-A-E-H-D), route 2 (S-B-G-D), route 3 (S-C-F-I-D), and route 4 (S-B-F-I-D). S will select 2 as it has the least cost. High node density is one of the system's disadvantages. For example, if there are more nodes in a given area, the system may broadcast several requests concurrently and this congests intermediary nodes leading to longer delays and greater routing overhead. Frequent node mobility would result in data packet drops and collisions.

In [23], nodes are combined in clusters based on their inter-distance and their energies. Due to node mobility, the

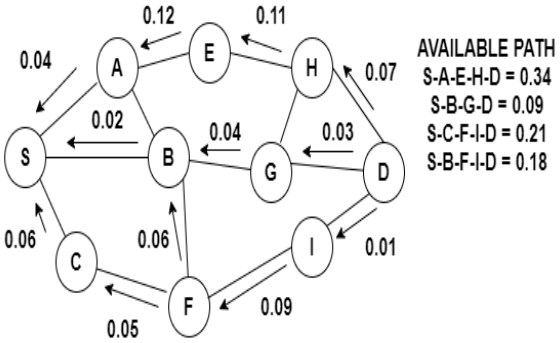


FIGURE 21. Cost associated with TA-AOMDV.

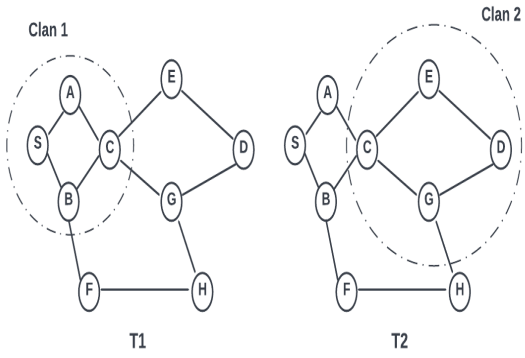


FIGURE 22. EHO-AOMDV at times T1 and time T2.

network topology changes, and as a result, there is a need to update the members of the clan. Clan members are updated according to the position of nodes and their residual energy. Nodes with more distance or less energy will be dropped from the clan and vice versa. In Figure 22 and at one time T1, some nodes form Clan 1. Later at time T2 and due to the nodes' mobility and topology change, some nodes from Clan1 are dropped and added to Clan 2. This ensures that at any given time, the nodes present in a given clan will have closer intra-distance and higher residual energy. However, this clustering concept acts as a drawback because if node "A" has a data packet and in which is removed from a clan, then that data packet will be dropped and the entire process needs to be repeated from the beginning. This will incur more damage to the network performance.

Our protocols are robust to a topology change in terms of link stability. Also, node congestion and data collision are considered. Our protocols select multiple reliable routes that can be utilized in case of a route disconnect. This greatly reduces data retransmissions and accordingly enhances the network performance in the sense of the throughput and the end-to-end delay. This in turn dwindles the routing cost and minimizes the overhead flood.

The GA computation would consume time to produce the optimized routes, however, the end-to-end delay with our algorithm is lower than other protocols as shown in Section VI.*C*. This is because our algorithm selects the most reliable routes and, therefore, the packet retransmissions will be minimized greatly. This also will reduce the energy consumption of nodes and the needed routing overhead packets as shown in Sections VI.*D* and VI.*E*, respectively. This in turn would maximize the lifespan of the network.

CONSLUSION

Due to the high mobility of nodes, data collision takes place and this results in packet loss and affects negatively the network performance by degrading its throughput. Random mobility of nodes leads to topological change and generates unstable links. Also, traffic congestion may happen at the bottleneck of the intermediate nodes and this produces data drops. In these cases, frame retransmission is triggered and thus augments the routing overhead and floods the network which makes the traffic problems worse. This in turn increases the end-to-end delay and node's energy consumption reducing the lifespan of the network.

In this paper, we utilize the routes returned by the AOMDV method and optimize these routes. We use CSMA/CA with CTS/RTS mechanism to detect and reduce the number of collisions in the selected routes. Our protocol also predicts the stability of the links and avoids congested routes. In this regard, we propose a fitness function and use a genetic algorithm to optimize routes returned by the AOMDV method in MANETs. Through our simulation experiments, we can see that our proposed protocols outperform recent competitors.

REFERENCES

[1] N. Singh, N. Hemrajani, and N. Blasie-Patrick, "Comparative analysis of single-path vs multipath routing: A case study of AODV and AOMDV protocols," *Impact Mobility Forecast Rural Kenya*, pp. 1–19, Aug. 2018, doi: 10.13140/RG.2.2.23985.28009.

[2] R. Singh, "An overview of MANET: Characteristics, applications attacks and security parameters as well as security mechanism," *Int. Res. J. Eng. Technol.*, vol. 5, no. 9, pp. 1–5, Sep. 2018.

[3] B. Aditya, A. K. Sharma, and A. Mishra, "Significance of mobile Ad-hoc network (MANET)," *Int. J. Innov. Technol. Exploring Eng.*, vol. 2, no. 4, pp. 2278–3075, 2013.

[4] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile Ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022, doi: 10.1109/ACCESS.2022.3144679.

[5] D. Zhang, G. Li, K. Zheng, and X. Ming, "An energy-balanced routing method based on forward-aware factor for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 766–773, Feb. 2014.

[6] Y. Richter and I. Bergel, "Optimal and suboptimal routing based on partial CSI in random Ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2815–2826, Apr. 2018.

[7] D.-G. Zhang, L. Chen, J. Zhang, J. Chen, T. Zhang, Y.-M. Tang, and J.-N. Qiu, "A multi-path routing protocol based on link lifetime and energy consumption prediction for mobile edge computing," *IEEE Access*, vol. 8, pp. 69058–69071, 2020, doi: 10.1109/ACCESS.2020.2986078.

[8] D. Manickavelu and R. U. Vaidyanathan, "Particle swarm optimization (PSO)-based node and link lifetime prediction algorithm for route recovery in MANET," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 107, Dec. 2014.

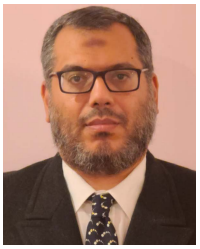
[9] R. Dixit and S. Kumar, "MANET: Challenges & application in real world," *Int. J. Latest Trends Eng. Technol.*, vol. 9, no. 3, pp. 42–46, 2018, doi: 10.21172/1.93.08.

[10] M. Bharti, S. Rani, and P. Singh, "Security attacks in MANET: A complete analysis," in *Proc. 6th Int. Conf. Devices, Circuits Syst. (ICDCS)*, Apr. 2022, pp. 384–387, doi: 10.1109/ICDCS54290.2022.9780760.

[11] V. K. Sharma and S. S. Bhadauria, "Mobile agent based congestion control using AODV routing protocol technique for mobile Ad-hoc network," *Int. J. Wireless Mob. Netw.*, vol. 4, no. 2, pp. 299–314, 2012.

[12] K. M. Zaini, A. M. Habbal, F. Azzali, S. Hassan, and M. Rizal, "An interaction between congestion-control based transport protocols and manet routing protocols," *J. Comput. Sci.*, vol. 8, no. 4, pp. 468–473, Oct. 2012.
[13] D. Krishnamoorthy, P. Vaiyapuri, A. Ayyanar, Y. H. Robinson, R. Kumar, H. V. Long, and L. H. Son, "An effective congestion control scheme for MANET with relative traffic link matrix routing," *Arabian J. Sci. Eng.*, vol. 45, pp. 6171–6181, 2020, doi: 10.1007/s13369-020-04511-9.
[14] H. Geng, X. Shi, X. Yin, Z. Wang, and S. Yin, "Algebra and algorithms for multipath QoS routing in link state networks," *J. Commun. Netw.*, vol. 19, no. 2, pp. 189–200, Apr. 2017.
[15] P. Goyal, V. Parmar, and R. Rishi, "MANET: Vulnerabilities, challenges, attacks, application," *Int. J. Comput. Eng. Manag.*, vol. 11, pp. 32–37, Jan. 2011.
[16] W. Xu, W. Liang, X. Lin, and G. Mao, "Efficient scheduling of multiple mobile chargers for wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7670–7683, Sep. 2016.
[17] K. Zheng and D. X. Zhao, "Novel quick start (QS) method for optimization of TCP," *Wireless Netw.*, vol. 22, no. 1, pp. 1–12, 2015.
[18] V. Kalpana, G. Saravanan, A. G. N. Julaiha, and R. Balamanigandan, "An intensify MANET based channel and QOS conscious routing using AOMDV," *Turkish J. Physiotherapy Rehabil.*, vol. 32, no. 3, pp. 1–14, 2022.
[19] B. Mathur and A. Jain, "AOMDV protocol: A literature review," *Int. J. New Technol. Res.*, vol. 4, no. 7, Aug. 2018.
[20] S. Jain and S. Sahu, "The application of genetic algorithm in the design of routing protocols in MANETs: A survey," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 4318–4321, 2012.
[21] Z. Chen, W. Zhou, S. Wu, and L. Cheng, "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET," *IEEE Access*, vol. 8, pp. 44760–44773, 2020.
[22] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy efficient multipath routing protocol for mobile Ad-hoc network using the fitness function," *IEEE Access*, vol. 5, pp. 10369–10381, 2017.
[23] S. Sarhan and S. Sarhan, "Elephant herding optimization Ad hoc on-demand multipath distance vector routing protocol for MANET," *IEEE Access*, vol. 9, pp. 39489–39499, 2021, doi: 10.1109/ACCESS.2021.3065288.
[24] M. K. Marina and S. R. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. IEEE 9th Int. Conf. Netw. Protocols (ICNP)*, Nov. 2001, pp. 14–23.
[25] J. Chen, Z. Li, J. Liu, and Y. Kuo, "QoS multipath routing protocol based on cross layer design for Ad hoc networks," in *Proc. Int. Conf. Internet Comput. Inf. Services*, vol. 4, Sep. 2011, pp. 162–165.
[26] 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, doi: 10.1109/ACCESS.2020.3027043.
[27] Z. Lin and J. Sun, "Routing protocol based on link stability in MANET," in *Proc. World Automat. Congr. (WAC)*, Aug. 2021, pp. 260–264, doi: 10.23919/WAC50355.2021.9559469.
[28] A. Vidwans, A. K. Shrivastava, and M. Manoria, "QoS enhancement of AOMDV routing protocol using queue length improvement," in *Proc. 4th Int. Conf. Commun. Syst. Netw. Technol.*, Bhopal, Apr. 2014, pp. 275–278.
[29] V. Tilwari, A. Bani-Bakr, F. Qamar, M. N. Hindia, D. N. K. Jayakody, and R. Hassan, "Mobility and queue length aware routing approach for network stability and load balancing in MANET," in *Proc. Int. Conf. Electr. Eng. Informat. (ICEEI)*, Oct. 2021, pp. 1–5, doi: 10.1109/ICEEI52609.2021.9611119.
[30] M. Farsi, M. Badawy, M. Moustafa, H. Arafat Ali, and Y. Abdulazeem, "A congestion-aware clustering and routing (CCR) protocol for mitigating congestion in WSN," *IEEE Access*, vol. 7, pp. 105402–105419, 2019.
[31] P. Pal, S. Tripathi, and C. Kumar, "Bandwidth estimation in high mobility scenarios of IEEE 802.11 infrastructure-less mobile Ad hoc networks," *Int. J. Commun. Syst.*, vol. 32, no. 15, p. e4080, Oct. 2019.
[32] Z. Na, L. Ningqing, and Q. Yu, "Improved RTS-CTS algorithm to solve mobile hidden station problem in MANET," in *Proc. Cross Strait Quad-Regional Radio Sci. Wireless Technol. Conf.*, Jul. 2011, pp. 812–815.
[33] N. R. Patel, S. Kumar, and S. K. Singh, "Energy and collision aware WSN routing protocol for sustainable and intelligent IoT applications," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25282–25292, Nov. 2021, doi: 10.1109/JSEN.2021.3076192.
[34] 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, doi: 10.1109/ACCESS.2021.3133882.
[35] N. Muruganantham and H. El-Ocla, "Routing using genetic algorithm in a wireless sensor network," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2703–2732, Apr. 2020.
[36] F. Sarkohaki, R. Fotohi, and V. Ashrafian, "An efficient routing protocol in mobile Ad-hoc networks by using artificial immune system," 2020, *arXiv:2003.00869*.
[37] M. Ghafouri Vaighan and M. A. Jabraeil Jamali, "A multipath QoS multicast routing protocol based on link stability and route reliability in mobile Ad-hoc networks," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 1, pp. 107–123, Jan. 2019, doi: 10.1007/s12652-017-0609-y.
[38] A. Naushad, G. Abbas, Z. H. Abbas, and A. Pagourtzis, "Novel strategies for path stability estimation under topology change using hello messaging in MANETs," *Ad Hoc Netw.*, vol. 87, pp. 76–99, May 2019.
[39] R. Hemalatha, R. Umamaheswari, and S. Jothi, "An efficient stable node selection based on Garson's pruned recurrent neural network and MSO model for multipath routing in MANET," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 21, Sep. 2022, doi: 10.1002/cpe.7105.
[40] A. Hassanat, K. Almohammadi, E. Alkafaween, E. Abunawas, A. Hammouri, and V. B. S. Prasath, "Choosing mutation and crossover ratios for genetic algorithms—A review with a new dynamic approach," *Information*, vol. 10, no. 12, p. 390, Dec. 2019, doi: 10.3390/info10120390.
[41] M. Marina and S. Das, "Ad hod on-demand multipath distance vector routing," *Wireless Commun. Mobile Comput.*, vol. 6, pp. 969–988, Oct. 2006.
[42] K. Sampath, C. Liyanapathirana, and P. Rupasinghe, "Improving trusted routing by identifying malicious nodes in a MANET using reinforcement learning," in *Proc. 7th Int. Conf. Adv. ICT Emerg. Regions (ICTer)*, 2017, pp. 1–8.
[43] J. Wu, M. Fang, H. Li, and X. Li, "RSU-assisted traffic-aware routing based on reinforcement learning for urban vanets," *IEEE Access*, vol. 8, pp. 5733–5748, 2020.
[44] G. Sun, Y. Zhang, H. Yu, X. Du, and M. Guizani, "Intersection fog-based distributed routing for V2V communication in urban vehicular Ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2409–2426, Jun. 2020.

NISHIT SHAH received the B.Tech. degree in computer science from Parul University, India, in 2019. He is currently pursuing the M.Sc. degree with Lakehead University, Canada. His research interests include wireless networks, routing, and network security.



HOSAM EL-OCLA (Senior Member, IEEE) received the M.Sc. degree from the Department of Electrical Engineering, Cairo University, in 1996, and the Ph.D. degree from Kyushu University, Japan, in 2001. He joined the Graduate School of Information Science and Electrical Engineering, Kyushu University, as a Research Student, in 1997. He joined Lakehead University as an Assistant Professor, in 2001, where he has been an Associate Professor, since 2007. He has more than 100 publications in international journals and conferences. His current research interests include wireless sensor networks, mobile networks, and the IoT communications.

PEARLY SHAH received the Bachelor of Engineering degree in information technology from Gujarat Technological University, India, in 2019. She is currently pursuing the M.Sc. degree with Lakehead University, Canada. Her research interests include wireless networks, routing, and network security.