International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209986 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

A Novel Golden Eagle Optimizer Based Trusted Ad Hoc On-Demand Distance Vector (GEO-TAODV) Routing Protocol

Sachidanand S Joshi
Department of Information Science and Engineering , SDM College of Engineering and Technology, Dharwad, Karnataka, India
sachinjoshi055@gmail.com

Sangappa Ramachandra Biradar
Department of Information Science and Engineering, SDM College of Engineering & Technology, Dharwad, Karnataka, India
srbiradar@gmail.com

Received: 02 August 2021 / Revised: 15 September 2021 / Accepted: 23 September 2021 / Published: 27 October 2021

Abstract – Mobile Ad-hoc Networks (MANETs) are a type of wireless network that allows people gaining more ubiquitous, as seen by their exponential rise over the last decade. They are made up of mobile nodes that connect remotely. The network's efficiency is highly dependent on the routing protocol used. This provided an opportunity for academics to design routing methods capable of increasing network efficiency. The literature focuses on building algorithms for route selection based on either the energy level or the distance between source and destination. However, there are other elements that affect the network's data transmission efficiency. Thus, this study work offers a unique Golden Eagle Optimizer-based Trusted Ad-hoc On-Demand Distance Vector (GEO-TAODV) routing protocol that optimizes route selection on the basis of criteria such as priority queue, trust degree, delay, hop count, and energy level. The trustworthiness of potential routes is determined using a consensus network model. By satisfying the reward expectations of the given multi-objective function, the suggested GEO method assists in determining the most efficient and trusted route for data transfer. Thus, the GEO-TAODV routing protocol assures that data is transmitted efficiently via a trusted path. The proposed GEO-TAODV protocol is simulated and compared to existing AODV and AODV-version 2 routing methods.

Index Terms – AODV, Consensus, Golden Eagle Optimizer, GEO-TAODV, MANET.

1. INTRODUCTION

Ad-hoc Network for Mobile Devices contains nodes that are mobile, self-contained, and capable of exchanging data among themselves [1]. For MANETs, the Ad-hoc On-Demand Distance Vector (AODV) routing protocol was created [2 – 6]. Because AODV is a reactive protocol in which routes are created as needed. [7]. The AODV method makes use of typical routing tables, to see if the numbers are in order routing data is current, a single entry for a single destination policy, and routing loop prevention. The AODV strategy uses route discovery and maintenance to connect a node that serves as a source and a node that serves as a destination via a route path [8]. The AODV protocol's primary advantage is that it discovers many routes for packet transmission [9].

One of the primary issues in MANET routing is the topology's dynamic behavior [10]. Because the nodes are mobile, the network organization changes during transmission, necessitating the selection of a new route. Another issue is energy consumption [11]. MANETs have nodes with a finite amount of battery power. If the battery power is completely depleted, the nodes are unable to conduct routing [12]. Another difficulty with MANET is dealing with security concerns. Due to the fact that MANET nodes interact by air, security becomes a worry [13].

As a result, routing must take various elements into account, including security, priority, distance, energy consumption, and time required. The proposed research utilizes a novel routing approach called Golden Eagle Optimizer-based Trusted AODV (GEO-TAODV) to provide an optimal routing that is low in delay, short in distance, high in priority, high in energy, and high in trust.

The proposed research proposal's primary objectives are as follows:

- To develop a novel GEO-TAODV routing protocol for packet forwarding based on a consensus method and a priority queue.

RESEARCH ARTICLE

- To evaluate the proposed GEO-TAODV routing algorithm's performance by various node counts, the ratio of nodes that aren't alive, the pause time and node speed.
- To compare the proposed GEO-TAODV routing algorithm to the AODV Version - 2 and Traditional AODV routing algorithms.

The following is how the paper is organized: section 2 contains a review of literature, section 3 contains an explanation of proposed routing methodology, section 4 contains discussion about obtained results, and section 5 contains research paper's conclusion.

2. LITERATURE REVIEW

This section discusses several AODV protocols that have been proposed in the literature. There are two broad categories of AODV protocols: conventional AODV protocols and meta-heuristic protocols.

2.1. Conventional AODV Protocols

The SAL-SAODV protocol was proposed by W. Fang et al. (2017) [14] in conjunction with fog-based mobile Adhoc networks application areas using the SAODV protocol. By substituting a cyclic redundancy check for electronic signatures, the SAODV protocol's complexity and energy efficiency were reduced, while the data integrity of packets was by using a random delay, we can be sure that we are getting the best results transmission mechanism. The SAL-SAODV protocol used approximately 35% less energy and had a BPUE of approximately 60% higher than the SAODV protocol, according to simulation results. Simultaneously, the energy-efficiency and information-tamper-proofing schemes could be applied to other AODV protocols. The SAL-SAODV protocol was designed for situations that were not time-critical but required a high level of security.

Shashwat, Y., et al., (2017) [15] described an algorithm for communication in a mobile Adhoc networks with a high possibility of packet loss, as explained in Lemma 1. Another parameter, RREP Count(t), was added to reduce the possibility of deceitful optimism. It increased whenever the node worked normally. As a result, the node was classified as malicious, and IDSs within its nodes transmission range broadcast a message to block it. We calculated the possible outcomes in the both cases, with or without the "REP Count" entry, to demonstrate this premise. Finally, by comparing the possibilities, it was determined that P2 will be less than P1, indicating that when the "RREP Count" entry was used, the likelihood of deceitful optimism was a substantial decrease.

The energy efficiency of the AODV routing protocol when used with TCP and UDP connections and a variety of nodes and connection agents was investigated by Shaf, A., et al., (2018) [16, 17]. Except for traffic agents, all remaining parameters are similar for TCP and UDP connections. As the network grows in size, so does the quantity of energy consumed. In the AODV routing protocol, UDP connections consumed less energy than TCP connections on a small scale (25-40 mobile nodes), but the results were completely reversed on a large scale. TCP connections using the AODV routing protocol used less energy than UDP connections. The development of a real-time energy-aware AODV routing protocol was aided by this analysis.

T. Kaur and R. Kumar (2018) [18] discussed different types of denial of service attacks and proposed a method for detecting and defending against worm -hole and black -hole attacks. Due to the methodology's lower overhead, it was successfully defended against worm hole and black hole attacks. As a result, battery power was conserved on the nodes, and the network's lifetime was increased.

K. A. Darabkh et al. (2018) [19] addressed an announcement mechanism for adaptive control packets that was directly linked to the regular hello message strategy, resulting in a significant decrease in control overhead as well as network congestion. The proposed modification to the protocol interchanging among 2 phases to ensure timely generation of efficient paths, which included the MA-DPAODV-AHM and AODV protocols. As per the findings, MA-DP-AODV-AHM successfully mitigates network destabilization by effective generation of optimum more stable routes and minimizing link failures.

S. Gurung and S. Chauhan (2019) [20] proposed a dynamically-generated sequence number threshold value to alleviate the effects of black-hole attacks using MBDP-AODV protocol. While it improved Normalized routing load, packet delivery ratio, and throughput, it come with a high cost in terms of routing overhead.

A reliability factor-based algorithm was proposed by P. Gupta et al. (2019) [21]. It calculated the nodes in the packet-forwarding path's reliability factor and only forwarded packets with a high reliability factor. The node may have had a low reliability factor value at some point, but this was not malicious. As a result, the fraudulent Route Request concept was used to detect malicious nodes, and packets were forwarded if the nodes were not malicious. The number of dropped packets was significantly reduced thanks to this algorithm.

A novel mechanism for defending against wormhole attacks in a MANET was described by S. Sankara Narayanan and G. Muruga boopathi (2020) [22]. Conventional methods used QoS for the complete network for the purpose of detecting attacks. The PDR as well as RTT of every node, as well as active and passive attacks, were used in this method. As a

RESEARCH ARTICLE

result, the suggested method was able to identify wormhole attacks completely.

A. M. Bamhdi (2020) [23] proposed Dynamic Power On-Demand Ad hoc Distance Vector (DP-AODV). This method is for dynamically adjusting transmission power usage by utilizing the AODV protocol. To achieve the improvement, the relationship between a transmission range and its density was taken advantage of. In networks with more than two hundred nodes, the results can be seen that DP-AODV had a lower delay and better performance than AODV as network density increased. Under medium to high-density conditions, results of simulation shows DP-AODV improved overall network performance by lessening control overhead and jitter, enhancing throughput, minimizing interference, and lastly, reducing end-to-end delay.

2.2. Meta Heuristic AODV Protocols

H. Singh and P. Singh (2017) [24] proposed a new ACO-based clustering approach for AODV-R with the goal of determining the optimal path and removing congestion. The new clustering algorithm depends on Ant Colony Optimization is evaluated using the packet delivery ratio, control overhead, end-to-end delay, and connection failures all affect the packet delivery ratio.

M. Zhang et al. (2018) [25] discussed the B-iHTRP, which is a routing protocol that is a hybrid that uses Autonomic Optimization and Cross-Layer perception to identify which paths are most advantageous for perceptive ants.

D. Sarkar et al. (2018) [26] proposed a novel to determine the optimal path in an AODV network. Their method is based on a pheromone value that is calculated using different QoS congestion, reliability, and energy consumption are just a few of the parameters that are taken into account.

S. Janakiraman (2018) [27] developed hybrid ACO/Artificial Bee Colony Optimization (ABCO) algorithm. In the Internet of Things, a hybrid algorithm is developed to select the right cluster head for each connected device. To select a cluster head in the Internet of Things, a hybrid algorithm has been developed.

Z. Sun et al. (2019) [28] designed a multi-objective ACO- a protocol for secure routing pertaining to Wireless Sensor Networks. The main goal is to improve security by using wireless nodes' less energy consumption. They concluded that their approach is capable of achieving the expected performance during black hole attacks based on experimental results.

M. H. Hassan et al., (2019) [29] described a novel algorithm that significantly improved the QoS of MANET routing protocols when applied to the African Buffalo Optimization (ABO). The path selection of the AODV routing protocol is optimized with ABO. The B-AODV routing protocol outperformed the standard AODV routing protocol on all performance metrics. MANET was chosen as a research topic because of its many benefits, including ease of installation, low cost, and quick implementation time. MANET, on the other hand, was still dealing with a number of issues that needed to be addressed. As a result, one of these issues is addressed by incorporating a new algorithm aimed at optimising the path selection process through the use of several quality parameters in this described attempt (like; energy, delay, and several hops).

T. A. N. Abdali et al. (2020) [30] proposed using the Optimized PSO (OPSO) for routing in MANETs, instead of a non-uniform mutation operation. The OPSO is a feature of the LAR protocol that helps to improve key performance measures such as packet delivery ratio (PDR), energy consumption, control packet overhead, and end-to-end delay.

Using a new fitness function, A. Bhardwaj and H. El-Ocla (2020) [31] described a Genetic Algorithm (GA) for determining optimal path from all those provided by the Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol (FFn). Even in the event of a random data packet loss, this protocol was created to give an optimization process for selecting the most efficient paths with the best fitness values while implementing shortest path, highest remaining energy, and least data traffic possible.

The proposed ACO-BFA technique addressed and resolved data transmission issues in the AODV protocol, according to Divya, K., and Srinivasan, B. (2021) [32]. The disadvantage of the AODV protocol was its high energy consumption, which was mitigated by an efficient routing process. When determining the routes to the destination, the energy consumption of nodes was taken into account. An Ant Colony Optimization – Bacterial Foraging Algorithm (ACO-BFA) is created to choose the optimal routes. The ACO method was used to start the paths, and it found one with a high probability that could be considered a bacteria's initial point, from which the best path could be found. BFA's strategy for ACO-optimization improved route selection and demonstrated convergence to the global optimum solution. In terms of simulation results, the proposed technique ACO-BFA was compared to existing techniques such as AODV, Enhanced Ant-AODV, and EE-AODV.

The MFR method for selecting neighbor nodes and HAODV for determining the shortest route was proposed by A. Goyal et al. (2021) [33]. The Hybrid AODV also uses the Firefly algorithm to determine the shortest route based on the updating equation. Performance was calculated using various network parameters they are end-to-end delay, average control packet overhead, throughput, and packet delivery ratio are all metrics that can be measured.. It was discovered that the proposed algorithm (HAODV) improved when

RESEARCH ARTICLE

AODV and DSR algorithms are compared in terms of overhead, end-to-end delay, packet delivery ratio, and throughput.

3. THE PROPOSED GEO-TAODV ROUTING PROTOCOL

The traditional AODV protocol creates a route from source to destination using two different messages: RREQ and RREP. The source sends an RREQ message to all possible destinations. The final destination node replies with an RREP message to source node. The path that transmitted first RREP is chosen as the data transmission route. The path chosen in this technique has the least delay or travels the shortest distance. However, other network efficiency factors such as hop count, energy consumption, and security are not considered. Ignoring these parameters can reduce network efficiency, exhaust the path, and increase the likelihood of link failure. Thus, the proposed novel GEO-TAODV protocol incorporates a Meta heuristic algorithm that considers consensus, minimum hops, energy efficiency, and priority queuing to find out the most suitable optimal route for data transmission. The proposed novel GEO-framework TAODV's is shown in Figure 1.

The proposed GEO-TAODV protocol is based on five-variable objective function: energy level, hop count, delay, priority request, and trust degree. Each and every single node in the network's energy consumption is measured on a regular basis. The number of intermediate points required to reach the destination is assigned as the hop count of a route. The time it takes for packets to arrive at their destination is proportional in relation to the distance between the source and the destination. The order in which the source received the RREP determines the priority ranking of each route. A consensus model of trust is used to calculate the trust degree. For each link in the list of possible routes, this degree of trust is calculated.

The meta-heuristic approach dispatches search agents in various directions within the search space in order to figure out which method is the most effective data transmission path.

QoS is improved as a throughput, end-to-end delay, energy conservation, control packet overhead, network life time, and reliability when the optimal path with the fewest hops, highest energy, highest priority, and greatest trust is chosen.

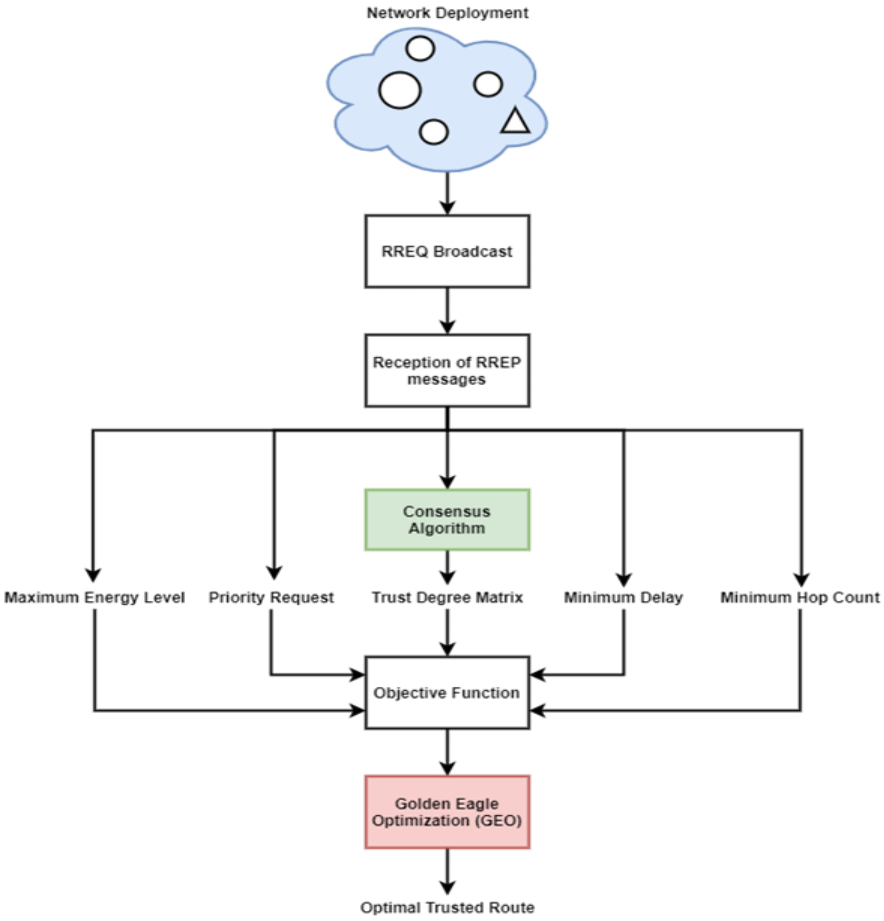

Figure 1 Proposed Framework of GEO-TAODV Routing Protocol

RESEARCH ARTICLE

The operation of the algorithm is described in detail in the following subsections.

3.1. Energy Level

Each and Every single node in the network has their energy levels initialized equally. Energy is consumed as data is transmitted between nodes. As a result, as the number of transmissions increases, the node's energy level decreases. When determining the best data transmission route, each node in the network's energy level is taken into account. Using the formula, energy or residual energy can be calculated from initial energy and energy spent.

$$E = E_i - E_s$$

Where E is Residual energy

E_i is the initial energy

E_s is the spent energy

3.2. Priority Request

When the source forwards RREQ, the destination transmits RREP via all possible routes. When a node generates or receives a high volume of traffic, a request queue is created. This priority queue is managed according to the First Come First Serve (FCFS) principle. As a result, the position of the relay node in the queue is determined for use in determining the optimal route for data transmission.

3.3. Consensus Model of Trust

A consensus model of trust is a type of trust coalition built on the basis of the nearby nodes' consensus level of trust for a particular node in the MANET. The routing behavior observed by a node is insufficient to confirm the presence of attackers. As a result, a set of trusted neighboring nodes is identified and used as decision makers. The trust level is determined using the trust score that each node possesses.

Let the network be directed graph $G(D, E)$, where D represents decision makers, $D \epsilon NH = 1,2, \dots, n$, $n \leq NH$, whereNH indicates the neighboring nodes and E denotes edges of the network.

To describe the graph$G(D, E)$, an adjacent matrix $A = (DT(m, NH_m))n \times n$ is created which is calculated using equation (1). Here $(d_m, d_p) = 1$ indicates that d_m has a trust factor on node d_p.

$$DT_{mp} = \begin{cases} 1, & (d_m, d_p) \in NH \\ 0, & (d_m, d_p) \notin NH \end{cases} \quad (1)$$

The adjacent matrix conveys whether there exists a trusted relationship between the node m and the decision maker $D \in NH$ or not. To determine the strength / degree of trust, a weighted adjacent matrix is computed as shown in equation (2).

$$A_w = (WDT_{mp})n \times n, d_{mp} \in [0,1] \quad (2)$$

Where, W is the weight of the weighted directed graph of MANET.

3.4. Delay

Delay is proportional to the source-to-destination distance. The time it takes for the RREP packet that reaches its destination is calculated so that shortest data transmission path can be considered. Delay is calculated as shown in equation (3).

$$Delay = t_r - t_s \quad (3)$$

Where t_r is the time it took to receive the packet, and t_s is the time it took to send the packet.

3.5. Hop Count

The hop count is connection count between the source node and destination networks is the number of hops. The developed Mobile Ad hoc network is a multi-hop environment in which data is routed via one or more relay nodes from source to destination. A hop refers to the sending a data from one node to another. Using all possible routes, the number of hops needed for sending the data from the originator to the destination node is determined. Thus, the hop count in relation to the initial TTL and the final TTL will be calculated as shown in equation (4).

$$h_c = t_i - t_f \quad (4)$$

t_i=Initial TTL; t_f=Final TTL

(TTL is the time of existence of "hops" before it is discarded by a router inside a network.)

3.6. Novel Golden Eagle Optimizer Based Trust Ad-Hoc On-Demand Distance Vector Protocol

Over the course of iterations, the best possible solution was discovered. The Golden Eagle Optimizer [34] can explore the landscape with extreme and sudden changes in the early converge toward promising areas at various stages of the search. Data transmission is secure thanks to the use of a consensus policy. As a result, the proposed GEO-TAODV routing protocol produces a path that is both efficient and reliable. The GEO algorithm is based on golden eagle spiral movements (GEs). The GE is drawn to attack prey and is on the lookout for better food. Every GE remembers the best position he or she has held thus far. As the number of iterations increases, the GE i choose another GEk's prey and circles around the best position of GEk. It can also choose to circle around the best memory position.

The GE population is given by $k \epsilon \{k_1, k_2, \dots, k_N\}$, where N denotes the population size and $k_i = \{Energy_i, Priority_i, A_w, Delay_i, Hopcount_i\}$.

RESEARCH ARTICLE

For every GE, fitness is calculated to know its best position. In this work, a multi-objective function is defined in order to choose an optimal route that includes major 5 factors that can affect the network lifetime to deteriorate.

Multi-objective function of the proposed GEO-TAODV is shown in equation (5).

$$Q = \{F_1, F_2, F_3, F_4, F_5\} \quad (5)$$

Where,

$F_1 = \max(P(\text{Energy}_i))$;

$F_2 = \max(P(\text{Priority}_i))$;

$F_3 = \max(P(A_w))$;

$F_4 = \min(P(\text{Delay}_i))$;

$F_5 = \min(P(\text{Hopcount}_i))$.

According to the fitness ranking, the GEs move to new positions for every iteration. The formula for updating the positions of GE is given by equation (6).

$$k(t+1) = k(t) + \Delta k_i(t) \quad (6)$$

Where $\Delta k_i(t)$ is calculated using the equation (7).

The current position is k(t), and the next position is k(t+1) (new position).

$$\Delta k_i = r_1 p_a \frac{A_i}{\|A_i\|} + r_2 p_c \frac{C_i}{\|C_i\|} \quad (7)$$

$$A_i = k_f - k_i \quad (8)$$

$$C_i = (c_1, c_2, \dots, c_n, \dots, c_N) \quad (9)$$

$$c_n = \frac{d - \sum_{j,j\neq n} a_j}{a_n} \quad (10)$$

$$d = H.P = \sum_{j=1}^{n} h_j p_j \quad (11)$$

$$\|A_i\| = \sqrt{\sum_{j=1}^{n} a_j^2} \quad (12)$$

$$\|C_i\| = \sqrt{\sum_{j=1}^{n} c_j^2} \quad (13)$$

Here, p_a and p_c are attack and cruise coefficients respectively, r_1 and r_2 are random vectors in the range [0,1], A_i and C_i are attack and cruise vectors respectively and can be calculated as shown in equation (8) and equation (9),a_j and c_j are the elements of attack and cruise vectors respectively,$\|A_i\|$ and $\|C_i\|$ are the Euclidean norm vector of A_i and C_i respectively and can be calculated as shown in equation (12) and equation(13), k_f is the best position of GE f and k_i is the current position of GE i, H is the hyper plane, and P is an arbitrary point on the hyperplane. If the new solution obtained from the new positions outperforms the previous best solution stored in the archive memory, the solution set is updated to include the new solutions. The GEO algorithm is explained in the provided pseudo code 1.

1. Establish a baseline population of golden eagles.
2. Assess fitness function
3. Set up the population memory
4. Initialize priority queue, delay, hop count, energy, trust degree
5. for each iteration

    Update priority queue, delay, hop count, energy, and trust degree

for each and every golden eagle

    Choose a prey at random from the population's memory.

    Calculate attack vector

    if the length of the attack vector is not zero Calculate cruise vector

    Calculate step vector

    Update position using equation (4)

    Assess your fitness for the new positions.

        if fitness of new set is better than the fitness of previous sets from memory

            Replace the new position with the one that eagle i remembers.

        end if

    end if

end for

end for

Pseudo Code 1 Pseudo Code of Proposed GEO-TAODV Algorithm

4. RESULTS AND DISCUSSIONS

The proposed GEO-TAODV routing protocol is employed in MANET with specifications shown in table 1. In Network Simulator – 3 we simulate the proposed network routing (NS-3).

Parameter	Value
Simulation Area	1000 x 1000 m
MAC Protocol	IEEE 802.11

RESEARCH ARTICLE

Number of nodes	20, 40, 60, 80, 100
Total Simulation Time	100s
Data Rate	1 Mbps
Packet Size	1500 Bytes

Table 1 Network Specifications

The proposed GEO-TAODV protocol will be compared to the traditional AODV protocol [35] and the AODV-version 2 protocol (AODV-V2) [36] on a variety of Throughput, end-to-end delay, packet success rate, routing overhead, and total energy consumption are all performance metrics. This section contains the obtained results.

4.1. Throughput

Throughput refers to the rate at which a network sends or accepts data packets over a specified time period. Throughput calculation is shown in equation (14).

$$\text{Throughput} = \frac{\text{Number of data packets sent}}{\text{Total time taken}} \qquad (14)$$

Comparative performance of AODV, AODV-V2, and GEO-TAODV with respect to throughput can be seen in Figure 2.

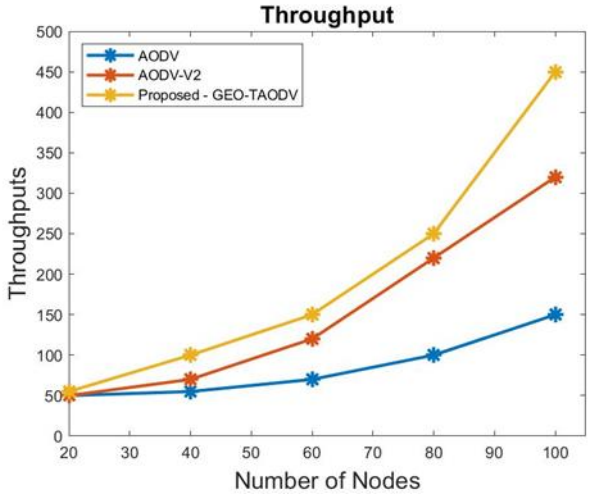

Figure 2 Comparison of Throughput

The throughput of the proposed GEO-TAODV appears to lead the AODV and AODV-V2 protocols. As AODV over a network of 50 nodes earns good throughput and more than the mentioned nodes have greater impact on the same and another factor Black hole attack that reduces throughput performance. When the number of nodes is as low as 20, the throughput of all three protocols tend to be the same. As the number of nodes grows, AODV and AODV-V2 throughput suffers significantly. In the case of AODV, the performance is affected by black hole attack that in turn reduces the throughput.

4.2. End-to-End Delay

The time it takes for a packet to be generated at the origin and obtained at the destination is referred to as the end-to-end delay. End-to-End Delay calculation is shown in equation (15).

$$\text{Delay} = t_r - t_s \qquad (15)$$

Where, t_r is the time it took to receive the packet, and t_s is the time it took to send the packet.

The comparison of performance analysis of different routing protocols in context with end-to-end delay is shown in Figure 3.

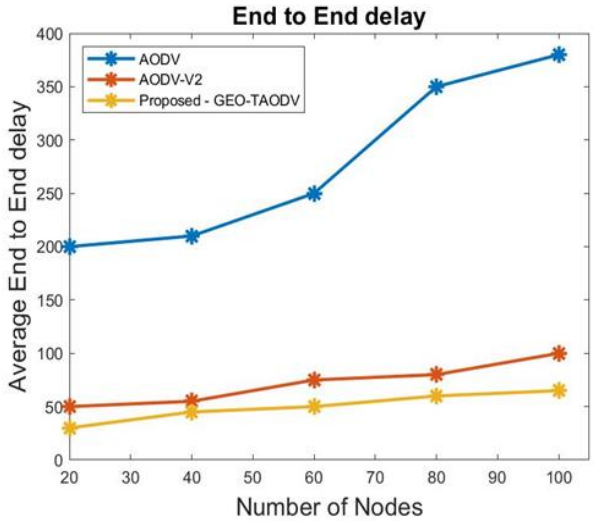

Figure 3 Comparison of End-to-End Delay

The end to end delay of the suggested GEO-TAODV appears to be lower comparing to AODV and AODV-V2 protocols. As the network size increases and Black hole attack affects the delay of AODV, The energy consumption of AODV and AODV-V2 are higher when compared to proposed vector that lead to higher delay. But, the delay is getting moderately affected for AODV-V2 due to the modification of previous version with additional parameters, and adversely affected for the proposed GEO-TAODV protocol.

4.3. Packet Success Rate

The ratio of packets received p_r to packets generated from the source p_s represents the network's packet success rate.

Packet Success Rate calculation is shown in equation (16).

$$\text{Packet success rate}(\%) = \frac{p_r}{p_s} \times 100 \qquad (16)$$

The performance analysis comparison of AODV, AODV-V2, and GEO-TAODV with respect to packet success rate is given in Figure 4.

RESEARCH ARTICLE

The packet success rate percentages of three protocols are parallel when the network size is equal to 40, as given in Figure 4, but as the network size increases, the ranges change. In comparison to AODV and AODV-V2, GEO-TAODV appears to have a higher packet success rate. AODV uses symmetric links to connect adjacent nodes. AODV, on the other hand, doesn't really attempt to follow node-to-node paths, instead relying on routes created dynamically at intermediate nodes. With an increasing number of nodes, AODV's packet success rate drops dramatically. The AODV-V2 protocol improves packet success rates as the number of nodes grows due to intermediate node route rebuilding, but the proposed GEO-TAODV protocol improves even further.

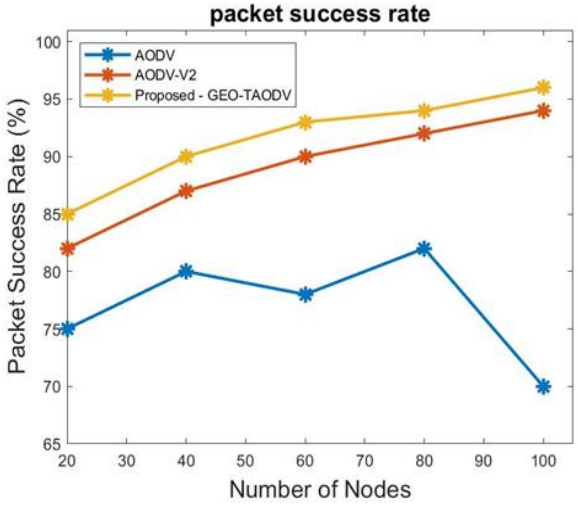

Figure 4 Comparison of Packet Success Rate

4.4. Routing Overhead

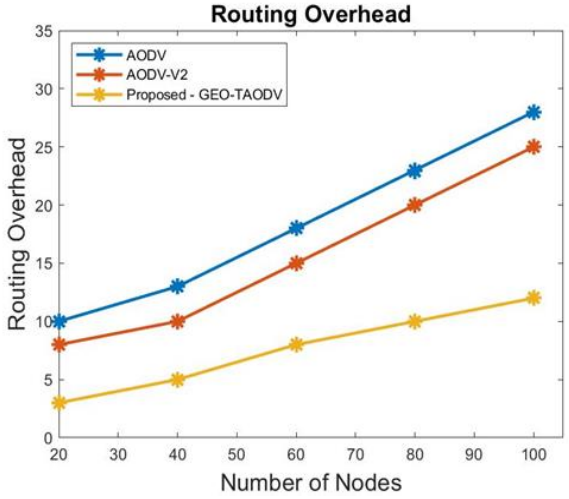

Figure 5 Comparison of Routing Overhead

Routing overhead refers to how much traffic a routing protocol generates. The ratio of packet transmissions (p_t) to packets received (p_r) at the destination is what it's all about. Routing Overhead calculation is shown in equation (17).

$$\text{Routing Overhead} = \frac{p_t}{p_r} \qquad (17)$$

Figure 5 shows comparison between AODV, AODV-V2, and GEO-TAODV with respect to routing overhead.

The proposed GEO-TAODV protocol appears to have a lower routing overhead than the AODV and AODV-V2 protocols. AODV is a reactive routing protocol, and the discovery process will begin only after the route discovery has been initiated. A valid route between two points is required for a node to communicate. While these protocols may be advantageous for applications with low traffic volumes, they may clog the network with unnecessary routing overhead. Thus, AODV has a higher routing overhead than AODV-V2, while AODV-V2 has a moderate routing overhead and the proposed GEO-TAODV protocol has a negative routing overhead.

4.5. Total Energy Consumption

The total energy consumption is computed by adding the energy expended by each network node during a data transmission. Total Energy Consumption calculation is shown in equation (18).

$$\text{Total Energy Consumption} = \sum_{i=1}^{n} \text{Energy}_i(t) \qquad (18)$$

The comparison of the performance of AODV, AODV-V2, and GEO-TAODV in terms of total energy consumption is illustrated in Figure 6.

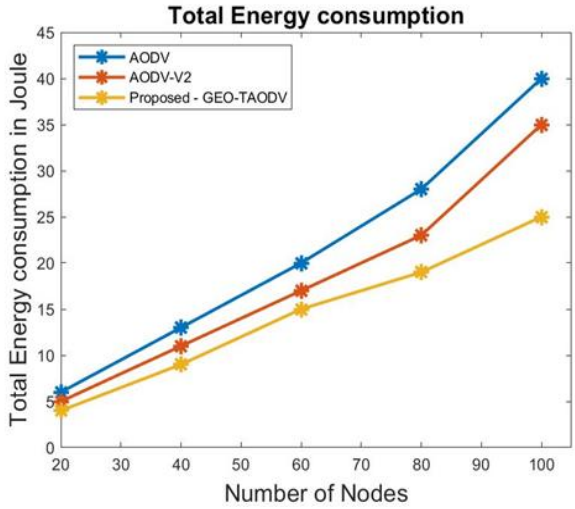

Figure 6 Comparison of Total Energy Consumption

The proposed GEO-TAODV protocol appears to consume less total energy than the AODV and AODV-V2 protocols. There is a transmission delay as well as a high energy consumption in AODV and AODV-V2 due to the end-to-end delay and lesser TTL. In general, the amount of energy

RESEARCH ARTICLE

consumed increases as the network size increases. In this scenario, increasing the number of nodes has a significant impact on AODV, a moderate impact on AODV-V2, and a negative impact on the proposed GEO-TAODV protocol.

4.6. Percentage of Dead Nodes

A node becomes dead when its energy drops from initial value to zero. For every round of data transmission, the percentages of dead nodes are calculated and are plotted as shown in the Figure 7.

The percentage of nodes that are alive increases with the rounds count. The proposed GEO-TAODV protocol maintains connectivity between nodes for 4850 rounds. AODV and AODV-V2 protocols, on the other hand, maintain nodes alive for 3987 and 4295 rounds, respectively. This shows that in terms of node survival, the presented algorithm performs better than the existing protocol by 17.79% and 11.44%, respectively.

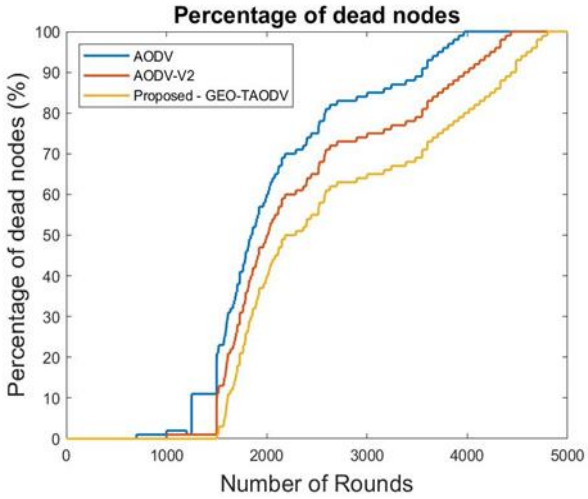

Figure 7 Comparison of Percentage of Nodes that are not alive

4.7. Network Lifetime

The lifespan of a network is determined by the quantity healthy nodes present in the network. The network lifetime, thus, depending on the situation of average energy consumption of nodes per data transmission round. Figure 8 shows comparison between AODV, AODV-V2, and GEO-TAODV with respect to network lifetime versus the rounds count.

The network lifetime decreases as rounds count increases, as shown in the comparison figure. The network that implemented the proposed GEO-TAODV has a lifetime of approximately 4850.

On the other hand, the lifetimes of networks that use the AODV and AODV-V2 protocols respectively expire at round 3987 and 4295. This demonstrates that the proposed protocol keeps the network alive by 17.79 percent and 11.44 percent, respectively.

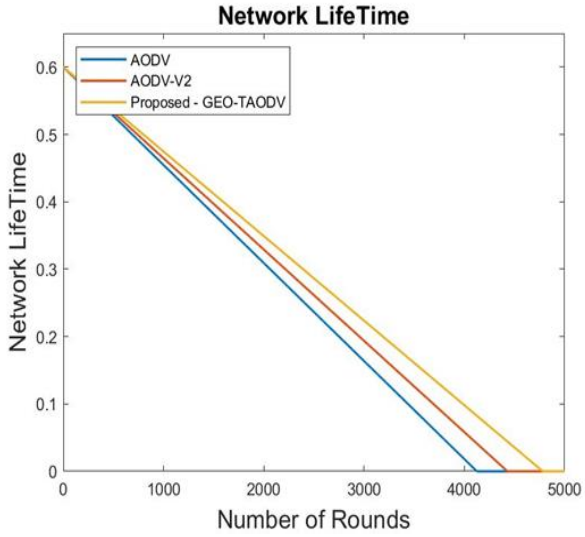

Figure 8 Comparative Analysis of Network Lifetime

4.8. Pause Time

The period of time during which all nodes in a network remain stationary but continue to transmit data is referred to as pause time. The network observes the transmission delay caused by this effect. Figure 9 shown the behavior of the network in view of the average end-to-end delay in relation to varying Pause times.

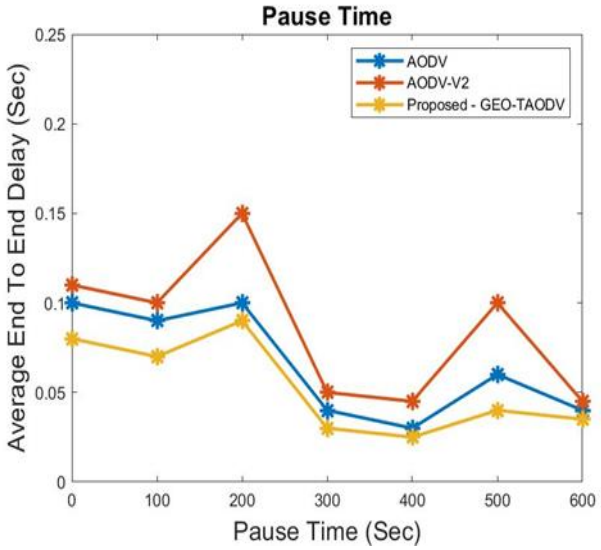

Figure 9 Comparison of Pause Time vs. End-To-End Delay

As the pause time increases, average delay decreases. As illustrated in the figure, the proposed GEO-TAODV has a lesser AODV has an average end-to-end delay that is longer.

RESEARCH ARTICLE

4.9. Speed

The figure 10 shows the comparing the performance analysis in terms of network lifetime for varying node speeds.

As the nodes' speeds increase, the network's lifetime decreases. Variations in speed of node have a negligible impact on the network lifetime of the proposed GEO-TAODV. In AODV and AODV-V2, energy consumption is high and end-to-end delay is affected. Packets are affected when nodes fail due to node symmetry, resulting in inefficient data transmission. Thus, performance compared with existing AODV and AODV-V2 protocols, results indicate that GEO-TAODV enables more efficient data transmission in MANETs.

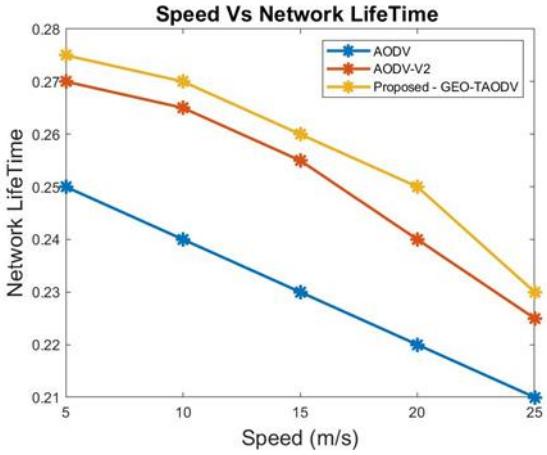

Figure 10 Comparison of Network Lifetime Vs Node Speed

5. CONCLUSION

In order to transmit data, a new GEO-TAODV routing protocol is used in MANETs in this paper. The GEO technique, a multiple-objective Meta heuristic optimization technique, is used in this algorithm. Based on energy level, hop count, delay, priority, and trust, the GEO provides an optimally efficient and trusted route for data transmission. To determine the routes' trust strength, the proposed routing scheme employs a consensus trust model. As a result, the protocol not only provides an efficient path for data transmission, but also one that is reliable and trustworthy. The proposed GEO-simulation TAODV's results are compared to AODV and AODV-V2 results to show that the GEO-TAODV is effective. In the future, the ability of other meta-heuristic algorithms to work with various MANET mobility models can be investigated.

REFERENCES

[1] Mafirabadza, C., Makausi, T. T., & Khatri, P. (2016, August). Efficient power aware AODV routing protocol in MANET. In Proceedings of the International Conference on Advances in Information Communication Technology & Computing (pp. 1-6).

[2] Bai, R., &Singhal, M. (2006). DOA: DSR over AODV routing for mobile ad hoc networks. IEEE transactions on Mobile Computing, 5(10), 1403-1416.

[3] Mhala, N. N., &Choudhari, N. K. (2010). Implementation possibilities for AODV routing protocol in real world. International Journal of Distributed and Parallel Systems (IJDPS), 1(2), 118-127.

[4] Liu, L., Zhu, L., Lin, L., & Wu, Q. (2012). Improvement of AODV routing protocol with QoS support in wireless mesh networks. Physics Procedia, 25, 1133-1140.

[5] Abu-Ein, A., & Nader, J. (2014). An enhanced AODV routing protocol for MANETs. International Journal of Computer Science Issues (IJCSI), 11(1), 54.

[6] Abbas, N. I., Ilkan, M., &Ozen, E. (2015). Fuzzy approach to improving route stability of the AODV routing protocol. EURASIP Journal on Wireless Communications and Networking, 2015(1), 1-11.

[7] Maurya, P. K., Sharma, G., Sahu, V., Roberts, A., Srivastava, M., & Scholar, M. T. (2012). An overview of AODV routing protocol. International Journal of Modern Engineering Research (IJMER), 2(3), 728-732.

[8] Liu, S., Yang, Y., & Wang, W. (2013). Research of AODV routing protocol for ad hoc networks1. AASRI Procedia, 5, 21-31.

[9] Ding, B., Chen, Z., Wang, Y., & Yu, H. (2011, November). An improved AODV routing protocol for VANETs. In 2011 international conference on wireless communications and signal processing (wcsp) (pp. 1-5). IEEE.

[10] Navale, M. M. P., &Chavan, G. T. (2014). Survey on QoS Improving Methods in MANET. International Journal of Engineering and Technology, 3(12), 22-25.

[11] Kumar, S. R., Gayathri, N., &Balusamy, B. (2019). Enhancing network lifetime through power-aware routing in MANET. International Journal of Internet Technology and Secured Transactions, 9(1-2), 96-111.

[12] Chitkara, M., & Ahmad, M. W. (2014). Review on manet: characteristics, challenges, imperatives and routing protocols. International journal of computer science and mobile computing, 3(2), 432-437.

[13] Eichler, S., & Roman, C. (2006, October). Challenges of secure routing in MANETs: A simulative approach using AODV-SEC. In 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems (pp. 481-484). IEEE.

[14] Fang, W., Zhang, W., Xiao, J., Yang, Y., & Chen, W. (2017). A source anonymity-based lightweight secure AODV protocol for fog-based MANET. Sensors, 17(6), 1421.

[15] Shashwat, Y., Pandey, P., Arya, K. V., & Kumar, S. (2017). A modified AODV protocol for preventing blackhole attack in MANETs. Information Security Journal: A Global Perspective, 26(5), 240-248.

[16] Shaf, A., Ali, T., Draz, U., &Yasin, S. (2018). Energy based performance analysis of AODV routing protocol under TCP and UDP environments. EAI Endorsed Transactions on Energy Web, 5(17).

[17] Jubair, M. A., Khaleefah, S. H., Budiyono, A., Mostafa, S. A., & Mustapha, A. (2018). Performance evaluation of AODV and OLSR routing protocols in MANET environment. Int. J. Adv. Sci. Eng. Inf. Technol, 8(4), 1277-1283.

[18] Kaur, T., & Kumar, R. (2018, August). Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using aodv protocol. In 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE) (pp. 288-292). IEEE.

[19] Darabkh, K. A., Judeh, M. S., Salameh, H. B., &Althunibat, S. (2018). Mobility aware and dual phase AODV protocol with adaptive hello messages over vehicular ad hoc networks. AEU-International Journal of Electronics and Communications, 94, 277-292.

[20] Gurung, S., & Chauhan, S. (2019). A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wireless Networks, 25(4), 1685-1695.

[21] Gupta, P., Goel, P., Varshney, P., &Tyagi, N. (2019). Reliability factor based AODV protocol: Prevention of black hole attack in MANET.

RESEARCH ARTICLE

In Smart Innovations in Communication and Computational Sciences (pp. 271-279). Springer, Singapore.
[22] Sankara Narayanan, S., &Murugaboopathi, G. (2020). Modified secure AODV protocol to prevent wormhole attack in MANET. Concurrency and Computation: Practice and Experience, 32(4), e5017.
[23] Bamhdi, A. M. (2020). Efficient dynamic-power AODV routing protocol based on node density. Computer Standards & Interfaces, 70, 103406.
[24] Singh, H., & Singh, P. (2017). Enhanced new clustering ant colony optimization based routing protocol AODV-R. International Journal of Computer Applications, 160(9).
[25] Zhang, M., Yang, M., Wu, Q., Zheng, R., & Zhu, J. (2018). Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs. Future generation computer systems, 81, 505-513.
[26] Sarkar, D., Choudhury, S., &Majumder, A. (2018). Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. Journal of King Saud University-Computer and Information Sciences.
[27] Hassan, M. H., Mostafa, S. A., Mohammed, M. A., Ibrahim, D. A., Khalaf, B. A., & Al-Khaleefa, A. S. (2019). Integrating African Buffalo optimization algorithm in AODV routing protocol for improving the QoS of MANET. Journal of Southwest Jiaotong University, 54(3).
[28] Janakiraman, S. (2018). A hybrid ant colony and artificial bee colony optimization algorithm-based cluster head selection for IoT. Procedia computer science, 143, 360-366.
[29] Sun, Z., Wei, M., Zhang, Z., & Qu, G. (2019). Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. Applied Soft Computing, 77, 366-375.
[30] Abdali, T. A. N., Hassan, R., Muniyandi, R. C., MohdAman, A. H., Nguyen, Q. N., & Al-Khaleefa, A. S. (2020). Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in MANET. Information, 11(11), 529.
[31] Bhardwaj, A., & El-Ocla, H. (2020). Multipath routing protocol using genetic algorithm in mobile ad hoc networks. IEEE Access, 8, 177534-177548.
[32] Divya, K., & Srinivasan, B. Energy-Aware-AODV: Optimized Route Selection Process based on Ant Colony Optimization–Bacterial Foraging Algorithm (ACO-BFA). European Journal of Molecular & Clinical Medicine, 8(03), 2021.
[33] Goyal, A., Sharma, V. K., Kumar, S., &Poonia, R. C. (2021). Hybrid AODV: An Efficient Routing Protocol for Manet Using MFR and Firefly Optimization Technique. Journal of Interconnection Networks, 21(01), 2150004.
[34] Mohammadi-Balani, A., Nayeri, M. D., Azar, A., &Taghizadeh-Yazdi, M. (2021). Golden eagle optimizer: A nature-inspired metaheuristic algorithm. Computers & Industrial Engineering, 152, 107050.
[35] Chakeres, I. D., & Belding-Royer, E. M. (2004, March). AODV routing protocol implementation design. In 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings. (pp. 698-703). IEEE.
[36] Clausen, T., Yi, J., & De Verdiere, A. C. (2012, September). Loadng: Towards aodv version 2. In 2012 IEEE Vehicular Technology Conference (VTC Fall) (pp. 1-5). IEEE.

Authors

Sachidanand S. Joshi is an Assistant Professor in the Department of Information Science at SDM College of Engineering and Technology, Dharwad, Karnataka, INDIA. He obtained his UG and PG from VTU, Belagavi. He is pursuing his Ph.D. from V.T.U., Belagavi-Karnataka, India.

Dr. Sangappa Ramachandra Biradar is a Professor in the Department of Information Science and Engineering, at S.D.M. College of Engineering and Technology, Dharwad, Karnataka, INDIA. He obtained his Bachelor of Engineering from BLDEA's College of Engineering & Technology, Bijapur. He obtained his Masters of Technology from M.I.T., Mahe-Manipal. He received his Ph.D. from Jadhavpur University, Kolkatta, India.

How to cite this article:

Sachidanand S Joshi, Sangappa Ramachandra Biradar, "A Novel Golden Eagle Optimizer Based Trusted Ad Hoc On-Demand Distance Vector (GEO-TAODV) Routing Protocol", International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 538-548, 2021, DOI: 10.22247/ijcna/2021/209986.