Hybrid Trust and Weight Evaluation Based Trust Assessment Using ECK-ANFIS and AOMDV-REPO Based Optimal Routing in MANET Environment

Lucindia Dupak
National Institute of Technology Arunachal Pradesh
Subhasish Banerjee (subhasishism@gmail.com)
National Institute of Technology Arunachal Pradesh https://orcid.org/0000-0003-1920-1913

Research Article

Keywords: Hybrid trust, Weight evaluation, Exponential Cauchy Kernelized Adaptive Neuro-Fuzzy Inference System (ECK-ANFIS), Improved K-Harmonic Mean (IKHM), Ad hoc On-demand Multipath Distance Vector- Range Emperor Penguin Optimization (AOMDV-REPO).

Posted Date: February 21st, 2022

DOI: https://doi.org/10.21203/rs.3.rs-829206/v1

Title Page

Manuscript Title

Hybrid Trust and Weight Evaluation Based Trust Assessment Using ECK-ANFIS and AOMDV-REPO Based Optimal Routing in MANET Environment

Author Details

Lucindia Dupak
Department of Computer Science & Engineering
National Institute of Technology, Arunachal Pradesh
Email:lucindia123@yahoo.in

Subhasish Banerjee
Department of Computer Science & Engineering
National Institute of Technology, Arunachal Pradesh
Email: subhasishism@gmail.com

Corresponding Author

Subhasish Banerjee
Department of Computer Science & Engineering
National Institute of Technology, Arunachal Pradesh
Email: subhasishism@gmail.com
M. No: +91 9434985900

Hybrid trust and weight evaluation based trust assessment using ECK-ANFIS and AOMDV-REPO based optimal routing in MANET environment

Abstract: In Mobile Ad hoc NETworks (MANET), the employment of trust-based routing has attained augmenting attention during the past years. A novel approach for ensuring dependable routing in an adversarial MANET is the Trust-based routing protocols. Most prevailing works were done on the routing protocols development for security augmentation on an adversarial environment. These protocols encompass some flaws and are not secured on the MANET environment. This research method utilizes the Exponential Cauchy Kernelized Adaptive Neuro-Fuzzy Inference System (ECK-ANFIS) centered trust assessment utilizing Hybrid Trust (HT) evaluation along with optimal routing on the MANET for tackling those issues. In this proposed model, the nodes are first initialized; next, ECK-ANFIS assessed the trust. For the evaluation, the HT together with the weight value is estimated for the nodes. Subsequently, the lower-level Trust Value (TV) nodes are secluded into a separate box. Next, the cluster is created on the trusted node. Improved K-Harmonic Mean (IKHM) algorithm forms the Cluster Head (CH). Ad hoc On-demand Multi-path Distance Vector (AOMDV) discovered the route. Range Emperor Penguin Optimization (REPO) selects the optimal route as of the manifold nodes. Next, the route is maintained utilizing the same algorithm. In the investigational study, the performance is examined with the prevailing methods centered upon performance metrics. Therefore, the better performance of the proposed work is proved.

Keywords: *Hybrid trust, Weight evaluation, Exponential Cauchy Kernelized Adaptive Neuro-Fuzzy Inference System (ECK-ANFIS), Improved K-Harmonic Mean (IKHM), Ad hoc On-demand Multipath Distance Vector- Range Emperor Penguin Optimization (AOMDV-REPO).*

1. INTRODUCTION

An autonomous cluster of mobile users communicate through unsteady wireless links is the MANET [1]. There is no definite infrastructure that it relies on. It manages the network connectivity and also realizes the data transform just via the collaboration amongst the mobile nodes with restricted communication scope [2]. When infrastructure wireless networks are infeasible, it is basically a cheap, smaller scale and also the powerful solution [3]. Since MANET is flexible as well as simple to deploy in an adversarial environment, it is used in military, Bluetooth operations, personal areas, vehicular network fields, along with industrial areas [4]; therefore, the requirement for trusted MANET. For MANET communications, the routing method functions as the heart. It is because, on the open wireless environment, the routing protocol does the key operations say the shortest pathfinding, Route Discovery (RD), along with data transmission as of the source-destination node [5]. In every network's type, the routing solutions' quality is the primary deciding factor aimed at overall network performance [6]. The path's lifetime is centered upon the strength of every link on this path in MANET. Every link's strength relies on disparate factors, say topology changes caused via node's mobility, disturbance on the transporting medium, battery ability, et cetera [7]. Exchanging the route information in addition to finding a possible path to a destination centered upon the hop count as well as minimal power required is the major accountability of routing on MANET [8]. Ad-hoc network signifies the path formation on a temporary basis because, with mobility, the path could well be interrupted on account of the '2' nodes' movement away as of one another beyond their communication gamut [9]. By augmenting the routine, the network can frequently change the path devoid of distressing the restraint that is the utmost considerable tackle of routing on MANET [10].

In MANET, routing protocols are typically separated into three methods in respect of their design as well as routing procedure, they are (1) proactive, (2) reactive, together with (3) hybrid routing protocols [11]. Destination Sequenced Distance Vectors (DSDV) [12] as well as Optimized Link States Routing (OLSR) [13] is commonly used proactive routing protocols, which instantly exhibit the network status once the malevolent nodes attach. Ad hoc on-demands distances vector (AODV) [14] together with Dynamics Sources Routing (DSR) [15] are the reactive routing protocols, which instantly get started when the nodes needed the data packets to be transmitted, and also lessens the cost of bandwidth. With the node's dynamic nature as well as changes that occur often in the topology, the optimum route selection aimed at communication is a demanding task [16]. Additionally, if the node acts maliciously or selfishly, then that will disturb the complete network. As MANET is executed in various applications, it is imperative to avert the network from those malicious nodes. Selfishness as well as maliciousness could well be the deliberate or unintended cause of a node. It is particularly vital to spot such behavior on the network to make the Network Life-Time (NLT) longer. Usually, a selfish node spreads fallacious information about the nodes or makes them unavailable by letting off the nodes [17]. The MANET is easily prone to several forms of malicious attacks when the ad hoc network devoid of network- or link-layer security [18]. And that will be the major cause for the unguided medium of MANET [19]. The hybrid evaluation-centered trust assessment utilizing ECK-ANFIS is utilized here and the REPO uses the optimal routing process in maximizing the NLT.

1.1 Contribution:

Nevertheless, a number of Algorithms subsist in literature to resolve optimization problems, yet, so far there is always a need of new algorithm which can quest for ideal solution in minimum time.

- Our study opens an aperture that exhibit the newest advancements in Bio-inspired routing as a inference to foreshadow the arising topics that escalate more to contribute for routing Quality.
- The primary goal of this paper is to propose a new scheme to combat trust issues and also ensure security in MANET.
- NS2 simulator has been applied for performance analysis.

The research paper's structure is organized as: section 2 elucidates the prevailing research methodologies associated with the proposed work, section 3 shows the proposed HT calculation and optimal route selection, section 4 shows the investigational study of the proposed work, and section 5 deduces the paper with future enhancement.

2. RELATED WORK

In the year 2018 , Muhammad Salman Pathan *et al.* [20] recommended a trust-centered secure Quality of Services (QoS) via uniting social with QoS trust. The principal approach depended on lessening nodes that showed disparate packet forwarding misbehavior as well as on path discovering that ensured dependable communication via the trust mechanism. Centered upon packet forwarding behavior together with capability, the best forwarding node was selected by the scheme with regard to QoS parameters. Under disparate network conditions along with QoS parameters, the system's performance was analyzed. Concerning overhead, Packets Delivery Ratios (PDR), together with Energy Consumptions (EC), the system's performance had enhanced security as well as QoS routing. But the system was not intelligent enough as the node capability along with reliability was not analyzed intelligently. Along with , Mingchuan Zhang *et al.* in 2018 [21] posited a bio-enthused Hybridized Trusted Routing Protocol (B-iHTRP) centered upon trusted appraisal, Ant Colony Optimizations (ACO), along with Physarum Autonomics Optimization (PAO). Initially, for attaining perceptive ants, the cross-layer perception was integrated into ACO while the network was divided into manifold zones. In every zone, the routing table was proactively maintained through the keen ants that sensed respective parameters. Whilst sensing respective parameters, the perceptive ants were sent for reactively finding routes to end amongst the zones. Also, B-iHTRP utilized PAO in selecting the optimum one as of the found paths and automatically optimized the local paths amid the way of multiple-zone communication. B-iHTRP attained superior performance in comparison to prevailing algorithms. However, Trust assessment wasn't an automatic system and regarded fewer link metrics aimed at trust evaluation. Again in 2018, Abdesselem Beghriche and Azeddine Bilami [22] offered a trusted routing intended for alleviating attacks. The conception of trust was integrated in the MANETs as well as grey relational examination theory united with fuzzy sets was applied for gauging a node's Trust Level (TL) centered upon observations as of neighbor nodes' TL. Then, those TL were utilized on the routing decision-making. Numerous experiments were done to attest to the presented solution's applicability. The technique was helpful in lessening the malevolent nodes' effects and for ameliorating the system's safety. Even so, the authentication process of the method had some complex issues. Meanwhile, in 2018, Ruo Jun Cai *et al.* [23] generated an Evolutionary Self-Cooperatives Trust (ESCT) that emulated the human cognitive process as well as relied on TL information for preventing disparate routing disturbance attacks. The trust information would be exchanged by the Mobile nodes, which then analyzed the received trust information centered upon their cognitive judgment. For excluding malicious entities, every node evolved its cognition dynamically. The system can't be compromised even if the interior attackers encompassed the knowledge concerning the security mechanism. The ESCT's performance under disparate routing disruption attack situations was evaluated. The ESCT promoted network scalability as well as ensured routing efficacy on the routing disruption attackers' presence on MANET. Besides, the performance was proved in the less coverage environment only. Afterwards in 2019, Moresh Madhukar Mukhedkar and Uttam Kolekar[24] suggested superior encryption standard-facilated trust-centered secure routing concerning the recommended Dolphin Cat Optimizer. The Optimizer was exhibited on the optimum route assortment. It was the amalgamation of Dolphin Echolocation with the Cat Swarm Optimizations that inherited the quicker universal convergence. The simulation was done utilizing '75' nodes. It exhibited that the protocol attained the maximum throughput, least packet drop, minimal delay, along with detection rate. Despite that the approach was not trusted as the algorithm encompassed a pre-mature convergence issue that affected the system's performance.

Further, Rahul K.Ambekar and Uttam D.Kolekar in 2019[25] rendered the trust-centered topology-hiding Multiple-Path Routing (MPR) algorithm aimed at the MANET. Grounded on the chosen neighbor nodes, the secured route betwixt the sender and receiver were ascertained by the MRP. Lastly, data communication was done via the chosen multiple-path. The MPR's performance was examined with the existent methods, like topology-hiding MPR, Fractional lion optimizations to topology-hiding MPR, along with Adaptive one aimed at the delay, throughput, energy, together with Packet Drop Rate (PDR). The MPR rendered better outcomes than the existent techniques. Nothing but if the distance betwixt the nodes was augmented, the TV might be varied.

3. PROPOSED TRUST EVALUATION BASED ROUTING IN MANET ENVIRONMENT

Securing routing protocols is very problematic on account of the augmented mobile devices functioning on an ad hoc manner. On account of the node's movement, recurrent topology changes as well as the reliance on the intermediary nodes to relay packets, finding a pathway betwixt source - destination on the MANET causes more challenges. Thus, the trust method is engaged in these environments for securing routing and stimulating nodes to oblige during the packet forwarding. However, the trusted routing still faced challenges in resolving those issues. The proposed work utilized the hybridized trust evaluation-centered trust assessment along with optimum route selection on the MANET. At first, the nodes are initialized; next, utilizing computed hybrid TV, weight value, together with ECK-ANFIS, the trust is assessed for the initialized nodes. The mistrust nodes are secluded subsequent to the trust assessment. Next, the cluster is formed as well as the CH is chosen as of the complete trusted node utilizing the IKHM. Next, the AOMDV protocol discovers the multi-route for data transmission betwixt the nodes and the REPO selects the optimum path, and next, the route is maintained. The block diagram of the research method is displayed in Figure 1,

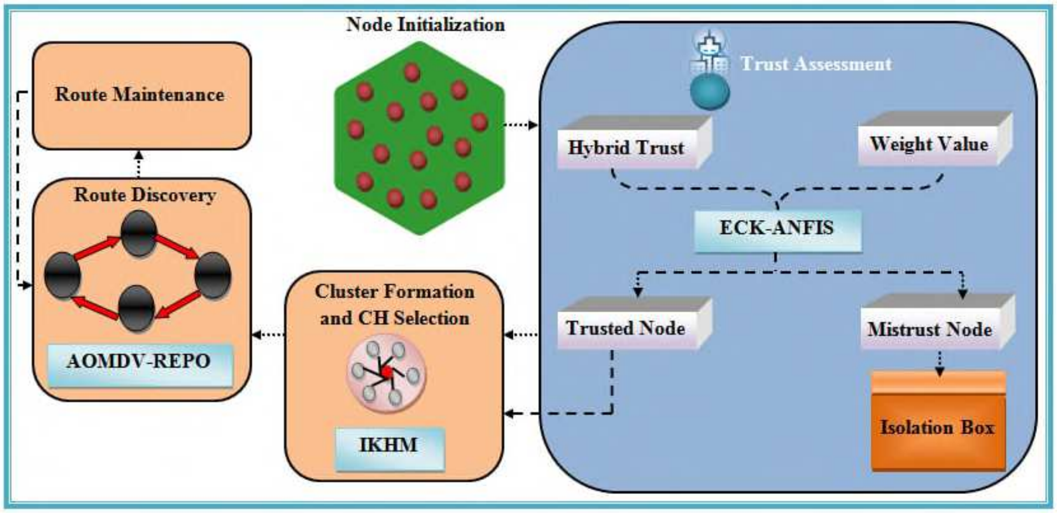


Figure 1: Block diagram for the proposed research method

3.1 Node Initialization

The n-number of nodes is initialized on the MANET, which is represented as,

$$\overline{S}_d = \{\overline{s}_1, \overline{s}_2, \overline{s}_3, ..., \overline{s}_n\} \tag{1}$$

Here, $\overline{S}_d$ signifies the MANET's nodes as well as $\overline{s}_n$ states the n-number of nodes.

3.2 Trust Assessment

The trust is evaluated for the initialized nodes utilizing HT evaluation along with the nodes' weight value via the ANFIS.

3.2.1 Hybrid Trust Evaluation

The proposed work gauged the HT. Direct Trust (DT) and In-Direct trust (IDT) is both considered. The derivation of trust, quantification, together with trust computation is the tasks that the DT agent carries out. The DT is estimated as,

$$IT_{\overline{s}_i, \overline{s}_{i+1}} = K_s / K_r \tag{1}$$

Wherein, $IT_{\overline{s}_i, \overline{s}_{i+1}}$ signifies the DT value of the node $\overline{s}_i$ and $\overline{s}_{i+1}$, K_s defines the successful packet sent as of the node $\overline{s}_i$ and K_r indicates the successful packet received as of the node $\overline{s}_{i+1}$. Next, the IDT is gauged for the node. Therefore, the IDT is well-known that the node with the witness factor is authenticated centered upon DT. The IDT evaluation $IIT_{\overline{s}_i}$ is derived as,

$$IIT_{\overline{s}_i} = \frac{1}{r} \sum_{i=1}^{r} IT_{\overline{s}_i + n} \tag{2}$$

Where, r states the total neighbors of the node. Lastly, the TV is implied as the amalgamation of DT and IDT, which is rendered in equation (3):

$$\delta_i = \sum_{i=1}^{n} IT_{\overline{s}_i, \overline{s}_{i+1}}, IIT_{\overline{s}_i} \tag{3}$$

Here, δ_i signifies the node's TV.

3.2.2 Weight Value Evaluation

Here, the node's weight is evaluated. The weight value is the amalgamation of data forwarding rate, consistency factor of the node, the time factor, together with a packet loss factor of the node, which is showed in equation (4):

$$\omega_i = \sum (\alpha(t), \beta(t), \chi(t), \lambda(t)) \tag{4}$$

Here, ω_i states the node's weight value, $\alpha(t)$ signifies the data forwarding rate, $\beta(t)$ indicates the consistency factor, $\chi(t)$ implies time factor, together with $\lambda(t)$ indicates the packer loss factor.

Data forwarding rate: Usually, it is impossible for most nodes to communicate straight with the base station, thus, Multi-hop is necessary. Certain times, the neighbor node transmits only their data and doesn't transmit the others' data, which is implied as to the selfish node. Thus, selfish analysis is vital, which is displayed in equation (5):

$$\alpha(t)=\begin{cases}\dfrac{an_{ij}(t)-er}{PEC_{ij}(t)-er} & an_{ij}(t)\leq PEC_{ij}(t)\\ \dfrac{ur-an_{ij}(t)}{ur-PEC_{ij}(t)} & an_{ij}(t)>PEC_{ij}(t)\end{cases} \tag{5}$$

Wherein, $\alpha(t)$signifies the data forwarding rate, $an_{ij}(t)$implies the quantity sending of the period t, $PEC_{ij}(t)$ denotes the expected value of the quantity sending of the period t, er implies the lower limit threshold together with the ur is the upper limit threshold.

Consistency factor: It is regarded for averting the malevolent nodes as of modifying primary data packets. The consistency factor is exhibited as,

$$\beta(t)=\frac{DAN_{ij}(t)}{DAN_{ij}(t)+COR_{ij}(t)} \tag{6}$$

Where, $\beta(t)$ signifies the consistency factor, $DAN_{ij}(t)$ implies the accordant packets, and $COR_{ij}(t)$ signifies the discordant packet.

Time factor: TV has a context association between time and content, as well as changes on the former base. The time grade's size depends upon the particular situation. If it is established largely, the integrated TV will be affected via history heavily, which might cause errors during node assessment. In contrast, if it is established way smaller, TV depends on a solo period excessively. The time factor is gauged concerning the network's security degree.

$$\chi(t)=\begin{cases}hh_h & high\\ ll_l & low\\ nn_n & normal\end{cases} \tag{7}$$

Where, $\chi(t)$ represents the time factor, andhh_h, ll_l and nn_n are the security degree high, low, and normal.

Packet loss factor: The packet might get lost during long transmission, so the packet loss factor is gauged here. It is exhibited below:

$$\lambda(t)=\frac{sd(t)}{rr(t)} \tag{8}$$

Where, $sd(t)$denotes the packet send by the sender at the time $t$and $rr(t)$ signifies the data packets received by means of the receiver at t.

3.2.3 Assessment by ECK-ANFIS

After the TV and weight value evaluation, the ECK-ANFIS assesses the TL. ANFIS comprises nodes and directed links, which stands as a multiple-layer feed-forward network. ANFIS operations rely on the fuzzy Sugenos model in the adaptive system framework for assisting its learning as well as adaptation. The ANFIS makes the it to be less reliant on proficient knowledge as well as be more systematic in its approach. Therefore, the Membership Function (MF) generates intricacy and may give training errors for solving that issue. To ameliorate the performance, the exponential Cauchy kernelized function is utilized as the MF. The '2' inputs δ_i and ω_i and one output z are designed; next, the rules are generated in which two fuzzy rules are created. Therefore, the rules can well be expressed as,

Rule 1: If δ_i is ε_i and ω_i is ε_i then,

$$R_i = p_i\delta_i + q_i\omega_i + \Psi_i \tag{9}$$

Rule 2: If δ_i is ε_{i+1} and ω_i is ε_{i+1} then,

$$R_{i+1} = p_{i+1}\delta_i + q_{i+1}\omega_{i+1} + \Psi_{i+1} \tag{10}$$

Wherein ε_i, and ε_{i+1} implies the fuzzy sets, $p_i, q_i, \Psi_i, p_{i+1}, q_{i+1}$ & Ψ_{i+1} values are the parameter set. The ANFIS comprises '5' layers. Each layer encompasses several nodes described via the node function. Each layer derivation is rendered in equation (1) to (3):

Layer 1: In this layer, every input variable will be interpreted as linguistic labels, as well as the total individual input signifies the total MF. The '1st' layer outcome is exhibited as,

$$La_{1,i} = \psi_i(\delta_i) \tag{11}$$

$$La_{1,i} = \psi_i(\omega_i) \tag{12}$$

Wherein, $La_{1,i}$ signifies the '1st' layer output, and ψ_i implies the exponential Cauchy kernel function that is exhibited as,

$$\psi_i = e^{\left(\frac{1}{1+\frac{\|p_i - q_i\|^2}{\Psi_i^2}}\right)} \tag{13}$$

Layer 2: Here, via multiplication, every node renders the rules' strength. The rule's firing strength is exhibited by the every node.

$$La_{2,i} = \zeta_i = \psi_i(\delta_i) \times \psi_i(\omega_i) \tag{14}$$

The output of this layer $La_{2,i}$ signifies the rule's firing strength.

Layer 3: This is the normalization layer. As per equation (15), it normalizes the rules' strength:

$$La_{3,i} = \overline{\zeta}_i = \frac{\zeta_i}{\sum \zeta_i}, \quad i = 1, 2....6 \tag{15}$$

Layer 4: Every node is essentially an adaptive node with a node function.

$$La_{4,i} = \overline{\zeta}_i . R_i \tag{16}$$

Here, $La_{4,i}$ signifies the 4th layer's output.

Layer 5: It is basically the output layer wherein the single node gauges the overall output through summing the entire rules as of the preceding layer.

$$La_{5,i} = \sum_{i=1}^{n} \overline{\zeta_i} R_i \tag{17}$$

The ECK-ANFIS assessed the trust. The conditions aimed at the TV assessment are,

Rule 1: If the δ_i is higher and ω_i is higher, then the TV is higher.
Rule 2: If the δ_i is medium and ω_i is medium, the TV is medium.
Rule 3: If the δ_i is low and ω_i is low, then the TV is low.

If the node has a lower TV, the node is secluded into the isolation box. If not, the medium TV along with high TV nodes is regarded for additional packet transmission. The medium as well as higher trusted nodes are signified as d_j , wherein $i = 1, 2, ...K$.

3.3 Cluster Formation and Cluster Head selection

The cluster is made for the medium as well as higher TV nodes. IKHM handles the cluster formation and CH selection. The K-Harmonic clustering is more effectual by means of initializing the initial cluster centers and lessening computational intricacy. An effectual technique is engaged for data point's allocation to cluster centers. However, the clusters' centroid is selected randomly so there is a chance of selecting the worst node. Thus, the average is computed for the initialized values. The new centroids are chosen centered on the gauged average.

$$c_j = \sum_{j=1}^{K} \frac{d_j}{t_n} \tag{18}$$

Wherein, t_n signifies the total nodes. Next, the cluster centers are signified as $C_l = \{c_1, c_2, ..., c_K\}$. The objective function $O_c(d_i, C_l)$ is found as,

$$O_c\left(d_i, C_l\right) = \sum_{i=1}^{n} \frac{K}{\sum_{j=1}^{K} \frac{1}{\left\|d_j - c_j\right\|^h}} \tag{19}$$

Where,‘ K ’ states the total centroids as well as nodes. For each data point d_i, gauge its membership function $\rho\left(c_j \middle| d_j\right)$ in every c_j and its weight $w\left(d_j\right)$ as per equation (20):

$$\rho\left(c_j \middle| d_j\right) = \frac{\exp\left(-\rho\left\|d_j - c_j\right\|^{-h-2}\right)}{\sum_{j=1}^{K}\left\|d_i - c_j\right\|^{-h-2}} \tag{20}$$

$$w\left(d_j\right) = \frac{\sum_{j=1}^{K}\left\|d_j - c_j\right\|^{-h-2}}{\left(\sum_{j=1}^{K}\left\|d_j - c_j\right\|^{-h}\right)^2} \tag{22}$$

Here, h signifies the parameter that is above 2, and ρ states another constant parameter. Next, the cluster center is updated via the subsequent equation:

$$c_j = \frac{\sum_{j=1}^{K}\rho\left(c_j \middle| d_j\right).w\left(d_j\right).d_j}{\sum_{j=1}^{K}\rho\left(c_j \middle| d_j\right).w\left(d_j\right)} \tag{22}$$

Until meeting the pre-specified cluster, the steps are repeated. Next, the final cluster set is denoted as $G_s = \left\{g_1, g_2, ..., g_n\right\}$ or g_i. The CH is chosen by means of considering the fitness function as the computed TV through the same algorithm. Mainly, the higher TV node takes the CH position; here, the CH is chosen for augmenting the NLT.

3.4 Route Discovery

Next, the AOMDV creates a multi-path to transport the packet towards the destination. Then, the REPO chooses the optimum route. Thus, the RD of this is labelled as the AOMDV-REPO. Manifold reverse paths at intermediary in addition to destination nodes were maintained through the RREQ propagation as of the source-destination in AOMDV. For forming manifold forward paths towards the destination at the source as well as intermediary nodes, Multiple RREP goes via these reverse paths. And also, for sending temporary messages, it forms alternative paths. The AOMDV core lies in making certain that manifold paths found are loop-free as well as disjoint, and effectively discovering such paths utilizing a flood-centered RD. AOMDV updates rules implemented locally at every node. It plays a main part in upholding loop-freedom together with dis-jointness properties. The designed routes are declared as S_i.

Subsequent to designing the MPR, the REPO selects the optimum one as of the designed routes to lessen the transmission delay. Amid the Antarctic winter, Emperor Penguins (EP) are the mere species that groups to stay alive. However, the arbitrary parameter is employed for initialization by the normal emperor algorithm. Sometimes, the arbitrary initialization misses the imperative points in the search space. Thus, this research method regards the range function rather than utilizing arbitrary parameter initialization. The huddling behavior of EP is decomposed into '4' phases that are: (a) create and ascertain the huddle boundary of EP, (b) compute the temperature profile about the huddle, (c) ascertain the distance betwixt EP, and (d) relocate the effectual mover.

In the preliminary phase, the EP i.e., S_i regards the designed paths and the huddle boundary is generated arbitrarily. Normally, EP positions them on a polygon shape grid boundary amid huddling. For finding the huddle boundary about a polygon, the wind flowing about the huddle is ascertained. Mathematically, the huddling boundary is devised as: let υ signifies the wind's velocity and μ implies the gradient of υ:

$$\mu = \nabla \upsilon \tag{23}$$

Vector κ is integrated with υ for obtaining intricate potential:

$$PP_y = \upsilon + im(\kappa) \tag{24}$$

Wherein, im signifies the imaginary constant as well as PP_y states the polygon plane function. Next, the EP forms a group to augment the ambient temperature and also conserve energy on the huddle. The situation can well be modeled mathematically using disparate assumptions. Those are, (i) the temperature is '0' when the polygon's radius is below one, and (ii) the temperature is '1' when the polygon's radius is above one. This temperature measure aids in performing exploration as well as exploitation tasks amongst EP. The temperature is gauged as:

$$U' = \left(U - \frac{M_{itr}}{f - M_{itr}} \right) \tag{25}$$

$$U = \begin{cases} 0, & if\ R_a > 0.5 \\ 1, & if\ R_a < 0.5 \end{cases} \tag{26}$$

Wherein, f signifies the current iteration, M_{itr} implies the maximal count of iterations, R_a signifies the radius, and U implies the time needed for identifying the best optimum solution.

Subsequent to generating the huddle boundary, the distance betwixt the EP and the best attained optimum solution EX is gauged. The solution with the highest fitness value in contrast to the preceding optimum solution is the current optimal solution. Here, the minimal distance betwixt sources to destination and the computed TV and weight values are set as the fitness function. The search agents' positions are updated in relation to the current optimum solution. The position updation is mathematically signified as:

$$EX = FO(A).E_p^{cp}(x) - J.E_p(x) \tag{27}$$

Wherein, $FO(A)$ signifies the social forces of EP, $E_p(x)$ implies the current position vector of the EP, $E_p^{cp}(x)$ signifies the vector of the best optimal solution, A, J implies the anti-collision factors betwixt neighbors that is accountable for tuning the distance EX , and therefore, the terms are computed utilizing equation (28) and (29):

$$J = a_1 \tag{28}$$

$$A = M \times (U_0 + G_g(yc)) \times a_2 - U_0 \tag{29}$$

$$G_g(yc) = E_p^{cp}(x) - E_p(x) \tag{30}$$

Wherein, M signifies the movement parameter that upholds a gap betwixt search agents aimed at collision avoidance, and $G_g(yc)$ signifies the polygon grid accuracy through comparing the difference betwixt EPs, and a_1, a_2 defines the range function that is exhibited as,

$$a_{ft} = \overline{pp}_1 + \overline{pp}_2 \times (l_r + u_r), \quad ft = 1,2 \tag{31}$$

Wherein, $\overline{pp}_1$, $\overline{pp}_2$ states the '2' constant values, l_r and u_r implies the lower as well as upper range values of the initialized population. The function $FO(\ )$ is stated as:

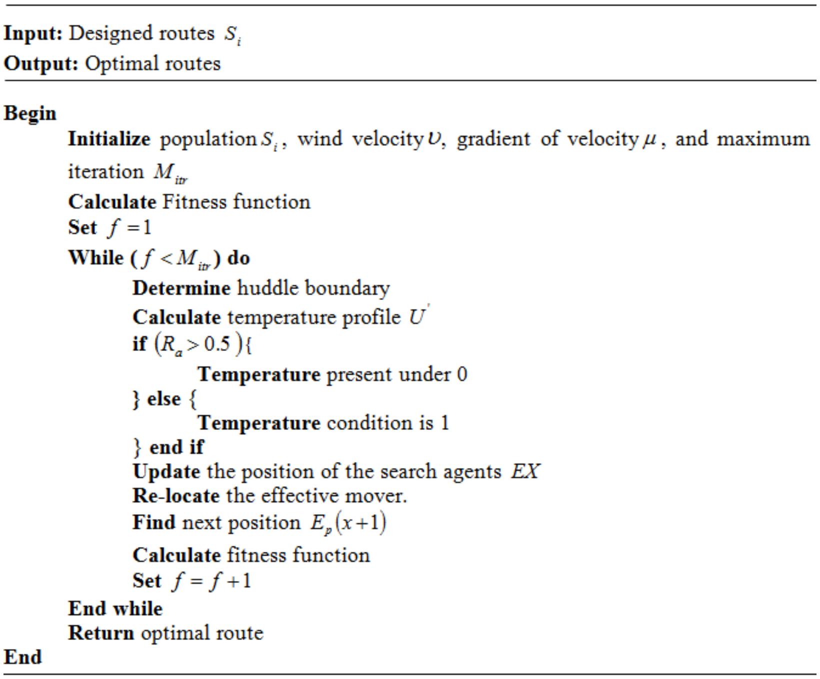
$$FO(A) = \left(\sqrt{b.e^{-x/m} - e^{-x}}\right) \tag{32}$$

Here, e signifies the expression function, b and m implies control parameters in support of better exploration as well as exploitation.

Lastly, relocate the effectual mover. For the updation of EP's position, the best attained optimum solution (mover) is utilized. The chosen moves brought about the movement of other search agents on a search space. The below equations are utilized for finding the subsequent position of an EP:

$$E_p(x+1) = E_p^{cp}(x) - A \times EX \tag{33}$$

Where, $E_p(x+1)$ signifies the EP's subsequent updated position.



```
Input: Designed routes $S_i$
Output: Optimal routes

Begin
    Initialize population $S_i$, wind velocity $\upsilon$, gradient of velocity $\mu$, and maximum
    iteration $M_{itr}$
    Calculate Fitness function
    Set $f = 1$
    While ($f < M_{itr}$) do
        Determine huddle boundary
        Calculate temperature profile $U^{'}$
        if $(R_a > 0.5)${
            Temperature present under 0
        } else {
            Temperature condition is 1
        } end if
        Update the position of the search agents $EX$
        Re-locate the effective mover.
        Find next position $E_p(x+1)$
        Calculate fitness function
        Set $f = f + 1$
    End while
    Return optimal route
End
```

Figure 2: Pseudo code for the REPO algorithm

Figure 2 elucidates the REPO pseudocode. Amid the iteration, the huddling behavior of EP is recalculated when the mover was re-located. Through the fitness assessment, the alternative optimum paths were attained.

3.5 Route Maintenance

The route failures particularly brought about, as a result of node's mobility or faulty nodes that are more recurrent, are managed through Route maintenance. If the route (damaged ones) associates with the nodes on the zone, the attained alternative optimum path is employed for the data transmission.

4. RESULT AND DISCUSSION

Utilizing the AOMDV-REPO, the proposed ECK-ANFIS and HT-centered trusted routing performance is examined. The proposed work is applied in the working platform of Network Simulator 2 (NS-2).

4.1 Performance Analysis for Trust Assessment

Concerning the accuracy, specificity, sensitivity, and F-Measure metrics, the proposed ECK-ANFIS centered trust assessment's performance is examined with the existent ANFIS, Artificial Neural Network (ANN), Convolutional Neural Networks (CNN), together with Support Vectors Machines (SVM).

Table 1: Accuracy analysis

Methods	Accuracy (%)
Proposed ECK-ANFIS	96
ANFIS	87
ANN	83
CNN	84
SVM	79

The accuracy examination of the ECK-ANFIS centered trust assessment with the existent method is in table 1. A major metric for proving the performance is accuracy. Here, a higher accuracy i.e. 96% is attained by the proposed one but the existent methods, namely ANFIS, ANN, CNN, and SVM possess the lower accuracy value of 87%, 83%, 84%, and 79%. Thus, it exhibits that superior outcomes in the node's trust assessment on the MANET environment are attained by the proposed work. Figure 3 exhibits the graphical depiction of the proposed method,

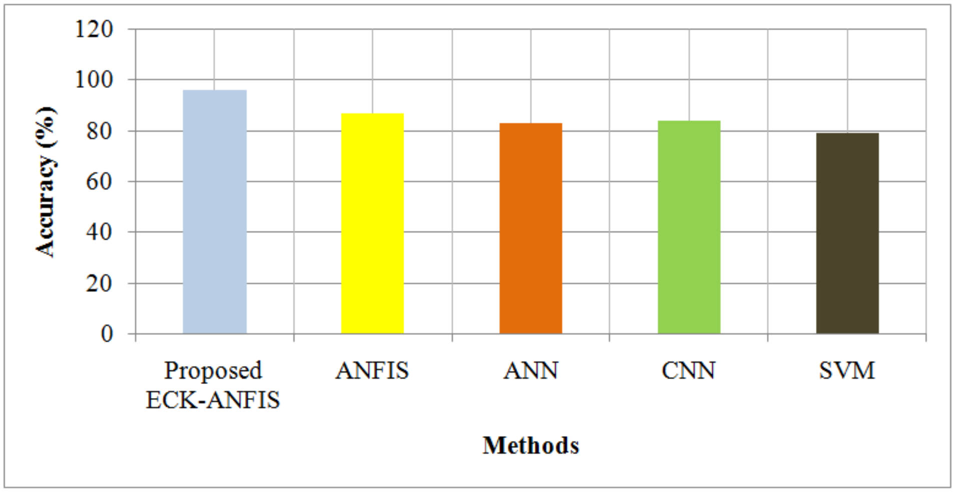


Figure 3: Graphical Representation of accuracy analysis

Table 2: Performance analysis of the proposed and existing research methodologies based on specificity, sensitivity, and F-Measure metrics

Performance Metrics	Proposed ECK-ANFIS	ANFIS	ANN	CNN	SVM
Specificity	94.75	89	86.38	85	78
Sensitivity	95.05	88.23	85	86.2	78.73
F-Measure	93	87	86.75	85.25	77.96

Regarding the specificity, sensitivity, and F-Measure metrics, table 2 tabulates the ECK-ANFIS's performance with the existent ANFIS, ANN, CNN, along with SVM. The proposed algorithm's specificity, sensitivity, and F-measure are 94.75%, 95.05%, and 93%. However, less performance is possessed by the existent methods when analogized to the proposed one. The worst performance is produced via the SVM when contrasted with every other method that is 78% for specificity, 78.73% for sensitivity, and 77.96% for F-Measure. The best outcome is attained by the existing ANFIS than the other existent methods but it encompasses less performance when analogized to the proposed one. It proves the proposed method's better performance.

4.2 Performance Analysis for Route Discovery

Regarding the EC, End-to-End Delay (EED), PDR, network size, along with throughput, the AOMDV-REPO's performance is weighted against the existing AOMDV, AODV, Dynamic Source Routing (DSR), along with OLSR routing protocols on this sub-section.

Table 3: NLT analysis of the proposed and existing methodologies

Number of Rounds	Proposed AOMDV-REPO	AOMDV	AODV	DSR	OLSR
0	1200	1200	1200	1200	1200
200	1182	1089	966	910	932
400	1007	989	896	818	892
600	965	901	848	792	835
800	872	789	682	614	652
1000	771	698	654	540	608

The NLT of the proposed and existing routing methodologies is tabulated in table 3. NLT indicates that how long the nodes are offered in the environments. Here, 1000 rounds are deemed wherein the NLT is examined in every round. The network area is 771m by utilizing the AOMDV-REPO routing methodology at the 1000 rounds, but the existing method centered network design has lost more network area that is the AOMDV has 698m, AODV has 654m, DSR has 540m, and OLSR has the 608m area in the same round. A better result contrasted to the existent research method is proffered via the proposed work intended for the remaining rounds. Hence, it proves the proposed one's superior performance. Figure 4 displays the pictorial representation of this analysis,

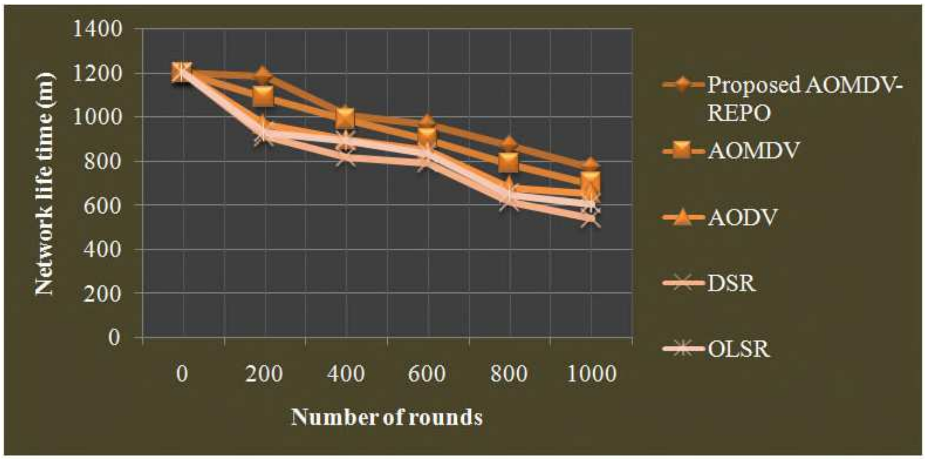


Figure 4: NLT analysis

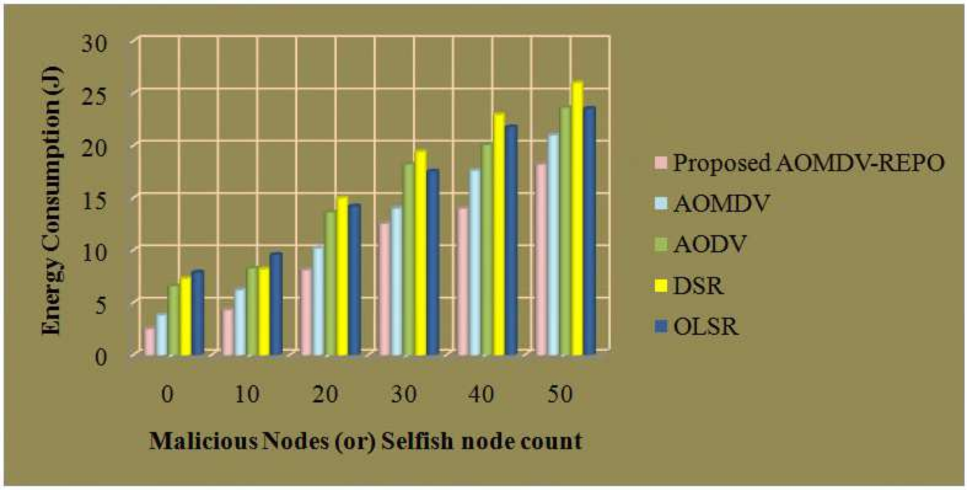


Figure 5: Demonstrate the performance of the proposed routing method with the existing method based on the EC metric

Figure 5 elucidates the EC of the proposed with the existent methods. The sum of receiving energy with the product of the total nodes and transmitted energy is called Consumption. The system is indicated as the effective system if less energy is consumed b the system. Here, concerning the total malicious (or) selfish nodes, the EC is examined. Only 12.56J energy is devoured by the proposed one but the prevailing research methods consume more energy analogized to the proposed work that is the AOMDV consumes 14J, AODV has 18.23J, DSR has 19.42J, and OLSR has 17.56J energy for 30 malicious nodes (or) selfish nodes. Less energy is devoured by the AOMDV-REPO centered routing contrasted to the existent methods as shown by the remaining malicious nodes-centered analysis.

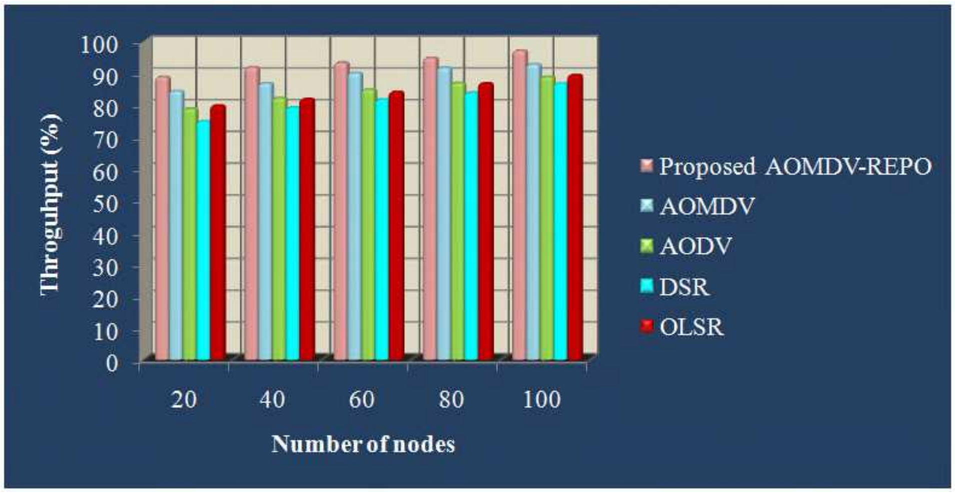


Figure 6: Illustrate the throughput analysis

The throughput of the proposed as well as existent research methods is displayed in figure 6. Concerning the sensor node counts, the throughput is examined in this analysis. Herein, the sensor node count is taken in the gamut of 20 to 100 sensor nodes for analysis. 92% throughputs are attained by the proposed one for the senor node count 40, but the existent methods like AOMDV, AODV, DSR, along with OLSR have the 87%, 82.36%, 79.36%, together with 82% throughput for the same node count. Likewise, the proposed attain a better result for every other remaining node count. The superior performance of the proposed work-centered route discovering is shown by the discussion of this throughput analysis.

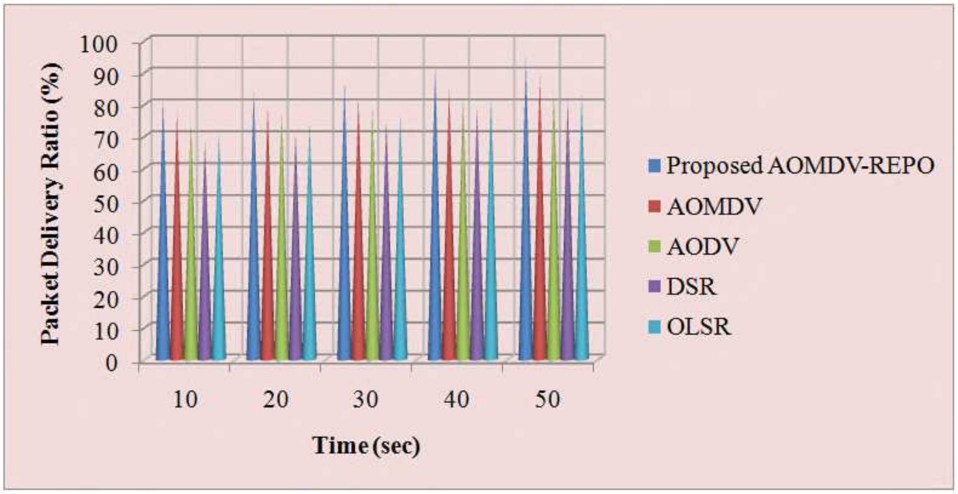


Figure 7: Graphical representation of PDR analysis

Figure 7 depicts the PDR analysis betwixt the proposed and existent methods. The data transmission's performance becomes more effective when the PDR is higher, and the transmitted packets are received with no loss. From the PDR analysis, the highest PDR at the 50s which is 94.53% is attained by the proposed one, whilst the existent AOMDV has 89%, AODV has 85.12%, DSR has 81.62% and OLSR has 83.12% PDR at the same 50s. Herein, less PDR analogized with the proposed work is proffered by the existent methods. The AOMDV is much better analogized to the other methods. Likewise, better results are attained by the proposed one contrasted to the prevailing research for the remaining times. Therefore, it confirms that a better performance is possessed by the proposed when weighted against other existing methods.

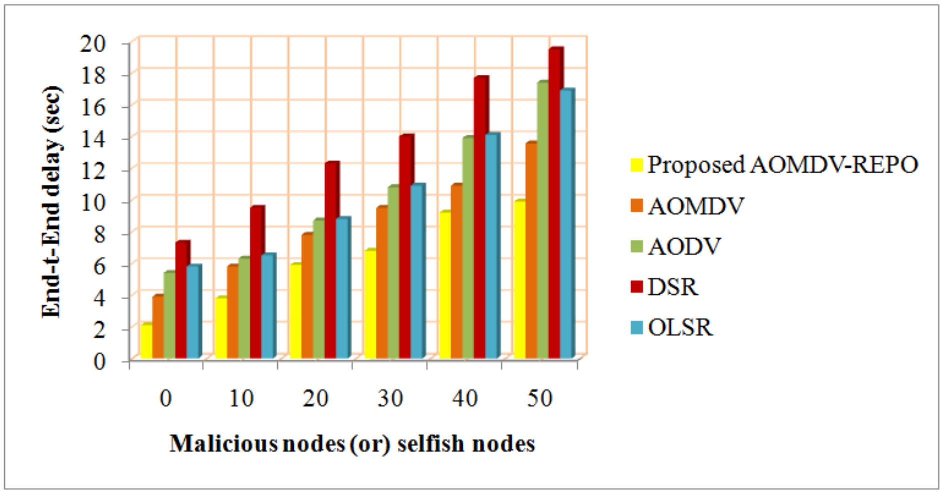


Figure 8: EED analysis

The EED of the proposed AOMDV-REPO with the existent AOMDV, AODV, DSR, and OLSR is displayed in figure 8. Centered on the total malicious nodes (or) selfish nodes present on the network, the performance is examined. The proposed takes 9.9s for transmitting the data as of sender to the receiver if the system encompasses a 50% malicious or selfish node. The long delay is possessed by the existent methods than the proposed one at the same time interval. Furthermore, the proposed work encompasses a 6.8s delay but the existent AOMDV has 9.5s, AODV has 10.8s, DSR has 14s, as well as OLSR 10.9s delay on the 30s. Less delay is possessed by the proposed one analogized to the existent methods for the other time interval also. Hence, it elucidated that the proposed has a superior result when weighted against the existent algorithms.

5. CONCLUSION

The ECK-ANFIS centered trust assessment utilizing HT evaluation and weight evaluation as well as optimal routing via the AOMDV-REPO is proposed. There are '5' phases: node initialization, trust assessment, cluster formation, and CH selection, RD, and route maintenance. The ECK-ANFIS assesses the trust utilizing HT and weight evaluation. Cluster is formed and CH is picked by the IKHM. The AOMDV-REPO discovers the route. In experimental analysis, the proposed method's performance is examined with the prevailing methodologies for the trust assessment together with the RD. In the trust assessment, the ECK-ANFIS's performance is weighted against the ANFIS, ANN, CNN, and SVM concerning the accuracy, specificity, sensitivity, together with F-measure metrics. The ECK-ANFIS attains higher accuracy (96%) in contrast to the existent methodologies. In RD, the proposed AOMDV-REPO's performance is weighed against the AOMDV, AODV, DSR, along with OLSR concerning the EC, PDR, EED, network size, together with throughput. The proposed design achieves better performance when weighted against the existent research method. The proposed AOMDV-REPO centered routing methodology covers 771m area at 1000 rounds concerning NLT. Therefore, the proposed method-centered routing reaches better performance. In the upcoming future, the proposed one can well be extended by considering more trust factors and utilizes the advanced method for enhancing trust.

Declarations:

Funding

This research did not receive any specific funding and it is carried out as part of the employment and higher degree of the authors.

Conflicts of interest

The authors of this paper have no conflict of interest towards the publication of this research article.

Availability of data and material

This research work utilizes no data or dataset. This research work utilizes the randomly generated data by the simulator as input.

Code availability

Custom code available on request due to privacy or other restrictions.

Authors' contributions

All authors of this research paper have directly participated in the planning, execution, or analysis of this study

REFERENCES

1. Geetha Sadayan and Karthiyayini Ramaiah, “Enhanced data security in MANET using trust-based bayesian statistical model with RSSI by AOMDV”, Concurrency and Computation: Practice and Experience, 2019, Doi.org/10.1002/cpe.5397.

2. De-gan Zhang, Jin-xin Gao, Xiao-huan Liu, Ting Zhang and De-xin Zhao, “Novel approach of distributed & adaptive trust metrics for MANET”, Wireless Networks, vol. 25, no. 6, pp. 3587-3603, 2019.

3. Aneri Mukeshbhai Desai and Rutvij H. Jhaveri, “Secure routing in mobile ad hoc networks: a predictive approach”, International Journal of Information Technology, vol. 11, no. 2, pp. 345-356, 2019.

4. Naveena S, Senthilkumar C and Manikandan T, “Analysis and countermeasures of black-hole attack in manet by employing trust-based routing”, In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 6-7 March 2020, Coimbatore, India, 2020.

5. Vaishali Vilas Sarbhukan and Lata Ragha, “ETSR: enhanced trust based secure routing scheme for mobile ad hoc networks”, Journal of Computational and Theoretical Nanoscience, vol. 16, no. 5-6, pp. 2265-2272, 2019.

6. Nareshkumar R. M, Phanikumar S and Manoj Kumar Singh, “Intelligent routing in manet using self-adaptive genetic algorithm”, In advances in systems, Control and Automation, vol. 442, pp. 595-603, 2018.

7. Fareena N and Sharmila Kumari S, “A distributed fuzzy multicast routing protocol (DFMCRP) for maximizing the network lifetime in mobile ad-hoc networks”, Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 5, pp. 4967-4978, 2021.

8. Balu Narasimha Rao G, Veeraiah D and Srinivasa Rao D. “Power and trust based routing for manet using rrrp algorithm”, In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), IEEE, 5-7 March 2020, Bangalore, India, 2020.

9. Niti Khanna and Monika Sachdeva, “Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation”, International Journal of Communication Systems, 2019, Doi.org/10.1002/dac.4012.

10. Harold Robinson Y, Subramanian Balaji and Golden Julie E, “PSOBLAP: particle swarm optimization-based bandwidth and link availability prediction algorithm for multipath routing in mobile ad hoc networks”, Wireless Personal Communications, vol. 106, no. 4, pp. 2261-2289, 2019.

11. Mohammad Sirajuddin, Ch Rupa, Celestine Iwendi and Cresantus Biamba, “TBSMR: a trust-based secure multipath routing protocol for enhancing the qos of the mobile ad hoc network”, Security and Communication Networks, 2021, Doi.org/10.1155/2021/5521713.

12. Fahad Taha AL-Dhief, Naseer Sabri, Salim M. S, Fouad S and Aljunid S. A, “MANET routing protocols evaluation AODV, DSR and DSDV perspective”, In MATEC Web of Conferences, EDP Sciences, vol. 150, pp. 1-6, 2018.

13. Zhinan Li and Yinfeng Wu, “Smooth mobility and link reliability-based optimized link state routing scheme for MANETs”, IEEE Communications Letters, vol. 21, no. 7, pp. 1529-1532, 2017.

14. Marwan Hamid Hassan, Salama A. Mostafa, Mazin Abed Mohammed, Dheyaa Ahmed Ibrahim, Bashar Ahmed Khalaf and Ahmed Salih Al-Khaleefa, “Integrating african buffalo optimization algorithm in aodv routing protocol for improving the QOS of manet”, Journal of Southwest Jiaotong University, vol. 54, no. 3, pp. 1-12, 2019.

15. Prasath N and Sreemathy J, “Optimized dynamic source routing protocol for MANETs”, Cluster Computing, vol. 22, no. 5, pp. 12397-12409, 2019.

16. Kefayat Ullah and Prodipto Das, “Trust-based routing for mitigating grayhole attack in MANET”, In Proceedings of the International Conference on Computing and

Communication Systems, Springer, Singapore, 2018, Doi.org/10.1007/978-981-10-6890-4_68.

17. Raju L Raghavendar and Reddy C. R. K, “Node activity based trust and reputation estimation approach for secure and QoS routing in MANET”, International Journal of Electrical and Computer Engineering, vol. 9, no. 6, pp. 5340-5350, 2019.

18. Vallala Sowmya Devi and Nagaratna P. Hegde, “Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer”, Wireless Personal Communications, vol. 100, no. 3, pp. 923-940, 2018.

19. Radha Raman Chandan, “Consensus routing and environmental discrete trust based secure AODV in MANETs”, International Journal of Computer Networks & Communications (IJCNC), vol. 12, no. 3, pp. -20, 2020.

20. Muhammad Salman Pathan, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon and Muhammad Iftikhar Hussain, “An efficient trust-based scheme for secure and quality of service routing in MANETs”, Future Internet, vol. 10, no. 2, pp. 1-16, 2018.

21. Mingchuan Zhang, Meiyi Yang, Qingtao Wu, Ruijuan Zheng and Junlong Zhu, “Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs”, Future Generation Computer Systems, vol. 81, pp. 505-513, 2018.

22. Abdesselem Beghriche and Azeddine Bilami, “A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile ad hoc networks”, International Journal of Intelligent Computing and Cybernetics, vol. 11, no. 2, pp. 2, pp. 309-340, 2018.

23. Ruo Jun Cai, Xue Jun Li and Peter Han Joo Chong, “An evolutionary self-cooperative trust scheme against routing disruptions in MANETs”, IEEE transactions on Mobile Computing, vol. 18, no. 1, pp. 42-55, 2018.

24. Moresh Madhukar Mukhedkar and Uttam Kolekar, “Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm”, The Computer Journal, vol. 62, no. 10, pp. 1528-1545, 2019.

25. Rahul K Ambekar and Uttam D. Kolekar, “T-TOHIP: Trust-based topology-hiding multipath routing in mobile ad hoc network”, Evolutionary Intelligence, vol. 6, no. 2, pp. 150-158, 2019.