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

Lucindia Dupak1 · Subhasish Banerjee1

Accepted: 17 March 2022 / Published online: 13 May 2022 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Many researchers have been inspired to work on diverse challenges by a particularly favourable platform, namely mobile ad hoc networks (MANET) routing optimization. However, the lack of trust assessment is one of MANET’s main flaws. As a result, trust-based routing has received increasing attention in MANET over the last few years. Hence, the majority of recent work has focused on the development of routing protocols for security enhancement in a hostile environment. However, on the MANET environment, these protocols have many weaknesses and are also not that much secure. Hence, the primary goal of this study is to design a framework for balancing multiple performance measures in order to find the optimal multipath routing solution. In this scheme, we have employed the exponential cauchy kernelized adaptive neuro-fuzzy inference system (ECK-ANFIS) focused trust assessment with hybrid trust (HT) evaluation and optimal MANET routing. The ECK-ANFIS evaluates the trust after the nodes are initialised where, HT and the weight value, which are estimated for each node throughout the evaluation. The performance of the proposed mechanism has been measured using the various metrics defined in the existing protocols and also proved the superiority of the scheme by comparing it with other related ones.

Keywords Hybrid trust · Weight evaluation · Exponential cauchy kernelized adaptive neuro-fuzzy inference system (ECK-ANFIS) · Improved K-harmonic mean (IKHM) · And Ad hoc on-demand multipath distance vector-range emperor penguin optimization (AOMDV-REPO)
1 Introduction

In recent years, the ubiquity of wireless communication systems and comparable expectations has prompted researchers and investigators to develop efficient, strong routing mechanisms in order to meet the burgeoning QoS demands. As a result, several efforts have been made to make reliable communications, but there are numerous threats that have gone unaddressed, such as Integrity, Privacy, Security, and Trust. The MANET [1] is an independent cluster of mobile users who connect via unreliable wireless links. It controls network connectivity and data transformations solely through collaboration amongst mobile nodes with limited communication scope [2]. MANET is employed in military, Bluetooth operations, personal areas, vehicle network fields, and industrial sectors because it is flexible and easy to deploy in an adversarial environment [3], necessitating the need for trusted MANET. As the heart of MANET communication, the routing protocol conducts important functions such as shortest pathfinding, Route Discovery (RD), and data transmission as a source–destination node in an open wireless environment [4]. Where, the quality of routing solutions is the major deciding element for total network performance in any network type [5]. Moreover, routing on MANET is primarily responsible for exchanging route information and determining a possible path to a destination based on the hop count and minimum power required [6]. By enhancing the routine, the network can regularly modify the path without disrupting the constraint, which is the most important aspect of MANET routing [7]. Routing protocols in MANET are often divided into three categories based on their architecture and routing procedure: (1) proactive, (2) reactive, and (3) hybrid routing protocols [8]. Destination Sequenced Distance Vectors (DSDV) [9] and Optimized Link States Routing (OLSR) [10] are commonly used as proactive routing protocols that display the network state immediately after the malicious nodes connect. Whereas, the reactive routing protocols are ad hoc on-demands distances vector (AODV) [11] and Dynamics Sources Routing (DSR) [12] start immediately when the nodes need data packets to be transferred, while simultaneously lowering bandwidth costs. Because of the node’s dynamic nature and the frequent changes in the topology, determining the best route for communication is a difficult task [13]. Furthermore, if a node acts maliciously or selfishly, the entire network will be disrupted. Because MANET is used in a variety of applications, it is critical to keep the network safe from rogue nodes. Therefore to withstand the specified complications and the most significant issues in MANET, the proposed approach is insinuate. This approach employs ECK-ANFIS centered trust assessment utilizing HT evaluation and weight value. The REPO (Range Emperor Penguin Optimization) algorithm is proposed for the Route Discovery and optimal selection of route.

Here, the ECK-ANFIS evaluates the trust after the nodes are initialised where, HT and the weight value, are estimated for each node throughout the evaluation. Later, the lower-level Trust Value (TV) nodes are kept isolated and placed in their own box. Whereas, the trustworthy node, forms the cluster. Moreover, the Cluster Head (CH) is created by using the Improved K-Harmonic Mean (IKHM)
technique. The route is discovered using the Ad hoc On-demand Multi-path Distance Vector (AOMDV) and the REPO uses the optimal routing process in maximizing the Network Life-Time (NLT). The list of abbreviations which have used throughout this article are summarized in Table 1.

The Proposed Scheme Comprises the following key contributions:–

1) A new REPO algorithm is instituted to discover and select optimal route. It manipulate the optimal routing technique to maximize the network life time.
2) The ECK-ANFIS scheme is introduced for the assessment of the trust value for the trust-sentient Routing Protocol.
3) It observed the huddling behaviour of EP, the fitness assessment is calculated and the possible optimal path is discovered.

The organisation of this article is defined as follows. Section 2 explains the current research methodology linked with the proposed work. Section 3 depicts the suggested HT calculation and optimal route selection procedure. The experimental results and comparison with the related works have discussed in Sect. 4. Finally, the overall conclusion of this research is defined in Sect. 5 and the future possible research direction is given in Sect. 6.

Table 1 List of Notations

| Abbreviation | Definition |
|--------------|------------|
| RD           | Route discovery |
| ECK ANFIS    | Exponential cauchy kernalized adaptive neuro-fuzzy inference System |
| HT           | Hybrid trust |
| TV           | Trust value |
| IKHM         | Improved K-harmonic mean |
| CH           | Cluster head |
| REPO         | Range emperor penguin optimization |
| PDR          | Packet delivery ratio |
| EC           | Energy consumption |
| NLT          | Network life time |
| DT           | Direct trust |
| IDT          | Indirect trust |
| MF           | Membership function |
| EP           | Emperor penguin |
| MANET        | Mobile network |
| ANN          | Artificial neural network |
| CNN          | Convolutional neural network |
| SVM          | Support vector system |
| ANFIS        | Adaptive neuro-fuzzy inference system |


2 Related work

In recent studies, many trust-based routing protocols have been developed in MANET, and they have attracted a lot of interest amongst researchers. In this regard, Muhammad Salman Pathan et al. [14] has proposed a trust-centered secure Quality of Services (QoS) by combining social and QoS trust. In their scheme, the main strategy relied on reducing the number of nodes that displayed inconsistent packet forwarding behaviour, as well as path discovery, which enabled trustworthy communication via the trust mechanism. The best forwarding node in terms of QoS criteria is chosen by the scheme based on packet forwarding behaviour and capability. The system’s performance have evaluated under a variety of network situations as well as QoS settings. Other than improvement in network overhead like, Packet Delivery Ratios (PDR) and Energy Consumptions (EC), the system’s performance has also enhanced in terms of security and QoS. Unfortunately, the system is not that much intelligent since the node capability and reliability has not intelligently examined.

In the same year, i.e. 2018, Mingchuan Zhang et al. [15], proposed a bio-inspired Hybridized Trusted Routing Protocol (B-iHTRP) based on trusted appraisal, Ant Colony Optimizations (ACO), and Physarum Autonomics Optimization (PAO). In their approach, initially, the cross-layer perception has merged into ACO in order to obtain perceptive ants. The network is then partitioned into multiple zones. The routing table has proactively maintained in each zone by alert ants that sensed various characteristics. Where, the perceptive ants have deployed to reactively identify paths to end amongst the zones while sensing corresponding factors. Then, using PAO, B-iHTRP choses the best of the identified paths and automatically optimised the local paths in the context of multiple-zone communication. In comparison to existing algorithms, B-iHTRP has achieved superior results. However, in their scheme, the trust evaluation has not an automatic process, and it took fewer link metrics into account for assessment.

Therefore, to address the Trust issue, Abdesselem Beghriche and Azeddine Bilami [16] proposed a trusted routing system that would mitigate the various attacks. In MANETs, the concept of trust has been incorporated, and grey relational examination theory combined with fuzzy sets have used to estimate a node’s Trust Level (TL) based on observations of neighbour node’s TL. After that those TL were used to make routing decisions. Several tests have conducted to verify the applicability of the proposed solution. The strategy is useful in reducing the effects of the hostile nodes and improved the system’s safety. However, the method’s authentication process has certain complications.

Later, Ruo Jun Cai et al. [17] suggested an Evolutionary Self-Cooperatives Trust (ESCT) system for countering divergent routing disturbance attacks that emulated the human cognitive process and depended on TL information. In their scheme, the Mobile nodes would exchange trust information, which would subsequently be assessed based on their cognitive judgement. For excluding malicious entities, every node evolved its cognition dynamically. The system can not be
compromised even if the interior attackers encompassed the knowledge concerning the security mechanism. The overall ESCT's performance has been measured under disparate routing disruption attack situations. The ESCT has promoted the network scalability as well as ensured routing efficacy on the routing disruption attackers’ presence on MANET. However, the performance has only proved under the less coverage environment only.

In 2019, Moresh Madhukar Mukhedkar and Uttam Kolekar [18] suggested superior encryption standard-facilitated trust-centered secure routing concerning the recommended Dolphin Cat Optimizer. The Optimizer is exhibited on the optimum route assortment. It has the amalgamation of Dolphin Echolocation with the Cat Swarm Optimizations that inherited the quicker universal convergence. The simulation has been done utilizing ‘75’ nodes. It exhibited that the protocol attained the maximum throughput, least packet drop, minimal delay, along with high detection rate. However, the approach has not trusted as the algorithm encompassed a premature convergence issue that affected the system’s performance.

Further, to remove the vulnerabilities and secured the route, Rahul K. Ambekar and Uttam D. Kolekar, in 2019 [19], has proposed the trust-centered topology-hiding Multiple-Path Routing (MPR) algorithm in MANET. In their scheme, the MRP determined the secure path between the sender and receiver based on the chosen neighbour nodes. Finally, data transfer has accomplished via the multiple-path option. The MPR’s performance has 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. However, if the distance between the nodes was increased, the TV might be changed.

Hence, in this article, the proposed technique, i.e. REPO, is designed to withstand the described challenges and the most major issues in MANET.

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.
between 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 Fig. 1.

3.1 Node initialization

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

$$\overline{S}_d = \{s_1, s_2, s_3, \ldots, s_n\}$$  \hspace{1cm} (1)

Here, $\overline{S}_d$ signifies the MANET’s nodes as well as $s_n$ 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,

$$IT_{\tilde{s}_i, \tilde{s}_{i+1}} = \frac{K_s}{K_r}$$  \hspace{1cm} (2)

where in, $IT_{\tilde{s}_i, \tilde{s}_{i+1}}$ signifies the DT value of the node $\tilde{s}_i$ and its neighbour node $\tilde{s}_{i+1}$, $K_s$ defines the successful packet sent from the node $\tilde{s}_i$ and $K_r$ indicates the successful packet received as of the node $\tilde{s}_{i+1}$. Next, the IDT is evaluated for the node. Therefore, the IDT is well-known that the node with the witness factor is authenticated centered upon DT. The IDT evaluation $IIT_{\tilde{s}_i}$ is derived as,
where \( r \) states the total neighbours of the node. Lastly, the TV is implied as the amalgamation of DT and IDT, which is rendered in Eq. (4):

\[
\delta_i = \sum_{i=1}^{n} \text{IT}_{i, i+1}, \ IIT_{\bar{i}}
\]

Here, \( \delta_i \) 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 Eq. (5):

\[
\omega_i = \sum [\alpha(t), \beta(t), \chi(t), \lambda(t)]
\]

where \( \omega_i \) 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 neighbour node transmits only their data and does not transmit the others’ data, which is implied as to the selfish node. Thus, selfish analysis is vital, which is displayed in Eq. (6):

\[
\alpha(t) = \begin{cases} 
\frac{an_{ij}(t)-er}{\text{PEC}_{ij}(t)-er} & \text{an}_{ij}(t) \leq \text{PEC}_{ij}(t) \\
\frac{ur-an_{ij}(t)}{ur-\text{PEC}_{ij}(t)} & \text{an}_{ij}(t) > \text{PEC}_{ij}(t)
\end{cases}
\]

wherein, \( \alpha(t) \) signifies the data forwarding rate, \( \text{an}_{ij}(t) \) implies the quantity sending of the period \( t \), \( \text{PEC}_{ij}(t) \) 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,

\[
\beta(t) = \frac{\text{DAN}_{ij}(t)}{\text{DAN}_{ij}(t) + \text{COR}_{ij}(t)}
\]

where \( \beta(t) \) signifies the consistency factor, \( \text{DAN}_{ij}(t) \) implies the accordant packets, and \( \text{COR}_{ij}(t) \) 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.

\[
\chi(t) = \begin{cases} 
    \text{hh} & \text{high} \\
    \text{ll} & \text{low} \\
    \text{nn} & \text{normal}
\end{cases}
\]  

where \( \chi(t) \) represents the time factor, and \( \text{hh}, \text{ll}, \text{nn} \) 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:

\[
\lambda(t) = \frac{sd(t)}{rr(t)}
\]

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 Sugeno model in the adaptive system framework for assisting its learning as well as adaptation. The ANFIS makes 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 \( \delta_i \) and \( \omega_i \), 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 \( \delta_i \) is \( \varepsilon_i \) and \( \omega_i \) is \( \varepsilon_i \) then,

\[
R_i = p_i\delta_i + q_i\omega_i + \Psi_i
\]  

**Rule 2** If \( \delta_i \) is \( \varepsilon_{i+1} \) and \( \omega_i \) is \( \varepsilon_{i+1} \) then,

\[
R_{i+1} = p_{i+1}\delta_i + q_{i+1}\omega_i + \Psi_{i+1}
\]

where in \( \varepsilon_i \) and \( \varepsilon_{i+1} \) implies the fuzzy sets, \( p_i, q_i, \Psi_i, p_{i+1}, q_{i+1}, \Psi_{i+1} \) 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 Eq. (1–4):

**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,
where in, $La_{1,i}$ signifies the ‘1st’ layer output, and $\psi_i$ implies the exponential Cauchy kernel function that is exhibited as,

$$\psi_i = e^{\left(\frac{-1}{\|q_i - q_i\|^2}\right)}$$

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

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

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

**Layer 3** This is the normalization layer. As per Eq. (16), it normalizes the rules’ strength:

$$La_{3,i} = \overline{\zeta}_i = \frac{\zeta_i}{\sum \zeta_i}, i = 1, 2, \ldots, 6$$

**Layer 4** Every node is essentially an adaptive node with a node function

$$La_{4,i} = \overline{\zeta}_i \cdot R_i$$

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.

$$La_{5,i} = \sum_{i=1}^{n} \overline{\zeta}_i R_i$$

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

**Rule 1** If the $\delta_i$ is higher and $\omega_i$ is higher, then the TV is higher.

**Rule 2** If the $\delta_i$ is medium and $\omega_i$ is medium, the TV is medium.

**Rule 3** If the $\delta_i$ is low and $\omega_i$ 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 $i = 1, 2, \ldots, K$. 
### 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 centres and lessening computational intricacy. An effectual technique is engaged for data point’s allocation to cluster centres. 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.

\[
c_j = \frac{1}{t_n} \sum_{j=1}^{K} d_j
\]

(19)

where in, $t_n$ signifies the total nodes. Next, the cluster centres are signified as $C_i = \{c_1, c_2, \ldots, c_K\}$. The objective function $O_c(d_i, C_i)$ is found as,

\[
O_c(d_i, C_i) = \sum_{j=1}^{K} \frac{K}{\sum_{j=1}^{K} \|d_j - c_j\|^n}
\]

(20)

where ‘$K$’ states the total centroids as well as nodes. For each data point $d_i$, gauge its membership function $\rho\left(c_j | d_j\right)$ in every $c_j$ and its weight $w(d_j)$ as per Eq. (21):

\[
\rho\left(c_j | d_j\right) = \frac{\exp\left(-\rho \|d_j - c_j\|^{-h-2}\right)}{\sum_{j=1}^{K} \|d_i - c_j\|^{-h-2}}
\]

(21)

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

(22)

Here, $h$ signifies the parameter that is above 2, and $\rho$ states another constant parameter. Next, the cluster centre is updated via the subsequent equation:

\[
c_j = \frac{\sum_{j=1}^{K} \rho\left(c_j | d_j\right) \cdot w(d_j) \cdot d_j}{\sum_{j=1}^{K} \rho\left(c_j | d_j\right) \cdot w(d_j)}
\]

(23)

Until meeting the pre-specified cluster, the steps are repeated. Next, the final cluster set is denoted as $G_s = \{g_1, g_2, \ldots, g_n\}$ 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 disjointness 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 behaviour 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 $\mathbf{u}_{1D710}$ signifies the wind’s velocity and $\mathbf{u}_{1D707}$ implies the gradient of $\mathbf{u}_{1D710}$:

\[ \mathbf{u}_{1D705} = \nabla \mathbf{u} \]

wherein, im signifies the imaginary constant as well as $\mathbf{PP}_{1D707}$ 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 modelled mathematically using disparate assumptions. Those are (1) the temperature is ‘0’ when the polygon’s radius is below one, and (2) 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:

\[ \mathbf{PP}_{y} = \mathbf{v} + \text{im}(\kappa) \]
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 between 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 between 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:

$$EX = FO(A) \cdot E_p^{cp}(x) - J \cdot E_p(x)$$  \hspace{1cm} (28)

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 between neighbours that is accountable for tuning the distance $EX$, and therefore, the terms are computed utilizing Eq. (29) and (30):

$$J = a_1$$ \hspace{1cm} (29)

$$A = M \times \left( U_0 + G_g(y_c) \right) \times a_2 - U_0$$ \hspace{1cm} (30)

$$G_g(y_c) = E_p^{cp}(x) - E_p(x)$$ \hspace{1cm} (31)

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

$$a_{ft} = \bar{pp}_1 + \bar{pp}_2 \times \left( l_r + u_r \right), ft = 1, 2$$ \hspace{1cm} (32)

wherein, $\bar{pp}_1$, $\bar{pp}_2$ 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:

$$FO(A) = \left( \sqrt{b \cdot e^{-x/m} - e^{-x}} \right)$$ \hspace{1cm} (33)

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:

$$E_p(x + 1) = E_{cp}^p(x) - A \times EX$$  \hspace{1cm} (34)

where $E_p(x + 1)$ signifies the EP’s subsequent updated position.

Figure 2 elucidates the REPO pseudocode. Amid the iteration, the huddling behaviour 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 [20] and F-Measure metrics [21], the proposed ECK-ANFIS centered trust assessment’s performance is examined with the existent ANFIS [22], artificial neural network (ANN) [23], convolutional neural networks (CNN) [24], together with support-vectors machines (SVM) [25].

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.

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 2 Parameters for the Network simulation |
|-----------------------------------------------|
| Parameter                  | Value                                    |
| Simulator                  | NS-2                                     |
| Topology                   | Arbitrary node placement                 |
| Simulation area            | 1000 × 1000 m                            |
| Packet size                | 512                                      |
| No.of nodes                | 200                                      |
| Simulation time            | 500 s                                    |
| Channel type               | Wireless                                 |
| Antenna type               | Omnidirectional                          |
| Initial energy             | 75 Joules                                |

| Table 3 Accuracy analysis |
|---------------------------|
| Methods                   | Accuracy (%) |
| Proposed ECK-ANFIS        | 96           |
| ANFIS [22]                | 87           |
| ANN [23]                  | 83           |
| CNN [24]                  | 84           |
| SVM [25]                  | 79           |
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 771 m 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 698 m, AODV has 654 m, DSR has 540 m, and OLSR has the 608 m 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 (Table 4).
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 by the system. Here, concerning the total malicious (or) selfish nodes, the EC is examined. Only 12.56 J 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 14 J, AODV has 18.23 J, DSR has 19.42 J, and OLSR has 17.56 J 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.

The throughput of the proposed as well as existent research methods is displayed in Fig. 6. Concerning the sensor node counts, the throughput is examined in this analysis. Herein, the sensor node count is taken in the gamut of 20–100 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%, and 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.

Throughput = packets delivered/Simulation Time

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 50 s 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 50 s. 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.

PDR = Total no. of packets received/Total no. of packets sent

The EED of the proposed AOMDV-REPO with the existent AOMDV, AODV, DSR, and OLSR is displayed in Fig. 8. Centered on the total malicious nodes (or) selfish nodes present on the network, the performance is examined. The proposed takes 9.9 s 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 6.8 s delay but the existent AOMDV has 9.5 s, AODV has 10.8 s, DSR has 14 s, as well as OLSR 10.9 s delay on the 30 s. 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.

End to End Delay = Time at reception of packet/Time at generation of packet

![Graphical representation of PDR analysis](image)
4.3 Time complexity analysis of the proposed model

Time complexity is the computational complexity that determine the amount of time system needs to execute a routing protocol. By flooding a RR message through Bi-directional flow in On-demand routing protocols which usually occurs for route discovery. Thereupon, AODV, DSR, OLSR have the identical time complexity $= O(2d)$ [26]. Our proposed AOMDV-REPO algorithm is loop free as well as disjoint, also update rules implemented locally at every node thus re-address messages homogenously with temperature $t$. Thus, the time complexity needed for all the nodes in a radius $= 0.5$ of the network with size $r$ is $O(\log r)$. The REPO is an extended algorithm which is more structured and adaptable than the basic flooding ad hoc routing protocols. To analyse the trustability, the REPO depends on temperature $t$. If $t = 1$ then its performance is more improved compare to the simple on demand routing algorithm. If $t = 0$, the nodes becomes malicious (Fig. 9).

5 Conclusion

In this paper, we have illustrated a new scheme which is a hybrid model based on trust assessment and route discovery. For methodical packet channelling the best possible route selection is the most consequential concern in MANET. Therefore, in this scheme, the hybrid model, i.e. REPO, has been proposed which utilizes ECK-ANFIS for ascertainment of the trust assessment applying HT evaluation, Weight evaluation and optimal routing via the AOMDV. The proposed mechanism consists of total six phases—node initialization, trust assessment, cluster formation, CH selection, RD and route maintenance. By using the IKHM algorithm, here the cluster is formed and cluster head is selected. In this proposed work, the scheme’s performance is examined with the current methodologies for the trust assessment and route discovery. Here, the experimental analysis exposed that the ECK-ANFIS attains higher performance (i.e. 96%) in contrast to existent methodologies (ANFIS, ANN, CNN, SVM) in terms of the accuracy, Specificity, Sensitivity and F-measure metrics. With the help of AOMDV-REPO several routes are established and near optimal route is selected. It covers 1200 sqm area at 1000 rounds with regard to NLT. The simulation results shows a significant improvement and outperforms the prevailing methods (AOMDV, AODV, DSR, along with OSR) in regard to EC, PDR,
Hybrid trust and weight evaluation-based trust assessment…

EED, network size, and throughput. Therefore, this approach elevated the trust and security, and could reach the better performance than others (Table 5).

### 6 Limitations and future work

It is witnessed that ANFIS undergo constraints like analytical expenses and dimensionality while using large inputs, therefore, we have introduce ECK-ANFIS in our proposed work to perform better. In the future work, the proposed model can be well extended by considering more trust factors and more advanced method for enhancing trust and path selection.

### References

1. Sadayan G, Ramaiah K (2019) Enhanced data security in MANET using trust-based bayesian statistical model with RSSI by AOMDV. Concurr Comput Pract Exp. https://doi.org/10.1002/cpe.5397
2. Zhang D-G, Gao J-X, Liu X-H, Zhang T, Zhao D-X (2019) Novel approach of distributed & adaptive trust metrics for MANET. Wirel Netw 25(6):3587–3603
3. Aveena S, Senthilkumar C, Manikandan T (2020) Analysis and countermeasures of blackhole attack in manet by employing trust-based routing. In: 2020 6th international Conference on advanced computing and communication systems (ICACCS). IEEE, Coimbatore
4. Sarbhukan VV, Ragha L (2019) ETSR: enhanced trust based secure routing scheme for mobile ad hoc networks. J Comput Theor Nanosci 16(5–6):2265–2272
5. Nareshkumar RM, Phanikumar S, Singh MK (2018) Intelligent routing in manet using self-adaptive genetic algorithm. Advances in systems control and automation. Springer, Singapore, pp 595–603
6. Rao GBN, Veeraiah D, Rao DS (2020) Power and trust based routing for manet using rrrp algorithm. In 2020 2nd international Conference on innovative mechanisms for industry applications (ICIMIA), IEEE, Bangalore
7. Harold Robinson Y (2019) 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.” Wirel Pers Commun 106(4):2261–2289
8. Sirajuddin M, Rupa CH, Iwendi C, Biamha C (2021) TBSMR: a trust-based secure multipath routing protocol for enhancing the qos of the mobile ad hoc network. Secur Commun Netw. https://doi.org/10.1155/2021/5521713
9. AL-Dhief FT, Sabri N, Salim MS, Fouad S, Aljunid SA (2018) MANET routing protocols evaluation AODV, DSR and DSDV perspective. In: MATEC web of Conferences, vol 150. EDP Sciences, pp 1–6
10. Li Z, Yinfeng Wu (2017) Smooth mobility and link reliability-based optimized link state routing scheme for MANETs. IEEE Commun Lett 21(7):1529–1532
11. Hassan MH, Mostafa SA, Mohammed MA, Ibrahim DA, Khalaf BA, Al-Khaleefa AS (2019) Integrating african buffalo optimization algorithm in adov routing protocol for improving the QoS of manet. J Southwest Jiaotong Univ 54(3):1–12
12. Prasath N, Sreemathy J (2019) Optimized dynamic source routing protocol for MANETs. Clust Comput 22(5):12397–12409
13. Kefayat U, Das P (2018) “Trust-based routing for mitigating grayhole attack in MANET”, In: Proceedings of the international Conference on computing and communication systems. Springer, Singapore. https://doi.org/10.1007/978-981-10-6890-4_68
14. Pathan MS, Zhu N, He J, Zardari ZA, Memon MQ, Hussain MI (2018) An efficient trust-based scheme for secure and quality of service routing in MANETs. Future Internet 10(2):1–16
15. Zhang M, Yang M, Qingshao Wu, Zheng R, Zhu J (2018) Smart perception and autonomic optimization: a novel bio-inspired hybrid routing protocol for MANETs. Futur Gener Comput Syst 81:505–513
16. Beghriche A, Bilami A (2018) A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile ad hoc networks. Int J Intell Comput Cybern 11(2):309–340
17. Cai RJ, Li XJ, Chong PHJ (2018) An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE Trans Mob Comput 18(1):42–55
18. Mukhedkar MM, Kolekar U (2019) Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm. Comput J 62(10):1528–1545
19. Ambekar RK, Kolekar UD (2019) T-TOHIP: trust-based topology-hiding multipath routing in mobile ad hoc network. Evol Intell 6(2):150–158
20. Hengpraprohm S, Chongstivatana P (2009) A feature selection by weighted–SNR for cancer micro array data classification. Int J Innovative Comput Inf and Control 5(12):4627–4635
21. Hand DJ, Christen P, Kirielle N (2021) F*: an interpretable transformation of the F-Measure. Machine Learning 110:451–456
22. Salleh MNM, Hussain K (2016) A review of training methods of ANFIS for applications in business and economics. Inte J u- and e- Serv 9(7):65–172
23. Abdolrasol MGM, Hussain SMS, Ustun TS, Sarker MR (2021) Artificial neural networks based optimization techniques: a review. Electronics 10(21):2689
24. Indolia S, Goswami AK, Mishra SP, Asopa P (2018) Conceptual understanding of convolutional neural network - a deep learning approach. International Conference on computational intelligence and data science, Elsevier
25. Cervantes J, Garcia-Lamont F, Mazahua LR, Lopez A (2020) A comprehensive survey on SVM classification: applications, challenges and trends. Neurocomputing 408:189–215
26. Srivastava M, Yadav P (2012) A performance analysis of routing protocols in mobile Adhoc networks. Int J Eng Res & Technol 1(8):11

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.