A CLUSTER-BASED TRUSTED SECURE MULTIPATH ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

Himanshu Bartwal [1], Himani Sivaraman [1], Jogendra Kumar [2]

[1] Department of Computer Science and Engineering, Jigyasa Univesity,Dehradun, Uttarakhand, India
[2] Department of Computer Science and Engineering, GBPIET Pauri Garhwal Uttarakhand,India

ABSTRACT

Mobile Ad Hoc Network (MANET) is a self-organizing and flexible system. MANET systems manage sensitive data from many distinct applications in various domains. Its dynamic nature increases its vulnerability to numerous types of security threats. Many of the present approaches using indirect approaches provide false approximations of trust degrees. It is significantly required a good routing system that meets Quality of Service (QoS) standards and enhances network performance. In this paper purposed cluster-based trustworthy safe multipath routing (CTSMP-Routing) for mobile ad hoc networks (MANETs). Load balancing challenge is addressed by using a modified proportional topology optimization (MPTO) approach using geographical data related to network nodes. The Enhanced Seeker Search Optimization (ESSO) approach is used to compute trust degrees after the clustering phase considering numerous network constraints including node mobility, received signal strength, energy consumption, and cooperation rate. Assumed to be the service node, the node showing the highest degree of trust manages inter-cluster routing. We have developed a hybrid soft computing approach termed the multi-layer deep recurrent neural network (ML-DRNN) to enhance the optimal path-finding process. This method selects, among many routes between source and destination nodes, the best one quickly. The outcomes of this paper demonstrate that CTSMP-Routing provides effective protection against several attack paths within the MANET environment and displays better performance in regard to quality of service (QoS) requirements.

KEYWORDS

Mobile Ad-Hoc Networks (MANET), Modified Proportional Topology Optimization(MPTO), Enhanced Seeker Search Optimization(ESSO), Multi-Layer Deep Recurrent Neural Network (ML-DRNN)

1. INTRODUCTION

All without depending on a permanent infrastructure, mobile ad hoc networks (MANETs) construct self-sustained wireless networks generated from mobile nodes [1]. These dynamically communicating nodes inside a MANET may use radio frequencies. MANETs provide a vital way for mobile users to interact with one another when either permanent infrastructure is not feasible or lacking [2]. The paths within a MANET often present difficulties including interference from outside sources, transmission issues, and node mobility by nature. Thanks in great part to the internet's explosive growth, MANETs have become somewhat popular recently [3]. These networks are unique in that they run free from any kind of supporting infrastructure. Furthermore easily integrated with current fixed infrastructure systems, they improve their communication capacity [4-5] MANET grew out of the explosion of affordable wireless networking devices and

desire for anytime, anywhere mobility. Here, several nodes are wirelessly linked and communication takes place between nodes inside each other's coverage zones. With this technology, mobile devices liberate themselves to go in any direction within the range of the radio connection, independent of permanent infrastructure [6]. The small transmission range emphasizes the need for every node's availability as it requires nodes to transmit messages across many hops [7]. Therefore, as it determines the best route between the data source and destination, the need for an effective routing protocol takes the front stage.

In this sense, routing refers to provision for multipath connections to surrounding nodes dynamically established mostly via the mobile nodes acting as routers [8]. Nevertheless, this dynamic architecture, unique to wireless networks with nodes in motion, makes MANETs vulnerable to many security flaws [9]-[11]. Many routing strategies have been studied solve these issues with an eye on consistent data broadcast and greeting among nodes [12]. The demand-based AODV technique[13] has shown amazing performance among the current routing protocols [14-16] in several circumstances including varied mobility patterns, network density, and traffic loads. It does, however, have a problem wherein the number of control packages increases to maintain course planning to the goal. Moreover, studies have explored many guiding assaults started by evil nodes. In response to these concerns, methods using the trustworthiness of mobile nodes helping in routing or node authentication via certificate issuing have been investigated [17-18]. Precisely, recreating a new route from the foundation to the terminal may be a time-consuming procedure that increases control packets and consequent overhead when packet damage or route interruptions arise from assaults along the way. Maintaining the seamless running of MANETs provides a significant difficulty for security. Maintaining basic network services, data confidentiality, and integrity during transmission depends on addressing these security concerns [19]. MANETs' natural characteristics—open communication medium, changing topologies, absence of centralized monitoring—all of which contribute to a variety of security concerns [20] Therefore, the whole consistency of MANETs depends on the development of safer and more effective safe routing techniques.

The rest of this paper is prearranged as follows. Section 2 offerings the appraisal of recent works linked to the secure routing for MANET. Segment 3 Network architecture of proposed CTSMP-Routing scheme. The thorough working procedure of planned CTSMP-Routing scheme is clarified in the Section 4. Simulation Parameters 5.The results and qualified analysis of planned and existing routing systems have debated in Section 6. Finally, the paper arranges in Section 6.

2. RELATED WORK

Rajashanthi et al. [21] have introduced an inventive system designed to ensure secure and reliable data communication, hinging on QoS requirements and encryption techniques. Their approach combines multipath routing utilizing the AODV-BR protocol with optimal fuzzy logic. The development of these paths is guided by an adaptive grey wolf optimization method, aimed at identifying the most efficient route. To enhance data security, the system employs homomorphic encryption for data key management.

Elmahdi et al. have [22] introduced an innovative approach to enhance the reliability and security of data transmission in MANETs, particularly in the face of potential black hole attacks. They achieved this by separating message distribution into many paths traveling toward the target using a modified AOMDV technique. For security reasons, a homomorphic encryption scheme was used to ensure data integrity and confidentiality.

Tripathy et al. have [23] suggested an adaptive routing system fit for MANETs. This protocol demonstrates how dynamically changeable routing capabilities based on various metrics—

including diverse demand criteria and contextual features—can be attained. Among numerous aspects, these demand models include performance, security, and functional requirements. Under examination in this protocol are many contextual elements: the mobility of nodes or groups of nodes, trust values given to nodes, individual node resource restrictions, geographical context, and network node duties.

Vatambeti [24] introduced the idea of grey wolf trust accumulation (GWTA). This approach greatly helps to identify prospective attacks by employing the fitness function of the GWTA model. Suspected attacked nodes are found and used for the final position of the network to greatly lower packet flow.

Sirajuddin et al. [25] have developed a trust-based multipath routing protocol (TBSMR) to enhance the complete MANET presentation. TBSMS displays interesting strengths all aimed at increasing QoS by addressing numerous factors, including congestion management, packet loss reduction, malicious node identification, and safe data transmission facilitation. It considers numerous factors like node trust standards, congestion levels, and node attainable battery capacity all through the routing process.

Simpson et al. [26] have offered a secure technique suited for the smart city scenario. Cooperative attacks need a coordinated effort across multiple IoT network nodes. Secure SEAL addresses challenges by building a fuzzy-based accountability scenario designed to lower security threats in smart cities.

Benatia et al. [27] have developed an enhanced multipath quality-based routing system for urban settings (EMQS-UA). By selecting paths with superior link quality and more stable connections, this protocol ensures consistent data transmission; thus, in urban areas the focus should be on link excellence and consistency. Two key measurements—SNR and EMQS—UA combine. The SNR measurement increases the accuracy of the quality estimation process, therefore lowering the link quality degradation. This device is specifically suited to operate in urban settings where shadowing effects and background noise might seriously degrade connection quality. Combining these characteristics ensures that EMQS-UA is prepared to handle the challenges given by urban networking environments.

Usha et al. [28] have shown an energy-efficient trust-aware routing (NETAR) to increase trust levels across nodes in MANETs. NETAR employs a varied approach to develop trust among nodes by analyzing the trust rate of neighboring nodes, evaluating the available bandwidth, predicting energy usage, and recognizing probable hostile activities.

Ran et al. [29] have introduced a multi-path QOS routing security algorithm by using blockchain, which enhances the traditional AODV protocol (AODV-MQS). This algorithm incorporates a chain of nodes within the network and preserves the states of all nodes by designating certain intermediate nodes along this chain. The Blockchain technology uses smart contracts to filter out nodes that adhere to QoS constraints. Through the application of smart contracts within the blockchain network, AODV-MQS identifies two distinct communication paths that are not significantly correlated. One path serves as the primary route, while the other acts as a standby route. It's important to note that this mechanism focuses primarily on un-trusted nodes within the network.

Hemalatha et al. [30] have introduced an approach for establishing optimal, loop-free routes using the equilibrium optimizer (EO) in combination with fuzzy logic, ensuring the continuity of data transmission. EO with fuzzy logic during route exploration to determine the most efficient path for packet transmission. The selection of appropriate nodes for routing, they incorporates the Levy Flight distribution mechanism. In the route conservation phase, the system assesses the

status of nodes before data broadcast. The direction retrieval process utilizes the backward reply which is generated from the destination node, and a reactive path setup process is employed. A multipath setup process is applied for handling header information by middle nodes, thereby enhancing the efficiency of data transmission.

The proposed Cluster-Based Trusted Secure Multipath Routing Protocol (CTSMP-Routing) enhances security, trust evaluation, and energy efficiency by integrating Multipath Trust Optimization (MPTO), Energy-Saving Service Optimization (ESSO), and Multi-Layer Deep Recurrent Neural Network (ML-DRNN), ensuring adaptability to node mobility and energy constraints. Unlike traditional protocols such as TMRP and TSR, which rely on static or probabilistic trust evaluation, CTSMP-Routing employs real-time trust computation using ML-DRNN, reducing misclassification risks. ESSO optimizes energy efficiency by balancing network load, and preventing premature node failures—an aspect often overlooked in existing protocols. MPTO's trust-aware multipath selection enhances resilience against blackhole, gray hole, and Sybil attacks, ensuring robust and secure data transmission in dynamic MANET environments.

3. PURPOSED CTSMP-ROUTING SCHEME AND NETWORK STRUCTURE

Figure 1 shows the Purposed CTSMP-Routing system and its whole structure as well as the sequence of operations engaged in its operation. The proposed CTSMP routing scheme structure for a MANET is based on a clustered approach, where mobile nodes or cluster members communicate within clusters through service nodes that facilitate intra-cluster routing and inter-cluster routing towards the base station. Each cluster operates independently for local communication, while inter-cluster routing ensures efficient data transmission by forwarding information through selected service nodes until it reaches the base station, optimizing network performance and reducing communication overhead. The program starts with mobile nodes placed within the MANET system. The network passes through a critical phase—that of cluster development—once the nodes are in place. The modified proportional topology optimization (MPTO) technique helps this process to be eased. The MPTO method assures that the network achieves load balancing and energy economy, hence organizing the mobile nodes into clusters primarily relies on it. The approach then generates trust degrees among the cluster members after cluster evolution. It does this using an enhanced search optimization (ESSO) method. The trust degree computation determines the reliability of cluster members and influences the choosing of and service node within every cluster as well. Key participants in the routing process, service nodes are carefully chosen based on several design criteria, therefore boosting security at the first level in addition to network performance. After the service nodes are established in place, the method employs a multi-layer deep recurrent neural network (ML-DRNN) comprising an optimal route finder. This neural network helps one to identify and decide on the most appropriate path between the source and destination nodes. Apart from increasing data transfer efficiency, this decision process is supposed to provide a robust protection against any risks and security breaches.

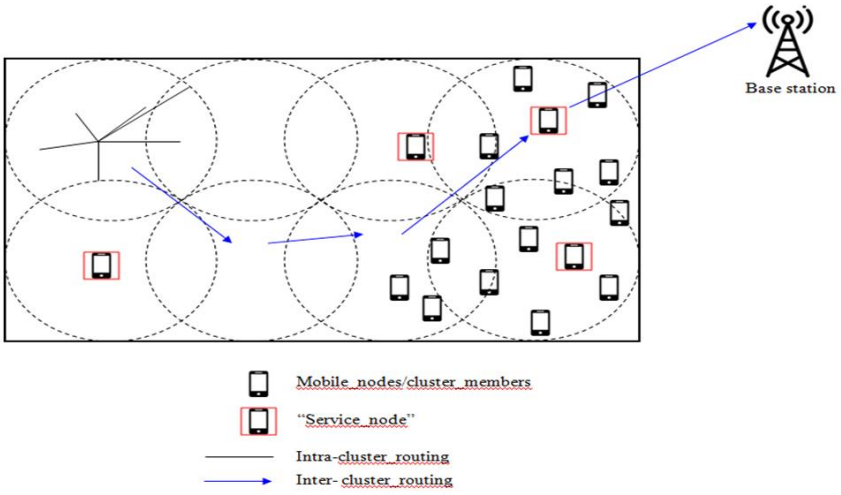

Fig. 1. Proposed_CTSMP- Routing-scheme-structure

ML-DRNN optimizes routing decisions by predicting node mobility patterns and selecting the most energy-efficient paths, reducing unnecessary retransmissions and prolonging network lifespan. ESSO dynamically adjusts service node selection based on residual energy levels, ensuring that nodes with higher energy reserves handle more communication tasks, thereby balancing energy consumption across the network. Together, these algorithms minimize power wastage, extend battery life, and enhance the overall sustainability of the MANET. The proposed protocol adapts to the highly dynamic nature of MANETs by integrating ML-DRNN (Multi-Layer Deep Recurrent Neural Network) for predictive routing and ESSO (Energy-Saving Service Optimization) for adaptive node selection. ML-DRNN continuously analyzes mobility patterns and anticipates topology changes, enabling proactive route adjustments before disconnections occur. Additionally, ESSO ensures that service nodes are dynamically reassigned based on network conditions, maintaining stable communication links. To handle frequent route recalculations, the protocol employs hierarchical clustering to localize route updates, reducing overhead and minimizing delays. By combining predictive analytics, adaptive node selection, and localized route updates, the protocol efficiently manages rapid topology changes while maintaining network stability and performance.

This paper introduces the Cluster-Based Trusted Secure Multipath Routing Protocol (CTSMP-Routing) for Mobile Ad Hoc Networks (MANETs), designed to improve routing security and network performance by integrating MPTO (Multipath Trust Optimization), ESSO (Energy-Saving Service Optimization), and ML-DRNN (Multi-Layer Deep Recurrent Neural Network). MPTO ensures secure multipath routing by evaluating trust levels among nodes, reducing the risk of malicious attacks. ESSO optimizes energy consumption by dynamically selecting service nodes based on residual energy, balancing network load. ML-DRNN enhances routing efficiency by predicting mobility patterns, reducing route failures, and minimizing packet loss. Together, these techniques strengthen MANET security, optimize energy efficiency, and improve overall network reliability. A key concern in the proposed CTSMP-Routing protocol is the evaluation of trust degrees, particularly in the ESSO (Energy-Saving Service Optimization) algorithm. The methodology for computing trust values must be explicitly validated to minimize approximation errors that could result in the misclassification of trust levels, potentially leading to security vulnerabilities. To strengthen the credibility of the protocol, the paper should include empirical validation of trust computation mechanisms, ensuring robustness against inconsistencies. Additionally, since security is a primary focus, a comparative security analysis against common MANET threats—such as wormhole attacks, blackhole attacks, and Sybil attacks—should be

Conducted. This analysis would highlight the protocol's resilience in realistic attack scenarios, demonstrating how MPTO (Multipath Trust Optimization) mitigates these risks and ensures secure multipath routing. MPTO enhances trust evaluation in MANETs by integrating multiple trust factors, improving security, and minimizing frequent re-clustering, unlike traditional methods like LEACH and K-Means. ESSO, a hybrid swarm intelligence approach, offers superior convergence speed, load balancing, and reduced routing overhead compared to GA and PSO. ML-DRNN is chosen for path optimization due to its ability to capture temporal dependencies and outperform models like SVM and Decision Trees in real-time route prediction under high mobility. Compared to ANN and DQN, ML-DRNN ensures adaptive decision-making, making it more efficient for dynamic MANET environments while balancing performance and computational efficiency.

3.1. The Modified Proportional Topology Optimization (MPTO)

The modified proportional topology optimization (MPTO) approach yields perfect clustering. This approach is supposed to take advantage of spatial data on network nodes—that is, their locations and the distances separating them. MPTO aims to create clusters wherein the demand on each one is balanced, therefore avoiding the development of a bottleneck for network traffic from one cluster by itself. The method considers many input variables, including network characteristics, node locations, and maybe additional aspects as energy energy levels or node mobility. A well-defined cluster structure produced by the MPTO method best balances the load of the network. Every cluster comprises a group of geographically close-knit nodes, hence lowering the average communication distance inside the cluster. By increasing the general effectiveness of resource use and routing within the MANET, this company guarantees better network dependability and performance. The MPTO method aims to negotiate the ideal delivery of items satisfying the constraints and thus improve the objective meaning of the mathematical perfect. Before solving the optimization problem, the first task is to mature its mathematical model. However, if the expensive cannot precisely construct a mathematical model according to the necessities of the problem, the optimal outcomes will be greatly pretentious.

$$\begin{cases} Min\ D = u^S\ ku = \sum_{h \in B} e(p_h) u_h^S K_0 u_h \\ S.T \begin{cases} ku = f \\ \sum_{h}^{B} p_h v_h - v_{SA} = 0 \\ 0 \le p_{Min} \le p_h \le p_{Max} \le 1 \end{cases} \end{cases} \tag{1}$$

Where D is the mechanical conformation, u and f are the global movement and external force trajectories of the construction, respectively, k is the global stiffness matrix and $e(p_h)$ the corresponding Young's modulus u_h, h is the element displacement vector, which is the unit size of element stiffness K_0. The matrix. The unit Young's modulus is the component size v_h, VTM is the board substantial capacity in the design domain p_h, B is the number of rudiments gotten by removing the enterprise field, individual element i, p_{Min} and p_{Max}. Its value regulates the retention and exclusion of rudiments and represents the upper and lower bounds of the element concentration variable p_h, respectively. In general, $p_{Max} = 1$, and p_{Min} , and should be given a lower bound slightly greater than zero to avoid the stiffness singularity; However, it is the

performance that determines the value p_{Min}. Based on the improved SIMP technique, the substantial interruption scheme is written as follows:

$$e(p_h) = e_{Min} + p_h^x(e_0 - e_{Min}), \quad p_h \in [0,1] \tag{2}$$

For the minimization optimization problematic, an better density filter is compute as follows.

$$\tilde{p}_h = \frac{1}{\sum_{g \in B_h} I_{h,g}} \sum_{g \in B_h} I_{h,g} p_g \tag{3}$$

All g elements at h element distance are filtered densities measured B_h from their respective centers R_{Min}. The $e(p_h)$ derivative is the weighting $I_{h,g}$ factor between the elements h and g

$$I_{h,g} = Max(0, R_{Min} - c(h,g)) \tag{4}$$

where h and g are the geometric center $c(h,g)$ distance between the elements and the radius R_{Min} of the filter. An additional optimization scheme was created for the density variable

$$\Delta p_h^{out} = v_{ra} \cdot \tilde{p}_g \cdot \Delta \tilde{D}_h \tag{5}$$

In order for the compliance coefficient to drama a larger role in updating the density mutable in the inner loop, the obedience coefficient filter introduces a q. parameter. Based on a combination of matching factor and filtering techniques, it expresses:

$$\Delta \tilde{D}_h = \frac{1}{\sum_{g \in B_h} I_{h,g}} \sum_{g \in B_h} I_{h,g} \Delta D_g^y \tag{6}$$

Correspondence coefficient is compute by Bickley threshold function,

$$\Delta D_h = \frac{D_h^\lambda}{\sum_{g=1}^{B} D_g^\lambda v_g} \tag{7}$$

The residual volume of the material VRM is an significant midway variable for updating the density adjustable in the inner loop, which is printed as:

$$v_{ra} = v_{Sa} - \sum_{h \in B} p_h^{pro} \cdot v_h \tag{8}$$

The p_h^{pro} density adjustable found at each restatement of the inner cycle, h is the variable increase in element density Δp_h^{out}, and λ is the conformational inspiration coefficient. h and g represent the item relevance Δp_h^{out}. D_h and D_g, represents the relevance ratio and filtered relevance ratio, respectively, ΔD_h and $\Delta \tilde{D}_h$, y is the influence ratio of the relevance ratio.

$$p_h^{out} = p_h^{pro} + \Delta p_h^{out} \tag{9}$$

Based on the weighting factor, the variable density gain of component h is designed as a prejudiced average of the variable thickness gains of its neighboring element. Then, using the drinkable density mutable increment and the density mutable, a density variable optimization system can be describe as follows.

$$p_h^{out} = p_h^{pro} + \Delta \tilde{p}_h^{out} \tag{10}$$

where $\Delta \tilde{p}_h^{out}$ is the elemental clean density adjustable increment, which is assumed as follows.

$$\Delta \tilde{p}_h^{out} = \frac{1}{\sum_{g \in B_h} I_{h,g}} \sum_{g \in B_h} I_{h,g} \Delta p_g^{out} \tag{11}$$

where Δp_g^{out} is the variable compactness augmentation of component g adjacent to element h. According to the MPTO algorithm and MAX-MIN system, the control scheme for the values of density variable star is articulated as follows.

$$p_h^{pro} = \begin{cases} p_{Min}, & p_h^{out} \le p_{\min} \\ p_h^{out}, & p_{Min} < p_h^{out} < p_{Max} \\ p_{Max}, & p_h^{out} \ge p_{Max} \end{cases} \tag{12}$$

where p_{Min} and p_{Max} are the higher and lesser limitations of density variable star, individually. Here, $p_{Min} = 0$ and $p_{Min} = 1$. The working step involved in the cluster creation using MPTO is explained in Algorithm 1.

Algorithm 1 Cluster formation using MPTO

Input	: Number of mobile nodes, maximum iteration, threshold condition
Output	: Cluster formation
1.	Setup FE and obedience analyses and sieving
2.	Define the material interpolation $e(p_h) = e_{Min} + p_h^x (e_0 - e_{Min}), \quad p_h \in [0,1]$
3.	Until convergence
4.	Check stop criteria, break if satisfied
5.	Compute density filter by using $\tilde{p}_h = \frac{1}{\sum_{g \in B_h} I_{h,g}} \sum_{g \in B_h} I_{h,g} p_g$
6	Compute correspondence coefficient $\Delta D_h = \frac{D_h^{\lambda}}{\sum_{g=1}^{B} D_g^{\lambda} v_g}$
7.	Apply filter
8.	Update density
9.	Find the density variable optimization $p_h^{out} = p_h^{pro} + \Delta p_h^{out}$

10. Perform clean density adjustable increment, $\Delta\tilde{p}_h^{out} = \frac{1}{\sum_{g\in B_h} I_{h,g}} \sum_{g\in B_h} I_{h,g} \Delta p_g^{out}$
11. End if
12. Update the final value
13. End

3.2. Enhanced Seeker Search Optimization (ESSO)

Enhanced seeker search optimization (ESSO) approach, trust degrees dependent on these design constraints are calculated. This optimization technique identifies the most reliable and trustworthy nodes in the network based on the already provided criteria. ESSO maximizes the choice of these nodes by weighing their conformity with these limitations. The ESSO technique computes a most highly trusted node that is chosen to be the service node. This node acts as a focal point for inter-cluster routing and is responsible for the routing of data between clusters and ensuring secure and efficient communication within the MANET. The egoistic direction $\vec{F}_{h,e}(s)$, altruistic direction $\vec{F}_{h,m}(s)$, and pre-emptive direction $\vec{F}_{h,X}(s)$ of the h-th individual in any dimension can be obtained as follows.

$$\vec{F}_{h,e}(s) = \vec{x}_{h,best} - \vec{p}_h(s) \tag{13}$$

$$\vec{F}_{h,m}(s) = \vec{j}_{h,best} - \vec{p}_h(s) \tag{14}$$

$$\vec{F}_{h,X}(s) = \vec{p}_h(s_1) - \vec{p}_h(s_2) \tag{15}$$

The chaser uses a random weighted average technique to obtain the search orientation.

$$\vec{F}_h(s) = sign(\omega\vec{F}_{h,X}(s) + \psi_1\vec{F}_{h,e}(s) + \psi_2\vec{F}_{h,m}(s)) \tag{16}$$

where: s_1, $s_2 \in$ {s, s − 1, s − 2}, $\vec{p}_h(s_1)$ and $\vec{p}_h(s_2)$ are the best advantages of $\{\vec{p}_h(s-2), \vec{p}_h(s-1), \vec{p}_h(s)\}$ separately; $j_{h,best}$ is the optimal position in the region where the h-th exploration factor is positioned; $x_{h,best}$ is the optimum neighborhood from the h-th exploration factor to the current locality; ψ_1 and ψ_2 are random numbers in [0,1]. ω is the weight of inertia.

$$\mu(\alpha) = E^{-\frac{\alpha^2}{2\delta^2}} \tag{17}$$

where α and δ are the parameters of the membership function and the probability that the output variable exceeds [−3δ, 3δ] is less than 0.0111. Under normal conditions, an individual's optimal level μ_{Max} = 1.0

$$\mu_h = \mu_{Max} - \frac{t - H_h}{s - H}(\mu_{Max} - \mu_{Min}), \quad h = 1,2,...t \tag{18}$$

$$\mu_{h,g} = Rand(\mu_h, 1), \quad g = 1,2,...C \tag{19}$$

Here H_h is the count of the arrangement $p_h(s)$ of the existing those arranged from high to low by meaning value. And the purpose rand $(\mu_h,1)$ is the real amount in any divider [μ_h,1].

$$\alpha_{hg} = \delta_{hg}(s) - \sqrt{-\ln(\mu_{hg})} \tag{20}$$

where, δ_{hg} is a restriction of the Gaussian circulation meaning, which is distinct as follows.

$$\delta_{hg} = \omega p * ABS(\vec{p}_{Min} - \vec{p}_{Max}) \tag{21}$$

Here, ω is the inertial weight. As the evolutionary algebra upsurges, ω decreases linearly from 0.9 to 0.1. $\vec{p}_{Min}$ and $\vec{p}_{Max}$ are are the minimum and maximum values of the function, respectively. After receiving the scout track and the person's scout step dimension, the location update is specified as follows

$$p_{hg}(s+1) = p_{hg}(s) + \alpha_{hg}(s)F_{hg}(s) \quad h = 1,2,....t; \; g = 1,2,....C \tag{22}$$

where h denotes the h-th searcher separate, g denotes the discrete dimension; $F_{hg}(s)$ and $\alpha_{hg}(s)$ respectively represents the seekers' search track and examination step size at time s, $p_{hg}(s)$ and $p_{hg}(s+1)$ correspondingly characterize the hunters' site at time s and (s + 1). The continuous brink x∈ [0,1] is set as the likelihood of seeker p_h being seized by a triple black hole system. For each seeker p_h, a accidental number l ∈ [0,1] is produced in each restatement. If l ≤ x, p_h is detained by a triple black hole scheme; otherwise, it is efficient in the outdated way.

$$p_{hg}(s+1) = \begin{cases} (jbest(s) + p_{Min})/2 + RR_3, & L_1 > x_1 \\ jbest(s) + RR_3 & x_2 \le L_1 x_1 \\ (jbest(s) + p_{Max})/2 + RR_3, & L_1 < x_2 \end{cases} \tag{23}$$

where h characterizes the h-th separate, g characterizes the discrete length; $jbest(s)$ is the global optimal solution of group t in the entire populace; p_{Max}/p_{Min} is the upper/lower limit of the seeker exploration region, the continuous verge x_1, x_2 ∈ [0,1], and $x_1 < x_2$, R_3 is a random number [−1,1]. The constant threshold xx∈ [0,1] is a random value K∈ [0,1] for each dimension of each seeker.

$$p_{hg}(s+1) = p_{hg}(s) + (1 + \psi R_4) \tag{24}$$

where: ψ is the meddling degree, and R_4 is the haphazard number [−1,1].the seekers' location is reset so that they are haphazardly distributed everywhere $jbest(s)$, to hypothetically jump out of local optimality, distinct as follows.

$$| f_j(s+1) - f_j(s) | < 0.01 \cdot | f_j(s+1) \tag{25}$$

$$p_{hg}(s+1) = (jbest'(s+1) + jbest(s)) \cdot R_m \quad (26)$$

where: $f_j(s)$ / $f_j(s-1)$ are the meaning values conforming to the global ideal of the s/s−1 cohort correspondingly, and R_m is the accidental number [−1,1]. $jbest'(s+1)$ is the current optimal explanation of group t + 1. The working process of trust degree computation and service node selection using ESSO is explained in Algorithm 2.

Algorithm 2 Trust degree computation and service node selection using ESSO

Input	: Number of clusters, Number of constraints, maximum iteration
Output	: Trust degree/service node
1.	Population initialization. Generate an initial species group.
2.	Define random prejudiced average to obtain the exploration orientation $\vec{F}_h(s) = sign(\omega\vec{F}_{h,X}(s) + \psi_1\vec{F}_{h,e}(s) + \psi_2\vec{F}_{h,m}(s))$
3.	If s =1
4.	While the stopping condition is not satisfied.
5.	Generate the search direction
6	Totalling the triple black hole system
7.	end if
8.	The elastic collision variation; Define Gaussian distribution function is $\mu(\alpha) = E^{-\frac{\alpha^2}{2\delta^2}}$
9.	Compute location update $p_{hg}(s+1) = p_{hg}(s) + \alpha_{hg}(s)F_{hg}(s) \quad h = 1,2,....t; \; g = 1,2,....C$
10.	Compute potentially jump out of local optimality $\| f_j(s+1) - f_j(s) \| < 0.01 \cdot \| f_j(s+1)$
11.	Calculate the fitness and judge the optimal solution.
12.	End if
13.	S=S+1
14.	If $s < S_{Max}$,then jump to 3;
15.	Else stop
16.	Find the best output values

3.3. Multi-Layer Deep Recurrent Neural Network (ML-DRNN)

An Optimal path finder is used to select the most suitable route for data transmission between the source and destination nodes in a MANET. The ML-DRNN excels in analyzing and predicting the optimal path from among multiple available options in the dynamic MANET environment. The ML-DRNN is trained on historical data, enabling it to learn the behavior of the MANET over time. It considers many network-specific criteria, node mobility, connection quality, interference, and other elements. The ML-DRNN has major benefits mostly related to its recurrent character, which enables the memory of previous states and use that knowledge to project future network circumstances. The ML-DRNN's main goal is to choose, among the many paths accessible between the source and destination nodes, the most best one for data transmission. Analyzing present network circumstances, using previous trends and real-time data helps one to choose the best path. The ML-DRNN's real-time decision-making capabilities, capacity to identify complicated patterns, and flexibility to changing network circumstances help to transmit data

effectively and lower resource usage. Applied as previously detailed, the Stockwell transform is a time-frequency based signal transform. We define the continuous T-transform of the q(s) time series as follows.

$$T(\tau,F)=\int_{-\infty}^{\infty} q(s)\,j(s-\tau.F)E^{-h2\pi Fs} \tag{27}$$

F=Frequency: s, τ =time

$$j(\tau,F)=\frac{|F|}{\sqrt{2\pi}}E^{\frac{s^3}{2\sigma^2}} : Gaussian\ \ Modulation\,Function$$

$$spreadparameter\sigma = 1/|F|\_$$

One defines the unconnected T-transform of a gesture as follows.

$$T[g,b]=\sum Q[a+b]z[a,b]E^{\frac{h2\pi ag}{B}} \tag{28}$$

where Q[a+ne]: Discrete Fourier Transmute of the indication loosened by b.

$$Q[a]=\frac{1}{B}\sum\sum_{K=0}^{B-1} q[K]E^{\frac{-g2\pi aK}{B}} \tag{29}$$

$$Z[a+b]=E^{\frac{-g2\pi a^2\beta^2}{b}} \tag{30}$$

Stockwell transform is applied to the vectorized representation of each amino acid sequence, resulting in a complex T-matrix that is A-valued and B-valued.

$$T-Mat=\begin{pmatrix} T_{11} & T_{12} & T_{13} & \llcorner & T_{1B} \\ T_{21} & T_{22} & T_{23} & \llcorner & T_{2B} \\ \llcorner & \llcorner & \llcorner & \llcorner & \llcorner \\ T_{A1} & T_{A2} & T_{A3} & \llcorner & T_{AB} \end{pmatrix}_{A*B}$$

Four different System features [SF] are calculated from the T-matrix of the encoded protein arrangement.:

$$SF_1=STD(c_1^{MAX},c_2^{MAX},c_3^{MAX},....c_B^{MAX})$$

$$SF_2=STD(r_1^{MAX},r_2^{MAX},r_3^{MAX},....r_A^{MAX})$$

$$SF_3=Energy(c_1^{MAX},c_2^{MAX},c_3^{MAX},....c_B^{MAX})$$

$$SF_4=STD(phase\_contour)$$

c_h : column wise supreme of absolute value of S-matrix.

r_h : row wise extreme of absolute value of T-matrix.

STD: average deviation.

Each amino acid sequence X can be characterized as,

$$X=[sSNE[0],sSNE[1],X_1...X_4X_5...X_8.....X_9...X_{13}...X_{16}]$$

$$\left.\begin{matrix} sSNE[0] \\ sSNE[1] \end{matrix}\right\} reduced\ Feature vectors$$

$$X_1 ... X_4 = stockwell\ transform\,[vector1]$$

$$X_5 ... X_8 = stockwell\ transform\,[vector2]$$

$$X_9 ... X_{12} = stockwell\ transform\,[vector3]$$

$$X_{13} ... X_{16} = stockwell\ transform\,[vector4]$$

The traditional recurrent network faces the gradient disappearing problem because the long-term dependences of the arrangements are masked by the short-term dependences.

$$i_s = F(z_i \cdot (p_s, i_{s-1})) \tag{31}$$

where F() is the nonlinear beginning function, p_s the current input and i_s and i_{s-1} are hidden unit states are s and s − 1, respectively. Closed loop units protect hidden level memory with reset r_s and w_s forget gates. The purpose of the GRU part is to reconstruct a new reminiscence $\tilde{i}_s$, which in attitude should characteristic of the current input and a non-linear alteration of the preceding memory. Adjust the top combination of forward and present inputs.

$$Hidden\ state: i_s = w_s \tilde{i}_s + (1 - w_s) i_{s-1} \tag{32}$$

$$Forget\ get: w_{(s)} = \sigma(Z^{(w)} p_s \cdot [p_s, i_{s-1}]) \tag{33}$$

$$New memory: \tilde{i}_s = \tan i(Z \cdot [p_s, R_s \Theta i_{s-1}]) \tag{34}$$

$$\mathrm{Re}\,set\ gate: r_s = \sigma(Z_R \cdot [p_s, i_{s-1}]) \tag{35}$$

$$\sigma(p) = \frac{1}{1 + E^{-p}} \tag{36}$$

where Θ is the component wise operator. The working process of optimal path finder using ML-DRNN is explained in Algorithm 3.

Algorithm 3 Optimal path finder using ML-DRNN

Input	: Number of paths, Number of attacks, attacks characteristics, threshold condition
Output	: Optimal paths among multiple paths
1.	Initialize the random population
2.	Define continuous T-transform of the $q(s)$ time series $T(\tau, F) = \int_{-\infty}^{\infty} q(s)\, j(s - \tau.F) E^{-h 2\pi F s}$
3.	If i=0 , j=1
4.	While **Do**
5.	Compute DFT of the signal loosened by b $Q[a] = \frac{1}{B} \sum \sum_{K=0}^{B-1} q[K] E^{\frac{-g\,2\pi a K}{B}}$
6	Define the updation process using $i_s = F(z_i \cdot (p_s, i_{s-1}))$
7	Compute the threshold for optimal combination of forward and current

inputs. $\sigma(p) = \frac{1}{1+E^{-p}}$

8. End if
9. Update the final output value
10. End

4. SIMULATION PARAMETERS

In this section, we delve into the outcomes and comparative analysis of the proposed CTSMP-Routing scheme alongside established routing schemes for MANETs under various simulation scenarios. To perform this evaluation, we have fully implemented the entire CTSMP-Routing scheme within the network simulator (NS3) tool [31]. The comparison encompasses the assessment of the CTSMP-Routing scheme against existing schemes, which include the standard AODV protocol, the evolutionary self-cooperative trust (ESCT) scheme [32], and the efficient trust-based routing scheme (ETRS) [33-34]. The evaluation is extensive and encompasses the analysis of diverse QoS metrics, including but not limited to packet delivery ratio, end-to-end delay, throughput, packet drop ratio, attack detection ratio, and benevolent detection ratio.

4.1. Simulation_Setup

A specific MANET scenario is designed, featuring randomly positioned nodes following a random waypoint mobility pattern. Within this context, certain nodes are deliberately designated as misbehaving nodes, tasked with the unauthorized action of discarding any data packets not belonging to them. Table 1 provides a comprehensive overview of the simulation parameters

Table 1 Simulation parameters

Parameter	Value
Network size	1500×1500
Number of mobile nodes	50, 100, 150, 200 and 250
Node mobility (mps)	5, 10, 15,20 and 25
Number of attacks	2, 4, 6, 8 and 10
Attack types	Selfish and black hole
Data rate	2 Mbps
MAC protocol	IEEE 802.11
Transmission range	250m
Mobility model	CBR (UDP)
Packet length	512 bytes
Packet arrival rate	4 packets/s
Default simulation time	2000s

5. RESULTS AND DISCUSSION FOR COMPARISON WITH VARYING NUMBER OF NODES

Table 2 presents a comparative analysis that examines the performance of the proposed CTSMP-Routing scheme in contrast to existing routing schemes across different scenarios characterized

by varying numbers of nodes. From Fig. 2, we observe a noticeable enhancement in the performance of CTSMP-Routing as the number of nodes in the network increases. The increase is particularly evident when comparing CTSMP-Routing with Standard AODV. For instance, with 50 nodes, CTSMP-Routing exhibits an approximately 31.1% increase in PDR over Standard AODV. As the network scales up to 250 nodes, the improvement remains substantial, with a PDR increase of approximately 41.6% compared to Standard AODV. For instance, with 50 nodes, CTSMP-Routing boasts an approximately 24.4% higher PDR than ESCT, and this gap widens to approximately 41.6% at 250 nodes. With 50 nodes, CTSMP-Routing exhibits a PDR increase of approximately 9.3% compared to ETRS. With a PDR rise of around 15.2% at 250 nodes, this improvement stays constant as the node count rises.

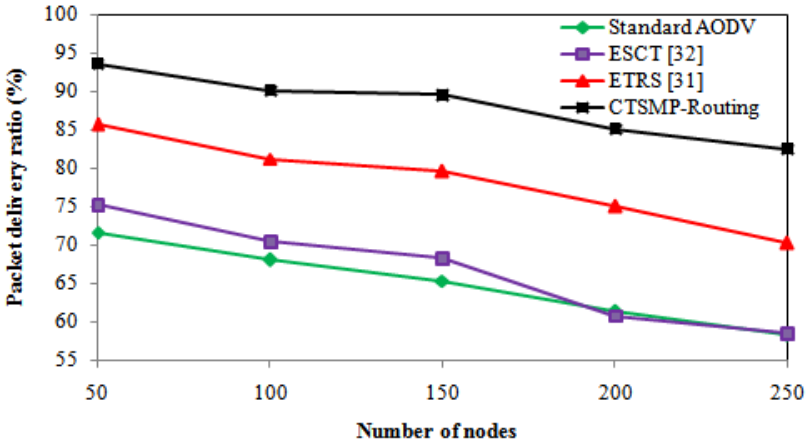

Fig. 2 Ratio of packet delivery depending in number of nodes

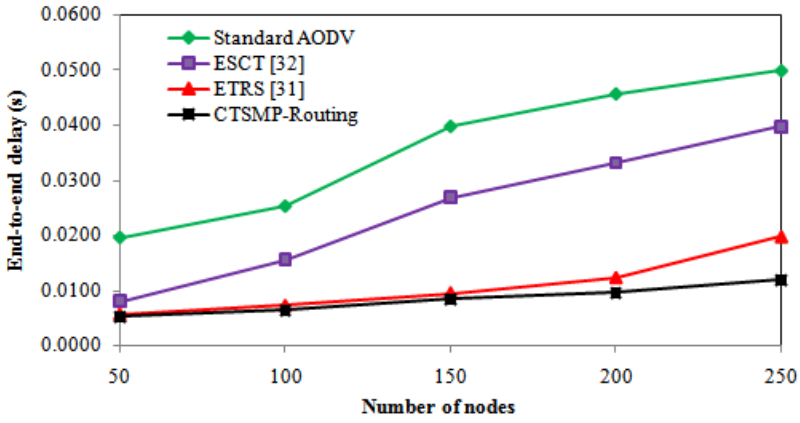

Fig. 3 End-to- end delay with different node count

As illustrated in Fig. 3, the suggested approach achieves lesser delays when compared CTSMP-Routing to Standard AODV. With 50 nodes, for example, CTSMP-Routing shows an amazing 73.5% reduction in latency relative to Standard AODV. With a latency drop of 75.9%, the network grows to 250 nodes, hence this improvement is still noteworthy. Comparatively, similar tendencies appear when comparing CTSMP-Routing to ESCT; CTSMP-Routing constantly shows smaller delays. Comparatively to ESCT, CTSMP-Routing shows an estimated 94.7% decrease in latency at 50 nodes; this reduces further to around 77.8% at 250 nodes. Moreover, comparing CTSMP-Routing versus ETRS shows how well the suggested system reduces delays.

CTSMP-Routing reduces latency by 7.1% relative to ETRS using 50 nodes. This drop stays constant as the number of nodes rises; at 250 nodes, it drops around 7.7%.

CTSMP-Routing approximates 12.4% improvement in throughput for 50 nodes over Standard AODV. This increase becomes much more significant once the network grows to 250 nodes, approaching 14.2%. Comparatively to ESCT, the findings once again illustrate CTSMP-Routing's superiority in Fig. 4. CTSMP-Routing offers a about 10.9% improvement in throughput with 50 nodes, compared to ESCT, which increases to around 8.3% with 250 nodes. Furthermore, the suggested approach always shows a better throughput when comparing CTSMP-Routing with ETRS. With 50 nodes, CTSMP-Routing achieves an increase of 7.7% in throughput compared to ETRS. This improvement persists as the number of nodes increases, with an approximately 9.5% increase at 250 nodes.

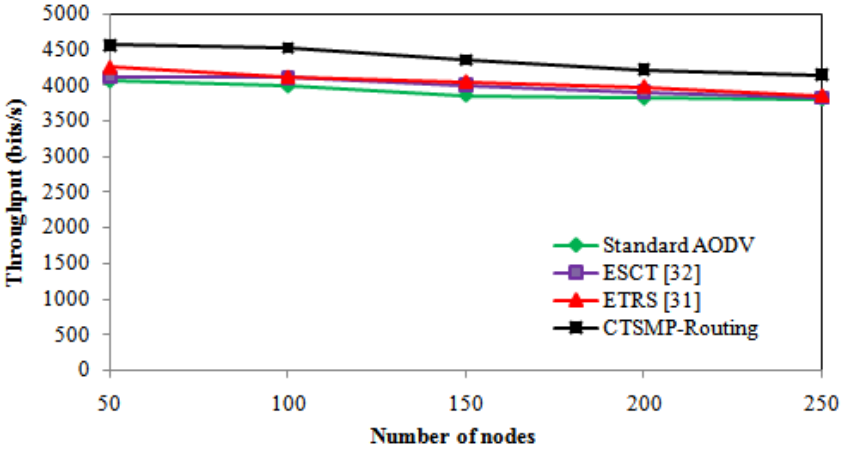

Fig. 4 Throughput with varying number of nodes

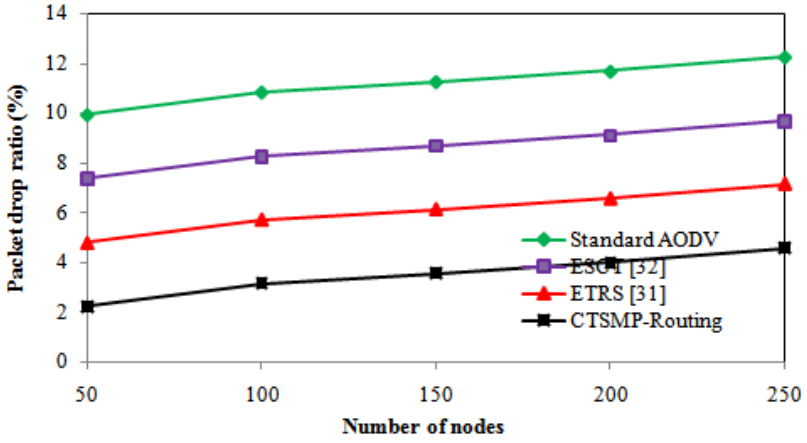

Fig. 5 Packet drop ratio with varying number of nodes

Compared to Standard AODV, CTSMP-Routing exhibits significant improvements in reducing the packet drop ratio. With 50 nodes, CTSMP-Routing achieves an approximate 77.5% decrease in packet drop ratio compared to Standard AODV. This improvement becomes even more substantial, reaching an approximately 63.0% reduction with 250 nodes. In comparison to ESCT, CTSMP-Routing once again demonstrates superior performance. At 50 nodes, CTSMP-Routing achieves an approximate 69.6% reduction in packet drop ratio compared to ESCT, which grows

to around 64.4% with 250 nodes. Additionally, when evaluating CTSMP-Routing against ETRS, the proposed scheme consistently displays a lower packet drop ratio as shown in Fig. 5. With 50 nodes, CTSMP-Routing achieves an approximate 53.4% reduction in packet drop ratio compared to ETRS. This improvement persists as the number of nodes increases, with an approximate 43.4% reduction at 250 nodes.

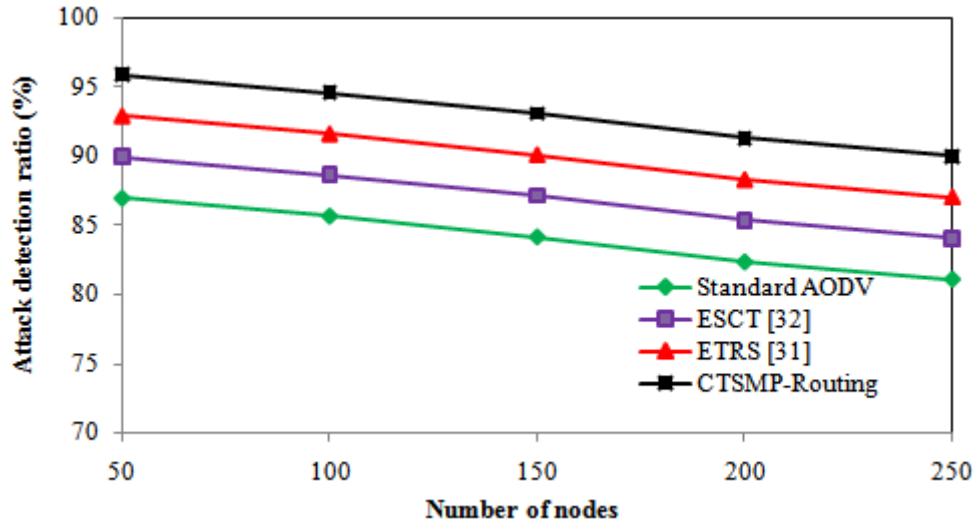

Fig. 6 Attack detection ratio with varying number of nodes

Table 2 Comparative analysis of proposed and existing routing scheme over varying number of nodes

Routing schemes	50	100	150	200	250	50	100	150	200	250
	Packet delivery ratio (%)					End-to-end delay (s)				
Standard AODV	71.689	68.047	65.349	61.323	58.236	0.0196	0.0253	0.0398	0.0457	0.0499
ESCT [32]	75.258	70.459	68.348	60.789	58.467	0.0980	0.0156	0.0269	0.0332	0.0398
ETRS [31]	85.632	81.235	79.589	75.023	70.198	0.0056	0.0072	0.0095	0.0123	0.0198
CTSMP-Routing	93.623	90.125	89.523	85.148	82.498	0.0052	0.0065	0.0085	0.0096	0.0120
	Throughput (bits/s)					Packet drop ratio (%)				
Standard AODV	4059	3985	3856	3810	3798	9.925	10.841	11.257	11.678	12.257
ESCT [32]	4112	4108	4002	3899	3821	7.362	8.278	8.694	9.115	9.694
ETRS [31]	4256	4123	4056	3985	3856	4.799	5.715	6.131	6.552	7.131
CTSMP-Routing	4568	4523	4359	4214	4139	2.236	3.152	3.568	3.989	4.568
	Attack detection ratio (%)					Benevolent detection ratio (%)				
Standard AODV	86.952	85.658	84.148	82.334	81.081	87.152	86.531	86.191	86.052	85.654
ESCT [32]	89.920	88.626	87.116	85.302	84.049	90.720	90.099	89.759	89.620	89.222
ETRS [31]	92.888	91.594	90.084	88.270	87.017	94.288	93.667	93.327	93.188	92.790

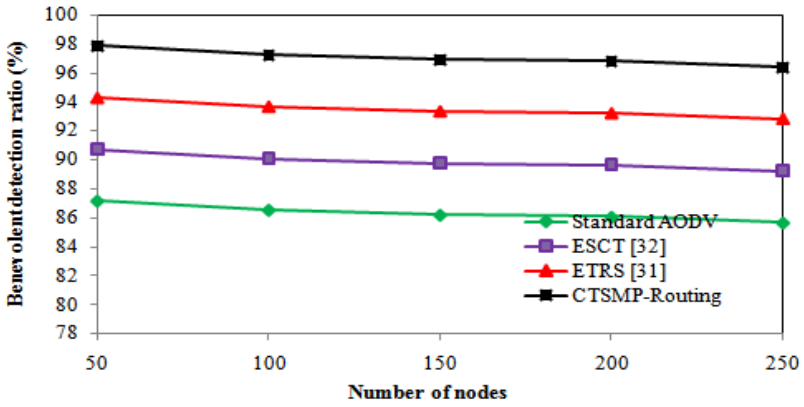

Fig. 7 Benevolent detection ratio with varying number of nodes

When comparing CTSMP-Routing with Standard AODV, it shows a significant improvement in attack detection. With 50 nodes, CTSMP-Routing exhibits an approximately 8.8% increase in the attack detection ratio compared to Standard AODV, and the advantage becomes more Pronounced, reaching an approximate 11.7% increase with 250 nodes. Against ESCT, CTSMP-Routing consistently displays superior performance in attack detection as shown in Fig. 6. At 50 nodes, the proposed scheme achieves an approximate 6.6% increase in the attack detection ratio compared to ESCT, growing to around 7.0% with 250 nodes. Furthermore, when comparing CTSMP-Routing with ETRS, it consistently maintains a higher attack detection ratio. With 50 nodes, CTSMP-Routing achieves an approximate 3.3% increase in the attack detection ratio compared to ETRS, which extends to around 3.0% at 250 nodes.Benevolent detection improves significantly when comparing CTSMP-Routing with Standard AODV. Comparatively to Standard AODV, CTSMP-Routing shows about 10.4% improvement in the benign detection ratio with 50 nodes; this benefit becomes more clear with 250 nodes. CTSMP-Routing has better performance in benign detection against ESCT as shown in Fig. 7. Growing to over 7.3% with 250 nodes, the suggested approach yields an almost 7.0% improvement in the beneficent detection ratio at 50 nodes over ESCT. Moreover, CTSMP-Routing has a constantly better beneficent detection ratio when compared to ETRS. CTSMP-Routing, with 50 nodes, increases the benign detection ratio approximatively 3.6% compared to ETRS, reaching about 3.6% at 250 nodes.

6. CONCLUSION

We have cluster-based trusted secure multipath routing (CTSMP-Routing), designed to address the intricate challenges posed by MANETs. We used the optimum clustering technique obtained using of the creatively modified proportional topology optimization (MPTO) algorithm, which makes use of spatial data about network nodes. An improved seeker search optimization (ESSO) method based on a variety of network constraints including node mobility, received signal intensity, energy consumption, and cooperation rate computes trust degrees. Identifying the most highly trusted node in the network depends on the trust degrees, which also play the function of the service node in charge of inter-cluster routing. This guarantees in the MANET a dependable and safe routing mechanism. Apart from these developments, we have created a novel hybrid soft computing method called multi-layer deep recurrent neural network (ML-DRNN), for the best path-finding mechanism. Our findings highlight how well CTSMP-Routing protects MANETs against different kinds of threats, therefore guaranteeing the security and dependability of data flow. Future research can focus on energy-efficient trust computation for IoT-enabled MANETs, blockchain-based decentralized trust management to prevent trust manipulation, AI-driven

adaptive routing mechanisms for dynamic decision-making, and cross-layer security approaches to defend against multi-layer attacks. Addressing these aspects will further refine MANET security, optimize routing efficiency, and contribute to the evolution of secure and intelligent network communication.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Ali, H., & Khan, M. (2022). Intelligent intrusion detection in MANETs using fuzzy logic and machine learning. IEEE Access, 10, pp. 17893–17906. DOI: 10.1109/ACCESS.2022.3147893

[2] Benatia, S.E., Smail, O., Meftah, B., Rebbah, M. and Cousin, B., 2021. A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas. Simulation Modelling Practice and Theory, 113, p.102397.

[3] Borkar, G.M. and Mahajan, A.R., 2017. A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks, 23(8), pp.2455-2472.

[4] Cai, R.J., Li, X.J. and Chong, P.H.J., 2018. An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE transactions on Mobile Computing, 18(1), pp.42-55.

[5] Chen, Y., & Wu, H. (2025). AI-driven QoS-aware MANET protocols: A deep learning-based approach for QoS prediction and adaptive routing. IEEE Transactions on Wireless Communications, 74(2), pp. 235–249. DOI: 10.1109/TWC.2025.3412345

[6] Devi, V.S. and Hegde, N.P., 2018. Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer. Wireless Personal Communications, 100, pp.923-940.

[7] Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P. and Dhurandher, P., 2010. Faces: friend-based ad hoc routing using challenges to establish security in MANETs systems. IEEE Systems Journal, 5(2), pp.176-188.

[8] Elmahdi, E., Yoo, S.M. and Sharshembiev, K., 2020. Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications, 51, p.102425.

[9] El-Sayed, H., & Omar, M. (2025). QoS-aware multipath routing using reinforcement learning in MANETs. IEEE Internet of Things Journal, 12(5), pp. 1075–1089. DOI: 10.1109/JIOT.2025.3578901

[10] Ghosh, A., & Roy, P. (2023). Hybrid trust management for secure routing in MANETs using blockchain and AI. Computer Networks, 225, 109876, pp. 1–18. DOI: 10.1016/j.comnet.2023.109876

[11] Gundeboyina Srinivasalu and Hanumanthappa Umadevi,"Cluster Based Routing Using Energy and Distance Aware Multi-Objective Golden Eagle Optimization in Wireless Sensor Network ", International Journal of Computer Networks & Communications (IJCNC) Vol.14, No.3, May 2022, PP 37-53, DOI: 10.5121/ijcnc.2022.14303

[12] Hammamouche, A., Omar, M., Djebari, N. and Tari, A., 2018. Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. Journal of information security and applications, 43, pp.12-20.

[13] Hemalatha, R., Umamaheswari, R. and Jothi, S., 2021. LF distribution and equilibrium optimizer based fuzzy logic for multipath routing in MANET. Wireless Personal Communications, 120(2), pp.1837-1861.

[14] Hurley-Smith, D., Wetherall, J. and Adekunle, A., 2017. SUPERMAN: security using pre-existing routing for mobile ad hoc networks. IEEE Transactions on Mobile Computing, 16(10), pp.2927-2940.

[15] Kala Venugopal and T G Basavaraju," Congestion and Energy Aware Multi-pathload Balancing Routing for LLNS", International Journal of Computer Networks & Communications (IJCNC) Vol.15, No.3, May 2023,PP 71-92, DOI: 10.5121/ijcnc.2023.15305

[16] Kasthuribai, P.T. and Sundararajan, M., 2018. Secured and QoS based energy-aware multipath routing in MANET. Wireless Personal Communications, 101, pp.2349-2364.

[17] Kumar, R., & Sharma, V. (2024). A trust-based secure routing protocol for MANETs using fuzzy logic. International Journal of Computer Networks & Communications *(IJCNC)*, **16**(2), pp. 45–60. DOI: 10.5121/ijcnc.2024.16203

[18] Mahamune, A.A. and Chandane, M.M., 2021. An efficient trust-based routing scheme against malicious communication in MANET. International Journal of Wireless Information Networks, 28(3), pp.344-361.

[19] Muneeswari, B. and Manikandan, M.S.K., 2019. Defending against false data attacks in 3D grid-based MANET using soft computing approaches. Soft Computing, 23, pp.8579-8595.

[20] Nguyen, T., & Park, J. (2024). Soft computing approaches for MANET security: A hybrid neural network-based trust model. Expert Systems with Applications, 237, 120345, pp. 1–20. DOI: 10.1016/j.eswa.2024.120345

[21] Paramasivan, B., Prakash, M.J.V. and Kaliappan, M., 2015. Development of a secure routing protocol using game theory model in mobile ad hoc networks. Journal of Communications and Networks, 17(1), pp.75-83.

[22] Patel, D., & Mehta, S. (2023). QoS-aware multipath routing for MANETs using AI-based decision-making. International Journal of Computer Networks & Communications *(IJCNC)*, **15**(4), pp. 78–92. DOI: 10.5121/ijcnc.2023.15405

[23] Radwan S.Abujassar," Enhancing Traffic Routing Inside a Network through IoT Technology & Network Clustering by Selecting Smart Leader Nodes", International Journal of Computer Networks & Communications (IJCNC) Vol.16, No.2, March 2024, PP 1-24, DOI: 10.5121/ijcnc.2024.16201

[24] Rahman, M., & Patel, S. (2022). Fuzzy logic-based trust evaluation system to improve routing reliability in MANETs. Future Generation Computer Systems, 134, pp. 567–580. DOI: 10.1016/j.future.2022.02.045

[25] Rajashanthi, M. and Valarmathi, K., 2020. A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs. Wireless Personal Communications, 112, pp.75-90.

[26] Rajendran, N., Jawahar, P.K. and Priyadarshini, R., 2019. Cross centric intrusion detection system for secure routing over black hole attacks in MANETs. Computer Communications, 148, pp.129-135.

[27] Ran, C., Yan, S., Huang, L. and Zhang, L., 2021. An improved AODV routing security algorithm based on blockchain technology in ad hoc network. EURASIP Journal on Wireless Communications and Networking, 2021(1), pp.1-16.

[28] Robinson, Y.H., Krishnan, R.S., Julie, E.G., Kumar, R. and Thong, P.H., 2019. Neighbor knowledge-based rebroadcast algorithm for minimizing the routing overhead in mobile ad-hoc networks. Ad Hoc Networks, 93, p.101896.

[29] Sharma, P., & Singh, R. (2023). A dynamic trust-based secure routing protocol to detect and mitigate insider attacks in MANETs. Ad Hoc Networks, 145, 103123, pp. 1–15. DOI: 10.1016/j.adhoc.2023.103123

[30] Simpson, S.V. and Nagarajan, G., 2021. A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Generation Computer Systems, 125, pp.544-563.

[31] Sirajuddin, M., Rupa, C., Iwendi, C. and Biamba, C., 2021. TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network. Security and Communication Networks, 2021, pp.1-9.

[32] Tripathy, B.K., Jena, S.K., Bera, P. and Das, S., 2020. An adaptive secure and efficient routing protocol for mobile ad hoc networks. Wireless Personal Communications, 114, pp.1339-1370.

[33] Vatambeti, R., 2020. A novel wolf based trust accumulation approach for preventing the malicious activities in mobile ad hoc network. Wireless Personal Communications, 113, pp.2141-2166.

[34] Zhang, L., & Wei, X. (2024). An adaptive QoS-aware routing algorithm optimizing delay and throughput in MANETs. IEEE Transactions on Communications, 72(3), pp. 459–472. DOI: 10.1109/TCOMM.2024.3309875

AUTHORS

Mr. Himanshubartwal Assistant Professor at PSIT Kanpur and doing currently PhD (Pursuing) with a Thesis Topic PhD is" An Analysis and Implementation of Multipath Based Secure Routing Algorithm in Mobile Adhoc Network" .Received M. Tech (CNE) degree from Graphic Era DEEMED university Dehradun (2012-2014) thesis topic is "Rumour routing Protocol". Having 01 patent and book is published.

Dr. Himani Sivaraman, Dean School of Science and Technology, received her Ph.D from Graphic Era Hill University, Dehradun 2024 a Thesis Topic is "An Efficient & Secure Framework in Supply Chain Management Based on Blockchain Technology" .Received M. Tech (SE) degree from Noida International University. Having 02 patents and 23 research articles in her credit. Research Area: Blockchain, Machine Learning, Cloud Computing .

Dr.Jogendra Kumar is working as Assistant Professor, Faculty of Computer Science and Engineering Department, G.B.Pant Institute of Engineering and Technology Pauri Garhwal Uttarakhand-246194. He has fifteen years of teaching experience in Engineering, UG and PG level. Her research interest includes Wireless Networks, IoT, Block Chain Technology, Big Data Analytics, Machine Learning and WSN. Two Ph.D scholars were pursuing their research under his guidance. He is also a International Scientific Committee member for Researchers in various universities. He has received two awards. He has published many research papers, books, book chapters in SCI, WoS, IEEE, and SCOPUS journals. He also published and granted many patents in IPR. He serves as Editor in Book Chapters, Editorial Board Member ,and Reviewer in various International Journals. He is an active member in Professional Bodies like ISTE, IAENG (USA) and IACSIT.