Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 08
Aug 2025

Trust-Based Energy Efficient Secure Multipath Routing Using Hybrid Algorithm Optimization Algorithm for MANET

Pallavi Singh[1], Durgesh Kumar Keshar[2]

[1] Atal Bihari Vajpayee Vishwavidyalaya, Koni Bilaspur, Chhattisgarh, India. Email: pallavisingh.prsu@gmail.com

[2] National Institute of Technology Raipur, Chhattisgarh, India. Email: durgeshkeshar.prsu@gmail.com

Abstract

A wireless Mobile Ad Hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. MANET is infrastructure-less and dynamic. As the nodes have limited battery power and communicate through a shared wireless channel, it is hard to design a secure and energy-efficient routing protocol in a MANET. Consequently, the article proposes a Trust-Based Energy-Efficient Secure Multi-Path Routing Protocol (TESMRP) supported by the MANET optimization algorithm. In this method, a scheme strives to predict a stable route by selecting the most stable neighbour relative to the transmitter of the route request message and nodes impending during the route discovery process. In multipath routing, a sender node waits for intermediate multiple paths to forward the ciphertext to the destination. In a routing discovery procedure, an SN broadcasts a route request (RREQ) message to discover the DN using a generic probabilistic-based route discovery procedure. After the DN has received the RREQ message, it will begin the routing reply process and will send a routing reply (RREP) message back to the SN. It also becomes essential to monitor the constraints in intermediate nodes (multi-hop routing). As a supplementary method to improve safe data delivery in a MANET, this research proposes and analyses the cluster head (CH) selection and optimum multipath scheme utilizing an improved fuzzy C-means algorithm. The computation is based on the trust threshold worth nodes found in addition. From the CHs, the network of interconnected hops is included, and a selection of the best routes is established using a projected hybrid protocol, and this determines the best routes by the delay, throughput, along with connectivity within this course. To accomplish such challenging objectives, the AODV protocol computes a hybrid optimization algorithm of the Levy flight distribution algorithm for optimal path selection. In addition, high energy consumption is addressed by the Firefly Optimization Algorithm to find the optimal values/fitness function for the objective parameter (i.e. energy). The performance analysis and numerical results show that the proposed protocol achieves significant performance gains in terms of energy consumption, delay, throughput, and security of routing protocols, respectively.

Keywords: Mobile Ad-Hoc Network, Multipath Routing, AODV, Fuzzy C-Means, Levy Flight Distribution, Optimal Path, Energy Efficiency.

1. Introduction

A collection of mobile nodes that interact outside of a fixed physical structure makes up a mobile ad hoc network (MANET) [1]. Every middle node in the network behaves as a router. MANET has a variety of intriguing features. MANETs include a variety of noteworthy characteristics, including quick deployment, variable topology, and multi-hop wireless communication. Using route discovery, the data packets can be sent from the source node to the neighbouring node until they get to the target node [2]. The MANET concept has received enough attention in recent years for better hardware and improved protocol architecture [3]. For quick setup, multiple-hop data transfer, changeable topology, etc., MANET is crucial in IoT-based systems [4]. They are inconsistent due to a finite energy supply for network mobility, similar to the wireless connections between nodes in the ad hoc network. Unprotected network nodes could develop malicious nodes and cause the network to lag. These inherent traits, such as dynamic topology, wireless medium, and bandwidth restrictions, put them at a higher risk of hostile attacks [3]. Any self-organizing communication system faces a significant barrier in route identification and potential route assessment. Different routing protocols for ad hoc networks are available in research and reality, and they are based on different techniques and performance trade-offs in route discovery [5-8].

In general, there are three types of routing protocols: on-demand, table-driven, and hybrid [5]. On-demand Multipath Routing (MR) methodologies have recently taken centre stage in MANET research. The Multipath Routing (MR) technique is widely used in Mobile Ad-hoc Networks (MANET) because it is effective in overcoming the specific drawbacks of single-path routing. The MR methods offer a variety of paths between a source and a destination. Energy Efficiency is the most important component to take into account in Manet for real-time applications because networks there are constrained by battery capacity and energy resources [6]. There are many benefits to using multipath approaches, including longer network life, better bandwidth usage, faster throughput, less end-to-end delay, etc [8]. It lessens network congestion and provides route failure prevention. However, achieving energy-effective secure MR is a huge issue in MANET due to the lack of trusted centralised authority and also inadequate resources. The most difficult task in developing an on-demand MR scheme for mobile ad-hoc networks is to provide a secure protocol while simultaneously preserving energy efficiency. By using any energy routing metric, numerous researchers have created numerous energy-efficient routing algorithms for MANETs. The cluster-based routing method divides the nodes into various groups, with each node inside a group only considering how to forward a packet to the cluster head [9]. Due to their disregard for node mobility and topology changes, the majority of prior research studies are less suitable for the distributed environment of MANETs. Therefore, the researchers changed their approaches based on optimizing the routing path selection while taking node mobility and topological changes into account [10]. However, these solutions sought to extend the life of the network by using several, disjointed channels for routing, which required unique control messages to gather data from all paths, increasing network overhead. As a result, optimization techniques were used to select the appropriate path based on the supplied parameters for the different paths without overhead [11].

The nature-inspired optimization algorithms such as Particle Swarm Optimization, Genetic Algorithm, Ant Colony Optimization (ACO) and Chimp Optimization approaches are used in optimal MANET routing [12]. The bio-inspired optimization algorithms' key characteristics include high speed, better performance, and search flexibility. Furthermore, these methods only use single paths and choose an efficient path, which causes the nodes along those paths to lose energy more quickly than nodes along alternative paths [13]. The energy-balanced routing over various paths must be started simultaneously to address this problem [14]. Various multipath routing techniques showed effective routing for multimedia material in WSN as well [15].

2. Literature Survey

In Bai *et al* [16] the authors employed the routing manager-based secure rate analysis (RMBSRA) technique. The adjacent table, routing manager, and routing table are the three main parts of the proposed system, which is a centralized mechanism. These parts are in charge of ensuring that packets are transmitted effectively and without data loss along the quickest path. The suggested solution enhances multicast routing by balancing bandwidth allotment and ultimately network load. The cluster head selection and backup cluster head selection proposed in [17] generate the best path between the cluster head and member node based on the reliability pair factor and node's energy, and the establishment of the path based on the maximum energy and number of hops between the nodes are all provided (minimum number of hops). The member node is given via an ORS route, which is superior to existing techniques in an energy-efficient way between the base station and cluster head.

An energy-efficient multi-path routing protocol supported by the MANET optimization algorithm is suggested in [18]. The usage of cluster head collection with fuzzy clustering and intrusion detection with fuzzy NB effectively challenges the energy efficiency within the MANET. By combining the bird's swarm optimization algorithm (BSA) and whale optimization algorithm (WOA), known as the Bird Swarm-Whale Optimization Algorithm, multipath routing can be achieved (BSWOA). To provide energy-efficient and safe routing for ad-hoc sensor networks, trust-based energy-aware routing using the GEOSR protocol is proposed in [19]. The sensor nodes in this trust-based energy-aware routing are initially set up in the ad hoc network. The cluster head (CH) is chosen based on the threshold value and the clustering is carried out based on the calculation of the distance between each node. The introduction of Golden Eagle Optimized Secure Routing (GEOSR) allows for the determination of the best routing path based on variables such as distance delay and energy goal function.

In Thirunavukkarasu *et al* [20], a unique methodology known as the Cluster and Angular-based Energy Proficient Trusted Routing (ACEPTR) protocol is suggested. To begin with, the Node Credit Score (NCS) is computed to determine the nodes' trust ratio. Both the Self-Trust computation and the Joint-Trust computation are factors in the credit score calculation. After determining the highest NCS, angular energy-based route selection is used to create clusters since it significantly reduces energy expenditure. An intelligent dynamic trust model (IDT) for wireless network security is discussed in [21]. For secure routing in ad hoc networks, this paradigm combines dynamic trust with beta reputation trust. The beta direct trust value is determined using intelligent agents and the Intelligent Dynamic Trust model. Here, the node trust is dynamically monitored by intelligent agents over a specific period. The suggested intelligent system presents each node's behaviour as a binary event. The distribution that is frequently used to represent the posterior probability of a binary event when using intelligent agents is utilised to model this binary event.

In Bondada *et al* [22], group key management is used to propose a routing protocol that is both safe and energy-efficient. Utilizing two specialized nodes known as the Calculator Key (CK) and the Distribution Key (DK), asymmetric key cryptography is implemented. Secret key generation, verification, and distribution are handled by these two nodes. As a result, no additional computation on the part of other nodes is required to create the secret keys. These nodes are chosen based on their energy usage and node trust ratings. The majority of the current routing protocols require that each node generate and distribute its secret keys, which spreads more energy throughout the system. In [23], an energy-efficient and double cluster-head routing (EEDCR) protocol is proposed. It is a cluster-based routing protocol with low energy consumption that aims to prolong network lifetime and reduce end-to-end delay. The random selection method, the energy method, the total number of nodes, and the cluster head's (CH) energy level all play a role in the CH's selection.

The Optimal Route Selection (ORS) proposed in [24] offers cluster head selection, alternate cluster head selection, generation of the best path between the cluster head and member node based on reliability pair factor and node energy, and establishment of the path based on maximum energy and number of hops between the nodes to prevent cluster head failure. To reduce the energy used by each node for data transmission, the Energy-Efficient Perspicacious Ant Colony Optimization Based Routing Protocol (EEPACORP) is presented in [25]. The foundation of EEPACORP is the ant's innate propensity to seek food. EEPACORP takes its cue from an ant's inherent disposition to seek out food. EEPACORP modifies pheromone concentration to choose the best path.

3. Research Problem Definition and Motivation

MANET is an infrastructure-less, self-configuring wireless network comprising mobile wireless nodes. These mobile nodes initiate communication among them arbitrarily through route request and reply packets without the need for any centralized administration and hence the MANET topology changes rapidly and unpredictably. MANETs have different applications like military operations, data networks, emergency rescue operations, communication networks, etc. and have become an active research concept. The major challenges faced in the MANET networks are the dynamic topology, energy constraint problem; bandwidth-limited varying links, higher loss rate, high delay and jitter, absence of centralized control and limited physical security but has to continuously maintain node information for routing. For that reason, proactive routing protocols cannot be efficiently utilized for MANETs as the dynamic topology requires a high amount of resources for maintaining routing information reliably. Hence to tackle these limitations and enhance the routing performance in MANETs, reactive routing protocols (on-demand routing protocols) were utilized.

Energy conservation in MANETs can be achieved by limiting the inordinate consumption and balancing the node energy consumption through efficient routing. Among the on-demand routing protocols suggested for MANETs, Ad hoc On-Demand Distance Vector (AODV) routing and DSR protocols are most commonly used. Specifically, the DSR protocol is considered the foremost protocol suitable for multi-hop Adhoc networks like MANETs. However, the DSR does not consider node energy consumption as a parameter in accessing the routing paths which becomes a significant disadvantage. This limitation, if not rectified, further increases the energy constraint problem of MANETs. Moreover, the DSR lacks the ability to multicasting and route prioritization mechanism in the multipath routing of high mobility nodes causing stake cache entries. The motivation of this research is to obtain energy-efficient secure MR in MANET is a big issue due to a lack of trusted centralised authority and also insufficient resources. The objective of this research is to offer a trust-based energy-efficient multipath routing strategy for MANET to address the issues.

4. Research Proposed Methodology

Wireless networks are considered the best-utilized network and in particular, Mobile Ad-hoc Networks are applied in a variety of real-time scenarios for reliable data transmission. The accompanying challenges restrict the current protocols for the routing being specifically used in MANETs. The function of routers is to choose the most effective route for delivering information from one point to another. Energy consumption is one of the foremost vital restrictions that deteriorate the performance of the whole network. Multi-path Routing (MR) is better than single-path routing in ad hoc networks because multi-path routing allows the establishment of multiple paths between a single source and a single destination node. The foremost challenging task to offer an MR scheme aimed at mobile ad-hoc networks is to attain a secure protocol by maintaining trust and also energy efficacy simultaneously. Since mobile nodes are powered by low-capacity batteries, energy consumption plays a critical role in mobile ad hoc networks. A hectic problem was the minimization of energy, which was solved by the use of multipath routing protocols. Consequently, the research proposes a trust-based energy-efficient secure multi-path routing protocol supported by the MANET optimization algorithm. The flowchart representing the proposed work is depicted in Figure 1.

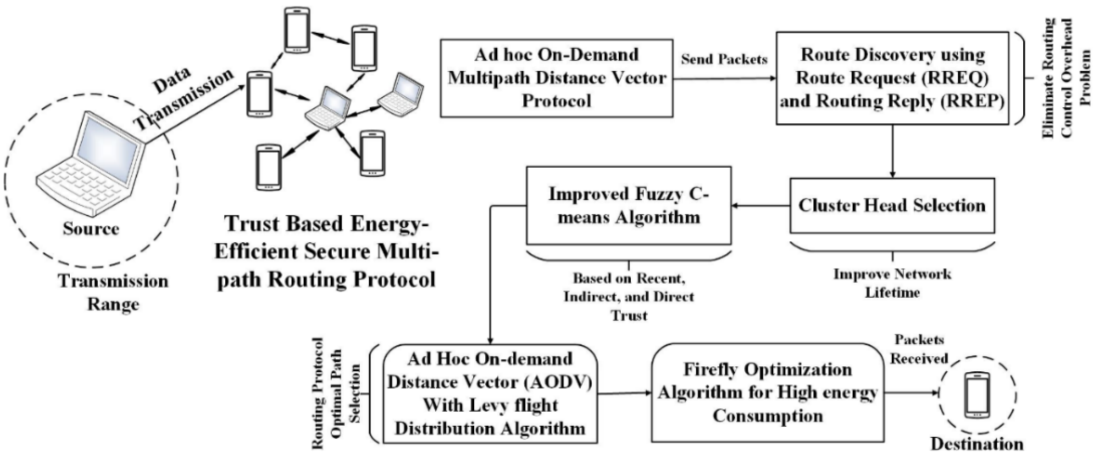


Figure 1: The flowchart representing the proposed work

The foremost challenging task to offer a Multipath Routing scheme aimed at mobile ad-hoc networks is to attain a secure protocol by maintaining trust and also energy efficacy simultaneously. As a supplementary method to improve safe data delivery in a MANET, this research proposes and analyzes the cluster head (CH) selection and optimum multipath scheme. Consequently, the research proposes a Trust-Based Energy-Efficient Secure Multi-Path Routing Protocol (TESMRP) supported by the MANET optimization algorithm**.** In Multipath Routing, an SN waits for intermediate multiple paths to forward the ciphertext to the destination. In a routing discovery procedure, an SN broadcasts a route request (RREQ) message to discover the DN. After the DN has received the RREQ message, it will begin the routing reply process and will send a routing reply (RREP) message back to the SN. Clustering is one of the significant techniques for expanding the lifetime of networks in wireless sensor networks (WSNs). The optimal CH is elected by an improved fuzzy C-means algorithm method built on density peak, and Cluster Heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust. Even the CHs participate in the multi-hop routing, and the assortment of the best route relies upon the projected hybrid protocol, and that selects the best routes determined. This research presents a hybrid trust-based secure multipath routing protocol that combines AODV with the Levy Flight Distribution (LFD) algorithm for optimal node selection and shortest path discovery, thereby enhancing MANET performance. To reduce energy consumption, the Firefly Algorithm is employed to optimize the energy-based fitness function. The resulting AODV-LFD protocol efficiently selects routes among multiple paths while meeting key performance metrics such as delay, throughput, energy usage, delivery ratio, loss ratio, and latency.

4.1. Trust Based Energy-Efficient Secure Multi-Path Routing Protocol (TESMRP)

Energy Consumption and secured routing are pondered as the most challenging operation in MANET owing to the deficiency of trusted centralized authority and also limited resources. Aimed at offering energy-effective secured MR-based ad-hoc network nodes, this work extends a Trust-Based Energy-Efficient Secure Multi-Path Routing Protocol (TESMRP) MANET. The scheme proposed comprises trust calculation, optimal routing path discovery, and then cluster head selection. In the proposed approach, each node detects malicious or victim nodes and selects secure, optimized routes using trust metrics, energy levels, and path distance. The AODV-LFD protocol applies a multi-objective optimization function to determine the optimum routing path. Unlike DSDV, which maintains complete routing tables, AODV reduces broadcast overhead by establishing routes only when required. During route discovery, an RREQ packet is broadcast and forwarded by neighboring nodes until it reaches the destination or a node with valid routing information. Duplicate requests are discarded, and sequence numbers ensure loop-free paths and the use of the most recent routing information.

4.1.1. Generic Probabilistic Route Discovery Process

During route discovery operation node's residual energy and link's quality which is estimated through received signal power are compared against their respective dynamic threshold values for subsequent hop selection. If both the values are above their respective thresholds, the node increases the stability factor of a route by one before forwarding the route request (RREQ) packet. This process continues till the destination node is reached. If at a later stage, an identical RREQ packet with a better stability factor arrives, the node processes that duplicate packet. When a source node **S** requires a route to a destination **D**, it broadcasts an RREQ packet to its neighbouring nodes. Each neighbour rebroadcasts the RREQ once if it lacks a valid route to the destination. Intermediate nodes that forward the RREQ establish a **reverse path** to the source. When the destination **D**, or an intermediate node with an active route to **D**, receives the RREQ, it sends back an RREP, which is unicast along the reverse path. Each forwarding node records a **forward route** to **D**, forming a hop-by-hop routing structure in which nodes store only the next hop.

In probabilistic route discovery, the source transmits the RREQ with probability **$p = 1$**, while intermediate nodes forward it with probability **$p < 1$** and drop it with probability **$1 - p$**. Because forwarding decisions are independent, the expected number of retransmissions is **$p \times (N - 1)$**. The forwarding probability is dynamically adjusted based on **local node density** and the **set of covered neighbours**. A lower forwarding probability is used when many 1-hop neighbours have already received the broadcast, and a higher probability when fewer neighbours are covered. Covered neighbours are defined as nodes that have already received the same broadcast packet. To further improve reliable data delivery, the proposed work also incorporates **cluster head (CH) selection** and an **optimized multipath routing strategy**.

When a source node **S** requires a route to a destination **D**, it broadcasts an RREQ packet to its neighbouring nodes. Each neighbour rebroadcasts the RREQ once if it lacks a valid route to the destination. Intermediate nodes that forward the RREQ establish a **reverse path** to the source. When the destination **D**, or an intermediate node with an active route to **D**, receives the RREQ, it sends back an RREP, which is unicast along the reverse path. Each forwarding node records a **forward route** to **D**, forming a hop-by-hop routing structure in which nodes store only the next hop.

In probabilistic route discovery, the source transmits the RREQ with probability **$p = 1$**, while intermediate nodes forward it with probability **$p < 1$** and drop it with probability **$1 - p$**. Because forwarding decisions are independent, the expected number of retransmissions is **$p \times (N - 1)$**. The forwarding probability is dynamically adjusted based on **local node density** and the **set of covered neighbours**. A lower forwarding probability is used when many 1-hop neighbours have already received the broadcast, and a higher probability when fewer neighbours are covered. Covered neighbours are defined as nodes that have already received the same broadcast packet. To further improve reliable data delivery, the proposed work also incorporates **cluster head (CH)** selection and an **optimized multipath routing strategy**.

4.2. Cluster Head Selection Algorithm

This section demonstrates the CH selection strategy in the proposed algorithm based on the acceptability factor, which uses three constraints, such as energy, distance, and trust. At first, the cluster centres are randomly initialized and the membership is defined for the cluster centres based on the FCM algorithm. In the next step, the cluster centres are updated based on the defined membership. Finally, the proposed Taylor KFCM selects a single cluster centre using the acceptability factor from the derived set of cluster centroids. Following is the acceptability factor used for the CH selection and the progressing steps of the proposed algorithm.

4.2.1. Formulation of the Acceptability Factor

The acceptability factor is designed as in Equation (1) based on the distance, energy, and trust, which is multiplied by the α, β and γ. The CH is selected based on the maximal acceptability factor, which is the cause of maximal energy, minimal distance, and maximal trust.

$$F = \alpha \cdot E + \beta \cdot D + \gamma . T \quad (1)$$

It is to be noted that the sum of the constants α, β and γ equals unity. The parameters, such as trust are divided by a normalized factor, which is given as follows.

Trust: The trust factor should be maximal for the node to act as a CH. The trust factor is formulated in Equation (2) as,

$$T = \frac{1}{h*n} \sum_{i=1}^{h} \sum_{\substack{j=1 \\ i \epsilon j}}^{n} \left[T_{ij}\right] \quad (2)$$

Equation (2) signifies that the trust of the node is computed as the trust of the ith CH on the jth neighbours of the node i, which is the average of the three trust factors, such as recent, direct, and indirect trust. The trust between the nodes i and j is computed as,

$$T_{ij} = \frac{T^{direct} + T^{indirect} + T^{recent}}{3} \quad (3)$$

The trust of the nodes is a significant factor that envoy the trust of the nodes in the presence of some malicious attacks in the network. The main aim of the trust relies on gathering, disseminating, and accumulating the feedback of various other nodes present in the network. The trust is computed between two nodes in the network, which finalizes the nodes that are trusted and non-trusted. The trust values of the nodes vary in the limit between -1 and +1, wherein the trust value '-1' specifies the non-trusted and '+1' specifies the trusted nodes. On the other hand, the trust value '0' specifies that the node is unknown. The trust factors considered to formulate the trusted node include direct, indirect, and recent trust.

Direct trust: Local or direct trust is based on the self-experience regarding a target node, which is formulated as,

$$T^{direct}(t) = \frac{P_{ij}(t)}{S_{ij}(t)} \quad (4)$$

Indirect trust: The recommendation or indirect trust depends on the experience of the neighbouring nodes with respect to the target node. The indirect trust is formulated as,

$$T^{indirect}(t) = \frac{1}{g} \sum_{k=1}^{g} T_{k,j}^{direct}(t) \qquad 1 \leq k \leq g \quad (5)$$

Recent trust: The recent trust is the combination of direct and indirect trust, which is integrated using weighing factors, and this trust interprets the recent behaviour of the target node.

$$T^{recent}(t) = \eta * T^{direct}(t) + (1 - \eta) * T^{indirect}(t) \quad (6)$$

Where the value of $\eta = 0.5$.This estimates the final trust with related direct and indirect trust.

4.2.2. Improved Fuzzy C-Means Clustering

All nodes in the network are organized using a clustering algorithm such as **Fuzzy C-Means (FCM)**. FCM is widely utilized in pattern recognition, where each data point is assigned a **membership value** relative to every cluster centre, and the sum of these membership values for each point is constrained to one. The clustering process in FCM is formulated as an optimization problem that minimizes the following objective function:

$$\min_{u_{ij}, m_j} v_q \quad (7)$$

Where,

$$v_q = \sum_{i=1}^{N} \sum_{j=1}^{M} u_{ij}^{q} \left\| \theta_i - m_j \right\|^2 \quad (8)$$

Where m is the number of clusters, q is the fuzziness exponent greater than 1, μ_{ij} is the degree of membership of ith sensor in cluster j, and m_j is the centre of cluster j. The membership value $\mu_{ij}$for each sensor node with respect to every cluster centre lies between 0 and 1. This fuzzy partitioning is achieved through iterative optimization of the objective function, where both the membership values $\mu_{ij}$and the cluster centres $m_j$are updated as follows:

$$\mu_{ij} = \frac{1}{\sum_{h=1}^{M}\left(\frac{\|\theta_i - m_j\|}{\|\theta_i - m_k\|}\right)^{2/q-1}} \quad (9)$$

$$m_j = \frac{\sum_{i=1}^{N}\mu_{ij}^{q}\cdot\theta_i}{\sum_{i=1}^{N}\mu_{ij}^{q}} \quad (10)$$

The iterative optimization process terminates when the stopping condition $\sigma$is satisfied, i.e., when

$$| \mu_{ij}^{(k+1)} - \mu_{ij}^{(k)} | < \sigma,$$

where $k$denotes the iteration step. After the clusters are formed, the network is divided accordingly, and the **Cluster Head (CH)** selection process is initiated locally within each cluster. The detailed CH selection procedure is presented in **Algorithm 1**.

Table 1: Improved Fuzzy C-Means Clustering Algorithm

Algorithm 1: Cluster Head Selection using Fuzzy C-Means Clustering

Initialization: CH selection for cluster
while $m = 1,2,\cdots,M$ **do**
Selecting Cluster Head for mth cluster
for $j = 1,2,\cdots,N_{m,j}$ **do**
Calculate $\mho_j^{(m)}, \gamma_j^{(m)}, PL_{j,i}^{(m)}, PL_{FC}^{(m)}$
if $\Psi_j^{(m)} = max_{ch}\left(\frac{\mho_j^{(m)}\gamma_j^{(m)}}{\alpha PL_j^{(m)} + (1-\alpha)PL_{FC}^{(m)}}\right)$ then
$mth\ ch \leftarrow jth\ node$
else
$Cluster\ member \leftarrow jth\ sensor$
end if
end for
end while

Table 1 shows that the first parameter encourages the selection of a CH located close to its cluster members, thereby reducing the overall energy consumption within each cluster. The second parameter also contributes to CH selection by ensuring that the chosen CH is not positioned too far from the Fusion Centre (FC). However, prioritising proximity between the CH and its cluster members may increase the distance between the CH and the FC. Therefore, the third parameter—**the SNR of the reporting channel from the CH to the FC**—is incorporated into the selection process. In addition to distance, location, and SNR, the fourth parameter, **residual energy**, also plays a critical role. Residual energy refers to the remaining energy available in a sensor for sensing and transmission tasks. Based on these parameters, the proposed objective function for selecting the CH of the m-th cluster is given by:

$$\Psi_j^{(m)} = \max_{CH}\left(\frac{\mho_j^{(m)}\gamma_j^{(m)}}{\alpha PL_j^{(m)} + (1-\alpha)PL_{FC}^{(m)}}\right) \quad (11)$$

Where, $\mho_j^{(m)}$ is the residual energy of the jth candidate sensor, $\gamma_j^{(m)}$ is the SNR of reporting channel of jth sensor to the FC, $PL_j^{(m)}$ the average path loss of the channels between the jth sensor and its cluster members, $PL_{FC}^{(m)}$is the path loss of jth sensor and FC, and α is a weight given to path losses $PL_j^{(m)}$ and $PL_{FC}^{(m)}$, i.e., sensor to CH and CH to FC. The $PL_j^{(m)}$ is defined as

$$PL_j^{(m)} = \frac{\sum_{i=1}^{N_m} PL_{j,i}^{(m)}}{N_m} \quad (12)$$

Where, N_m is the number of sensors in the mth cluster. The $PL_{j,i}^{(m)}$ is the path loss between jth sensor and its cluster member ith sensor, which is given by

$$PL_{j,i}^{(m)} = 10\ nlog_{10}\left(R_{j,i}^{(m)}\right) \quad (13)$$

Where, $R_{j,i}^{(m)} = \left\|\theta_i^{(m)} - \theta_j^{(m)}\right\|$ is the distance between the jth and ith sensors with $\theta_i^{(m)} = \left\{x_i^{(m)}, y_i^{(m)}\right\}$ the position of jth sensor and n is the path loss exponent. The path loss between the cluster head (CH) of the m-th cluster and the fusion center (FC) is expressed as:

$$PL_{FC}^{(m)} = 10n\log_{10}\left(R_{FC}^{(m)}\right) \quad (14)$$

Where,$R_{FC}^{(m)} = \left\|\theta_j^{(m)} - \theta_{FC}\right\|$ with $\theta_{FC} = \{x_{fc}, y_{fc}\}$the position of FC.

4.3. Levy Flight Distribution Algorithm for Path Selection

In uncertain environments, the Levy flight (LF) showed that it can increase the effectiveness of resource searches. LFs can be inspired by many natural-inspired or physical-inspired phenomena in the environment. Natural species such as spider monkeys, fruit flies, and humans especially in the Juhoansi gatherers for hunters, can trail the paths of LF styles. Additionally, foraging patterns of albatrosses have been observed as an inspiration phase for the LFs. The diffusion of fluorescent molecules can be considered a physically-inspired phenomenon for the inspiration of LFs, and noise and cooling behaviours show the characteristics of LFs under the right conditions. Furthermore, in exploring unknown large search spaces, LFs are more efficient compared to Brownian random walks.

The algorithm starts its mechanism by calculating the Euclidean distance between every two adjacent sensor nodes and then the algorithm determines whether the sensor node will be in its original position based on the calculated distance or moving to another position. Another position will be performed using the LFs model in which the new position will be in a place close to a sensor node that has a low amount of neighbour's nodes or in a place which has no sensor nodes in the deployment area (search space) to decrease the opportunities for occurring the overlapping among sensor nodes. For implementing LFs or generating random walks, two characteristics must be identified: the step length of this walk that follows the chosen Levy distribution and the direction that makes it move towards the target position in the proposed algorithm, which can be derived from the uniform distribution. Levy flight is defined as a kind of non-Gauss stochastic process with a random walk in which the step lengths are drowning from a Levy stable distribution. Many methods can determine these features, but the simplest and efficient one is the well-known Mantegna algorithm for a symmetric and stable Lévy distribution. The Mantegna algorithm is one of the most efficient and straightforward ways to generate symmetric Levy distribution values. According to Mantegna's algorithm, the step length S is defined as

$$S = \frac{u}{|w|^{1/\beta}} \quad (15)$$

Where β is the Levy distribution index bounded as $\beta \epsilon [1,2]$, u and w are obtained from normal distribution as

$$u \sim N(0, \sigma_u^2)\ ,\ w \sim N(0, \sigma_w^2) \quad (16)$$

The symbol $\sim$ in Equation (16) denotes the random variable obeys the distribution on the right-hand side; that is, samples should be drawn from the distribution. The standard deviation σ_u and σ_w are defined by

$$\sigma_u = \left\{\frac{\Gamma(1+\beta) sin(\pi\beta/2)}{\Gamma[(1+\beta)/2]\beta 2^{(\beta-1)/2}}\right\}, \sigma_w = 1 \quad (17)$$

Where the Gamma function Γ for an integer z is expressed as

$$\Gamma(z) = \int t^{z-1} e^{-z} dz \quad (18)$$

Levy flight is a function that performs the work of Levy flights in terms of step length and direction. The proposed LFD algorithm calculates the Euclidean distance ED between the positions of the first two adjacent agents, namely X_i and X_j (the neighbour of X_i) using

$$Euclian\ Distance(X_i, X_j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \quad (19)$$

Where, (x_i, y_i) is the position coordinate of X_i and(x_j, y_j) is the X_j position coordinate. The distance ED is compared with a given threshold until the agents are finished after a specific number of iterations. If the resultant distance is less than the threshold (this means there is a problem in deploying the agents in the search space), then the algorithm starts its mechanism by adjusting the positions of these agents using

$$X_j(t+1) = Levy(X_j(t), X_{leader}, LB, UB) \quad (20)$$

Where t is an index for a number of iterations, $Levy$ is a function that performs the work of Levy flights in terms of the step length and direction. The $Levy$ is a function illustrated in Algorithm 1 and TP is the position (solution) that achieved the best fitness value of the objective function, which is called the target position. The random numbers $\alpha_1, \alpha_2, \alpha_3$ are such that $0 < \alpha_1, \alpha_2, \alpha_3 \leq 10$. The total target fitness of neighbours $TF_{Neighbours}$ around $X_i(t)$ is given by

$$TF_{Neighbours} = \sum_{k=1}^{NN} \frac{D(k) \times X_k}{NN} \quad (21)$$

Where, X_k is the neighbour position of $X_i(t)$, k is the neighbour's index, NN is the total number of $X_i(t)$ neighbours and $D(k)$ is the fitness degree for each neighbour given by

$$D(k) = \frac{\partial_1(V - Min(V))}{Max(V) - Min(V)} + \partial_2 \quad (22)$$

This proves the efficiency of the LFD algorithm in finding the optimal path with AODV in the multipath routing protocol.

4.4. Firefly Optimization Algorithm for Energy Efficiency

The objective of this subsection is to demonstrate that the proposed algorithm attains superior network performance while maintaining low energy consumption. Network performance is evaluated using the **energy efficiency** metric, defined as the ratio of the network's average throughput to its total energy consumption. The proposed FF algorithm uses the fitness function to regulate the optimization, and it is derived to be a maximization function. $Ener$ indicates the amount of energy present in the loss node x in the network. The $Ener$ calculation is given in Equation (23)

$$Ener(x) = \frac{E_{present}}{E_{initial}} \quad (23)$$

For transmitting n bits of the data packet, energy application of a path E_{path} should be minimum when compared with essential lower energy E_{req} . Hence, the energy objective function f_E helps to reduce the overall power utilization on a path and is determined by,

$$f_E = \min\{E_{path_i}\} \quad (24)$$

For developing the fitness criterion, the distance between the nodes and the energy possessed by the node is considered as the parameter. The fitness function (fit) is a sub-objective function for selecting the optimal parent for data transfer. The fitness function is calculated from the amount of ETX and RER. The ETX (Expected Transmission Count) path metric represents the estimated number of transmissions required to successfully deliver a packet along a given path, including any necessary retransmissions. If a packet is not successfully received, the sender retransmits it. The ETX for a link is defined as follows:

$$ETX_L = \frac{1}{P_f \cdot P_r} \quad (25)$$

If P_f denotes the probability of a packet being successfully transmitted and P_r represents the probability of successfully receiving the corresponding ACK packet, then the probability of successful packet transmission and acknowledgment is: $P_f \cdot P_r$. The w_1 and w_2 are average weight values. The weight values are adjusted from 0 to 1. Finally, the optimal solution is obtained where the weight w_1 and w_2 values are 0.5. The fitness function is calculated in Equation (26).

$$FIT = w_1 \times Ener(y_i) + w_2 \times ETX(y_i) \quad (26)$$

The firefly-based parent selection strategy selects the parent node efficiently with less convergence time.

$$EC = E_d + E_r \quad (27)$$

The minimum energy consumption between two adjacent nodes consists of E_d and E_r. Here, E_d denotes the energy required for data transmission, while E_r represents the energy consumed for receiving information between the two nodes.

5. Experimentation and Results Discussion

The proposed algorithm selects routing nodes based on their trust values and residual energy. Only nodes with high trust and adequate remaining energy are permitted to participate in the routing path. High-trust nodes ensure reliable packet forwarding, whereas nodes with sufficient residual energy reduce path failures and packet drops. Consequently, the algorithm improves both network lifetime and throughput. Moreover, by restricting routing to legitimate nodes, it significantly lowers control packet overhead associated with frequent route re-discovery.

Table 2: Simulation Parameters

Simulator	MATLAB
Simulation Time	600 sec
Bandwidth	25 Mb
Number of nodes	50
Packet Size	512 bytes

Table 2 summarizes the MANET simulation parameters. The proposed algorithm is evaluated in MATLAB over a **900 m × 900 m** area with **25–200 nodes**. Each node has a **250 m** transmission range, uses the **Two-Ray Ground** mobility model, starts with **100 J** of energy, and transmits packets of **512 bytes**.

5.1. Performance Metrics

To evaluate the simulation results, two scenarios are considered. In the first scenario, node mobility is analyzed by varying the pause time from **0 to 600 seconds**. A pause time of 0 indicates continuous mobility, whereas a pause time of 600 seconds represents static nodes. In the second scenario, for a pause time of 0 seconds, the number of malicious nodes is varied to assess the effectiveness of the proposed approach. The simulated MANET area for both scenarios is **500 m × 500 m**.

5.1.1. Energy Efficiency

Energy efficiency (EE) is the ratio of channel capacity over total power consumption. It is measured in the unit of bits per joule. In other words, energy efficiency is the number of bits transmitted by consuming one joule of energy. The energy model can be computed as follows,

$$EE = \frac{c}{P_{total}} \quad (28)$$

5.1.2. Packet Delivery Ratio

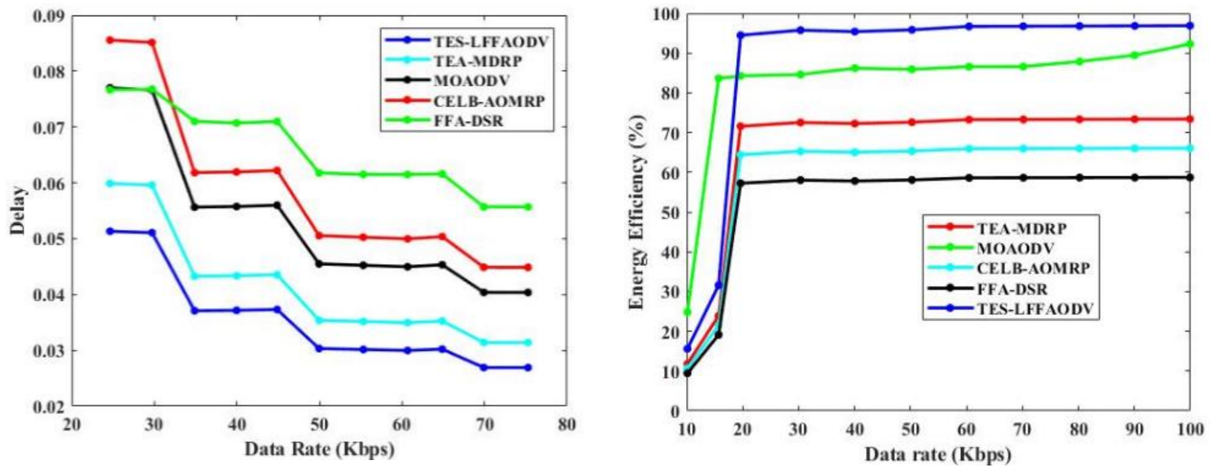
The packet delivery ratio (PDR) is the fraction of CBR-generated packets that successfully reach their destinations. Figure 4 presents the effect of node mobility on PDR in the absence of malicious nodes.

$$Packet\ Delivery\ Ratio = \frac{Total\ Packets\ Received}{Total\ Packets\ Sent} \quad (29)$$

5.1.3. Throughput

Throughput is the effective data transfer rate, measured here in bytes per second (Bps). It is calculated by dividing the total number of successfully received packets by the duration of the observation period. Throughput indicates available bandwidth and the amount of traffic the network can support. After data transmission, Equation (15) is used to compute this value.

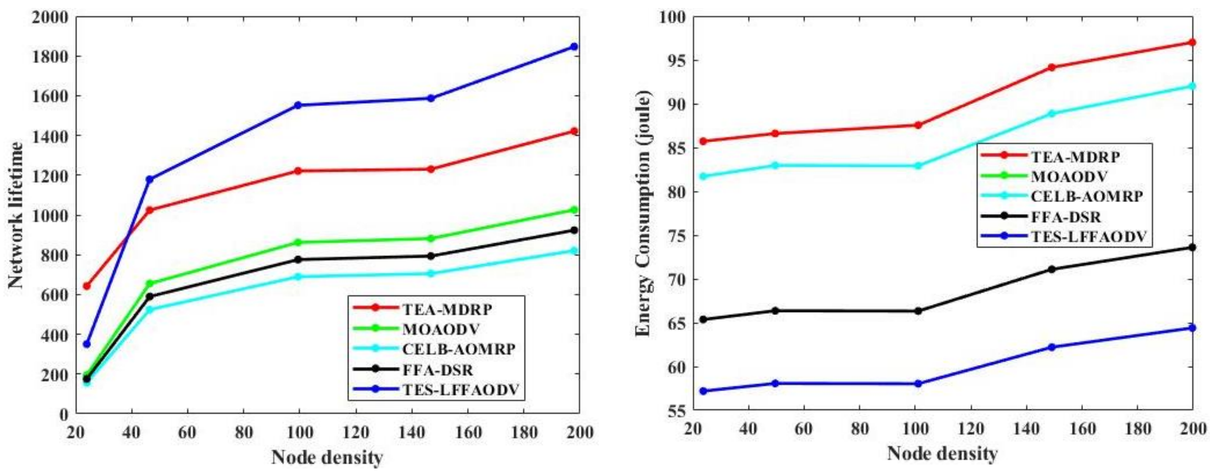
$$Throughput = \frac{Total\ Packet\ Sent}{Total\ Data\ Sending\ Time} \quad (30)$$



(a) (b)

Figure 2: Delay and Energy Efficiency Vs Data Rate

From the average queuing delay and energy efficiency graph as presented in Figure 2, as the data rate increases, the average queuing delay increases as well. It has been observed that the result of the proposed protocol shows the lowest average queuing delay at each data rate. TES-MDRP has the highest average queuing delay at 100 packets/second and 100 packets/second data rate. Figure 2(b) shows the result before and after the data rate is reduced. Although the differences are not apparent, it has an improvement of about 10 Mbits/joule at the peak of energy efficiency. The energy efficiency of the proposed system is 95.78%.



(a) (b)

Figure 3: Network Lifetime and Energy Consumption Vs Node Density

Figure 3 depicts the comparison of network lifetime and energy consumption versus different network sizes among AOMDV and TEA-MDRP. From Figure 3(a), the proposed protocol TESMRP-AODV outperforms the other three protocols regarding the network lifetime for all network size cases. Secondly, the energy consumption (Ec), which is another vital factor in opportunistic networks where most mobile nodes are usually equipped with limited power resources, is shown in Figure 3(b). The x-axis represents node density and the y-axis is the Ec in a unit of energy consumption per message. This graph shows that the value of Ec linearly increases when a network becomes denser.

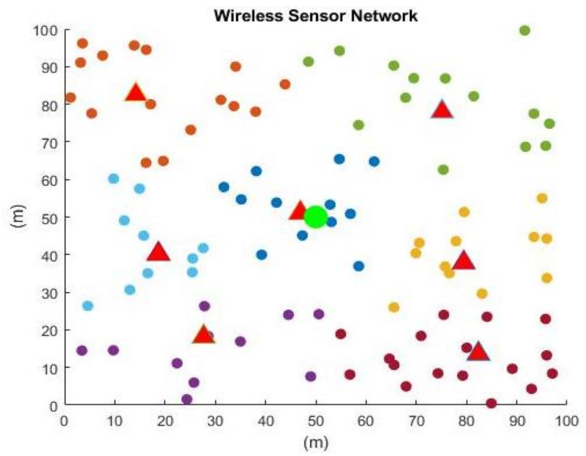


Figure 4: Cluster Head Selection Using Fuzzy

Figure 4 shows the analysis using 50 nodes and 5 CHs and the results of clustering at various rounds are revealed. The triangle shape refers to the CH, small balls denote the nodes, and the bright red coloured star signifies the sink node. Additionally, the green-coloured star specifies the data transmission occurring among the nodes. The location of the nodes at rounds 10-100 is depicted in Figure 4, respectively.

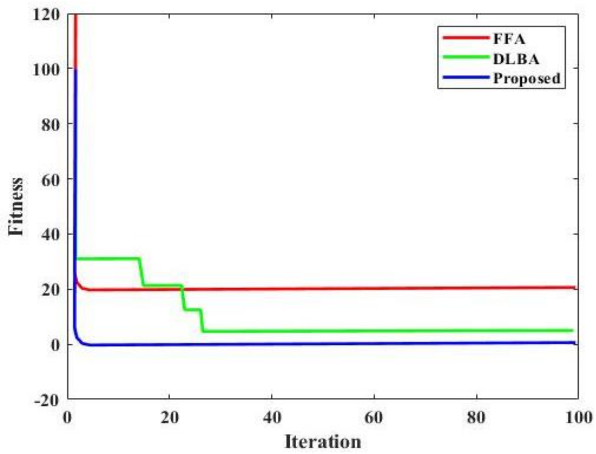


Figure 5: Fitness Vs Number of Iterations

Figure 5 evaluated the likelihood that the proposed strategy is the best (i.e., achieves the highest fitness) for all benchmark problems studied with FFA, DLBA, and with the proposed LFF algorithm. The graph can observe that although the proposed strategy does not allow for high fitness in the beginning, its performance begins to improve after around 20-100 iterations.

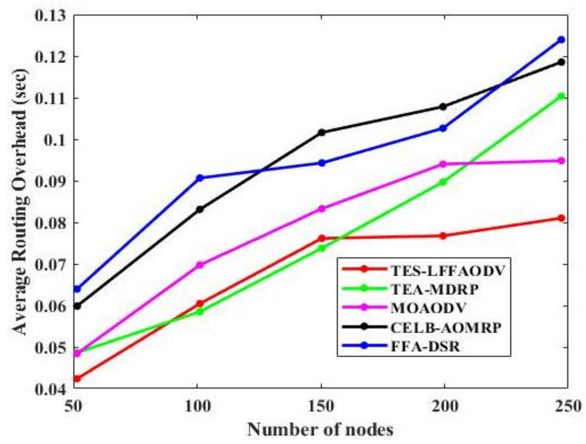


Figure 6: Average Routing Overhead Analysis

The experiment shows that the routing overhead for FCM and FGSA is increased when the numbers of mobile nodes increase because both protocols are based on the source routing approach (figure 6). In addition, the proposed TESMRP-AODV enhances the route discovery process at the destination node by replying only to those route request packets that are node disjoint routes. On the other hand, in the AODV protocol, the destination node replies all the route request packets that are reached the destination along with the route reply packet to the source. The impact of such route reply packets on the network performance is similar to that of RREP. The routing overhead of the proposed protocol slightly is increased compared to the AODV protocol.

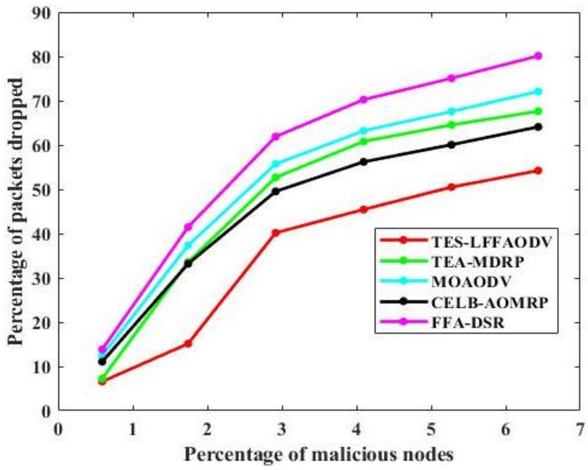


Figure 7: Percentage of Malicious Nodes

The trust-based routing method efficiently detects malicious node behaviour, enabling the proposed approach to achieve a higher PDR than existing techniques. As illustrated in Figure 7, it outperforms RBT and NETAR, with the packet drop percentage measured at **52.34%**.

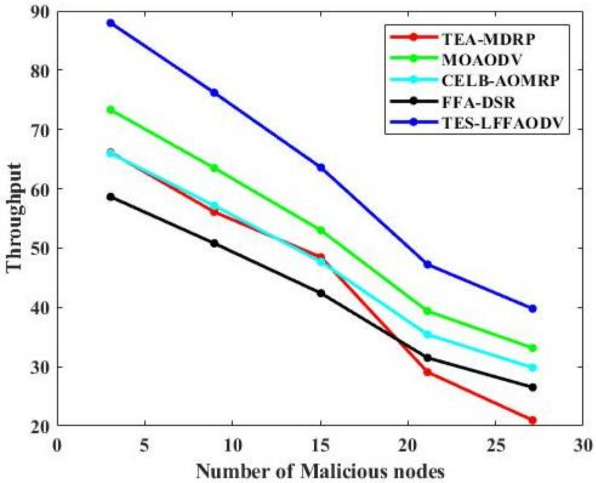


Figure 8: Throughput Vs Number of Malicious Nodes

The effect of increasing malicious nodes on throughput for normal AODV and TESMRP-AODV is evaluated. As shown in Figure 8, normal AODV—without malicious nodes—maintains a constant throughput of **237.22 kbps**. Under multiple attacks, the proposed AODV exhibits decreasing throughput as the proportion of malicious nodes rises from **20% to 90%**.

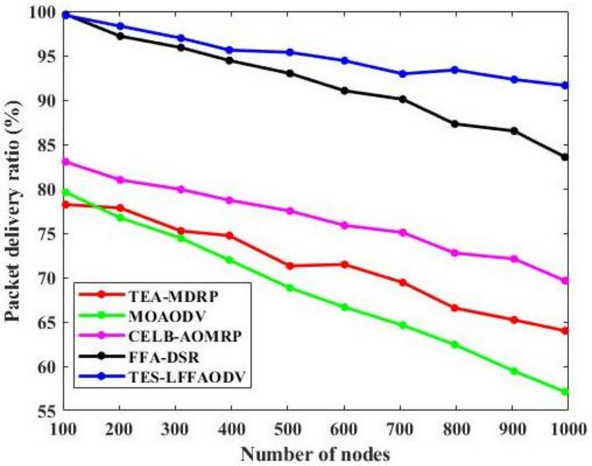


Figure 9: Packet Delivery Ratio Vs Number of Nodes

The results obtained from the simulation indicate that whenever the numbers of mobile nodes increase, the packet delivery ratio decreases gradually. As the number of mobile nodes increases, the network is congested which causes more link failures. Figure 9 presents the results for the packet delivery ratio where the numbers of mobile nodes are varying with the range of 100, 300, 500, 600, and 1000 nodes. In this respect, the packet delivery ratio at the destination node is also decreased.

5.2. Comparison Analysis

To find the optimal paths between the communicating nodes, the traditional DSR algorithm is modified by using the TES-LFFAODV algorithm. The performance of the AODV protocol in presence of a malicious node is compared with the performance of the proposed technique in this work. Further, describes the packet size variation between the existing and proposed systems. It can be seen that the proposed system performs well than the existing system. This is due to the use of an intelligent trust-based secure routing protocol.

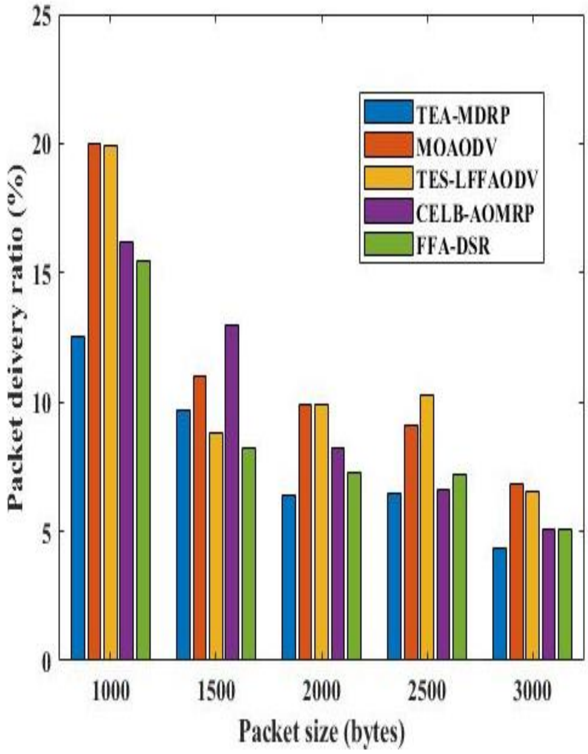


Figure 10: Packet Delivery Ratio Vs Packet Size

Figure 10 shows better results for the proposed protocol than the other four protocols. TEA-MDRP, MOAODV, CELB-AOMRP, and FFA-DSR show a decrease in the percentage of Packet Delivery Ratio when packet sizes increase. When using TCP traffic connection, the performance of TES-LFFAODV is around 20% while the other protocols have a higher Packet Delivery Ratio percentile.

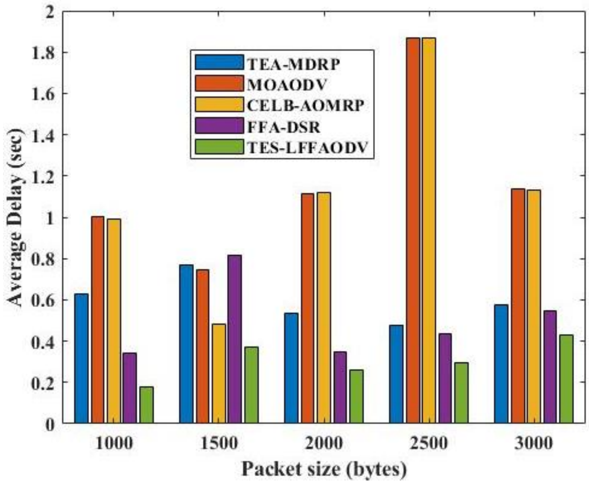


Figure 11: Average Delay Vs Packet Size

Figure 11 shows the average E2E delay in a variety of packet sizes, the outcomes showed that the two protocols have almost the same average E2E delay when the packet size is 128 2000 kbps. But when increasing the packet size, the graph observed that routing protocol TES-LFFAODV has better results in terms of average E2E delay. As the routing overhead on the proposed protocol is less than AODV that leads to consuming less bandwidth.

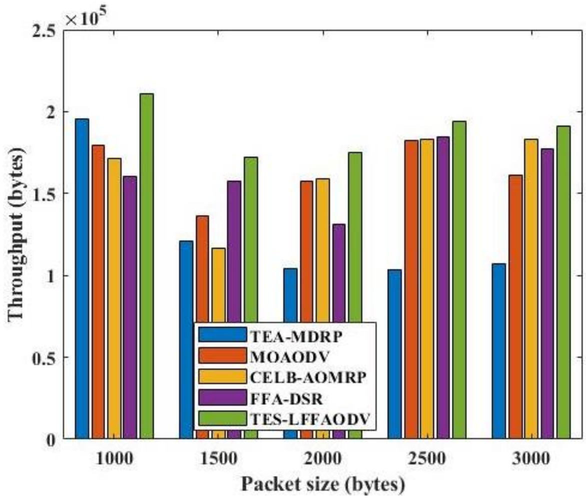


Figure 12: Throughput Vs Packet Size

Figure 12 presents the throughput versus packet size. The article can notice that TES-LFFAODV outperform the standard IEEE 802.11 protocol. As the packet size increases the throughput improvement increases. When cooperation is performed, a direct low-rate link is replaced by a two-hop high-rate link, hence, the number of delivered packets per unit of time is increased which enhances the throughput.

6. Research Conclusion

The foremost challenging task to offer a multipath routing scheme aimed at mobile ad-hoc networks is to attain a secure protocol by maintaining trust and also energy efficacy simultaneously. As a supplementary method to improve safe data delivery in a MANET, this research proposes and analyses the cluster head (CH) selection and optimum multipath scheme. Consequently, the research proposes a Trust-Based Energy-Efficient Secure Multi-Path Routing Protocol (TESMRP). In a routing discovery procedure, an SN broadcasts a route request (RREQ) message to discover the DN using a generic probabilistic routing procedure. Clustering is one of the significant techniques for expanding the lifetime of networks in wireless sensor networks (WSNs). The optimal CH is elected by an improved fuzzy C-means algorithm method built on density peak, and Cluster Heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust. The best route relies upon the projected hybrid protocol, accordingly, the research studied the hybrid trust-based secure multipath routing protocol of Ad hoc on-demand distance vector (AODV) with the Levy flight distribution algorithm to attain the optimal shortest path selection to enhance the MANETs. In addition, high energy consumption is addressed by Firefly Algorithm to find the optimal values/fitness function for the objective parameter (i.e. energy). The proposed TES-LFFAODV protocol is designed with a multi-objective function using an optimization algorithm and implemented in MATLAB. The main aim of the AODV-LFD protocol is to achieve an efficient path among multiple paths to satisfy quality requirements such as delay, throughput, energy consumption, delivery ratio, loss ratio, and latency. The suggested clustering protocol outperforms delay-based, and reliability-based routing protocols, according to simulation results. These simulation findings reveal that the performance of the proposed firefly optimization is increased in terms of increased connectivity probability, reduced delays, and increased packet delivery ratio of the mobile when the entire system was considered.

References

[1] 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.

[2] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S.A., Khalaf, O.I. and Subbayamma, B.V., 2021. An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9, pp.163043-163053.

[3] Alghamdi, S.A., 2022. Cuckoo energy-efficient load-balancing on-demand multipath routing protocol. Arabian Journal for Science and Engineering, 47(2), pp.1321-1335.

[4] Bai, P.K., RMBSRA: Routing Manager Based Secure Route Analysis Mechanism for Achieving Secure Routing Protocol in IOT MANET.

[5] Alappatt, V. and PM, J.P., 2021. Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E. Int. J. Comput. Netw. Appl., 8(4), p.400.

[6] Dhanapal, R., Kalpana, V., Chiwariro, R., Thangadurai, N., Sentamilselvan, K. and Immanuel, D.J., 2021. An Energy Efficient Secure Routing for Mobile Nodes for Multihop Adhoc Network. Journal of Computational and Theoretical Nanoscience, 18(3), pp.973-976.

[7] Singh, P., Khari, M. and Vimal, S., 2021. EESSMT: an energy-efficient hybrid scheme for securing mobile ad hoc networks using IoT. Wireless Personal Communications, pp.1-25.

[8] Lavanyaa, R., 2021. Energy Efficient with Trust and Qos-Aware Optimal Multipath Routing Protocol Based on Elephant Herding Optimization for IoT Based Wireless Sensor Networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), pp.979-990.

[9] Muruganandam, S. and Renjit, J.A., 2021. Real-time reliable clustering and secure transmission scheme for QoS development in MANET. Peer-to-Peer Networking and Applications, 14(6), pp.3502-3517.

[10] Mohan, P., Subramani, N., Alotaibi, Y., Alghamdi, S., Khalaf, O.I. and Ulaganathan, S., 2022. Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks. Sensors, 22(4), p.1618.

[11] Amudha, S. and Murali, M., 2021. DESD-CAT inspired algorithm for establishing a trusted connection in energy efficient FoG-BAN networks. Materials Today: Proceedings.

[12] Veeraiah, N. and Krishna, B.T., 2020. An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence, pp.1-15.

[13] Nayyar, A. and Singh, R., 2020. IEEMARP-a novel energy efficient multipath routing protocol based on ant Colony Optimization (ACO) for dynamic sensor networks. Multimedia Tools and Applications, 79(47), pp.35221-35252.

[14] Ghaleb, S.A.M. and Vasanthi, V., 2020. Energy efficient multipath routing using multi-objective grey wolf optimizer-based dynamic source routing algorithm for MANET. International Journal of Advanced Science and Technology, 29(3), pp.6096-6117.

[15] Murugan, S. and Jeyakarthic, M., 2020, March. An energy efficient security aware clustering approach using fuzzy logic for mobile adhoc networks. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (pp. 551-555). IEEE.

[16] Bai, P.K., RMBSRA: Routing Manager Based Secure Route Analysis Mechanism for Achieving Secure Routing Protocol in IOT MANET.

[17] Suresh Kumar, R., Manimegalai, P., Raj, V., Dhanagopal, R. and Johnson Santhosh, A., 2022. Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing, 2022.

[18] Neenavath, V. and Krishna, B.T., 2022. An energy efficient multipath routing protocol for manet. Journal of Engineering Research.

[19] Kumar, R., Tripathi, S. and Agrawal, R., 2022. Trust-based energy-aware routing using GEOSR protocol for Ad-Hoc sensor networks. Wireless Networks, pp.1-24.

[20] Thirunavukkarasu, V., Senthil Kumar, A. and Prakasam, P., 2022. Cluster and angular-based energy proficient trusted routing protocol for mobile ad-hoc network. Peer-to-Peer Networking and Applications, pp.1-13.

[21] Shanmugasundaram, D., 2022. Trust Aware Energy Efficient Routing Protocol In Ad Hoc Networks.

[22] Bondada, P., Samanta, D., Kaur, M. and Lee, H.N., 2022. Data security-based routing in MANETs using key management mechanism. Applied Sciences, 12(3), p.1041.

[23] Deepa, C., Latha, B. and Jenish, I., 2022. Development and Performance Evaluation of a New Energy-Efficient Double Cluster-Head Routing (EEDCR) Protocol for Wireless Sensor

Networks. Wireless Communications and Mobile Computing, 2022.

[24] Sivapriya, N. and Mohandas, R., 2022. Optimal Route Selection for Mobile Ad-hoc Networks based on Cluster Head Selection and Energy Efficient Multicast Routing Protocol. Journal of Algebraic Statistics, 13(2), pp.595-607.

[25] Sumathi, K. and Kumar, D.V., Energy-Efficient Perspicacious Ant Colony Optimization Based Routing Protocol for Mobile Ad-Hoc Network.