Journal of Theoretical and Applied Information Technology
30th November 2022. Vol.100. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SRABDE: SECURE ROUTING ALGORITHM BASED ON DIFFERENTIAL EVOLUTION FOR MOBILE ADHOC NETWORKS

[1]K.VIMALA, [2]DR. D. MARUTHANAYAGAM

[1]Research Scholar, Periyar University,Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India

[2] Head/Professor, Periyar University, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India

E-mail: vimalak0087@gmail.com, kesimaruthu@gmail.com

ABSTRACT

Mobile ad-hoc network is an infrastructure-less spontaneously formed wireless environment that is deployed without any centralized unit. In this type of network, all nodes are assumed to be trustworthy but in the real scenario, a few can be malicious and, therefore, secure and reliable route for data transmission is always a matter of question. A new protocol called **Secure Routing Algorithm Based on Differential Evolution (SRABDE)** is proposed for Mobile Adhoc networks with effective fitness function. Differential Evolution (DE) is an evolutionary computational method inspired by the biological processes of evolution and mutation used to minimize routing overload in terms of battery power, node reliability and stability. The objective of this algorithm is to find the most suitable path for data transmission taking into account three influencing factors: **reliability, battery power and node stability,** then to resolve the malicious **performing nodes such as black hole and gray hole attacks.** The component indices for the effective fitness function involved are **trust factor, residual battery power and node stability** for the purpose of selecting the most promising routes through the proposed SRABDE algorithm. The trust is developed to predict the nature of the node, whether malicious or not; while the stability of the nodes ensures longer stable routes.The simulation is carried out in various scenarios to evaluate the performance of the differential evolutionary secure routing algorithm with packet delivery ratio, average end-to-end delay, routing overhead, energy consumption, detection accuracy, and throughput. Results are compared with three existing algorithms **Intruder Free Route Discovery (IFRD)**, **Trust Path Ant Colony Optimization (TPACO)**, and **DE algorithm-based ad hoc on-demand multi-path distance vector (DE_AOMDV).**

Keywords: *MANET, Routing Protocol, Differential Evolution, Trust, Node, Path, Security, Attacks, Algorithm and Networks.*

1. INTRODUCTION

MANETs are self-organizing wireless nodes that connect with each other across a wireless medium, without the need for network administration or infrastructure, and with constantly changing topologies. MANET faces various difficulties in terms of Quality of Service (QoS) due to above characteristics, which is the essential in present scenarios in environment to guarantee of reliable data delivery, battery power, and network node stability. In traditional routing algorithms example (AODV- Ad-hoc On-demand Distance Vector) and (DSR- Dynamic Source Routing) the working procedure is basically done by hop count or node distance (Source (S) to Destination (D)), further factors for example consistent data delivery, node battery power, and mobile node stability are not considered in any of the traditional routing algorithms. Investigators have introduced many variants that method such as SEAD [1], ARAN [2] and SRP [3].Mainly MANETs are susceptible to various types of attack [4], which are categorized into two categories: (i) active (ii) passive attacks.The active attacks aim to disturb the routing information by producing, dipping, altering, and injecting mobile data packets while passive attack just attempts to seek some valuable information about mobile data packet like location disclosure, traffic exploration, etc. Various investigators have understood security in the MANETs as a foremost

dominant issue to sustain the mobile network's lifetime and recommended various methodologies to provide solutions such as cryptographic algorithm [9]**.** Trust is defined as estimating the creditability between two communicating nodes. Trust can be understood as a subjective probability, belief, and risk measures. Trust commonly reveals the opinion or confidence on the integrity, honesty, truthfulness about the target node's future behavior. Therefore, for MANETs, trust turns to be a decision-policy maker for more secure communication. Additionally, trust is security aid (assist) against the malicious mobile node; it is classified into two types of trust: direct trust and indirect trust. Evolutionary algorithms have an explicit influence on the configuration parameters of routing protocols.The purpose is to determine most optimal configuration parameter which increases performance of MANET routing protocols. The proposed **Secure Routing Algorithm Based on Differential Evolution (SRABDE)** algorithm is according to a meta-heuristic evolutionary method that intends to examine most reliable and secure route for mobile data transmission. **SRABDE** is encouraged from a type of nature-inspired evolutionary approach, termed as Differential Evolution. Storn and Price [10] created DE, an artificial mathematical evolutionary suit, to find best-suited solutions for optimization problems by taking current restrictions and flexibilities into account. It's, more precisely, a technique for guiding search using distance and direction statistics. Scaling Factor (F) and Crossover Factor (CR) are two control factors in differential evolution; their values are set or created according to application requirement. The fitness function is linked to the evaluation of the solution for the desired application. Another crucial feature of the fitness function is its capacity to quantify the quality of the final solution by framing distinct components in it according to the application requirement. **The following are contributions to the SRABDE:**

- ***To determine the most appropriate trusted path*** for data transmission by taking into account three influencing factors: trust, battery power, and node stability.
- ***SRABDE selects only the nodes having secure good link quality*** so that no of route failures is decreased.
- ***Defending against malicious activity nodes*** such as black-hole and grey-hole attacks.
- *Differential evolution* is a well-known meta-heuristic for lowering routing costs in terms of battery power, trust, and node stability.

algorithm [5], intrusion detection system [6], game theory [7], trust-dynamics [8] and nature-inspired evolutionary

2. BACKGROUND STUDIES

In this section, existing works mentioned in various scientific journals related to different trust methodologies that are yet to be used to improve the performance of the network by securing data transmission. To provide a clear picture of background studies the current section is divided into as below.

2.1 Differential Evolution

DE is a type of evolutionary technique that is based on a stochastic population and is the latest technique for resolving real-valued optimization issues [11]. DE has numerous advantages, the first of which is that it's far simpler than any other evolutionary method. Its simplicity drew academics from other domains to use it to address their domain-specific challenges. Second, it only has a few parameters to deal with: F, NP, and Cr, all of which have a direct impact on DE's performance. Third, in terms of convergence speed, accuracy, and resilience, the overall performance of this evolutionary algorithm is still superior to that of other evolutionary algorithms. Fourth, handling big scale higher dimension problems necessitates less storage space complexity. All of these factors combine to make DE an excellent global optimization technique [12]. The basic nomenclature for multiple DE variants is DE/a/b/c, where a stands for perturbed vectors that are randomly picked according to (DE variations), b stands for number of difference vectors, and c indicates for crossover types (bin or exponential). The classical DE consists of four main steps: initialization, mutation, crossover or recombination, and selection which are described below as follows:

- **Initialization:** The DE method only performs initialization once while searching for global optima in multi-dimensional space; the remaining three phases are continued until the termination criteria are met. It begins with the initialization of the NP_g population in d-dimensional real-value vector space, and the successive generations are indicated by $g=\{0,1,2,3,\ldots\ldots\ldots\ldots\ldots\ldots,g_{max}\}$.
- **Mutation strategy:** Mutation is the biological term for a rapid change in genetic material. Following initialization, the next step is to generate $\vec{M}_{i,g}$ donor vectors (mutant

vectors) for each target vector$\vec{x}_{ra,g}$from the current population. [13].

- **Crossover operators:** After mutation, the information from the donor vector$M_{i,j,g}$and the target vectors $x_{i,j,g}$is exchanged to create a new offspring vector. Binomial (uniform) and exponential crossover are the two most prevalent crossover strategies (two-point modulo).
- **Selection:** In the selection process, the next step is to choose best candidate. The best candidate can be either the target vector or the created trail vector.

2.2 Trust Computation

Trust computation is a method of quantifying security risks in order to improve network performance. To handle the security problems in MANET an AP trust method was proposed by Xia et al. [14]. The AP trust algorithm into two parts: (i) trust assessment (ii) trust prediction. The trust assessment module computed the indirect trust and direct trust of each mobile node in each direction ('t'). The second module trust prediction was used to forecast the future performance of a mobile node by using an advanced dynamic grey markov chain scheme. Wei et al. [15] submitted another paper that addressed the trust management component in terms of uncertain reasoning for security enhancement. The Bayesian inference criterion was used to assess direct trust. The Dempster-Shafer Theory was used to assess indirect trust (DST). In order to fade the reputation, the malicious node was managed and punished by the penalty factor. With higher throughput and packet delivery ratio, the findings have bolstered the network's efficacy and performance. In addition, the average end-to-end delay and message overhead increased somewhat. The trust components in the algorithm **SRABDE** enhance the security performance of a MANET by ignoring low-trust node, not to participate in data dissemination. In this proposed work, direct trust has been assessed in a distributed manner and each node maintains its own trust table. The trust table maintains trust statistics for each neighbor node evaluated by the node (owner of the trust table) on the basis the interactions. The Proposed **SRABDE** fitness function has **three** components: trust, node stability, and remaining battery power which assist to search and secure optimal path.

3.TRUST BASED ALGORITHMS

3.1. Intruder Free Route Discovery (IFRD)

In this paper the detailed description of the methods involved in the proposed Intruder Free Route Discovery (IFRD) which includes model definition of the proposal, the intrusion preventive measures depicted, which used in Differential Evolution as fitness scale to measure the optimality of the newly framed routes by differential evolution technique. The initial phase of the proposed algorithm discovers the set of routes through route request process. Further measures node level and route level fitness by intrusion preventive measures. Later the process, initiates the Differential Evolution process on these initial routes until it discovers the routes having max possible fitness under depicted intrusion preventive measures. These intruder preventive measures in regard to each of the node appeared in one or more routes discovered through route request phase of the routing process.

3.2. DE algorithm-based ad hoc on-demand multi-path distance vector (DE_AOMDV)

In this paper proposed a DE algorithm-based ad hoc on-demand multi-path distance vector (DE_AOMDV) protocol for mobile ad hoc network(MANET). The proposed DE_AOMDV routing protocol has better performance and improves the quality of the MANETs. The main objective of this research paper is to find the optimal path from available multiple paths between source and destination to be used in route recovery process. The author first presents the network model and then formulates the DE_AOMDV. The author next focus on ad hoc on-demand multipath distance vector (AOMDV) routing protocol (Ibrahim et al., 2009). AOMDV provides multiple loop free disjoint paths. Eachroute discovery is associated with high latency and overhead. This inefficiency can beavoided by havingmultiple redundant paths available. The author used AOMDV to findnode-disjoint or link-disjoint paths.

Implementation of DE

Finally, the design of the DE has components like population initialisation, fitness function, mutation, crossover and selection scheme. A routing path contains the sequence of nodes in network. The DE algorithm is applied to node disjoint paths that is been obtained from the route discovery phase. A routing path is encoded by a string of positive integers that indicating the IDs

of the nodes in the network. The length of the string should not be more than the number of nodes present in the network.

- **Initialisation:**DE starts with the population of NP D-dimensional search variable vectors. These vectors are referred in literature as 'genomes' or 'chromosomes'. In DE, each chromosome represents a potential solution and this can contain more than one solution initially. The node disjoint paths obtained from route discovery phase are considered asinitial chromosomes.
- **Mutation operation**: After initialisation, DE employs the mutation operation to produce a mutation vector v_i, G, with respect to each individual x_r, G, so called target vector, in the current population.
- **Crossover operation:**After the mutation phase, crossover operation is applied to each pair of the target vector x_i, G, and its corresponding mutant vector v_i, G
- **Selection operation:**DE actually involves the principle of Darwinian 'survival of fittest' in this selection process which may be outlined as
- **Backup routing using DE:**In this section we discover backup paths from source to destination in case of primary path link failure. We proposed a new protocol to improve existing on-demand multiple path routing protocols by constructing multiple backup routes using DE algorithm in the last section. By using DE (Aswani et al., 2015), we obtain the optimal path from source to destination, and in the same phase we find an alternate path to be used in link failure. The alternate path will be next best path when compared to the optimal path.
- **Path discovery phase:**The primary paths and backup paths are established during the route discovery phase itself when we find optimal paths by using DE.
- **Path recovery phase:**The data packets are delivered via the primary path till the primary path is disconnected. When a node detects a link failure, it utilises the backup paths in place of primary path. This is done with the help of RERR message when a node faces the link or node failure it will send a RERR message to the source node that initiates the routing process.

3.3. Trust Path Ant Colony Optimization (TPACO)

The path of Trust S. Sugumaran's (TPACO) algorithm [14] is a swarm intelligent scheme for selecting a trust path from multiple routes between source (S) and destination (D). Proposed algorithm controls the Data Packet dropping occurrence and consent in network by serving as best route. TPACO algorithm, trust mobile node from sender (S) to destination (D) employed with ant colony algorithm, it consists of three steps: (1) discovered potential path, (2) path selection and updating, than (3) trust path selection. In this case, Trust value is calculated by choosing a probable path between the source (S) and destination (D), counting the no of hops, and calculating node's battery deviation in percentage.

1.Discovered Potential Path

Because sources (S) do not have a route to destination (D) at first, the ant's agent initiates the source requested message and distributes it to all the neighbouring nodes in the network. When the Forward ANT reaches a neighbour node that is not a destination node, it proceeds to the next hop with updated information about the neighbour node. Otherwise, Destination destroys Forward ANT requests and provides Backward ANT replay to sources. The Ant pheromone density is being deposited on paths at this time. If the pheromone value is less than the threshold value, the path is unsuitable for data transmission than should be terminated.

2. Path selection, Route update

Density of pheromones along the route and probability of period interval between the paths determine the path chosen from sender (x) to receiver (y). The time interval indirectly indicates distance of path. Thereby, one of major factors determines best network path. Forward ANTs typically move from sources in all directions around the node. The deposit of forward ANTs is pheromone, than it updates pheromone level in each mobile node. Multiple paths from sender to receiver are generated by the ant colony concept. Uncertainty malicious nodes are dropped the data packets, the ant agent forwards the data packets that were data dropped by the vulnerable mobile node, and the reduced pheromone density is set to zero, causing a time delay increase. Nonetheless, they only forward a percentage of data packets to next hop, and the pheromone density between two adjacent nodes is reduced compare to a level less than another path density level. Thereby, malicious nodes within network can be easily identified.

3.Trusted path Selection

The three factors such as average deviation of battery level, shortest route path, and lowest hop count between mobile nodes are used in this proposed method. Best path equation probability is regularly used to determine the shortest path (1).When compared to other direction route and battery deviation the trust path is selected by

smaller no of hops. Both hop and battery deviation conditions provide a secure communication path while reducing packet drops and selfish attacks caused by vulnerable network nodes. Trusted mobile nodes provides efficient than possible data packet transmission paths. TPACO optimization algorithm is using to implement route protection techniques. The deposit pheromone of choose path was assigned the greatest route for data packet transmission. Where the source chooses the shortest route and other routes are saved for future use. MANET enables a larger number of nodes to enter and exit the network. A transmission delay in this case collapses the wireless network route and depletes node energy. Above this problem is avoided by employing the frequent path selection probability method and choosing the route from wireless network periodicals.

4.PROPOSED ALGORITHM (Secure Routing Algorithm Based on Differential Evolution (SRABDE))

4.1. Problem and route encoding

The problem is to discovery a secure route between source mobile node (S) and destination mobile node (D) in a MANET network represented by graph G = (V, E). Every mobile node in network is a portion of route (chromosome) encoding scheme and participates in its evolution. There are various pathways between source mobile node (S) and destination mobile node (D) in MANET; each node is considered a gene, which is a single chromosome unit. The first and last genes, respectively, are designated for the source (S) and destination (D).

At first, each chromosome's length must not exceed N, which is total no of nodes in the network. During route creation, each node is only accessible once. Each route's combinatory possibilities try for every potential link, whether convenient or not. It's self-evident that the lengths of all routes vary. The built chromosome is set up to undergo mutation and crossover in order to find the optimum path. The value of fitness function, which is derived using the metrics defined in fitness function, then verifies its optimality. The algorithm determines the best route.

4.2 Metrics and fitness function (FF)

Three criteria determine the fitness of a route configuration: trust, residual battery power, and mobile node stability. The transmission path is chosen based on these three characteristics. The solution paths are represented by R = {r_1, r_2, r_3, ...,r_n}. To determine the fitness value, the framed fitness function for the secure route is used as a minimization function. The following are the metrics:

4.2.1 Metrics

(A) Trust factor: In simple terms, trust develops throughout time as a result of personal encounters. Trust can be defined as belief or behavioral uncertainty between any two nodes in a MANET. The forwarding ratio is a mathematical representation of trust.

$$\alpha = \frac{Successfully\ forwarded\ packet\ (Pact_F)}{Total\ no\ of\ packet\ (Pact_T)} \quad (1)$$

Data packets and control packets are two types of packets that exist. Trust is computed mathematically as the total number of interactions between two nodes A and B, as estimated by the equation (2).

$$T_{AB} = t1 * DataPact_\alpha + t2 * ControlPact_\alpha \quad (2)$$

where $t1$ and $t2$ ($t1$, $t2 \geq 0$ and $t1 + t2 = 1$) are weights for data packet forwarding ($DataPact_\alpha$) and control packet forwarding ratio ($ControlPact_\alpha$), respectively. We must calculate the node's not-to-trust factor by subtracting the node's trust factor value from one because we are minimizing an objective function. This will encourage the use of equations (3) and (4) to identify the best possible route with the least amount of fitness (4).

$$T' = 1 - T_{AB} \quad (3)$$

$$T'_r = \sum_{\substack{x=sn+ \\ x \in r}}^{dn-1} T'_x \quad (4)$$

T'_r is the r-th route's not-to-trust factor, and T is the node not-to-trust factor.

(B) Residual battery power: Total power consumed and dissipated power required by the equipment for each sort of interaction. Assuming that each node possesses power E, the Residual Battery Power (RBL) can be calculated as follows: (5).

$$Residual\ Battery\ Level\ (RBL) = \frac{Energy}{Energy_F + Energy_Q} \quad (5)$$

where EnergyF and EnergyQ are the power necessary to transmit and receive a single packet, as well as the equipment's dissipated power. The total of residual battery power available in each node can be used to calculate residual battery power available from source to destination, as shown in equation (6).

$$RBL_r = \sum_{\substack{x=sn+ \\ x \in r}}^{dn-1} RBL_x \quad (6)$$

RBL_r Denotes the remaining battery power for the r-th route, while RBL_x denotes the remaining battery power for node x.

(C) Mobility model and node stability:In MANETs, mobility is a big challenge. We used the Random Waypoint Mobility (RWM) model. Because of its simplicity and wide availability, it is a widely popular model. According to the model, the node stays in the same place for a set amount of time (pause time 'p'). The node adjusts its speed and direction after the stop time is over. The value of 'p' is somewhere between a certain range and a certain speed, depending on the necessity, which can be either set from a range or fixed.

While it comes to data transmission, the node's stability is always a factor to consider when deciding on the best path for improved service quality. In terms of packet forwarding, the stable node set provides better assurance. **The following two factors are used to calculate node stability:**

1 **Node's own stability:** The node's mobility is calculated by referring to its previous position.

2 **Neighbour stability:** To compute node stability with mobility, locate the most stable neighbour node.

Node's own stability: When a node exists throughout its transmission range R, it is considered to be stable. The node's own stability is calculated by estimating the node's distance d_a^{tw} travelled during the time window 'w' while accounting for the mobility factor.As shown in equation (i_2, j_2) and (i_1, j_1) the current and prior location coordinates are (i_2, j_2) and (i_1, j_1), respectively(7).

$$d_a^{tw} = \sqrt{(i_2 - i_1)^2 + (j_2 - j_1)^2} \quad (7)$$

The node with the most mobility travels the greatest distance and has the least stability. The equation calculates the node's 'a' own stability metrics $NoS_a(w)$ based on the node's mobility in each time window 'w' (8). The value of a node's own stability ($NoS_a(w)$) tends to fluctuate between 0 and 1. The value of 'R' can be changed to 'R/2, R/4, R/8,' and so on.

$$NoS_a(w) = \begin{cases} 1 - \frac{d_a^{tw}}{\frac{R}{4}} if\ 0 \le d_a^{tw} \le R/4 \\ 0 \qquad otherwise \end{cases} \quad (8)$$

Neighbour stability ($\boldsymbol{NS_a(w)}$) ***:*** It's defined as a node's 'a' stability in terms of connectivity with its neighbours when travelling through a network. The Neighbour List (NL) is maintained by each node by collecting connectivity information. The equation calculates the node's neighbour stability with the time window (9).

$$NS_a(w) = \beta \frac{1}{NL_a} \sum_{i=1}^{NL} NoS_i(w) + (1 - \beta).NS_a(w-1) \quad (9)$$

where β is the balancing factor between [0, 1], $NS_a(w-1)$is the most recent neighbour node stability, and $NoS_i(w)$is the node 'i' own stability in the node 'a' neighbour list. We are analyzing the stability model (the node's own stability and neighbour stability) in order to choose the most prominent route that will remain stable for the longest time.

Node stability (SN(w)): It is defined as the stability of node 'a' in terms of node's own and neighbor's stability in the time period 'w', as computed by the equations (8) and (9) and derived through the equations (8) and (9) (10).

$$SN(w) = f\big(NoS_a(w).NS(w)\big) = \gamma.NoS_a(w) + (1-\gamma).NS_a(w) \quad (10)$$

Where γ is the balancing factor that lies between [0,1] and is determined by the relative importance of the node's own stability vs that of its neighbours. The higher the value of SN(w) the more stable the system is. Only when the node's own and neighbouring stability are both greater than zero is node stability calculated. Because the route must have stable nodes for data distribution, the equation can be used to determine it (11).

$$SN(w)_r = \sum_{\substack{x=sn+ \\ x \in r}}^{dn=1} SN(w)_x \quad (11)$$

4.2.2 Fitness function

The quality of solution is determined by the estimated fitness function value in evolutionary method. Fitness function values in the SRABDE determine the quality of created chromosomes (routes) formed by interpreting physical changes. The fitness function's component measures are trust, residual power, and node stability. These indicators support the route's viability in terms of reliability and security. As a result, equation (12) can be used to express the defined function:

$$f_r = T_r' + \frac{1}{RBL_r} + 1/SN_r(w) \quad (12)$$

Where the components T_r',RBL_r , and$SN_r(w)$are combined in the fitness function to create the best-fit route for secure transmission, as stated in equation (12). Because the fitness function is minimized in order to discover the best-fit solutions (routes), the estimated trust factor is further adjusted in terms of the not-to-trust factor in order to meet the criterion. There's a chance that in a low-battery-power and low-trust circumstance, a trusted route with promising packet delivery services won't build any route. Then, if another path is accessible, proposed **SRABDE** discovers it by taking care of every situation using fitness functions. To find the secure path, the algorithm iterates; in stage 4, it

randomly selects the chromosomal vector, which is then subjected to mutation techniques as mentioned in step 7 of the proposed algorithm SRABDE.

4.3.Secure Routing Algorithm Based on Differential Evolution (SRABDE)

SRABDE is a secure and dependable data delivery mechanism based on meta-heuristics. Three metrics have been mapped by the fitness function to obtain required solution. The trust system has evolved to forecast if a node is malevolent or not, whereas node stability ensures longer-lasting routes. Algorithm 1 contains the SRABDE pseudo code.

4.3.1 Discussion on SRABDE

- **Initialization:**The value of the scaling factor 'F' and the crossover parameter 'CR' are set to 1 and 0.8, respectively, in step 1. The nodes in the network are initialized as a population of the SRABDE algorithm (step 2) and proceed to chromosomal encoding in order to acquire better results on these control parameter values during the simulation (step 3). Fitness function in equation 4 is used to initialize all feasible 'k' solutions (step 4) in (12). These solutions are also subjected to mutation and crossover.
- **Mutation:**$P_g = [x_{(1),g}, x_{(2),g}, x_{(3),g}, \dots\dots\dots\dots x_{(D),g}]$ is the population of the basic DE method. where $x_{(i),g}(i = 1,2, \dots . n)$ is an n-dimensional vector and g is the next generation. Mutation is the biological term for a rapid change in genetic material. The next stage in the DE method is to produce a donor vector$\vec{m}_{i,g}$for each target vector $\vec{x}_{a,g}$ from the current population after initialization. The most common mutation strategy: 'DE/rand/1' has been employed in the suggested algorithm SRABDE, as specified in the equation (13).

$$\vec{d}_{i,g} = \vec{x}_{ra,g} + F * (\vec{x}_{rb,g} - \vec{x}_{rc,g}) \quad (13)$$

ra, rb and rcare three unique values randomly selected (step 4) from [1... Pg], (that is 'k' solutions). These solution vectors are subjected to a mutation approach (step 7) in order to investigate all possible paths between source and destination.

- **Crossover and selection:**To increase potential diversity of the trial vector, a crossover operation is conducted on the created donor vector $\vec{d}_{i,g}$ by exchanging components with associated target vector (in step 10). The created trial vector is chosen for the next generation if its fitness function value is less than or equal to the target vector value; otherwise, the target vector is kept in the current population. Nodes are taken into account to investigate all available partial routes with identical crossing points, which also provide more optimality to the associated route creation. It will perform binomial crossover to assess all routes and identify the most secure one, taking into account the trust factor, node stability, and residual battery power (in step 8). The process of creating a secure route might lead to the creation of infeasible routes or loops inside the route. To circumvent this, node stability is used to validate authenticity of each route. New routes and partial pathways are discovered with each iteration mutation and crossover. Any shortfalls in newly identified new routes are addressed if possible, or abandoned if infeasibility is discovered. Furthermore, the selection technique (step 10) selects the optimum path by comparing the trial vector $u_{i,j,g}$ with a target vector.

Steps Algorithm 1: Proposed SRABDE Algorithm

1. Set the scaling and crossover parameters to their default values.

F = 1, CR = 0.8, trust > threshold

2. Pop_size = no of nodes*D
3. Proceed route (chromosome) encoding.
4. Randomly generate 'k' solution vectors for each individual based on the fitness function.
5. For I =1 to Pop_size
6. At random, choose three solution vectors.
7. Using equation (13), apply mutation to construct a donor vector to uncover all viable alternative paths.
8. To explore available partial routes, use crossover to produce all trial vectors

$$u_{i,j,g} = \begin{cases} d_{i,j,g} if rand(0,1) \leq CR or j = j_{rand} \\ x_{i,j,g} \qquad otherwise \end{cases}$$

9. Validate the trial vector$u_{i,j,g}$.
10. Select the best candidate route for data transfer via selection.

$$\mu_{i,g+1} = \begin{cases} u_{i,j,g} iff(\vec{u}_{i,g}) \leq (x_i, g) \\ x_{i,g}, \qquad otherwise \end{cases}$$

11. End for
12. If necessary, make changes in accordance with the fitness solution.
13. i = i+1
14. Transmit the data

Journal of Theoretical and Applied Information Technology
30th November 2022. Vol.100. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. EXPERIMENTAL RESULTS

5.1 Parameter Analysis and Result and Discussion

All simulations are executed on NS2 simulations on Microsoft Windows 7 machine with configuration CORE i5, 4 GB RAM and 2.2 GHz processor.The proposed SRABDE based trust model is compared with other algorithms like **IFRD, TPACO and DE_AOMDV.** Table-1 characterizes the simulation parameters as shown. The results of existing and the proposed scheme are compared using the QoS parameters, including data **packet delivery percentage**, **average end-to-end delay**, **routing overhead,energy consumption**, **accuracy**, and **throughput**by respect to the number of nodes. Initially, each node inMANET is considered with the trust value of 0.5. The simulation has been carried with different node densities as of 50, 100, 150 and 500 nodes. Here, the total number of mobile nodes in the network is considered to be the population of trusted model. The numbers of malicious nodes tested are 2, 4, 6, 8, and 10 up to 20 in multiples of 2 increasing by 2 for 10 different topologies.

Table 1: Simulation Parameters

Parameter	Values
Simulation Time	100s
Area Size	100m^2
Pause time	10s
Traffic Type	Constant Bit Rate
Transmission Radius	250m
Mobility Model	Random Way point
Packet Size	512 bytes
Connection Rate	4 packets/sec
Amplification Factor(F)	1
Cross Over Rate(Cr)	0.8
Trust Thershold(ΔT)	ΔT>0.5
No.of iterations(NP)	20

A. Packet Delivery Ratio (PDR)

The total number of successfully delivered data packets to the destination node is represented by the Packet Delivery Ratio. **Figure 1** depicts the packet delivery analysis ratio as a function of the number of malicious nodes. When there is no malicious node, the packet delivery ratio loss is 5%, however when the malicious node number increases, the packet delivery ratio loss increases dramatically to 30%.

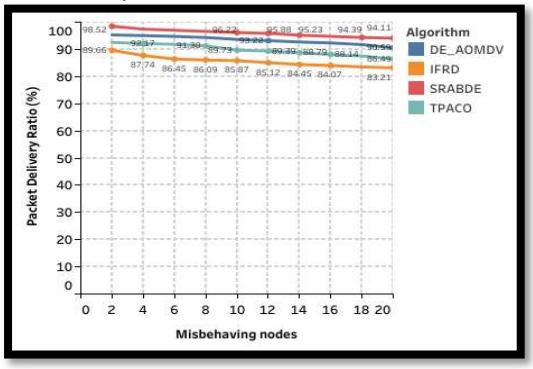

Figure 1: Packet Delivery Ratio vs. the Number of Malicious Node

Figure 1 show how the proposed trusted sensing model degrades over time when compared to other strategies. Protocols like TPACO, IFRD and DE AOMDV degrade quickly, and the proposed Algorithm follows suit. The key benefit of the proposed technique is that it has a higher distrust factor, which causes the algorithm to find a secure path by preventing harmful nodes from acting as good ones. Because of the participation of low trustworthy nodes, when the malicious node reaches 20, the drop will still be 15%. **As a result, the proposed approach achieves a packet delivery ratio of 98 to 94 percent,** which aids in the detection of black hole and grey hole attacks.

B. Energy Consumption

In Figure 2 represents Energy Consumption analysis of SRABDE method with various techniques. The numbers of nodes are in the range of 50 to 500. The Proposed SRABDE method gives better energy consumption performance than other existing routing methods. The proposed **SRABDE consumes lower energy (0.63 Mega Joules) in 100 nodes**. When it comes to 100 nodes, other techniques obtained an energy consumption value of 0.71mJ (**IFRD**), 1.18mJ (**DE_AOMDV**), and 1.47 **(TPACO).** The value of energy consumption is increasing as the no of mobile nodes grows.

Journal of Theoretical and Applied Information Technology
30th November 2022. Vol.100. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

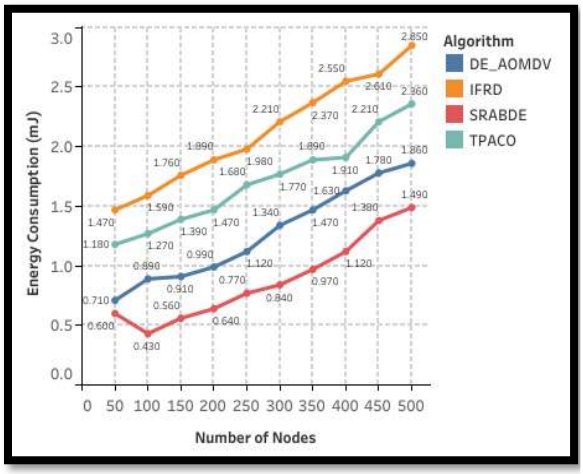

Figure 2: Performance Analysis of Energy Consumption

C. End-to-End Delay

When the no of wireless mobile nodes in network grows, the end-to-end delay grows as well. A larger no of nodes increase the likelihood of data congestion, which lengthens the queuing time. Furthermore, because the network wireless channel is more congested, a mobile node in network must wait longer to access the medium, lengthening the mobile data transmission period. As a result, selecting a route with highest energy level can help to maintain load balancing across nodes. The proposed SRABDE is a multipath routing technology that uses residual energy to optimize routes. As a result, when nodes fail, different routes and nodes are employed. In all of these circumstances, **the SRABDE mechanism will skip the route finding procedure, resulting in a low end-to-end latency,** as shown in Figure 3.

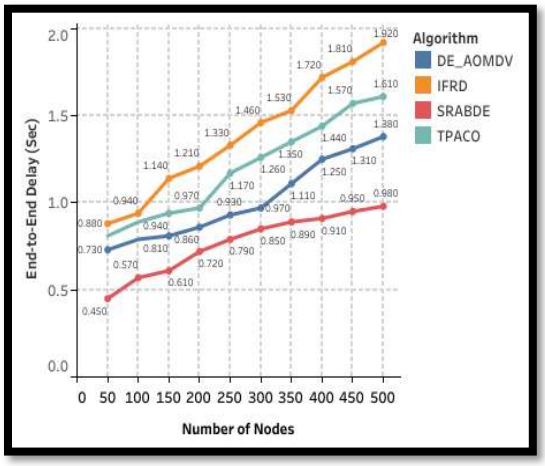

Figure 3: End-to-End Delay

D. Throughput

Throughput indicates the measure of total size of correct received packets by the destination for each second called as throughput. In the analysis of throughput here with the number of malicious nodes for IFRD, TPACO, DE_AOMDV and SRABDE shown in Figure 4. **The Figure 4** describes the relationship between throughput with the number of malicious nodes for IFRD, TPACO, DE_AOMDV and SRABDE methods. With the increase of malicious nodes, the effective separation of malicious behavior from the faulty behavior by the **SRABDE algorithm provided the high throughput compared to IFRD, TPACO and DE_AOMDV.**

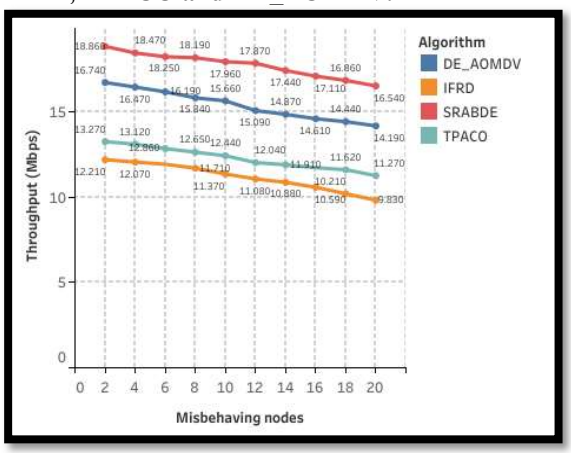

Figure 4: Throughput vs. Malicious Nodes

E. Overhead

Routing Overhead is any grouping of excess or incidental computation time, memory, bandwidth, or other resources that are essential to accomplishing a specific task. By way of nodes number rises, the overhead also rises. **In Figure 5** represents the comparison of energy used up by a wireless network of SRABDE with IFRD, TPACO, and DE_AOMDV. **The proposed technique allows a lower overhead than the existing method,** because it selects only the nodes having secure good link quality so that no of route failures is decreased.

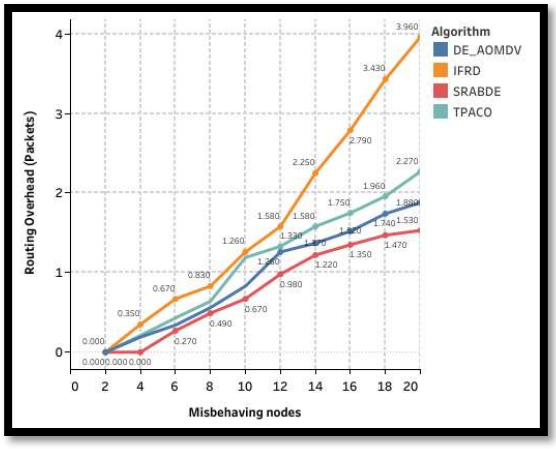

Figure 5: Routing Overhead

F. Detection Accuracy

In Figure 6, detection accuracy rate of **proposed SRABDE** system with respect to trust level is shown.

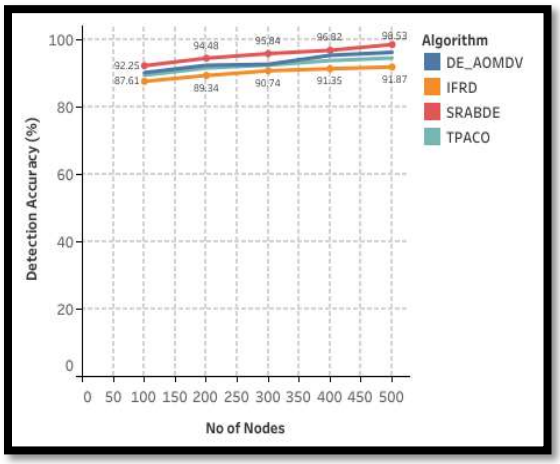

Figure 6: Detection Accuracy

From the results, it is observed that system with trust shows detection accuracy rate between **92% and 98.5%** where as for the system without trust detection accuracy rate ranges from **88% to 92.5%.** Thus it's clearly proven from the figure 6 system with SRABDE; our proposed trust estimation algorithm **detects the malicious node better** when compared to system without trust. The reason is that in our SRABDE algorithm the trust level of the nodes are estimated by using both the **behaviour analysis** and **REL (Reliability, Energy of node, and link stability)**.

6. CONCLUSION

Most of the time, ad-hoc mobile networks with no infrastructure and self-configuration are vulnerable (weak) to numerous forms of attacks. SRABDE places a greater emphasis on data distribution via the most trusted and reliable route as determined by the fitness function. ***The trust factor, remaining battery power, and node stability are the building components of the designed fitness function for picking a good path.*** According to the experimental data, the **SRABDE** performance measures outperform the **IFRD, TPACO and DE_AOMDV.** Average end-to-end delay in presence of malicious nodes does not affect the desired performance of the **SRABDE** algorithm, as it follows the strategy to ignore the routes having malicious node. From empirical results, **SRABDE** is considered to be more efficient than **IFRD, TPACO and DE_AOMDV**. **The advantage of SRABDE** is that its performance is unaffected by the number of nodes in a network growing larger, whereas DE_AOMDV, TPACO has a low impact and IFRD has a higher impact. The SRABDE algorithm outperforms the other three methods IFRD, TPACO and DE_AOMDV in terms of overall network performance.

REFERENCES

[1]. Hu, Y-C., Johnson, D. and Perrig, A. (2002) 'SEAD: secure efficient distance vector routing inmobile wireless ad hoc networks,' *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications*, pp.3–13.

[2]. Dahill, B., Levine, B.N., Royer, E. and Shields, C. (2002) *ARAN: A Secure Routing Protocol forAd hoc Network*, UMass tech Report 02-32.

[3]. Papadimitratos, P. and Haas, Z. (2002) 'Secure routing for mobile ad hoc network,' *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'02)*, San Antonio, TX.

[4]. Wu, B., Chen, J., Wu, J. and Cardei, M. (2007) 'A survey of attacks and countermeasures in mobile ad hoc networks', in Xiao Y., Shen X.S. and Du DZ. (eds): *Wireless Network Security. Signals and Communication Technology*, Springer, Boston, M.A.

[5]. Fernandes, N.C., Moreira, M.D.D. and Duarte, O.C.M.B. (2013) 'Safeguarding ad hoc networks with a self-organized membership control system,' *Computer Networks*, Vol. 57, pp.2656–2674.

[6]. Nadeem, A. and Howarth, MP. (2013) 'A survey of MANET intrusion detection and prevention approaches for network layer attacks', *IEEE communications Surveys and Tutorials*, Vol. 15, No. 7, pp.2027–2045.

[7]. Liang, X. and Xiao, Y. (2013) 'Game theory for network security, *IEEE Communication Surveys and Tutorials*', Vol. 15, No. 1, pp.472–486.

[8]. Govindan, K. and Mohapatra, P. (2012) 'Trust computations and trust dynamics in mobile ad-hoc networks', *IEEE Communications Surveys and Tutorials*, Vol. 14, No. 2, pp.279–298.

[9]. Reina, D.G., Ruiz, R., Ciobanu, R., Toral, S.L., Dorronsoro, B. and Dobre, C. (2016) 'A survey on the application of evolutionary algorithms for mobile multihop ad hoc network optimization problems', *Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks*, Vol. 12, No. 2. Doi: 10.1155/2016/2082496.

[10]. Storn, R. and Price, K.V. (1995) *Differential evolution: a simple and efficient adaptive scheme for global optimization over continuous spaces*, Technical Report TR-95-012, ICSI, USA, [Online]. Available: http://icsi.berkeley.edu/storn/litera.html.

[11]. R. Storm, K. Price, "Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces", J Global Optim 1997, Vol. 11, Issue. 4, pp. 341–59, 1997.

[12]. K. Price, R. Storn, J. Lampinen, "Differential evolution – a practical approach to global optimization", Springer, Berlin, 2005.

[13]. S. Das, P.N. Suganthan, "Differential Evolution: A Survey of the State-of-Art" , In Evolutionary Computation, IEEE Transaction on, Vol. 15, Issue. 1, pp. 4-31, 2011.

[14]. Xia, H., Jia, Z., Li, X., Ju, L. and Edwin, HM. (2013) 'Trust prediction and trust-based sourcerouting in mobile ad hoc networks', *Ad Hoc Networks*, Vol. 11, No. 7, pp.2096–2114.

[15]. Wei, Z., Tang, H., Yu, F.R., Wang, M. and Mason P. (2014) 'Security enhancements for mobile adhoc networks with trust management using uncertain reasoning', *IEEE Transaction onVehicular Technology*, Vol. 63, No. 9, pp.4647–4658.