JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# NESTED GENETIC ALGORITHM AND FUZZY SECURED NODE SELECTION ROUTING PROTOCOL FOR MANET

**S.Venkatasubramanian**[1]

[1]Department of Computer Science and Engineering, Saranathan college of Engineering, Trichy, India

**Abstract:** Due to its way of installation and management, as well as aspects like Node level in energy, randomly moveable nature, and signal processing, the general behavior of MANETs differs at varying phases. This form of dynamicity leads to or necessitates over-concentration, as well as a higher level of security and routing stability. A novel technique is called Fuzzy Secured Node Selection Routing (FSNSR). It has been proposed to address these challenges and increase security. It offers the TNS and good productivity with energy consumption in terms of dynamicity and security. This method FSNSR delivers dynamicity and high reliability to nodes, allowing them to move often without compromising security and achieving greater efficiency instability. Transmission is a crucial aspect of the infrastructure of MANETs, is one of the key problems that these networks confront. This research provides a layered (GA) methodology that optimizes the transmitting ability of these networks using neural network fitness. Rather than treating programming optimization as an inter-problem with multiple model outputs that must be tuned, the suggested method takes a different approach which concentrates on just one evaluation metric or network strategy time. This is the time it takes for information to reach a particular % of the channel's connected customers. Various decision factors of the DFCN broadcasting system are tuned to maximize the time.

**Keywords:** Broadcasting, f-logic, FSNSR, MANET, routing algorithm, stability, energy consumption, security

## I. INTRODUCTION

Because of its adaptability, MANET has been prominent in recent decades for a variety of applications[1]. Because MANET has no established infrastructure, this capability makes mobile networks ideal for military use. To move information from one device to another, each node requests a neighbor node utilizing various network topologies like OLSR, AODV, and DSR. However, MANET is resistant to several assaults due to aspects like changeable topology, wireless communication, and resource limits.

Many IDS have been created for MANET to identify different kinds of cyberattacks. IDS plays a critical function in MANET to identify any form of assault. An IDS is a programming language that analyses wrongdoing and policy violations and then generates a report based on the findings. O outlier detection, Signature-based detection, and formulation detection are the three main types of IDS The biometrics detection compares the signatures of existing forms to the indications of network trends. if any existing offensive model matches the network design, the network is hacked. Fuzzy logic is divided into three categories: learning-based, statistical, and knowledge-based. Anomaly detection takes into account regular network behaviour while also identifying anomalous behaviour and issuing an alert as a result.

With the rise in popularity of wireless units, MANET has gotten a lot of interest in recent years as a way to provide connections between these nodes without the need for a permanent architecture or unified management. Each unit in this network serves as both a router and a host, passing packets from other networks to targets outside of its direct communication range. Nodes can choose the next unit and forward data depending on a network algorithm. AODV, DSR, DSDV, and TORA [2] have all been reported to the Internet Research Task Force group focusing on various hypotheses. When creating paths, almost all of these protocols use the quickest route as the primary measure. This methodology has several network consequences.

Among these impacts, traffic absorption was a small number of nodes, which results in a huge level of energy usage by those nodes. Because most terminals in MANET are powered by batteries that cannot be regenerated in most situations, energy is an important resource. Energy-efficient routing methods must be designed to keep the system operational for as long as needed. This paper proposes an improvement to the AODV protocol by introducing an f-logic program that utilizes as inputs 3 main metrics which

have a significant impact on route security namely the average power of the route, network congestion, and the difference between the two network entities to select more stable routes.

Conventional wireless network designs are primarily concerned with user-friendliness and achieving greater coverage distances to provide better assistance to their customers, but they lack privacy and reliability. Because the threat possibilities are great and stability is poor, those phases of network architecture are considered critical, and the networks cannot assure for vulnerabilities like hostile interventions, network congestion, route modifications with adaptability management, and so on. Many researchers are still developing techniques to prevent intrusions and protect the network from threats like invasions and cyberattacks by enabling network operations, authorization and authentication principles, access-algorithm Strategies, and decryption-and-encryption logics.

All of these tactics were developed to reduce cyberattacks while also providing excellent service for network users and their source text. However, the existing network is insufficient to support security rules via MANET due to their inaccuracy, slowness, and lack of privacy, which can offer protection to the existing network scenario to avoid hackers and offenders. As a result, a protocol specification is required to assist MANET in establishing integrity communication and providing the best assistance to its customers in working in an intruder-free network environment, with the plausible protocol focusing on energy consumption over mobility and rechargeable batteries maintenance. Trust-Manipulation and Trust-Establishment are the most important problems.[3] The typical network scenario considers the navigation process in the following manner: network formation, parent module starts interaction with next neighbor, and it continues till the receiver or destination port is achieved; however if any neighbor produces a problem in the middle, the parental node forwards the data packet to another possible path to achieve the destination. If the measuring proportion is one, it is trustworthy; otherwise, if the measuring proportion is zero, it is not trustworthy.

The lack of a communication system is the most prominent aspect of MANETs. Routing configuration finding and data dissemination are two examples of sensor networks that none of the networks are to support separately or specifically. NF, CA, database, and other facilities management are examples of tasks that cannot depend on the main service but are nevertheless appropriate to this research. The design of a routing algorithm for MANET is influenced by several considerations, including mobility, limited resources, speed, disguised and visible endpoint issues, and so on. As a result, the routing algorithm is designed to be fully decentralized, flexible, regular, robust, loop-free, and with the fewest possible errors.

## II. LITERATURE SURVEY

The goal of recent MANET research is to prevent and detect a network security threat. For AODV, [4]developed a methodology for detecting black holes. [5]presented an f-based GA that uses beginning rules from an f-algorithm and final principles from a GA. [6] suggested a genetic-based IDS for IP/TCP networks. [7] investigated RREQ flooding threats and devised a new strategy focused on following node monitoring to counter RREQ flooding threats

In DSR, [8]tested how an attacker could utilize a rushing assault in the network and built a novel way for preventing rushing attacks for MANET. Even though many analysts were attempting to protect the system from the threat, other experts were recommended to take a broader approach. [9] suggested a synthetic immune response for IDS, that is focused on a methodological structure influenced by the human defense response. Ariadne has proposed a technique for E-E delivery based on shared keys using a similar methodology. To protect the network from assault, more effort is required. The mechanism provided in the above approach is to use routing to safeguard the network from other attackers.

[10]. Power issues are regarded as the most serious hazard to sensor networks. This research focuses entirely on the power problem in mobile ad hoc networks, which is regarded as a critical issue in this area and generates considerable anxiety over battery levels, making node failure a possibility. Many geometrical techniques are being examined to mitigate these problems, with the major focus falling on the GEAND and MR approach being used to remove the process of packet loss owing to power concerns.

In this study [11], a new congestion-reduction model with a scheduling method is developed, to greatly reduce power-related concerns. The following are the main benefits indicated in this paper: increased network lifespan, reduced transmission time, and energy efficiency The problem of this work is that it performs poorly at the operational level and is difficult to work because of the modeling aspect.

Many changes to these techniques have been suggested to address these issues. The authors of [12]suggest a back propagation algorithm as an adaptive analytical methodology for calculating a node's trust factor depend on its residual level of energy and velocity. Introduce an effective routing method by choosing the most reliable nodes to create a stable path. To reduce the likelihood of route failures throughout the data relay phase. If the RREQ signal has not been intercepted previously, the transitional node starts a timeout to wait for another RREQ from the node with the greatest trust model. However, this method results in a longer latency.

On the other hand, the authors of [13] suggest the same approach. Only the target node, however, uses the f-logic method to choose the optimum route. In addition, based on f logic and deep learning, the authors of [1] develop a modified fuzzy power state-based AODV routing algorithm for MANETs . Each node employs a Mamdani FLS in the route discovery process of this protocol, using the remaining battery capacity and power drain speed of the mobile node as inputs to determine its RREQs forwarding possibility.[14] reduces a route's entire power usage for transmission. It's the dispersed Bellman-Ford method with communication protocol, but instead of the number of hops. The cost is the overall power usage. MINPOW has a significant drawback in that it determines the path only based on the connection cost. Taking into account both the link and node costs is a superior method.

The authors suggested a low-energy clustering method relying on the DS marking technique [15]. The system is managed as a graph G = (V, E), with V representing the edges and E representing the connections. The DS is a group D of G edges in which every G edge is in D or next to a node in D. Gateways are nodes in the DS, and other network nodes link the portals to form clusters. The DS nodes must be interconnected for messages to be routed between groups. [1] devised a simple different algorithm that identifies a unit as a portal if two of its neighbors are not directly connected. To transmit traffic from a destination node, the source node sends it to its portal and delivers it to the intermediate nodes.

## III. PROPOSED SYSTEM

Nested GA with f-based fitness is the proposed methodology. The goal is to detect particular trends for each of the distinct scenarios while optimizing the DFCN decision methods based on the reachability duration. The reachability duration for 15% of the networks is used as a metric, which is the time needed for 15% of the devices in the system to effectively transmit their communications. The DFCN variables and the simulators to be measured output are contained in the outer genetic algorithm. [16] Each cell symbolizes the complete f-set, and the inference result denotes the inner efficiency, and the inner GA develops norms for the fuzzy logic. The outer GA's fitness value is determined by the final inner objective function measured once the integration is achieved. The suggested system was created in C using Microsoft Visual Studio 2017 on a 64-bit Windows 10 machine with 8GB of RAM and an Intel Core i5-6500 processor. To do this, the built application executes the NS2 simulator as a command-line program running inside a virtual sandbox system, with all conventional subsystems diverted to the application [17]. The system is depicted in Figure 1.

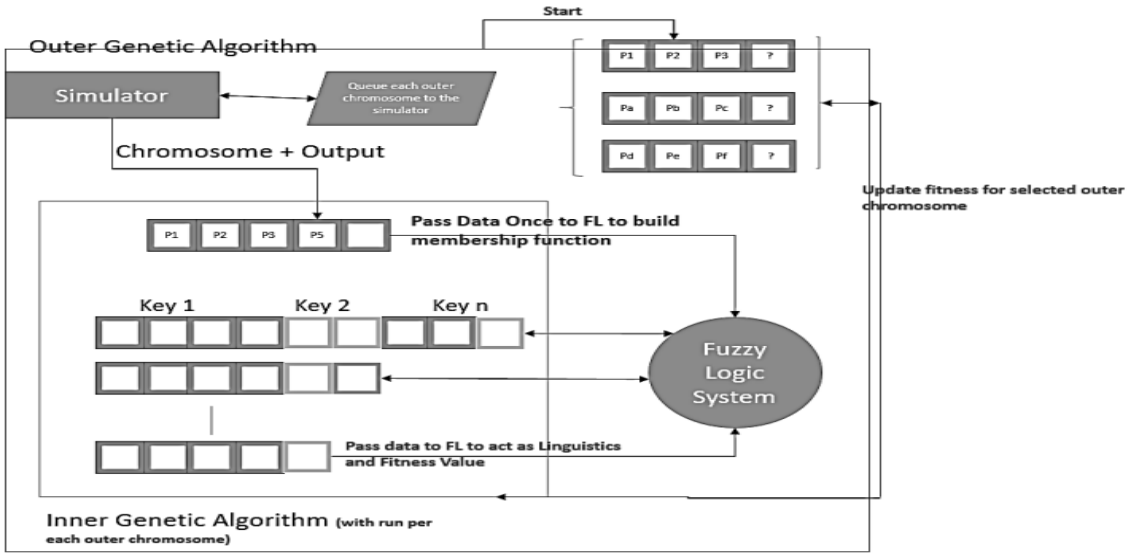



Figure 1. Proposed System

The Run Outer GA method is the program's starting point. The InnerPopulation function populates the beginning crowd with arbitrary f-logic keys that match the language phrases. The external chromosome transmitted from the outer GA to the internal generation which was the chromosome factor. The permitted range of keys per cell is represented by the keyMax and keyMin variables. The f-logic system is initialized and f-sets are formed by external chromosome elements at line 5, languages are constructed by using internal chromosome Pi[j] at line 9, and viability is determined using the observation result for the generated f-logic at line 10.

### 3.1 F-Logic method

The inner GA's fitness is calculated using a fuzzy approach. The inner GA chromosomes will function as a whole fuzzy set. Each DFCN variable will function as a fuzzy term, with the values HIGH, LOW, and MED. Every factor has a triangle linear model which is equally distributed over the testing parameters of the values it depicts. The inner GA is used to produce and optimize the constraints for the fuzzy set. To calculate fitness probabilities, we should first estimate each chromosome's fitness. To avoid a divide-by-zero error, F obj's value is multiplied by 1.

Fitness[1] = 1 / (1+F_obj[1]) = 1 / 94 = 0.0106
Fitness[2] = 1 / (1+F_obj[2]) = 1 / 81 = 0.0123
Fitness[3] = 1 / (1+F_obj[3]) = 1 / 84 = 0.0119
Fitness[4] = 1 / (1+F_obj[4]) = 1 / 47 = 0.0213
Fitness[5] = 1 / (1+F_obj[5]) = 1 / 95 = 0.0105
Fitness[6] = 1 / (1+F_obj[6]) = 1 / 56 = 0.0179
Total = 0.0106 + 0.0123 + 0.0119 + 0.0213 + 0.0105 + 0.0179 = 0.0845

The values of the arrays RS, R1, R2, R3, and R4 are used to do fuzzy estimating. The vectors statistics are determined depending on the sensitivity values T1 and T. Examine the array RS, whose value is indicated by RS value, which is derived by using network number and associated member task value. The complex exponential method is used to estimate the value of the derived class.

Membership value = (x-a)/ (b-a)

Two fuzzy values x and y, we define the following operations:
(x and y) = min(x,y)
(x or y) =max(x,y) (1)

not x =1 – x(x implies y) = max(x,1 –y) (2)

Where x represents the threshold value, a represents the no. of packets forwarded, and b represents the no. the number of packets deleted. Based on the preceding value, R0 and RC are predicted.

$$R0 = \begin{pmatrix} 1 & 0.5 & 0.5 \\ 0.5 & 1 & 0.5 \\ 0.5 & 0.5 & 1 \end{pmatrix} \quad R1 = \begin{pmatrix} 1 & 0.5 & 0.5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

If R[1] is bigger than C[1] but smaller than C[2], In the new population, chromosome[2] will be chosen as a chromosome for the following generation if NewChromosome is NC:

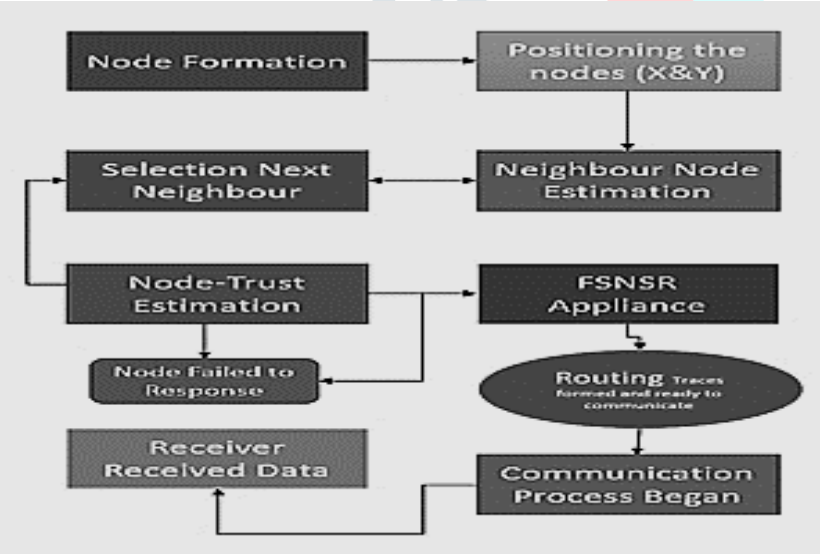
NC[1] = Chromosome[2]
NC[2] = Chromosome[3]
NC[3] = Chromosome[1]
NC[4] = Chromosome[6]
NC[5] = Chromosome[3]
NC[6] = Chromosome[4]

The RS value is generated and modified in the table based on the attribute values. The remaining values of R1, R2, R3, and R4 are computed and modified in the table depending on this RS value.

i. Indicator of occurrence R1 = RS*R0
ii. Indication of conformabilityR2 = RS * RC,
iii. Indications of non-occurrence R3 = RS * (1-R0),
iv. Indications that are not symptomatic R4 = (1-RS) * R0

### 3.2 FSNSR

The major purpose of this suggested system is to solve the issue that has plagued previous systems and increase network quality by improving routing methods in a MANET system Finding intruders in the environment and removing them from the networking scenario when information is being sent between sites. The overall control approach ensures node longevity and, as a result, enhances connection speeds and network durability indirectly. The proposed technique FSNSR [18]ensures network longevity, energy consumption, privacy, and other benefits. F-logic, which functions as a questionnaire and answerer, generally enhances the output in all scenarios more than other techniques. By generating the Route-Request and awaiting the result from the appropriate network the fuzzy works as a questioner and enquires about the next neighbor node and its properties during connectivity. As a result, the proposed method ensures that network reliability and scalability issues induced by cyber attackers are not compromised in the MANET environment [5].




### 3.3 Outer GA

The outer GA's chromosomal architecture has a mix of floating-point and numeric values which correlate to the DFCN variables, as well as an input parameter that relates to the reachability duration estimated with the Madhoc model. The outer GA has a set length of 6 genes on its chromosome. The chromosomal structure is depicted in Figure 3. The crossover is a commonly affected operator which takes gene position into account to ensure that the switched parameters are still acceptable and fall within the prescribed limits. A non-uniform activator is employed to accomplish the modification, that can be utilized to restrict the bottom and higher limits for the genes - this is important to avoid out-of-boundaries variables - as well as to keep the population from deteriorating during the early phases of development. The outer population has a set size of 100 chromosomes and can last up to 250 generations. The mutation and crossover probability have been set at 40% and 20%, correspondingly.

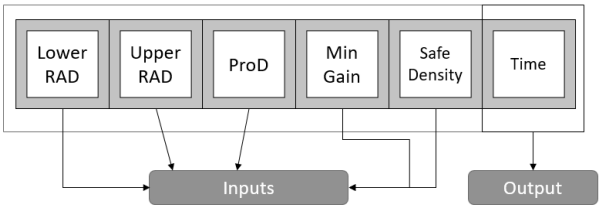



Figure 3. Structure of the Outer Chromosome .

Table 1. Numerical to Linguistic Sequence Transformation

| Value | 2 | 3 | 1 | -3 | -2 | -1 | 0 |
|---|---|---|---|---|---|---|---|
| Equivalent Linguistic | MED | HIGH | LOW | NOT HIGH | NOT MED | NOT LOW | NOT APPLICABLE |

A typical Roulette-Wheel controller is used to make the decision. It's worth mentioning that the final gene is left out of the evolutionary process and is instead preserved within the chromosome before being handed on to the f-system afterward. Inside the criterion, all of the other factors in the development are produced at random.

### 3.4. Inner GA:

The operators used by the inner GA are the same as those used by the outer GA. The chromosome architecture is distinct. It has a varied no. of genes, varying from four to eighteen. As previously shown, each gene is a key that encodes a verbal sequence into data variables. [19] It was necessary to do so to use the genetic algorithm to update the norms. Each key is six characters long, which denotes the number of output and input parameters. The inner GA's membership is limited to 60 people, with a maximum of 150 years. Figure 4 shows a sample inner GA with a population density of seven and random chromosomal sizes, denoted by Sn, where n is the population's chromosome quantity. It also demonstrates how the key is converted into a linguistic expression. For each outer chromosome, the inner GA completes a 60-generation run. The goal is to broaden the languages of f- logic to achieve the best feasible result.

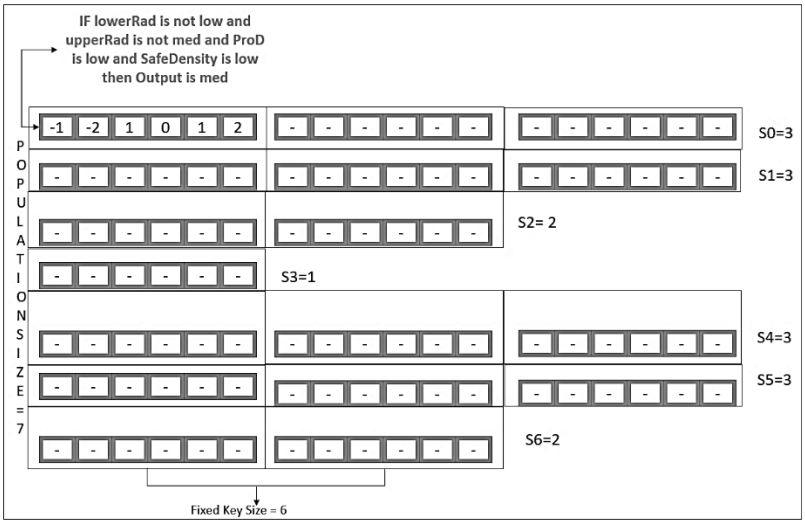



Figure 4. Example for Inner GA

## VI. RESULTS AND DISCUSSION

The trials are repeated five times, with the averaged results. The result and selection parameters have converged, as seen in the statistics. To offer a statistical equation for the choice [20] parameters, the exponential regression line is also computed. The findings for the highway transportation environment are shown in Figure 5. The output regression line for each selection parameter and the comparable exponential regression formulas, are shown in Tab. 2.

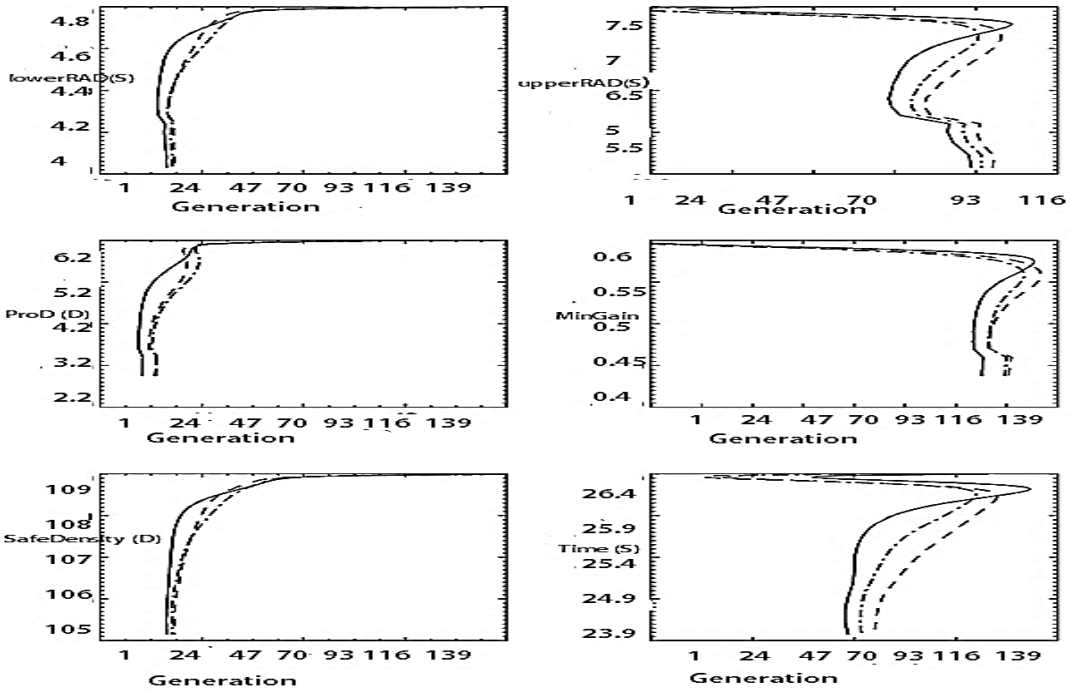



Figure 5. Unification of highway mobility design.

Table. 2. Trend - line Requirements in highway

| Parameter | Expression | Trendline |
|---|---|---|
| SafeDensity | -2.515 * In(G) + 0.6734 | ↓ |
| ProD | 4.2343 * In(G) + 32.876 | ↑ |
| UpperRAD | -0.9876 * In(G) + 3.6762 | ↓ |
| LowerRAD | -0.2453 * In(G) + 7.8953 | ↓ |
| MinGain | -0.0456 * In(G) + 0.6372 | ↓ |

The findings for the Mall mobility model are shown in Fig. 6, and the regression line for the decision variables is shown in Table VII. Figure 7 depicts the findings of the individual model of mobility, while Table 3 lists the associated major horizontal parameters.

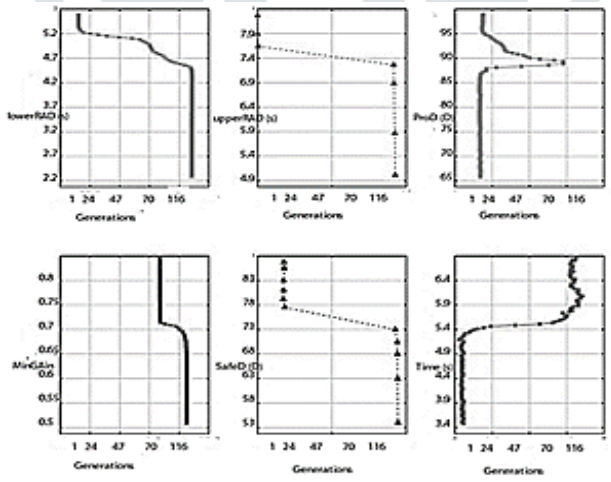


Figure. 6. Mall Transportation Model's Convergence

Table. 3. Mall Scenario Trend-line Metrics

| **Parameter** | **Expression** | **Trendline** |
|---|---|---|
| SafeDensity | -3.5615 * In(G) + 3.234 | ↓ |
| ProD | 4.4563 * In(G) + 23.123 | ↑ |
| UpperRAD | -0.8766 * In(G) + 3.3452 | ↓ |
| LowerRAD | -0.2343 * In(G) + 7.9873 | ↓ |
| MinGain | -0.1236 * In(G) + 0.1232 | ↓ |

**4.1 Model and Parameters for Simulation:**

To test our suggested protocol, we use NS2. The bandwidth ability of network devices is set to a similar value in our modelling: 2 Mbps. For wireless LANs, we employ IEEE 802.11's DCF)as the MAC layer algorithm. It can send a link breakdown notification to the core router. In the simulation, mobility nodes of sizes 30, 40, 65, and 99 moves for hundred seconds in an 899-meter x 899-meter rectangular area. We'll suppose that each unit moves at the same speed. The coverage area is 300 meters for all nodes. The speed restriction in the simulation was 6 m/s, while the maximum speed is 15 m/s. CBR communication is used in the simulation of CBR.Table 4 summarises the model parameters and settings.

Table. 4. Parameters for simulation

| | |
|---|---|
| Number of nodes | 30, 40, 65 and 90 |
| Size of area | 899 * 899 |
| Size of packet | 500 |
| Traffic source | CBR |
| Mobility design | Random |
| Velocity | 6metre per second to 19 m/s |
| Mac | 802.12 |
| Stop time | Five second |
| Simulation time | 80 second |

**4.2 Metrics of Performance**

The results of our FSNSR protocol with the AODV protocol**.**By adjusting the nodes as 25, 50, 75, and 100, we primarily analyse performance according to the following metrics.

**Average end-to-end delay:** From the sources to the destinations, the end-to-end latency is averaged over all surviving data packets.

**Average Packet Delivery Ratio:** The number of packets successfully received divided by the total number of packets transmitted is the ratio.

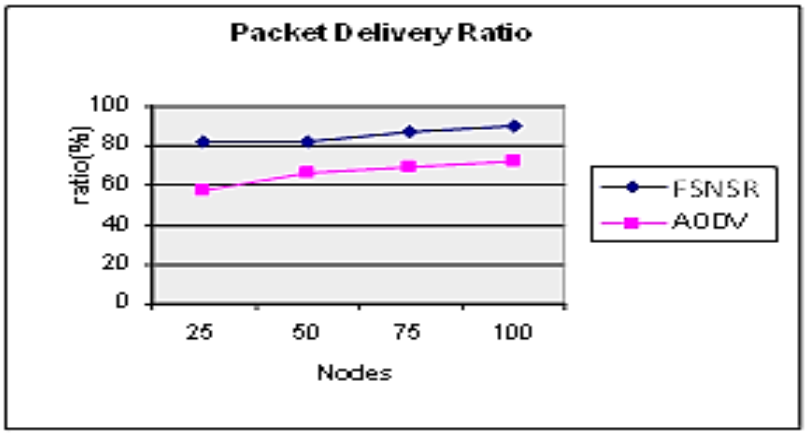



Figure.7. Nodes Vs Delivery Ratio

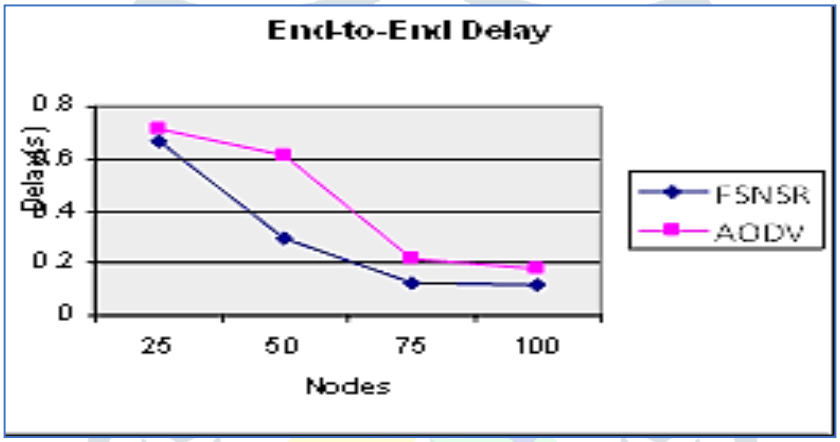



Figure. 8 Nodes Vs Delay

From the above figures 7 and 8, it is understood the proposed FSNSR protocol gives a better packet delivery and experience less end-to end delay compared to the AODV protocol.

## V. CONCLUSION

The problems in the current system can be readily remedied by using the provided solutions and a newly established method FSNSR, which rapidly identifies suspicious networks and protects the network from damaging threats as well as hackers or intruders. This FSNSR method optimizes network speed and lifetime while saving energy, allowing the destination and source to interact successfully without experiencing any network difficulties. The nodes are divided into two categories: untrusted and trusted. In the mobile network situation, trusted networks are permitted to connect further to complete the process, whereas untrusted networks are indicated as zero in modelling and are not authorized to interact further. The entire task is more complicated and mistake-free owing to the use of f-logic, and the output generated by this approach is effective and fault-tolerant. By optimizing the decision factors for the DFCN method, the suggested system was able to reduce the message transmission time for the 3 actual-life situations. The mall routing algorithm gained the most from the DFCN parameter estimation, which is mostly due to the unpredictability of mobility, as the human aodv protocol has very similar characteristics but varies only in movement purpose. The mobility of individuals in the human mobility pattern is guided by their intents to achieve a periodic list of targets, which reduces the randomness greatly. Furthermore, the highway routing algorithm had the longest average signal delivery time, which can be related to the absence of nodes and data transmission speed, as well as the fact that the DFCN protocol focuses on 1-hop neighbors to transport messages to their destinations.

## REFERENCES

[1] M. K. Rafsanjani and H. Fatemidokht, “FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs,” *AEU-International J. Electron. Commun.*, vol. 69, no. 11, pp. 1613–1621, 2015.

[2] D. Leiber and G. Reinhart, "A bi-level optimisation approach for assembly line design using a nested genetic algorithm," *Int. J. Prod. Res.*, pp. 1–16, 2020.

[3] L. L. Zhang, D. U. Gang, W. U. Jun, and M. A. Yujie, "Joint production planning, pricing and retailer selection with emission control based on Stackelberg game and nested genetic algorithm," *Expert Syst. Appl.*, vol. 161, p. 113733, 2020.

[4] B. Wu, T. Cheng, T. L. Yip, and Y. Wang, "Fuzzy logic based dynamic decision-making system for intelligent navigation strategy within inland traffic separation schemes," *Ocean Eng.*, vol. 197, p. 106909, 2020.

[5] C. Kang *et al.*, "A heuristic neural network structure relying on fuzzy logic for images scoring," *IEEE Trans. Fuzzy Syst.*, 2020.

[6] V. Rishiwal, S. K. Agarwal, and M. Yadav, "Performance of AODV protocol for H-MANETs," in *2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring)*, 2016, pp. 1–4.

[7] G. T. Reddy, M. P. K. Reddy, K. Lakshmanna, D. S. Rajput, R. Kaluri, and G. Srivastava, "Hybrid genetic algorithm and a fuzzy logic classifier for heart disease diagnosis," *Evol. Intell.*, vol. 13, no. 2, pp. 185–196, 2020.

[8] R. S. Krishnan *et al.*, "Fuzzy logic based smart irrigation system using internet of things," *J. Clean. Prod.*, vol. 252, p. 119902, 2020.

[9] M. H. Qais, H. M. Hasanien, and S. Alghuwainem, "Whale optimization algorithm-based Sugeno fuzzy logic controller for fault ride-through improvement of grid-connected variable speed wind generators," *Eng. Appl. Artif. Intell.*, vol. 87, p. 103328, 2020.

[10] S. Sayed, M. Nassef, A. Badr, and I. Farag, "A nested genetic algorithm for feature selection in high-dimensional cancer microarray datasets," *Expert Syst. Appl.*, vol. 121, pp. 233–243, 2019.

[11] A. H. Mohammed, M. M. Hamdi, S. A. Rashid, and A. M. Shantaf, "An optimum design of square microstrip patch antenna based on fuzzy logic rules," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1–7.

[12] K. Kumar and V. P. Singh, "Power consumption based simulation model for mobile ad-hoc network," *Wirel. Pers. Commun.*, vol. 77, no. 2, pp. 1437–1448, 2014.

[13] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, 2014.

[14] S. Chettibi and S. Chikhi, "Dynamic fuzzy logic and reinforcement learning for adaptive energy efficient routing in mobile ad-hoc networks," *Appl. Soft Comput.*, vol. 38, pp. 321–328, 2016.

[15] R. Logambigai and A. Kannan, "Fuzzy logic based unequal clustering for wireless sensor networks," *Wirel. Networks*, vol. 22, no. 3, pp. 945–957, 2016.

[16] A. Ghaffari, "Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms," *Wirel. Networks*, vol. 23, no. 3, pp. 703–714, 2017.

[17] C. Pu, S. Lim, J. Chae, and B. Jung, "Active detection in mitigating routing misbehavior for MANETs," *Wirel. Networks*, vol. 25, no. 4, pp. 1669–1683, 2019.

[18] W. Peng, C. Li, G. Zhang, and J. Yi, "Interval type-2 fuzzy logic based transmission power allocation strategy for lifetime maximization of WSNs," *Eng. Appl. Artif. Intell.*, vol. 87, p. 103269, 2020.

[19] Y. Al-Halabi, N. Raeq, and F. Abu-Dabaseh, "Study on access control approaches in the context of Internet of Things: A survey," in *2017 International Conference on Engineering and Technology (ICET)*, 2017, pp. 1–7.

[20] V. S. Janani and M. S. K. Manikandan, "Efficient trust management with Bayesian-evidence theorem to secure public key infrastructure-based mobile ad hoc networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 2018, no. 1, pp. 1–27, 2018.