International Journal on Emerging Technologies 10(3): 286-295(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Neuro Fuzzy Based Dynamic Secure Routing Protocol for QoS Frameworks of MANET

Santosh Sahu[1] and Sanjeev Sharma[2]
[1]*Research Scholar, School of Information Technology,*
Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal, (Madhya Pradesh), India.
[2]*School of Information Technology,*
Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal, (Madhya Pradesh), India.

(Corresponding author: Santosh Sahu)
(Received 16 July 2019, Revised 17 September 2019 Accepted 03 October 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: A QoS framework is a complete system that provide required QoS services to each node. All protocols of QoS framework work together to provide the quality of services. In MANET environment the provision of QoS guarantees is more challenging and difficult than wired network because of lack of centralized coordination, node mobility and a limited recourses. Routing protocols tend to be vulnerable to a number of threats and attacks like, attacks on information in transit, information disclosure, replay attack, flooding attack, and attacks against routing table. In the literature many researchers proposed routing protocols based on fuzzy logic and neural networks. But no one consider the security in routing protocols for QoS frameworks while Security is a critical aspect for QoS routing in the MANET environment. So it is necessary when designing routing protocols for QoS framework, the harmony between security and QoS must be present as one impacts the others. In this paper we proposed a routing algorithm "neuro fuzzy based dynamic secure routing (NFBDSR)", in which routing is performed by using Fuzzy Logic Controller (FLC) with neural network. The proposed routing protocol calculate route metric value using five crisp input variables, Residual Energy (RE), Processing Capability (PC) of node, Available Bandwidth (AB), Node Mobility (NM), and Node Trust Value (NTV). To calculate the node trust value we used Neighbor node Surveillance method. The real world applications of our algorithm is that it consider MANET environment applications such as multimedia, audio/video, images, animations, graphics, video conferencing, VOIP and webcasting need uninterrupted, rigorous and inflexible Quality of Service (QoS). The NFBDSR routing algorithm detects malicious node and prevents network from various types of threats and attacks. In result analysis we find out that NFBDSR routing protocol achieves better performance compared to FBRP routing protocol in metrics of throughput, PDR, end-to-end delay, and average jitter, link establishment time and hop count per route in both conditions when malicious node existing and not existing in the network.

Keywords: Quality of service (QoS), Cross layer QoS framework, Fuzzy Logic Controller (FLC) System, Fuzzy Inference System (FIS), NFBDSR, and MANET.

I. INTRODUCTION

Mobile nodes [1] connected by wireless links which can be created on-the-fly without any infrastructure or administrative support is called mobile ad hoc network (MANET). In MANET applications such as multimedia, audio/video, images, animations, graphics conferencing, VOIP and webcasting need uninterrupted, rigorous and inflexible Quality of Service (QoS). The provision of QoS guarantees in MANET is more challenging and difficult than wired network because of node mobility, lack of centralized coordination and a limited recourses. Quality of service (QoS) is the performance [2] level of a service offered by the network to the user. A framework for QoS is a complete system that attempts to provide required/assured services to each users or applications. The core component of any Cross layer QoS framework [3] is the QoS service model which describes the way user requirements are fulfil. The other components of the framework are, QoS signaling which is the combination of resource reservation, admission control and packet scheduling. QoS routing [10] is used to find all possible paths in the network.

The routing protocol in a MANET includes facilitating continuous communication between two mobile nodes during required period of time. The basic feature of routing protocol is selection of the most suitable forwarding node to proceed the real time packets from source to destination. The main objective of routing protocol is to, maximum utilization of available resources in such a way that the optimization of the network can be achieved. Considering that real time applications are one of the most challenging issue in MANET, due to transportation of high volume of data including audio, video, images, animation and graphics. A lot of researches have been accomplished and also ongoing so far to offer QoS guarantees by designing QoS models and protocols.

Karibasappa & Muralidhara (2011) [4] has proposed "Neuro fuzzy based routing protocol for mobile ad-hoc networks". They use two techniques of soft computing 1. Fuzzy Logic & Genetic Algorithms 2. Feed-Forward Artificial Neural Networks. The neural network will learn and upgrade itself over a period of time with usage. Author used crossover Neural Network capacities with the participation of Fuzzy Logic, working on sources of info and producing a lot of arrangements in the arrangement space with negligible looking through utilizing Genetic calculations.

Gupta *et al.*, [5], has proposed "Fuzzy logic based routing algorithm for mobile ad hoc networks". The basic test in developing a MANET is preparing each gadget to consistently protect the realities required to genuine course the traffic. The proposed routing calculation is completely founded on Fuzzy Logic which is having low discussion overhead and capacity

prerequisites. The proposed calculation takes three information factors: signal power, node versatility and postponement. The outright cost of every parameter can take a monstrous change at extraordinary factors on the network.

Chaythanya (2014) has proposed "Fuzzy logic based approach for dynamic routing in MANET". In this paper, another dynamic routing protocol is proposed dependent on portability, signal power, data transfer capacity and PFR, where the division of nodes will generously decrease the overhead and accelerate the routing procedure. A course positioning is given to the node estimating the basic leadership increasingly adaptive and naturist [6].

Mallapur & Patil (2014) has proposed "Fuzzy Logic Based Trusted Candidate Selection for Stable Multipath Routing". The creator shows a fluffy rationale stable spine based multipath routing protocol (FLSBMRP) for MANET. In this routing protocol, fluffy rationale method is utilized for competitor node choice. Parameters utilized for competitor node determination, leftover data transfer capacity, lingering power, connect quality, node portability and notoriety list. Between the source and the goal numerous ways are set up utilizing up-and-comer nodes, in the event that any applicant node in the way will in general come up short, at that point, a backup way to go through another up-and-comer node is set up before the course breaks [7].

Tabatabaei & Hosseini (2016) has proposed "A fuzzy logic-based fault tolerance new routing protocol in mobile ad hoc networks". The FBRP protocol utilizes the fluffy rationale technique to choose a steady course to improve framework execution. Two parameters intensity of battery and speed of mobile nodes are utilized in FBRP to compute the connection dependability of the possible way. To choose the suitable course fluffy rationale is utilized on each possible way [8].

Dhawan & Singh (2019) has proposed "Comprehensive Comparison and Analysis of Nature Inspired ACO based Routing Algorithms in Ad Hoc Networks". They compared and analysed six major algorithms to its depth from which one of the algorithms is proposed in our previous work i.e. Ant Colony Optimization Based Energy Efficient Routing Algorithm (ACO-EERA) which is based on the behaviour of ants from the real world. The proposed algorithm is a nature inspired optimization technique which optimizes certain factor for energy efficient routing in Ad Hoc Networks which are very much important for the network operation [14].

II. RESEARCH METHODOLOGY

In the literature many researchers proposed routing protocols dependent on fluffy rationale and neural networks. Be that as it may, nobody consider the security in routing protocols for QoS systems while Security is a genuine perspective for QoS routing in the MANET. Routing protocols will in general be helpless against various dangers and assaults like, data uncover, flooding assault, replay assault, assaults on data in movement and assaults against routing table.

So it is obligatory the amicability among security and QoS must be exist as one impacts the others when planning protocols for QoS system.

Empirical or experimental or hypothesis-testing research design is used in our research work. We used Informal experimental designs with Before-and-after with control design model is used. For research procedure both algorithms and pseudo code are used. The detail description of research component are given below

A. Proposed Neuro Fuzzy Based Dynamic Secure Routing protocol (NFBDSR)

NFBDSR is an expanded and secure version of Dynamic source Routing (DSR). In NFBDSR routing is performed by using Fuzzy Logic Controller (FLC) with neural network.The objective of proposed NFBDSR routing algorithm is to improve the routing quality by using FLC and increase the quality of route finding by using neural network. By using fuzzy logic control each node calculate the route metric value of node present in his routing table. The node which have route metric value higher than threshold value are selected to perform routing. The node which are selected for routing we called candidate nodes. In DSR routing protocol we perform two modifications one is the way of candidate node selection by using a fuzzy logic control and second is the finding optimal routing path using neural network. The candidate nodes are used to established path between the source and destination node using neural network. Every node in the network broadcasts a HELLO packet to its neighbors periodically. The format of HELLO packet which is used to select the candidate nodes. Each hello message comprises the sender's node id (Node ID), RE, PC, ABW, NM, and neighbor node addresses. Each node updates its routing table containing these values after receiving the Hello message. The layout of the HELLO packet is shown in Fig. 1.

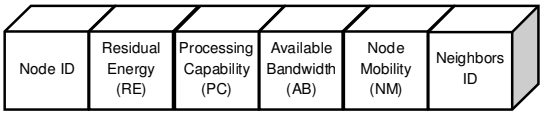

Fig. 1. Format of Hello packet.

1. Fuzzy Logic Control Based Trusted Node Selection. Proposed Architecture of Fuzzy Logic Control to calculation of Routing Metric (RM) is shown in Fig. 2. The parameters Residual Energy (RE), processing capability (PC), Available Bandwidth (ABW), Node Mobility of (NM), and Node Trust Value (NTV) are used to calculated RM value.

The detail description of metrics used for RM calculation is given below.

(a) **Residual Energy**

The Markov chains energy model [9] is used to calculate the nodes residual energy. The residual energy *Er* of a node at time t is computed as

$E_r = E_i - E(t)$

where E_i is the node *i* initial energy.

$E(t)$ is the $E(t) = ntx*\varepsilon + nrx*\delta$

Energy consumed by the node at time t

Where ntx and n_{rx} is the number of packets transmitted and received by the node at time t.

ε and δ are constants in the range (0, 1).

(b) **Processing Capability**

It is the number of instruction executed per second. Processing capability (PC) is the power of processing element which is measured in MHz or GHz.

(c) **Available Bandwidth**

When a node needs to transfer data, it has to be know the local bandwidth [10], interference and transmission range of the neighboring nodes.

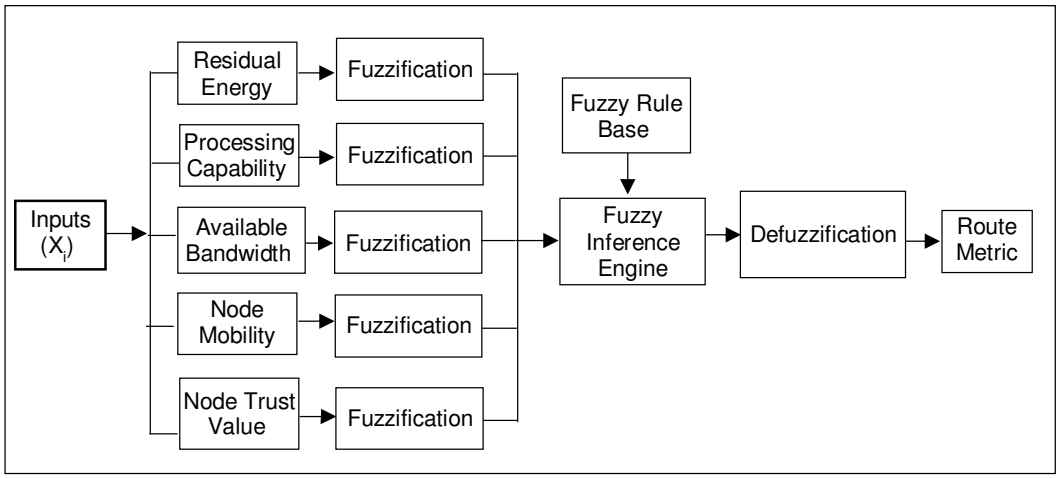

Fig. 2. Proposed Architecture of Fuzzy Logic Control to calculation of Routing Metric (RM).

The Available bandwidth (ABW) of a node is given by
$ABW = BW_L - BW_{min}$
where BWL is the local bandwidth given by
$BW_L = C_{CH} * (T_i / T_{in})$,
C_{CH} is the channel capacity,
BW_{min} is the minimum bandwidth of all of the nodes within the interference range.
T_i is the idle time during the predefined time period T_{in}.

(d) **Node Mobility**

Random Waypoint model [11] is utilized in our proposed strategy. The versatility of node I regarding node j is evaluated dependent on the proportion of the got sign quality (RSS) between two continuous parcel transmissions from a neighbor node, as given underneath.

$$M_i^j(i) = 10 \log \frac{RSS_{j \to i}^{new}}{RSS_{j \to i}^{old}}$$

Where RSS is given by $RSS = \beta * \partial * Ptx$
∂ is the channel gain,
β is a constant that depends on the wavelength and the antennas,
P_{tx} is the signal power of the transmitter.

(e) **Node Trust Value**

To calculate the node trust value [12] we used Neighbor node Surveillance method. When source nodes have packets to send then it store that packet in buffer and send it. After sending a packet source node waits for a fixed time of interval to overhear the neighbor node. When neighbor node forward that packet to next hope then source node compare the overheard packet to the buffered packet if packet is similar then source node assume that the corresponding node is the trusted node and increase the trust value by one of corresponding node in routing table. If source node don 't overhear the send packet within fixed time interval then source node assume that the corresponding node is black hole or wormhole node and broadcast a message in whole network that particular node is black hole node.

When broadcast message is received by other node they update own routing table and decrease the trust value one of corresponding node. And if neighbor node change or alter the field of data packets then source node found that packet comparison is dissimilar and assume that corresponding node is malicious or selfish node and broadcast a message that particular node is malicious or selfish. By using this method we prevent the network by different types of attacks like black hole attack, wormhole attack, Dropping Attacks etc.

As shown in Fig. 3 source node S send the packet to neighbour node A and wait for fixed time interval. Since node A is also the neighbour of node S so node S also listen the packet that are send or forwarded by node A. Now node S compare the buffered packet with overhearing packet if packet is similar then node S broadcast the message in whole network that node A is trusted node. If node A not forwards the packet then node S not overhear the particular packet within fixed time interval. Then node S broadcast the message that node A is black hole node or wormhole node. And if node A alter the packet then forward it then node S found that comparison is dissimilar and broadcast a message that Node A is malicious node or selfish node.

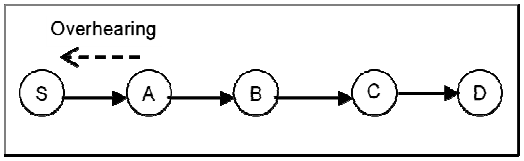

Fig. 3. Operation of Node Trust Value.

Following is the Pseudo code or Algorithm used to calculate the trust value

1. Initialize trust value by zero of each node.
2. Let initially source node transmit TRIAL_DATA packet before actual data transmission to the destination.
3. After finding the paths store the available path in path vector $P_1, P_2, P_3 \ldots\ldots p_n$ like
$P_1 = [N_1, N_2, N_3 \ldots\ldots N_i \ldots\ldots]$
$P_2 = [N_1, N_2, N_3 \ldots\ldots N_i \ldots\ldots]$
.
.
.
$P_n = [N_1, N_2, N_3 \ldots\ldots N_i \ldots\ldots]$
4. Let routing algorithm select p_i path vector as an efficient path to sending TRIAL_DATA packet.
5. Each intermediate node that receive TRIAL_DATA packet check condition

If path vector p_i node no. j is (j>2) then send two hop back TRIAL_ACK.

6. If node (j-2) receives TRIAL_ACK then check that
{

(i) TRIAL_ACK received by them is from path vector p_i 's node no j or not

(ii) If yes; then node (j-2) flood message that node j-1 is a trusted node or an authorized node.

(iii) All nodes that receive flood message increase the trust value by one in routing table at corresponding node.

}

Else

{

(i) Node (j-2) flood message that node j-1 is malicious node or unauthorized node

(ii) All nodes that receive flood message decrease the trust value by one in routing table at corresponding node.

}

7. If node (j-2) does not receives TRIAL_ACK then

{

(i) Node (j-2) flood message that node j-1 is malicious node or unauthorized node

(ii) All nodes that receive flood message decrease the trust value by one in routing table at corresponding node.

}

Proposed routing algorithm we use fuzzy logic control (FLC) system to calculate the routing metric (RM) value of each nodes available in routing table of a node. In our FLC system we consider five inputs (RE, PC, AB, NM and NTV) and one output parameter which we called routing metric is calculated by each node.

$$\mathrm{RM_i} = \frac{E_r(i)+PC_i+\mathrm{AWB_i}+\mathrm{NTV_i}}{\mathrm{M_j^i(i)}} \quad (1)$$

where i is the node number

By calculating the route metric value nodes are classified into four categories best node, better node, average node and malicious node. If route metric value is between (0.81-1.0) then node is defined as best node. If node metric value is (0.61-0.8) then node is defined as better node. If RM value is between (0.41-0.60) the node is defined as average node. If RM value is between (0-0.4) then node is declared as bad node or malicious node.

Table 1 defines the input/output relationship of values for membership functions and various parameters.

Fuzzy inference rules. There are only 243 rules are applied on the membership function for optimal routing. Table 2 show all possible combination of fuzzy rule base. The crisp value of input parameters are given and a defuzzified crisp value of route metrics is calculated.

Table 1: The Values for Membership Function and various Parameters.

Parameters	Input/output Membership function	Parameter value										
		Low				Medium			High			
Residual Energy	Input	0-0	0-0.1	0.1-0.2	0.2-.0.3	0.3-0.4	0.4-0.5	0.5-0.6	0.6-0.7	0.7-0.8	0.8-0.9	0.9-1.0
Processing capability	Input	Z	VL	ML	LL	LM	MM	HM	LH	MH	HH	VH
Available Bandwidth	Input	Z	VL	ML	LL	LM	MM	HM	LH	MH	HH	VH
Node Mobility	Input	Z	VL	ML	LL	LM	MM	HM	LH	MH	HH	VH
Node Trust Value	Input	Z	VL	ML	LL	LM	MM	HM	LH	MH	HH	VH
Route Metric	Output	Z	VL	ML	LL	LM	MM	HM	LH	MH	HH	VH

Table 2: Fuzzy rule base.

Rule no.	Inputs					Output
	Residual Energy	Processing Capability	Available Bandwidth	Node Mobility	Node Trust Value	
1	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is low	Then RM is low
2	If RE is Medium	And PC is Low	And AB is Low	And NM is Low	And NTV is low	Then RM is low
3	If RE is High	And PC is Low	And AB is Low	And NM is Low	And NTV is Medium	Then RM is High
4	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is High	Then RM is Medium
5	If RE is Low	And PC is Medium	And AB is Low	And NM is Low	And NTV is low	Then RM is low
6	If RE is Low	And PC is high	And AB is Low	And NM is Low	And NTV is low	Then RM is low
7	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is low	Then RM is low
8	If RE is Low	And PC is Low	And AB is Medium	And NM is Low	And NTV is low	Then RM is low
9	If RE is Low	And PC is Low	And AB is High	And NM is Low	And NTV is low	Then RM is low
10	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is low	Then RM is low
11	If RE is Medium	And PC is Low	And AB is Low	And NM is Medium	And NTV is low	Then RM is Medium
12	If RE is Low	And PC is Low	And AB is Low	And NM is High	And NTV is low	Then RM is low
13	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is low	Then RM is low
14	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is Medium	Then RM is low
15	If RE is Low	And PC is Low	And AB is Low	And NM is Low	And NTV is High	Then RM is Medium
…	……	……	……	……	……	……
…	……	……	……	……	……	……
…	……	……	……	……	……	……
243.	If RE is High	And PC is High	And AB is High	And NM is High	And NTV is High	Then RM is High

B. NFBDSR Route Discovery using Neural Network

After calculating the route metric value using fuzzy logic control by each node present in the network. Now suppose source node S has traffic to be send then node S use the BPN neural network to forward the payload on the network. Architecture of Conjugate Gradient [13] Back propagation Neural network (BPN) is shown in Fig. 4.

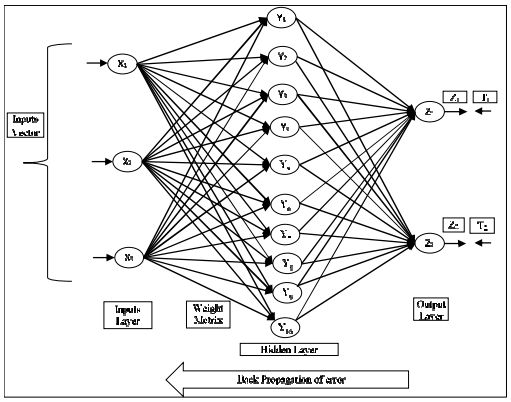

Fig. 4. Architecture of Conjugate Gradient Backpropagation Neural network (BPN).

By using BPN network node S select the optimum and secure path.

Node S take route metric, route cost of neighbor node and pay load type Base QoS (BQ)/Enhanced QoS (EQ) as input for scaled conjugate gradient back propagation neural network (SCGBPN) and set the service type Best Effort (BE) / Reserved (RES) as target value

X_1 = RM_i

X_2 = Route cost of neighbor node

X_3 = pay load type (BQ/EQ)

Z_1 = BE

Z_2 = RES

1. Training Algorithm. The steps of SCGBPN algorithm as follows;

(a) Initialization:

The gradient vector g_0=0, gain value c_0 =1, scalar β_0=0, the weight vector randomly, epoch =1 and n =1. Let the first search direction $d_0 = g_0$. Let N_w is the total number of weight parameters. Set the convergence tolerance CT for Best Effort (BE) traffic (0.3- 0.5) and for Reserved (RES) traffic (0.8-1.0).

(b) Calculate gradient vector $g_n(c_n)$ with respect to gain value c_n

(c) Calculate gain vector.

(d) Calculate error $E(w_n)$.

If ($E(w_n)$ <CT)

{STOP training}

ELSE

{Go to step 5}

(e) Calculate a new search direction:

$$d_n = g_n(c_n) + \beta_{n-1} d_{n-1}$$

(f) If (n >1)

{Update the function of gain,

$$\beta_{n-1} = \frac{g_{n+1}^T(C_{n+1}) g_{n+1}(C_{n+1})}{g_n^T(C_n) g_n(C_n)}$$

}

ELSE

{Go to step 7}

(g) If [(epoch +1) / N_w] = 0

{The gradient vector with $d_n = - g_{n-1}(c_{n-1})$}

ELSE

{Go to step 8}.

(h) Calculate the learning rate η_n

$$E(w_n + \eta_n d_n) = \min_{\lambda \geq 0} E(w_n + \eta_n d_n)$$

(i) Update

{

$$w_n: w_{n+1} = (w_n + \eta_n d_n)$$

$$g_n(c_n) = g_{n+1}(c_{n+1})$$

$$d_{n+1} = - g_{n+1}(c_{n+1}) + \beta_n(c_n)\, d_n$$

}

(j) Set $n = n + 1$ and go to step 2.

C. NFBDSR Route Maintenance

NFBDSR Route maintenance module start work when link is failure due to the mobility of node. Then the node that is in active route unable to transmit data and generate a route break (RB) packet to notify the other nodes on both sides of the link which is lost.

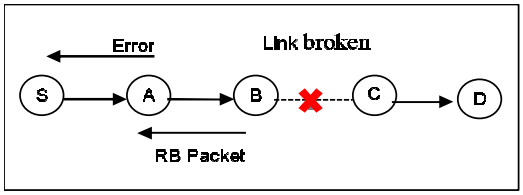

Fig. 5. NFBDSR Route Maintenance on link break.

Mobile nodes that receive the RB packet will update their route cache. When source node receiving an RB packet, then it initiates a new route discovery process. Suppose that link is broken between Node B and C as shown in Fig. 5. After route break node B send RB packet to its neighbors. When node A receives an RB packet, A sends the error packet to S. When source node receives the error packet. It stops the sending of data and restarts the route discovery process to find another path.

III. SIMULATION ENVIRONMENT

NFBDSR QoS framework is implemented in MATLAB R2016a in window 10 Enterprise Edition. The simulation parameters are shown in Table 3.

A. Simulation parameter

Table 3: Parameters are set during simulation.

S. N.	Parameter	Value
1	Simulation	MATLAB R2016a
2	Area (Length*Width)	2000*2000
3	Channel type	Wireless Channel
4	Radio Propagation Model	Two Ray Ground
5	Interface queue Type	Drop Tail/ PriQueue
6	Antenna	Omni directional Antenna
7	MAC Protocol	CSMA
8	Routing Protocol	NFBDSR, FBRP
9	Type of traffic	CBR
10	Simulation Time	300 m sec
11	No. of Nodes	50
12	Node Speed,	10-40 (m /s)
13	Mobility type	Radom (in m/s)
14	No. of Malicious Nodes	10
15	Neural Network	CGBPN

B. Snapshot of simulation

In this section we take snapshot of simulation environment. Fig. 6 shows the Membership function of FLCBDSR architecture of proposed routing. Here Gaussian membership function is used for input/output parameters. Fig. 7 shows FLCBDSR architecture to calculate route metric value. Here Mamdani fuzzy inference system is used.

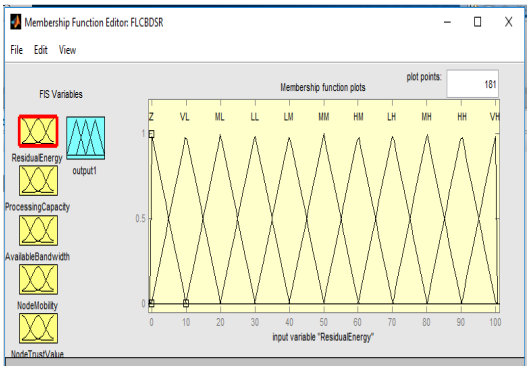

Fig. 6. Membership function of FLCBDSR architecture of proposed routing.

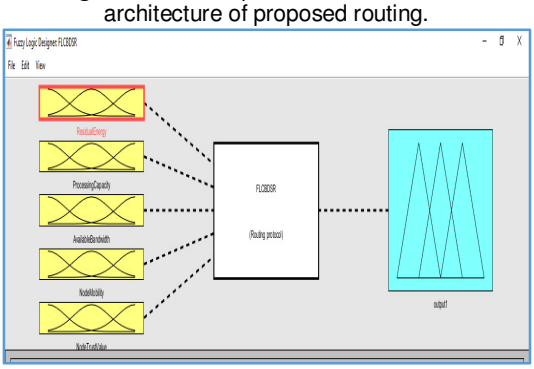

Fig 7. FLCBDSR architecture to calculate route metric value.

Fig. 8 shows the Fuzzy inference rule of FLCBDSR architecture. 243 rules are used for Defuzzification. Fig. 9 shows the Implementation Architecture of BPN neural network in matlab

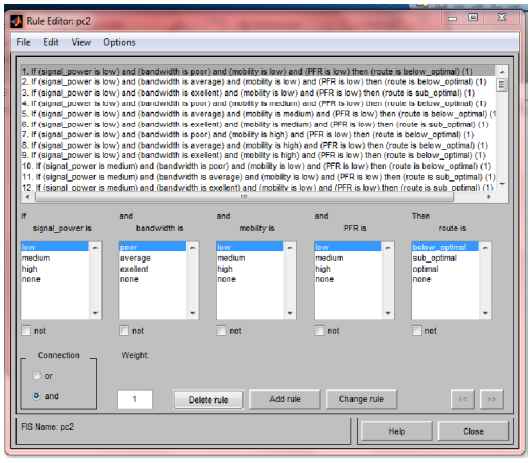

Fig 8. Fuzzy inference rule of FLCBDSR architecture.

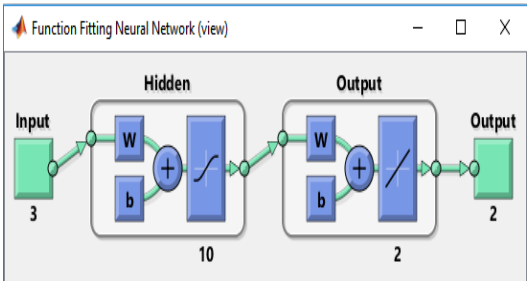

Fig. 9. Implementation Architecture of BPN neural network.

Fig. 10 shows Simulation scenario of mobile ad hoc network in Matlab. Snapshot is taken during running simulation environment. Fig. 11 shows the Simulation scenario of mobile ad hoc network with neural network. Neural network is invoked when route is find out.

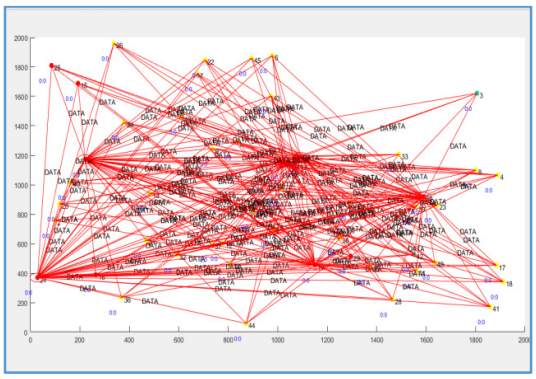

Fig. 10. Simulation scenario of MANET.

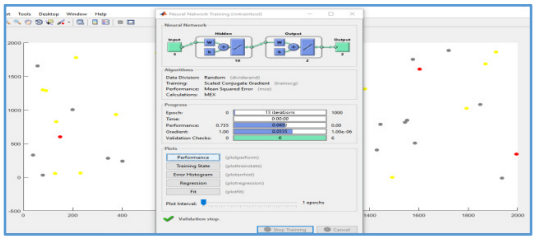

Fig. 11. Simulation scenario of MANET with neural network.

IV. RESULTS AND ANALYSIS

In this paper, we are comparing the performance of NFBDSR algorithm with FBRP in terms of LET (link establishment time), number of hop count per route, throughput, packet delivery ratio (PDR), end-to-end delay and average jitter by plotting the graph.

A. Performance analysis of scenario when no malicious node existing in the network

1. Throughput. Fig. 12 represents the throughput of NFBDSR and FBRP. The throughput of any network is degraded as speed of a node increased. Here we compare the average of throughputs at different time of simulation. The throughput of NFBDSR are increased 7.30% compare to FBRP.

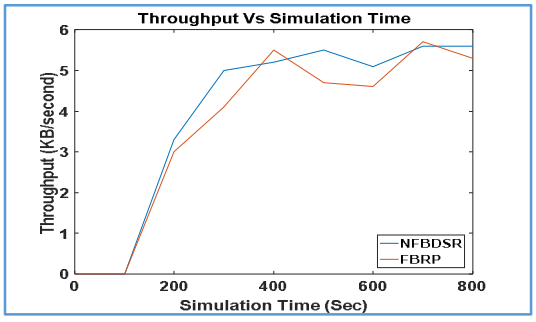

Fig. 12. Throughput of routing protocols.

2. End-To-End Delay. Maximum End-To-End Delay can lead to low performance and minimum End-To-End Delay is the indication of high efficiency of the MANET. Fig. 13 shows End to End delay of NFBDSR

and FBRP in seconds. E-2-E delay of NFBDSR is decreased by 0.27% compare to FBRP.

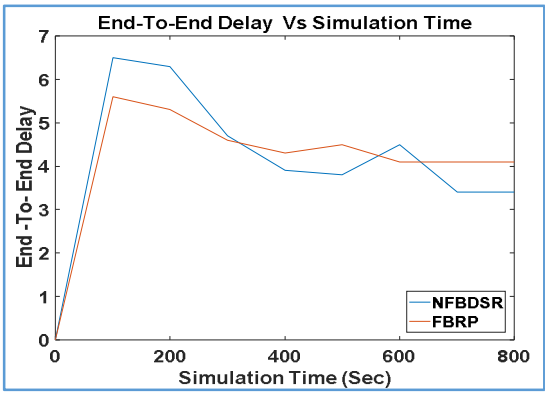

Fig. 13. End-To-End Delay of routing protocols.

3. Packet Delivery Ratio. Packet Delivery ratio (PDR) is the packets that are successfully delivered to a destination divide by total number of packet send. Fig. 14 shows graph between PDR and simulation time. PDR of NFBDSR is increased 5.07% compared to FBRP framework.

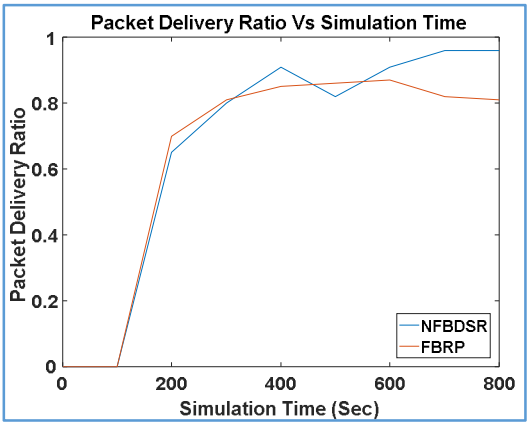

Fig. 14. Packet Delivery Ratio of routing protocols.

4. Average Jitter. Jitter is the delay variance in the time between packets arriving. It should be less for better performance. Average jitter of NFBDSR is lower than FBRP protocol as shown in Fig. 15. Average jitter of NFBDSR is decreased by 10.22% compare to FBRP.

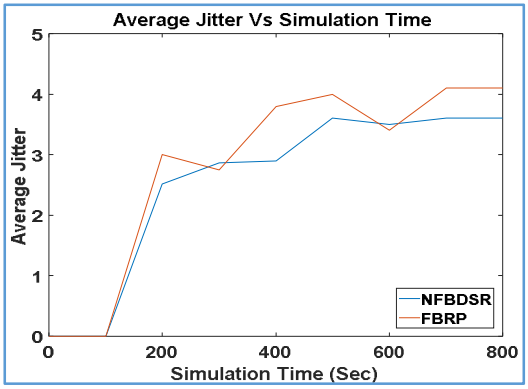

Fig. 15. Average Jitter of routing protocols.

5. Link Establishment Time. Link establishment is the time to establish path from source to destination. It should be less for better performance. Link Establishment Time of NFBDSR, is lower than FBRP protocols as shown in Fig. 16. Link Establishment Time of NFBDSR is decreased by 13.85% compare to FBRP.

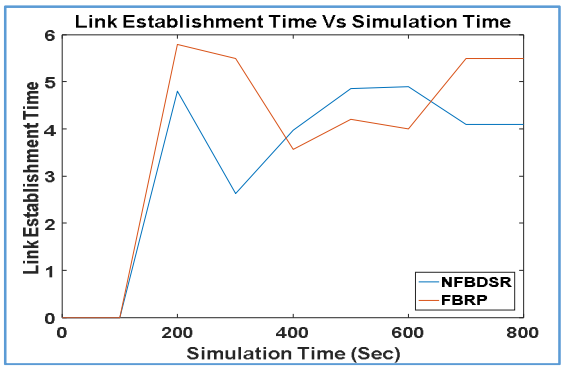

Fig. 16. Link Establishment time of routing protocols.

6. Hop Count per Route. The Fig. 17 illustrate the comparison of the hop count of NFBDSR and FBRP. The hope count of NFBDSR, is lower than FBRP as shown in figure. The hope count of NFBDSR is improved 7.54% by FBRP.

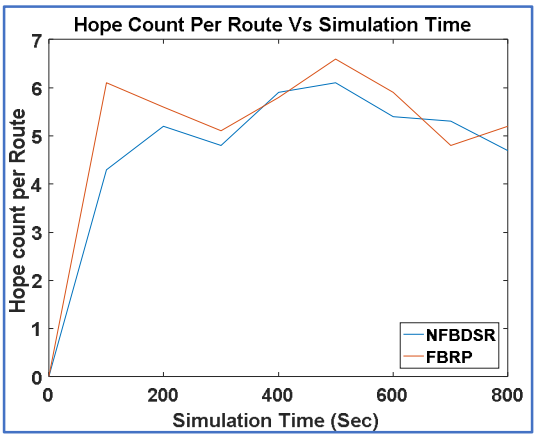

Fig. 17. Hope count per route of routing protocols.

B. Performance analysis of scenario when ten malicious node existing in the network

1. Throughput. The throughput of NFBDSR is degraded due to the presence of malicious node. But still NFBDSR has better throughput than FBRP protocols as shown in Fig. 18. The throughput of NFBDSR are increased 12.70% compare to FBRP.

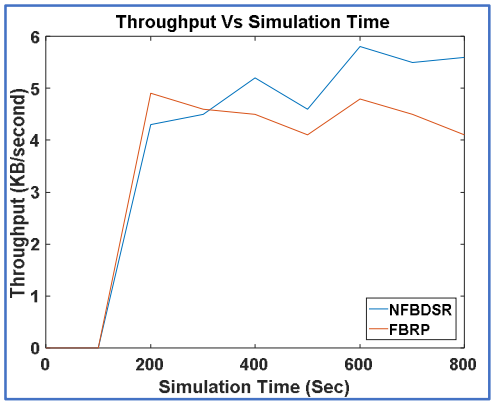

Fig. 18. Throughput of routing protocols.

2. End-To-End Delay. As we know that end to end delay of network is increased as malicious node present in the network. But if we compare it with FBRP protocols the NFBDSR has compare to lower end to end delay shown in Fig. 19. E-2-E delay of NFBDSR is decreased by 7.66% compare to FBRP.

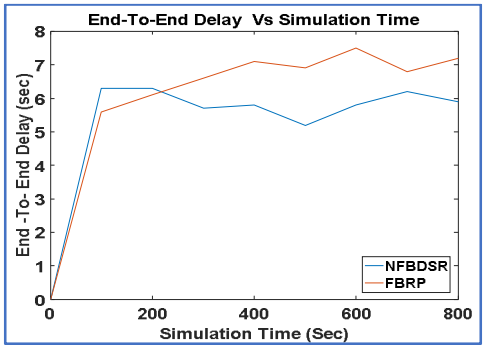

Fig. 19. End-to-End Delay of routing protocols.

3. Packet Delivery Ratio. PDR also affected by malicious node for better performance PDR must be high. Here PDR of NFBDSR is better for varying node speed as shown in Fig. 20. PDR of NFBDSR is increased 04.62% compared to FBRP.

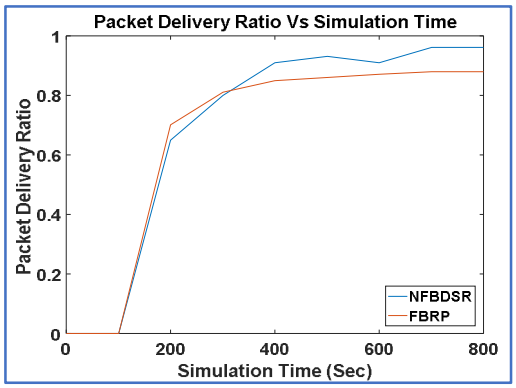

Fig. 20. Packet Delivery Ratio of routing protocols.

4. Average Jitter. Jitter is the delay variance in packet delivery so jitter must be lower for better performance. If we compare average jitter of NFBDSR with FBRP protocols, it is lower for every node speed as shown in Fig. 21. Average jitter of NFBDSR is decreased by 16.15% compare to FBRP.

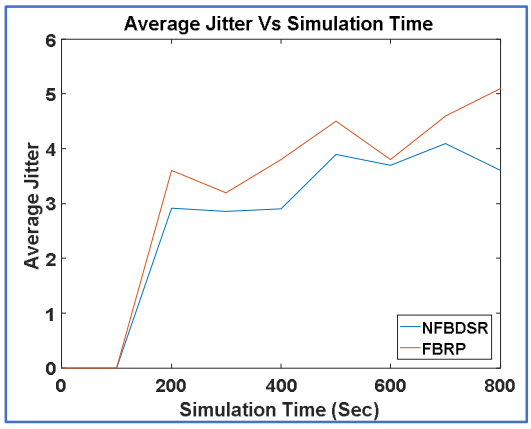

Fig. 21. Average Jitter of routing protocols.

5. Link Establishment Time. Link establishment is the time to establish path from source to destination. It should be less for better performance. Link Establishment Time of NFBDSR, is lower than FBRP protocols as shown in Fig. 22. Link Establishment Time of NFBDSR framework is decreased by 14.74% compare to FBRP.

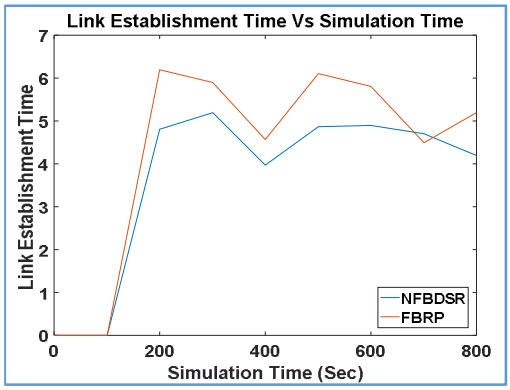

Fig. 22. Link Establishment Time of routing protocols.

6. Hop Count per Route. The Fig. 23 show the graph of the hop count of NFBDSR, and FBRP. The hope count of NFBDSR, is lower than FBRP protocol as shown in Fig 23. The hope count of NFBDSR is improved by 5.12% compare to FBRP.

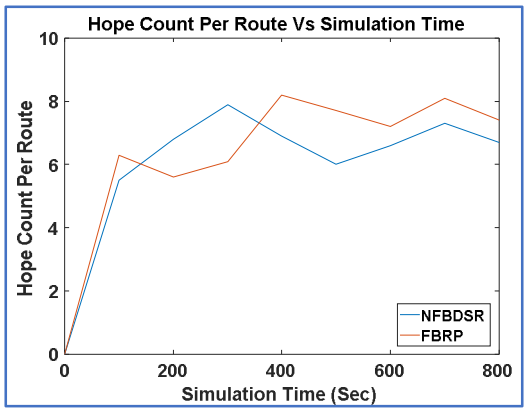

Fig. 23. Hope count per route of routing protocols.

C. Deep Analysis of Results

Here we have evaluated the performance by considering, throughput, packet delivery ratio (PDR), end-to-end delay, average jitter, LET (link establishment time) and number of hop count per route of Proposed NFBDSR with FBRP. In the protocol performance analysis, we investigate the routing performance of the NFBDSR compared with FBRP. We evaluate the performance of the NFBDSR at varying mobile speeds. In mobile scenarios, the node speed is an important metric that affects the network topology. We fix the number of nodes at 50, number of malicious node 10, vary the maximum speed from 10 to 40m/s and simulation time 800 sec. Fig. 14 and 20 shows the packet delivery ratio for the NFBDSR and FBRP protocols at different scenario when malicious node existing and not existing. The packet delivery ratio decreases as the maximum speed increases because the network becomes less stable. The NFBDSR shows significantly better performance than the FBRP protocols. This is because the NFBDSR considers the Residual Energy

(RE), processing capability (PC), Available Bandwidth (ABW), Node Mobility of (NM), Node Trust Value (NTV) and SCGBPN in the route selection. Because the FBRP protocol only considers the power of battery, speed of mobile nodes and number of hops in the route selection, it produces poorer performance.

The NFBDSR performs better than the FBRP protocol because it takes Link Establishment Time into account. However, the performance of the FBRP drops as the simulation time increases. The NFBDSR can switch to a better route before a route breaks, resulting in a significant improvement. Fig. 13 and 19 shows the end-end delay for packets at different scenario when malicious node absent and present that are received at the destination. As the speed increases, the frequency of link breakage increases. Frequent route reconstructions incur more control overhead, increasing the probability of congestion and packet collisions. Fig. 13 and 19 shows that the NFBDSR is effective in reducing the end-to-end delay, particularly when the malicious node is existing and speed is high. As the speed increases, the topology changes faster. Because the FBRP protocol do not take trusted node into account in the route speed increases, the throughput of network decrease because of the low stability in the network. Therefore, no matter what routing scheme is used, the routing load is increased. The throughput by the NFBDSR is more than FBRP protocol because the NFBDSR always chooses the most stable route for transmission and finds an alternate path through the candidate nodes before the path breaks. Consequently, it reduces the number of packets" dropped.

V. CONCLUSION

The proposed NFBDSR routing algorithm finds the efficient path dynamically in secured manner. FLC is used to calculate the route metric value of each node. Neural network is used to find out the efficient and secure path to increase the routing quality and decreases the routing overhead and the number of hops in finding path. A key contribution of proposed routing protocol is that it uses very simple methods to secure the network rather than complex algorithms used in existing secure routing protocols. By using fuzzy variables as input fuzzy logic control give quick response compare to crisp value. With the help of back propagation neural network we easily find out the suitable path for QoS traffic. Back propagation network neural network decreases the number of hops and overhead in finding route. Back propagation network neural network create optimizes and stable path. By result analysis we found that Link Establishment Time is decreased by NFBDSR. The number of hops also decreased by NFBDSR. The throughput of proposed routing protocol increased some fraction. Packet delivery ratio also increased somewhat. Average jitter, E-2-E delay are decreased in both situations when malicious node existing and not existing.

Real world engineering applications of our algorithm is that it consider MANET applications such as multimedia, audio/video, images, animations, graphics, VOIP, video conferencing, and webcasting need uninterrupted, rigorous and inflexible QoS.

VI. FUTURE SCOPE

As a future scope the proposed QoS routing protocol NFBDSR can be further expand using selection, they produce longer delays when malicious node is existing and the node mobility is high. This is because route discovery is time consuming. Using its neuro fuzzy logic technique, the NFBDSR chooses the best route, which can efficiently reduce the number of route rediscoveries. As a result, the NFBDSR produces the lowest end-to-end" delay.

Fig. 17 and 23 shows the hop count per route of the NFBDSR and FBRP protocol at different conditions. The hop count per route increases as the malicious node and speed increases because when the malicious node and speed increases, the stability of the network decrease and leads to frequent path breaks. The hop count per route of the NFBDSR is lower than the FBRP protocols. This is because the NFBDSR finds quick paths in a single route discovery process using candidate nodes. Another reason is that the NFBDSR restarts the route discovery process when all backbone paths have failed. The hop count per route of the NFBDSR is less than the FBRP because the FBRP finds weak links using the link quality measure. Fig. 12 and 18 shows a comparison of the throughput of the NFBDSR and FBRP protocols at different conditions. As the malicious node and different neural networks and some optimizing techniques from soft computing with security features. Applied different neural networks simulation is performed on the basis of different simulation times to observe its behavior and significance. It may also advantage to researchers to think directions to security issues involved in providing quality of services in a MANET.

ACKNOWLEDGEMENT

We owe our deep gratitude to Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal and the Department School of Information Technology for providing better research environment for successfully completing our research work. Also, we would like to extend our sincere thanks to my guide Prof. Sanjeev Sharma for their timely guidance and supports.

Conflicts of interest. There is no conflict of interest.

REFERENCES

[1]. Toh, Chai K. *Ad hoc mobile wireless networks: protocols and systems*. Pearson Education, 2001.

[2]. Reddy, T. B., Karthigeyan, I., Manoj, B. S., & Murthy, C. S. R. (2006). Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions. *Ad Hoc Networks*, *4*(1), 83-124.

[3]. Sahu, S., & Sharma S. (2018). Analysis of Security threats and Vulnerability Issues in QoS Frameworks of MANET. *International Journal of Research in Electronics and Computer Engineering*, Vol. *6*, no. 2, pp. 1490-1496.

[4]. Karibasappa, A. S. G., & Muralidhara, B. K. N. (2011). Neuro fuzzy based routing protocol for mobile ad-hoc networks. In *2011 6th International Conference on Industrial and Information Systems* (pp. 216-221). IEEE.

[5]. Gupta, S., Bharti, P. K., & Choudhary, V. (2011, July). Fuzzy logic based routing algorithm for mobile ad hoc networks. In *International Conference on High Performance Architecture and Grid Computing* (pp. 574-579). Springer, Berlin, Heidelberg.

[6]. Chaythanya, B. P. (2014). Fuzzy logic based approach for dynamic routing in MANET. *International Journal of Engineering Research*, *3*(6).

[7]. Mallapur, S. V., & Patil, S. R. (2014, December). Fuzzy logic-based stable multipath routing protocol for

mobile ad hoc networks. In *2014 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE.
[8]. Tabatabaei, S., & Hosseini, F. (2016). A fuzzy logic-based fault tolerance new routing protocol in mobile ad hoc networks. *International Journal of Fuzzy Systems*, *18*(5), 883-893.
[9]. Rishiwal, V., Verma, S., & Bajpai, S. K. (2009). QoS based power aware routing in MANETs. *International Journal of Computer Theory and Engineering*, *1*(1), 49.
[10]. Tung-Shih Su, Chih-Hung Hsieh Lin, and Wen Shyong (2006). A Novel QoS-Aware Routing for Ad Hoc Networks. In *Proc. of the 9th Joint Conference on Information Sciences* (*JCIS*), Taiwan.
[11]. Basu, P., Khan, N., & Little, T. D. (2001, April). A mobility based metric for clustering in mobile ad hoc networks. In *Proceedings 21st International Conference on Distributed Computing Systems Workshops* (pp. 413-418). IEEE.
[12]. Sahu, S., & Sharma, S. (2019). Secure and Proficient Cross Layer (SPCL) QoS framework for mobile ad-hoc network. *International Journal of Electrical & Computer Engineering* (2088-8708), *9*.
[13]. Al, Bayati, A. Y., Sulaiman, N. A., & Sadiq, G. W. (2009). A Modified Conjugate Gradient Formula for Back Propagation Neural Network Algorithm 1.
[14]. Dhawan, D., & Singh, R. (2019). Comprehensive Comparison and Analysis of Nature Inspired ACO based Routing Algorithms in Ad Hoc Networks. *International Journal on Emerging Technologies*, *10*(2): 60-66.

How to cite this article: Sahu S. and Sharma S. (2019). Neuro Fuzzy Based Dynamic Secure Routing Protocol for QoS Frameworks of MANET. *International Journal on Emerging Technologies*, **10**(3): 286–295.