IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

Analyzing Trust Categories and Generating Trusted Network Path of MANET using Fuzzy Credibility Distribution Function

S.Bandyopadhyay[1*], S. Karforma[2]

[1]Department of Computer Science & Technology, Dr.B.C.Roy Polytechnic, Durgapur, India
[2]Department of Computer Science, The University of Burdwan, Burdwan, India

**Corresponding Author: sohamban@gmail.com, Tel.: +91-9732014976*

Available online at: www.ijcseonline.org

Abstract— Mobile ad-hoc network (MANET) is one of the significant approaches with highly decentralized and dynamic configured architecture. For transferring packets from one node to another node in MANET security is a big challenge. Trust between two consecutive nodes is a prime important factor for secure data transmission through a trusted network path. As we all know trust of any particular node observed by other one varies with time for different constrains. Here we try to depict the variation of trust with fuzzy mathematics where trust value for each node is represented with triangular fuzzy number. Using fuzzy credibility distribution function we convert the triangular fuzzy trust value in interval based form and represent the trust variation in much more reliable format. These interval based trust values are used to generate direct, indirect trust value in interval based matrix format and from them we prepare overall communication trust matrix to generate the secure network path to send data from particular source to destination.

Keywords— fuzzy credibility distribution, inverse credibility distribution, triangular fuzzy number, membership value.

I. Introduction

Dispersed framework and data sharing are the essential properties of MANET for detecting and observing the event. Dynamic trustworthiness among the nodes of MANET can be accomplished by the reliable conduct of the nodes. But the deployment of MANET is done in a distributed environment in such a way that the reliability of nodes is a major constraint for transmitting the data. Therefore, establishing and quantifying the behavioral property of nodes in MANET, are most significant tasks. In expansive scale MANET organize structure, choice of nodes for transmitting the packets safely is a major challenge. As to issue, numerous specialists took a shot at the diverse trust-based model and recognized the pernicious and secure nodes for a specific system [12]. On the other hand fuzzy model on intrusion detection [7] to flow data through MANET is explained by many researchers. Trust models generation and trust evaluation metrics representation for MANET [5] enhanced the quality of research on trust based ad-hoc network. Movement of MANET nodes and changing topological structure generate the variation in trust between two nodes in MANET. Due to this fluctuation in trust value, here we try to analyze the issue of uncertainty on the performance of nodes in MANET. Because of a few physical and environmental hindrances, the trust estimation of a specific node can fluctuate. Here we use triangular fuzzy data to represent the variation of trust. Using fuzzy credibility distribution function [9] on triangular fuzzy number we generate interval based trust value in matrix format to form direct, indirect trust [1]. Using these trusts finally we generate communication trust matrix, from where we find the intermediate trusted nodes for transmitting data from one source to destination. To analyze the overall details we organize the rest of the paper in the following way: In section 2, the mathematical models are generated where fuzzy credibility distributed function is applied on triangular fuzzy data to generate trust values of the nodes in interval based format and these trust values are used to generate direct, indirect, communication trusts to simulate the overall process. Through Section 3, an example MANET structure is explained where node to node trust is represented with triangular fuzzy number. Using these trust values we generate direct, indirect and communication trust in interval based matrix format and find secure network path for transmitting data from source to destination. At section 4, we analyze the communication trust matrix and generate trusted network path for transmitting data from source to destination. Finally, at section 5, we conclude and generate an idea for further improvements.

II. MATHEMATICAL MODELING

A. Triangular Fuzzy number

A triangular fuzzy number $\tilde{F} = \{m_1, m_2, m_3\}$ is depicted with the membership functions and holds the conditions as

1. From m_1 to m_2 the membership value gets increased.
2. From m_2 to m_3 the membership value gets decreased.
3. $m_1 \leq m_2 \leq m_3$

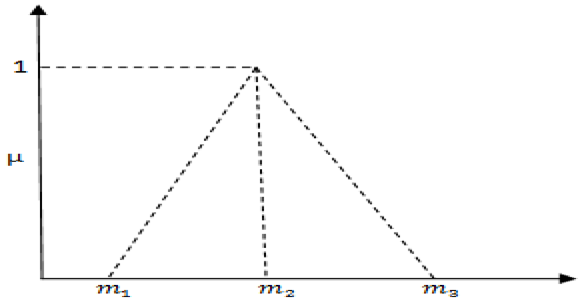

Figure 1. Tiangular fuzzy number.

Suppose for a value *x*, the membership function is $\mu_{\tilde{F}}(x)$, where $0 \leq \mu_{\tilde{F}}(x) \leq 1$
According to Figure 1 it can be defined as

$$\mu_{\tilde{F}}(x) = \left\{ \begin{array}{cc} 0 & if\ x < m_1 \\ \dfrac{x - m_1}{m_2 - m_1} & if\ m_1 \leq x \leq m_2 \\ \dfrac{m_2 - x}{m_3 - m_2} & if\ m_2 < x \leq m_3 \\ 1 & if\ x > m_3 \end{array} \right\} \quad (1)$$

B. Credibility distribution of triangular fuzzy data

The credibility distribution [9] of a fuzzy variable σ is defined as

$$\zeta(x) = \left\{ \begin{array}{cc} 0 & if\ x < m_1 \\ \dfrac{x - m_1}{2(m_2 - m)} & if\ m_1 < x \leq m_2 \\ \dfrac{x + m_3 - 2m}{2(m_3 - m_2)} & if\ m_2 < x \leq m_3 \\ 1 & if\ x > m_3 \end{array} \right\} \quad (2)$$

This credibility distribution generates inverse credibility distribution values, which are basically interval, estimated fuzzy values with lower and upper bound limit.

$$\zeta^{-1}(\alpha) = \left\{ \begin{array}{ll} m_1 + 2(m_2 - m_1)\alpha & if\ 0 \leq \alpha \leq 0.5 \\ 2m_2 - m_3 + 2(m_3 - m_2)\alpha & if\ 0.5 < \alpha \leq 1 \end{array} \right\} \quad (3)$$

C. Euclidian distance

The Euclidian distance [8] between two points x, y in Euclidian space R^n is given by

$$\mathrm{e}(\mathrm{x}, \mathrm{y}) = \sqrt{\sum_{\mathrm{i}=1}^{\mathrm{n}} (\mathrm{x_i} - \mathrm{y_i})^2} \quad (4)$$

D. Queuing (M/M/1) service rate, arrival rate

Packet service rate

$$\mathrm{m} = \frac{\mathrm{L_C}}{\mathrm{P}} \quad (5)$$

Where, link capacity of data packets (Mbps/sec) and payload size of the packets (Byte) are $\mathrm{L_C}$ and p respectively.

Packet arrival rate

$$\beta = \frac{1}{\mathrm{i_T}} \quad (6)$$

Where $\mathrm{i_T}$ = interarrival time of data packets (Micro seconds)

E. Data packet forwarding ratio

Data packet forwarding ratio defined as the ratio of the total number of successful packet transmission to the total number of packet transmission at a particular time instance.
Suppose, for transmitting the data packet from node X to Y at time instance t we have, numbers of packets are forwarded by node Y, observed by X and numbers of packets are dropped by node Y, observed by X are $\mathrm{fp_t}$, $\mathrm{dp_t}$ respectively.

$$\mathrm{pf(A, B)} = \frac{\mathrm{fp_t}}{\mathrm{fp_t} + \mathrm{dp_t}} \quad (7)$$

F. Fuzzy direct trust

Consider, a MANET has k number of nodes of $\mathrm{n_1, n_2, n_3, n_4} \ldots \ldots \ldots \ldots .. \mathrm{n_k}$

Suppose, the initial direct trust value of $\mathrm{n_j}$, observed by $\mathrm{n_i}$ for particular time instance t1, is $\widetilde{\mathrm{dt}}_{\mathrm{t1}}(\mathrm{n_i}, \mathrm{n_j})$.

Where
$\widetilde{\mathrm{dt}}_{\mathrm{t1}}(\mathrm{n_i}, \mathrm{n_j}) = \{\mathrm{dt^1}_{\mathrm{t1}}(\mathrm{n_i}, \mathrm{n_j}), \mathrm{dt^2}_{\mathrm{t1}}(\mathrm{n_i}, \mathrm{n_j}), \mathrm{dt^3}_{\mathrm{t1}}(\mathrm{n_i}, \mathrm{n_j})\}$

Here after spending Δt amount of time at a t2 time instance, we calculate direct trust value of $\mathrm{n_j}$, observed by $\mathrm{n_i}$ with triangular fuzzy number system and symbolically we represent it as $\widetilde{\mathrm{dt}}_{\mathrm{t2}}(\mathrm{n_i}, \mathrm{n_j})$

Say, the trust-aging factor [2] t_a is $\mathrm{e}^{-\gamma}$

$$\text{Where, } \gamma = \frac{\Delta \mathrm{t}}{1 + \Delta \mathrm{t}} \quad (8)$$

Δt = changing in time.

$\mathrm{w_1}$ and $\mathrm{w_2}$ are data and control packet weight respectively.

If $\mathrm{pf_{t2}}(\mathrm{n_i}, \mathrm{n_j})$ is symbolized as packet forwarding ration from $\mathrm{n_i}$ to $\mathrm{n_j}$ at t2 time instance, then from equation (7)

$$\mathrm{pf_{t2}}(\mathrm{n_i}, \mathrm{n_j}) = \frac{\beta_{\mathrm{i,j}}}{\beta_{\mathrm{i,j}} + \rho_{\mathrm{i,j}}} \quad (9)$$

If total number of packets $\delta_{i,j}$, is transferred by n_j

So, dropped packets by n_j will be

$$\rho_{i,j} = \left(1 - \frac{\beta_{i,j}}{m_{i,j}}\right)\left(\frac{\beta_{i,j}}{m_{i,j}}\right)^k * \delta_{i,j} \qquad (10)$$

Where k = Total number of nodes.

$$\widetilde{dt}_{t2}(n_i, n_j) =$$

$$\widetilde{dt}_{tmp}(n_i, n_j) * \tau^{dt_{t1}} + pf_{t2}(n_i, n_j) * \tau^{dt_{t2}} \qquad (11)$$

Where,

$\tau^{dt_{t1}}$ and $\tau^{dt_{t2}}$ are direct trust weight for $t1, t2$ time instances respectively.

$\widetilde{dt}_{tmp}(n_i, n_j)$ is calculated from trust-aging factor, t_a.

$$\widetilde{dt}_{t2}(n_i, n_j) = \{dt^1{}_{t2}(n_i, n_j), dt^2{}_{t2}(n_i, n_j), dt^3{}_{t2}(n_i, n_j)\}$$

G. Fuzzy interval based direct trust

Here fuzzy credibility distribution function and inverse fuzzy credibility distribution function is used on fuzzy direct trust [2] matrix $dt_{t2_{kxk}}$ to form interval estimated fuzzy direct trust value.

$$\widetilde{dt}_{t2}(n_i, n_j) = [\widetilde{dt}_{t2}(n_i, n_j)^L, \widetilde{dt}_{t2}(n_i, n_j)^H] \qquad (12)$$

Where according to equation (2), (3) we get

$$\beta_{i,j}{}^{-1}(m) =$$
$$\left\{\begin{matrix} dt^1{}_{t2}(n_i, n_j) + 2(dt^2{}_{t2}(n_i, n_j) - dt^1{}_{t2}(n_i, n_j))m \quad 0 \le m \le 0.5 \\ 2dt^2{}_{t2}(n_i, n_j) - dt^3{}_{t2}(n_i, n_j) + 2(dt^3{}_{t2}(n_i, n_j) - dt^3{}_{t2}(n_i, n_j))m \\ if\ 0.5 < m \le 1 \end{matrix}\right\} \qquad (13)$$

H. Fuzzy similarity matrix and weightage factor

Fuzzy Euclidian distance [8] from equation (4) we get

$$\widetilde{ut}_2(n_i, n_j) = [\widetilde{ut}_2(n_i, n_j)^L, \widetilde{ut}_2(n_i, n_j)^H] \qquad (14)$$

Where,

$$\left.\begin{matrix} \widetilde{ut}_2(n_i, n_j)^L = \sqrt{\sum_{v \in cn(n_i,n_j)} \left[\widetilde{dt}_{t2}(n_i, v)^L - \widetilde{dt}_{t2}(n_j, v)^L\right]^2} \\ \widetilde{ut}_2(n_i, n_j)^H = \sqrt{\sum_{vu \in cn(n_i,n_j)} \left[\widetilde{dt}_{t2}(n_i, v)^H - \widetilde{dT}_{t2}(n_j, v)^H\right]^2} \end{matrix}\right\} \qquad (15)$$

Here fuzzy Euclidian distance is used to calculate the difference of fuzzy direct trust and similarity factor [1]$\widetilde{sm_{t2}}(n_i, n_j)$ value of two nodes .

We use fuzzy weight factor $\widetilde{\vartheta_{t2}}(x_i, x_j)$ as recommendation value for node n_j , calculated by node n_i.

$$\widetilde{\vartheta_{t2}}(n_i, n_j) = [\widetilde{\vartheta_{t2}}(n_i, n_j)^L, \widetilde{\vartheta_{t2}}(n_i, n_j)^H] \qquad (16)$$

Where,

$$\left.\begin{matrix} \widetilde{\vartheta_{t2}}(n_i, n_j)^L = 0.5 * \widetilde{sm_{t2}}(n_i, n_j)^L + 0.5 * \widetilde{dt}_{t2}(n_i, n_j)^L \\ \widetilde{\vartheta_{t2}}(n_i, n_j)^H = 0.5 * \widetilde{sm_{t2}}(n_i, n_j)^H + 0.5 * \widetilde{dt}_{t2}(n_i, n_j)^H \end{matrix}\right\} \qquad (17)$$

I. Fuzzy indirect trust

Recommendation to any particular node from the intermediate node for showing the trustworthiness to any other particular node is a significant parameter for calculating indirect trust value. If fuzzy indirect trust [1] value of node n_j , observed by n_i , is originated as interval based format, it will be

$$\widetilde{it}_{t2}(n_i, n_j) = [\widetilde{it}_{t2}(n_i, n_j)^L, \widetilde{it}_{t2}(n_i, n_j)^H] \qquad (18)$$

Where,

$$\left.\begin{matrix} \widetilde{it}_{t2}(n_i, n_j)^L = \frac{\sum_{v \in n} \widetilde{dt}_{t2}(v, n_j)^L * \widetilde{\vartheta_{t2}}(n_i, v)^L}{\sum_{i \in n} \widetilde{\vartheta_{t2}}(n_i, v)^L} \\ \widetilde{it}_{t2}(n_i, n_j)^H = \frac{\sum_{u \in n} \widetilde{dt}_{t2}(v, n_j)^H * \widetilde{\vartheta_{t2}}(n_i, v)^H}{\sum_{i \in n} \widetilde{\vartheta_{t2}}(n_i, v)^H} \end{matrix}\right\} \qquad (19)$$

J. Fuzzy communication trust

Here we generate interval based fuzzy communication trust [2] using $\widetilde{dt}_{t2}(n_i, n_j)$ and $\widetilde{it}_{t2}(n_i, n_j)$

We represent interval based fuzzy communication trust as

$$\widetilde{ct}_{t2}(n_i, n_j) = [\widetilde{ct}_{t2}(n_i, n_j)^L, \widetilde{ct}_{t2}(n_i, n_j)^H] \qquad (20)$$

Where,

$$\left.\begin{matrix} \widetilde{ct}_{t2}(n_i, n_j)^L = \alpha_{n_i,n_j} * \widetilde{dT}_{t2}(n_i, n_j)^L + (1 - \alpha_{n_i,n_j}) * \widetilde{it}_{t2}(n_i, n_j)^L \\ \widetilde{ct}_{t2}(n_i, n_j)^H = \alpha_{n_i,n_j} * \widetilde{dT}_{t2}(n_i, n_j)^H + (1 - \alpha_{n_i,n_j}) * \widetilde{it}_{t2}(n_i, n_j)^H \end{matrix}\right\} \qquad (21)$$

Where α_{n_i,n_j} is the weight of direct trust value of node n_j computed by n_i and it is represented as

$$\alpha_{x_i,x_j} = \frac{\gamma_{t2}(n_i,n_j)}{\gamma_{t2}(n_i,n_j) + \overline{\gamma_{t2}}(n_i,n_j)} \qquad (22)$$

$\gamma_{t2}(n_i, n_j)$ is the number of packets of node n_i, forwarded by x_j and $\overline{\gamma_{t2}}(n_i, n_j)$ is the number of packets forwarded by n_j, except n_i

Using the fuzzy communication trust value $\widetilde{ct}_{t2}(n_i, n_j)$ for n_j computed by n_i we can derive the fuzzy communication trust matrix $\widetilde{ct}_{t2_{kxk}}$.

III. SIMULATION STUDY

In order to generate fuzzy communication trust, here we take a MANET network structure. In packet transmitting system, we emphasize on two types of packet, data packets and control packets. At our simulation-based technique, we consider the separate weight for data and control packets. Here the frequency of each node is considered with Hz unit. We use Mbps/sec and Byte as the unit for link capacity and payload size respectively. The microsecond is used as the unit for the inter-arrival time between two consecutive packets for delivery. We use ANSI C, Maple12, Ns-2.35 and Microsoft Office Excel 2007 to simulate the overall structure and analyze the fuzzy trust values with several factors programmatically. The proposed simulation related parameters are followed through Table 1.

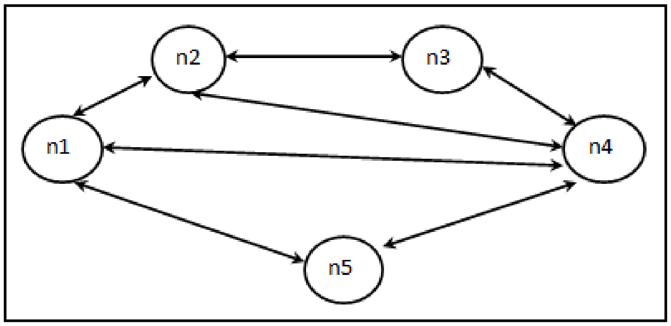

Figure 2. MANET network structure.

Table 1. Simulation details

Parameters	Values
MAC protocol	IEEE802.11
Physical protocol	IEEE802.11b
Number of nodes	5 (Can be increased according to need)
Transmitting frequency of each node	5Mz
Bandwidth reduction factor for direct link	0.18
Bandwidth reduction factor for indirect link	0.42
Network protocol	IPv4
Propagation path loss model	Two way
Network structure	Full duplex
Transport protocol	UDP
Simulation area	1000× 1000
Inter-arrival time unit between two successive packet transfer	Micro second

According to the MANET, network structure of figure 1

Total number of nodes n=5

The data packet forwarding ratio matrix is represented as

$$\begin{vmatrix} 0.999999 & 0.975000 & 0.807018 & 0.796875 & 0.829787 \\ 0.840909 & 0.906977 & 0.958333 & 0.750000 & 0.696429 \\ 0.660714 & 0.928571 & 0.978723 & 0.850000 & 0.684211 \\ 0.698113 & 0.722222 & 0.821429 & 0.962264 & 0.829787 \\ 0.860465 & 1.000000 & 0.958333 & 0.927273 & 0.829787 \end{vmatrix}$$

Initially direct trust matrix at t1 time instance is represented with triangular fuzzy number system as

$$\mathrm{dt}_{t1_{5x5}} =$$

$$\begin{vmatrix} (0.0,0.2,0.4) & (0.3,0.5,0.7) & (0.1,0.3,0.5) & (0.4,0.6,0.8) & (0.3,0.5,0.7) \\ (0.2,0.4,0.6) & (0.2,0.4,0.6) & (0.4,0.6,0.8) & (0.4,0.6,0.8) & (0.4,0.6,0.8) \\ (0.1,0.3,0.5) & (0.4,0.6,0.8) & (0.4,0.6,0.8) & (0.3,0.5,0.7) & (0.2,0.4,0.6) \\ (0.0,0.2,0.4) & (0.0,0.2,0.4) & (0.2,0.4,0.6) & (0.1,0.3,0.5) & (0.1,0.3,0.5) \\ (0.5,0.7,0.9) & (0.2,0.4,0.6) & (0.1,0.3,0.5) & (0.0,0.2,0.4) & (0.0,0.2,0.4) \end{vmatrix}$$

According to equation (11), the current direct trust matrix $\mathrm{dt}_{t2_{5x5}}$ is represented with interval based format, using inverse credibility distribution function formulated at equation (3)

$$\mathrm{dt}_{t2_{5x5}} =$$

$$\begin{vmatrix} 1.000, 1.000 & 0.667, 0.686 & 0.473, 0.556 & 0.594, 0.654 & 0.618, .638 \\ 0.603, 0.618 & 1.000, 1.000 & 0.675, 0.735 & 0.581, 0.641 & 0.542, 0.602 \\ 0.417, 0.499 & 0.655, 0.715 & 1.000, 1.000 & 0.612, 0.629 & 0.513, 0.521 \\ 0.410, 0.487 & 0.429, 0.508 & 0.575, 0.585 & 1.000, 1.000 & 0.478, 0.560 \\ 0.663, 0.723 & 0.655, 0.669 & 0.519, 0.599 & 0.492, 0.569 & 1.000, 1.000 \end{vmatrix}$$

Where we consider $\Delta t=0.45$

Both $\tau^{dt_{t1}}$ and $\tau^{dt_{t2}}$ are considered as 0.5.

The weight matrix $\widetilde{\vartheta_{t2_{5x5}}}$, generated from equations (16), (17) is

$$\widetilde{\vartheta_{t2_{5x5}}} =$$

$$\begin{vmatrix} 1.000,1.000 & 0.834,0.843 & 0.737,0.778 & 0.797,0.827 & 0.809,0.819 \\ 0.801,0.809 & 1.000,1.000 & 0.838,0.868 & 0.790,0.820 & 0.771,0.801 \\ 0.709,0.750 & 0.828,0.858 & 1.000,1.000 & 0.806,0.814 & 0.757,0.761 \\ 0.705,0.744 & 0.714,0.754 & 0.787,0.793 & 1.000,1.000 & 0.739,0.780 \\ 0.831,0.861 & 0.828,0.834 & 0.759,0.800 & 0.746,0.785 & 1.000,1.000 \end{vmatrix}$$

The indirect trust matrix, generated from equation (17) and (19) is represented as

$$\tilde{\imath}\mathrm{t}_{t2_{5x5}} =$$

$$\begin{vmatrix} 1.000,1.000 & 0.578,0.629 & 0.584,0.635 & 0.576,0.628 & 0.560,0.611 \\ 0.494,0.567 & 1.000,1.000 & 0.508,0.574 & 0.528,0.588 & 0.530,0.584 \\ 0.557,0.607 & 0.567,0.612 & 1.000,1.000 & 0.563,0.616 & 0.558,0.611 \\ 0.557,0.613 & 0.608,0.651 & 0.591,0.644 & 1.000,1.000 & 0.582,0.630 \\ 0.481,0.536 & 0.534,0.588 & 0.548,0.601 & 0.560,0.611 & 1.000,1.000 \end{vmatrix}$$

The weight of direct trust value calculated from equation (22) is represented here with matrix form as

$$\widetilde{\alpha}_{5x5}=$$

$$\begin{vmatrix} 1.000,1.000 & 0.200,0.200 & 0.048,0.048 & 0.262,0.262 & 0.138,0.138 \\ 0.385,0.385 & 1.000,1.000 & 0.219,0.219 & 0.094,0.094 & 0.071,0.071 \\ 0.450,0.450 & 0.300,0.300 & 1.000,1.000 & 0.197,0.197 & 0.051,0.051 \\ 0.463,0.463 & 0.441,0.441 & 0.350,0.350 & 1.000,1.000 & 0.026,0.026 \\ 0.297,0.297 & 0.071,0.071 & 0.283,0.283 & 0.162,0.162 & 1.000,1.000 \end{vmatrix}$$

Using the matrices $\widetilde{dt}_{t2_{5x5}}$, $\widetilde{it}_{t2_{5x5}}$ and $\alpha_{x_i,x_{j(5x5)}}$ at equation (21), we finally generate the interval based communication trust matrix as

$$\widetilde{ct}_{t2_{5x5}} =$$

$$\begin{vmatrix} 1.000,1.000 & 0.596,0.640 & 0.579,0.631 & 0.581,0.635 & 0.568,0.615 \\ 0.536,0.587 & 1.000,1.000 & 0.544,0.609 & 0.533,0.593 & 0.531,0.585 \\ 0.494,0.559 & 0.594,0.643 & 1.000,1.000 & 0.573,0.618 & 0.556,0.607 \\ 0.489,0.554 & 0.529,0.588 & 0.585,0.624 & 1.000,1.000 & 0.580,0.628 \\ 0.535,0.592 & 0.543,0.594 & 0.540,0.600 & 0.549,0.604 & 1.000,1.000 \end{vmatrix}$$

IV. Results and Discussion

Using middle of maxima method on interval based communication trust matrix, we get defuzzified communication trust matrix as

$$ct_{t2_{5x5}} =$$

$$\begin{vmatrix} 1.000 & 0.618 & 0.607 & 0.608 & 0.5915 \\ 0.5615 & 1.000 & 0.563 & 0.563 & 0.558 \\ 0.5265 & 0.6185 & 1.000 & 0.5955 & 0.5815 \\ 0.5215 & 0.5585 & 0.604 & 1.000 & 0.604 \\ 0.5635 & 0.5685 & 0.5765 & 0.5765 & 1.000 \end{vmatrix}$$

Here we consider the threshold trust limit is 0.6 and our source and destination nodes are n_1 *and* n_5 respectively.
Analyzing defuzzified matrix we get for node n_1 maximum communication trust is 0.618 and the most trusted (Except n_1 to n_1, the communication trust as 1) node is n_2 . But from n_2
No such node is there where trust value reaches the threshold limit. So for node n_1 the next trust value is 0.608 the most trusted node is n_4. From n_4 the maximum trust value is 0.604, which satisfies the threshold trust limit and most trusted node is n_5.
So the packet transmission path is $n_1 \rightarrow n_4 \rightarrow n_5$

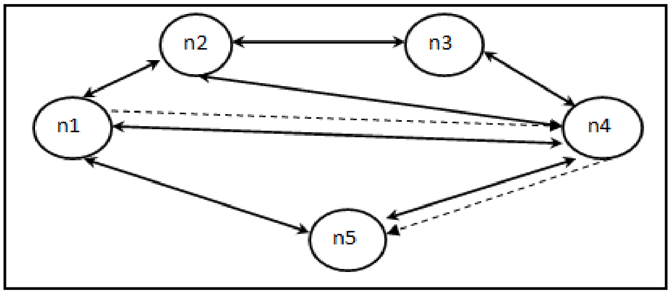

Figure 3. Transmission path.

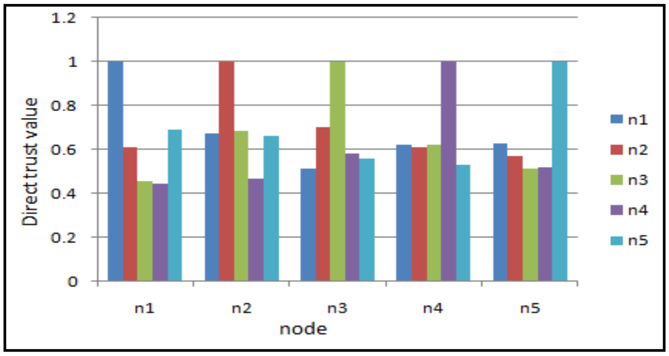

Figure 4. Direct Trust.

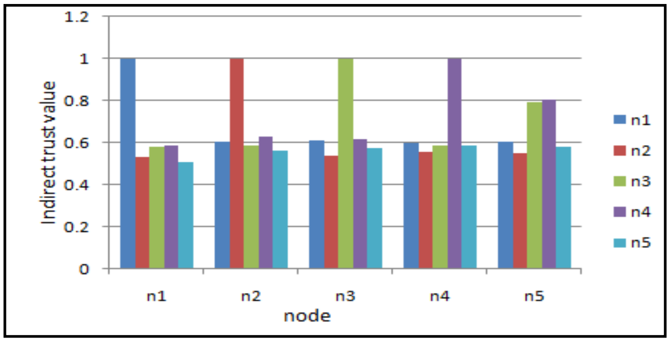

Figure 5. Indirect Trust.

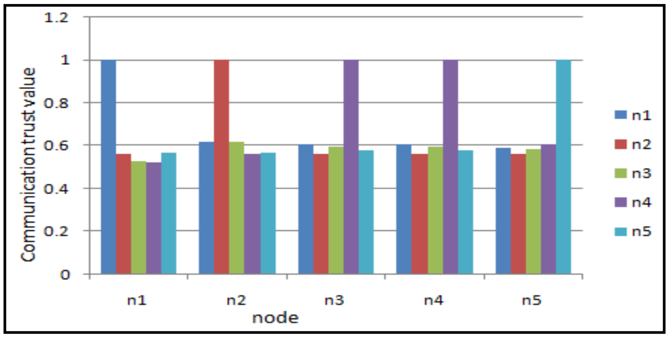

Figure 6. Communication Trust.

V. Conclusion and Future Scope

To transmit data from one node to another node in MANET is one of the significant challenges due to dynamic reconstruction of MANET topology. Trust between two consecutive nodes is an essential factor for secure data transmission from source to destination. Here we represent trust value of any node observed by other one with triangular fuzzy number for depicting the trust evaluation more realistic way in changeable atmospheric condition and in physical obstacles. Using credibility and inverse credibility distribution functions we change the triangular fuzzy trust values in interval based format .Generating communication trust matrix ultimately we get the most secure network path with trusted intermediate nodes to flow data from source to destination node. Here we only try to show the applicability of inverse credibility function on trust value to represent it more realistically. But at changing topological structure variation in trust value between two nodes and according to that reformation of new network path for same source and destination are not discussed here. In future we can work on trust variation process with variable MANET architecture at fuzzy environment.

REFERENCES

[1] V.B.Reddy, S.Venkataraman, A. Negi, "Communication and Data Trust for Wireless Sensor Networks using D-S Theory", IEEE Sensors, Vol. 12, Issue.12, pp.3921 –3929, 2017.

[2] S. Subramaniam, , R. Saravanan, P. K Prakash, "Trust Based Routing to Improve Network Lifetime of Mobile Ad Hoc Networks", Journal of Computing and Information Technology , Vol. 21, Issue.3, pp.149–160, 2013.

[3] G. Dhananjayan, J.Subbiah, "T2AR : trust-aware ad-hoc routing protocol for MANET", SpringerPlus, Vol. 5, Issue.1,pp.1-6,2016.

[4] R.Akbani, T.Korkmaz, G. Raju, " Mobile ad-hoc networks security", In Recent Advances in Computer Science and Information Engineering, Springer Publisher, Berlin, Heidelberg, pp-659–666,2012.

[5] Theodorakopoulos , J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-hoc Networks", IEEE Journal on selected Areas in Communications, Vol. 24, Issue.2, pp.318-328,2016.

[6] J.Sen, "A Distributed Trust Management Framework For Detecting Malicious Packet dropping Nodes In a Mobile Ad Hoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol. 2, Issue.4, pp-92-104,2010.

[7] P. M. Nanaware, S. D. Babar, " Fuzzy Model for Intrusion Detection using Trust System based Bias Minimization & Application Performance Maximization In MANET", International Journal of Computer Applications,pp.6-8,2016.

[8] I.Dokmanic , R. Parhizkar , J. Ranieri , M. Vetterli , "Euclidean Distance Matrices: Essential theory, algorithms, and applications", IEEE Signal Processing Magazine, Vol. 32, Issue.6, pp.12-30, 2015.

[9] S. Bandyopadhyay, S.Karforma,"Improving the Performance of Fuzzy Minimum Spanning Tree based Routing Process through P-Node Fuzzy Multicasting Approach in MANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.6, pp.16-26, 2018.

[10] H. Yang, , H. Luo, F. Ye, S. W. Lu, L. Zhang, " Security in Mobile Ad Hoc Networks: Challenges and Solutions" , IEEE Wireless Communications, Vol. 11, Issue.1, pp. 38-47,2004.

[11] Y. Ren, A. and Boukerche, "A trust-based security system for ubiquitous and pervasive computing environments", Elsevier Journal on Computer Communications, Vol. 31, Issue.18, pp.4343–4351, 2008.

[12] [12] T. Camp, J. Boleng, V. Davies , "A survey of mobility models for ad-hoc network research", Wireless Communications and Mobile Computing (WCMC): Special Issue Mobile Ad Hoc Network, Vol. 2,pp.483–502, 2002.

Authors Profile

Soham Bandyopadhyay is the Lecturer in the Dept. of Computer Science and Technology at Dr.B.C. Roy Polytechnic, Durgapur, India. He received B.TECH in Computer science and Engg. from West Bengal University of Technology, M.TECH from National Institute of Technology(NIT), Durgapur India, MBA in systems from SMU,.His research interests are in the areas of wireless ad-hoc network systems, soft computing, fuzzy logic.

Sunil Karforma is the Associate Professor in the Dept.of Computer Science at The University of Burdwan, West Bengal, India. He received B.TECH and M.TECH in Computer Science and Engineering from Jadavpur University, West Bengal, India. He received his Ph.D from The University of Burdwan, West Bengal, India in Computer Science. His research interests are in the areas of wireless network systems, e-commerce, network security, soft computing.