International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217125

Opinion Based Trust Model for Delay Tolerant Networks using Fuzzy Logic

Santhana Lakshmi M[1], Hemaanand M[2]
[1]IT, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India
[2]ECE, Amrita Vishwa Vidhyapeetam, Coimbatore, Tamil Nadu, India

Article Info
Volume 7, Issue 1
Page Number: 113-130

Publication Issue :
January-February-2021

Article History
Accepted : 25 Jan 2021
Published : 02 Feb 2021

ABSTRACT

Delay Tolerant Network is designed for long distance communication where end-to-end connectivity is not established due to frequent disconnections or delay. Long latency is encountered in this type of network. This work proposes a reliable model for secure communication in DTN that aims to achieve correct estimation of trust value between the nodes and to minimize the relay rate i.e cost involved in the message transmission with minimum delay based on the history of ownership of information. In this model, we have used data driven approach so that the malicious or selfish nodes are prevented from consuming more resources in the resource constrained network environment. This approach checks the trustworthiness of the source of information. This work adopts computing based approach to evaluate the performance of the proposed model using fuzzy logic. We conduct two comparative analyses in which one compares the four variants of the proposed model to find the best variant of the proposed model and other compares our trust model with the other existing trust models to prove the efficiency of our model over other routing protocols.

Keywords: Delay Tolerant Networks, Trustworthiness, Fuzzy logic.

I. INTRODUCTION

Delay Tolerant Network is a type of network that is usually operated in the extreme terrestrial network, smart environment, and planned networks in space. In Delay Tolerant Networks, the nodes are placed far away from each other, and they do not communicate often among themselves. This type of network is used in the extreme terrestrial environment where there is no provision for well-developed network infrastructure. In network environment, one node needs to interact with the other node in order to get the opinion about the former node. This is in case of the encounter-based routing. But in delay tolerant networks the nodes do not encounter with each other often, so direct opinion is always not possible. It leads to high delay. Because of lack of direct opinion collections, it leads to poor performance and inaccurate calculation of trust level.

The main features of DTN are

- Deliberately misconducting nodes.
- Inaccurate trust level calculation.
- No assurance for connectivity of two nodes.
- Poor performance.

It fails to maintain goals like low cost, low delay, QOS factors, etc. In this work we propose a trust model based on history of ownership or origin of message. The main motto of this model is to find the malicious attacker who can modify or drop the packet using fake information. The goals of our model are

1) To minimize trust bias
2) Maximize delivery ratio.
3) Minimize delay.
4) Minimize cost.

Unique Contributions:

- In our model, the characteristics of an intermediate node cannot be collected from the third party. Because collecting this will lead to extra overhead and increase in cost. By using the history of ownership of information, indirect opinion can be collected.
- We provide the opinion about a node based on accessibility, rectitudinous and proficiency of a node.
- We have considered advanced attack conditions such as ID modification attack and Message modification attack. We have used fuzzy logic to evaluate the performance of the proposed trust model for selecting good message carrier.
- We have used four criteria to ensure the reliability of a node.
- We have conducted a comparative analysis to demonstrate the superiority of our model against existing algorithms.

II. EXISTING MODEL

Due to the characteristics of DTN such as high delay or disruption, intentionally misbehaving nodes, inaccurate trust evaluation, lack of end-to-end connectivity some routing models based on flooding and partial flooding approaches such as epidemic[1], PROPHET[2] have been considered. However, these approaches cause network congestion and high resource consumption. To avoid these limitations, researchers have proposed opportunistic routing protocol. E.Ayday and F.Fekri [3] proposed an iterative algorithm for trust Management and adversary detection for delay-tolerant network which includes message passing techniques. This ITRM mechanism is used to decode the parity check codes which are having low density. The decoding mechanisms are done over the bipartite graphs. Here each node gives rating to nearby node based on that rating trust level is calculated. Rating which deviates most from the other nodes is considered as malicious. This model reduces cost and causes large overhead in communication. Y. Zhu, B. Xu, X. Shi, and Y. Wang [4] proposed a survey of social-based routing in delay tolerant networks which categorize social behaviors-based routing features as positive and negative properties. The positive properties will be used to select the message carrier by their social characteristics like friendship, community. The performance of the epidemic routing is degraded by the negative properties such as selfishness of the node. This model reduces the delay and predicts the dynamics of DTN. Due to time varying environment it will be hard to estimate some social characteristics. I.R. Chen, F. Bao, M. Chang, and J.H. Cho [5] proposed a trust management for encounter-based routing in delay tolerant networks. Here Bayesian estimation of trust scheme is used. In this model it will update the encounter rate of the node that has been chosen to leverage the message. It controls the overhead at the time of high traffic and reduces latency time. But multicopy message forwarding is not possible and also the number of replicas of each message is less. U. Lee, S. Y. Oh, K.-W. Lee, and M. Gerla, RelayCast [6] proposed a scalable multicast routing in delay tolerant networks which is used in multicast scenario. Here message carriers have been chosen based on history of mobility patterns called

RelayCast. It reduces the network congestion. In this model inter-contact time between the nodes is high. A.Vahat and D.Becker proposed an epidemic routing for partially connected adhoc networks. In this model, a message is transmitted to whoever it encounters. It is also called flooding because it increases the message delivery ratio. The number of replicas of each message is high when compared to encounter-based routing. It incurs minimum delay for delivering the message to the node. In this model the trustee node is calculated based on probability of delivered messages. M. Musolesi and C. Mascolo [7] proposed a CAR: Context- aware adaptive routing for delay-tolerant mobile networks which uses store and forward mechanism. CAR approach is used for unicast communication. It is the provision of asynchronous communication in DTN. This method gives maximum performance in delivering messages to its destination. It incurs minimum delay for delivering the message to the node and less overhead in communication. The limitation of this model is that only small buffer is available for storage. Costa et al [8] proposed SocialCast, a social based routing protocol. The performance of the epidemic routing is affected by the selfishness behavior of node which has been studied by Li et al. [9] Gao and Cao[10] studied the effectiveness of node selection and cost to maintain network information. Gao et al. [11] proposed M-Dimensions, a multidimensional routing. The author proposed multidimensional routing protocols in DTN for secure message delivery[12]. Abdelkader et al. [13] proposed SGBR, a social group based routing protocol. Li and Shen [14] proposed a distributed utility-based routing protocol, called SEDUM for DTN. Zhu et al.[15] proposed iTrust, a trust based secure protocol. The eigentrust algorithm has been proposed for peer to peer network. [16] The author proposed ITRM protocol in which neighbor nodes provide rating to a trustee node [17]. The works [18], [19], [20], [21], [22], [23] have studied how to protect history of information of nodes. The works [24], [25], [26], [27], [28] focused on evaluating trustworthiness of node. The works [29], [30], [31], [32], [33], [34], [35], [36] proposed how to frame fuzzy rules.

SYSTEM MODEL

We proposed a trust model based on history of ownership of messages for secure communication in DTN environments where trusted members communicate with other nodes by their symmetric key. The key is provided by the trust authority for secure group communication. In Delay Tolerant Networks, a node cannot predict the neighbor node within a short period of time. We classify the opinion in three factors: good, bad and uncertain. When a neighbor node's behavior cannot be properly monitored by a node then it is termed as uncertain opinion. However, the mobility behavior and low contact time cannot be used to predict good or bad opinion. In this case the uncertain opinion is the best choice. In Section 4, we have given four ways to merge good, bad and uncertain opinion in positivism, negativism, practivism and hybrid.

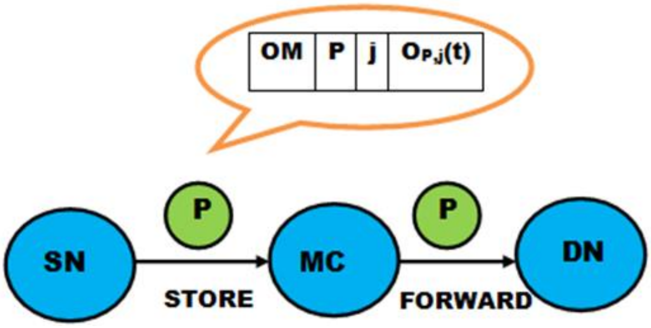

Fig. 1 Diagrammatic representation of System model

In Section 5, we analyze the metrics by their accuracy, bias, correctness, relay rate, delay. A node is able to find trustee node based on their past experience. Each node is delivering the message using store and forward technique. Each node has different speed, lifetime, detection error and behavior seeds. Each node in the network sends the message by attaching its information in the packet. The information about all the nodes through which the message passes is called the history of information (HI). From HI the past behavior of a node can be calculated. Based on behavior, new opinion is calculated.

The packet is composed of two things

(i) Original message (OM)
(ii) History of information (HI)

A. Attack model:

We have considered two possible inside attackers:

- **No/fake identity:** In our model, ID of an intermediate node should be inserted in HI. However, an attacker may insert fake ID or may not add its real ID in HI. If this attack is successful, the attacker's misbehavior may be considered as another node's behavior, leading to incorrect trust evaluation.
- **Message Modification:** A legitimate node with a symmetric key may modify OM. To prevent HI modification by other nodes we use HI encryption key, hashing. In section 6, our trust protocol uses three dimensions to find a node's behavior in packet routing. A malicious node with less trust will be penalized with isolation. In proposed model, a node with trust lower than the threshold will not be selected as an MC, practically isolating it from participating in packet routing activities.

B. Packet format:

HI Composed of **p, j, Op,j(t)**

History of information

OM	P	J	O $_{p,j}$(t)

p - Sender id

j - Previous MC's id

Op,j(t) - **p**'s direct opinion about attack behavior of **j** at time t. We denote **(p, j, Op,j(t))** as **H$_{p,j}$** representing the History of Information (**HI**) provided by **p** with its direct trust opinion towards previous MC ' **j**'.

$$\left[OM(H_0,\phi)_{k_n},(H_1,0)_{k_{n-1}},(P_2,1)_{k_{n-2}}\ldots P(m,m-1)_{k_{n-m}}\right]_{k_{s,t}} \quad (1)$$

The intermediate message carriers transmit the message to the next message carrier after encryption. This is continued until the destination node is reached. After the destination node receives the encrypted message it decrypts the message with the key received from TA in order to find the original message. The encryption of the message prevents the inside attackers only. The opinion is given to the MC by their neighbor MC based on the past experience and attack behavior exhibited by that MC. The opinion is categorized as good, bad and uncertain. The good opinion is given to the node only if it does not exhibit any attack behavior and performs good routing else node is given the bad opinion.

PROPOSED MODEL

The source and the destination node request the key from the trusted authority as shown in fig. 2. The trusted authority maintains the key required for transmission of messages. The trusted authority (TA) will give the key to source node and the destination followed by their request. The source node and the destination node store the key send by the TA. The source node finds the next MC and checks the trust value of that MC. After checking the trust of that node it will check three dimensions like accessibility, rectitudinous and proficiency. The next step is to update the new opinion for that node. After updating the opinion trust factors like trust bias, relay rate, delay and the message correctness are evaluated for the particular node. This step is continued for each node until the message reaches the destination node. Each MC's trust can be evaluated based on accessibility, rectitudinous, proficiency and other trust determining factors.

Trust Measurements:

Each node's trust level is evaluated by using three trust measurements:

- **Accessibility:** It refers to accessibility of a node, which depends on the network or condition of nodes such as resource availability, service request, movability and clogging.
- **Rectitudinous**: It refers to the capacity of the node not to change or modify the message passed to it, also refers the honesty of the node which can be measured by checking the correctness of the message.
- **Proficiency**: It refers to a node's remaining energy status in battery life and cooperativeness behavior. Here energy represents the capacity of the node to the basic routing function and cooperativeness behavior refers to reliable delivery of packets so that the received requests can be served.

These trust measures will be evaluated dynamically. In the network, the accessibility of the node is less, if it runs to congestion condition and the node will regain it's accessibility trust after the congestion is cleared.

B. Trust Estimation

The trust estimation among the nodes is based on the amount of good opinion **g**, amount of bad opinion **b** and unsure opinion **u** about the nodes which can be estimated by either direct opinion collection or by indirect collection using the history of information which is attached to the messages itself during message delivery. The trust value of the node can be calculated by using $\frac{g}{g+b}$. Initially the g and s will be initialized with the value 1(i.e) g=1 and b=1 thus the trust value will be 0.5.

The trust value is calculated based on both past and new opinion. The two nodes do not often encounter with each other in delay tolerant network, so new opinion may not be available. In case of absence of direct opinion, indirect opinion is considered based on Bayesian update. The direct opinion is detected when one node interacts with another node, where as indirect opinion is collected from the destination when it receives the HI which is embedded with the mission message. It is based on the assumption that the two nodes can observe one another during their encounter period. Because of distrust or unreliable link or due to short contact time, it is not always possible to survey other node. This will lead to uncertainty in evidence collection. This can be avoided by using HI. In addition to this, when the node receives the message which contains the HI embedded in it, if the indirect trust opinion embedded in the **HI** is found as false, the opinion will not be used. Because the correct opinion is not available in this interval, this is considered as uncertain opinion. We have denoted the amount of uncertain opinion as '**u**'. In this, we have evaluated the effect of uncertainty as trust bias (i.e, the difference between measured and ground trust value) by forming four variants as positivism, negativism, practivism and hybrid. In this we have used the notation '**p**' to refer a trustor and **'q'** refers to a trustee.

Here we have discussed how to calculate four variants based on negative, positive and uncertain opinion.

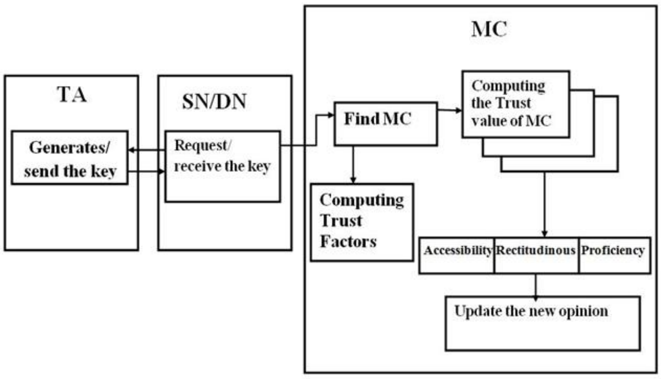

Fig. 2: Flow Chart for Proposed Model

Negativism:

It treats uncertainty as negative opinion in case of no correct evidence is available. The trust value is computed by

$$T_{p,q}^{neg} = \frac{g_{p,q} + g'_{p,q}}{g_{p,q} + b_{p,q} + u_{p,q} + g'_{p,q} + b'_{p,q} + u'_{p,q}} \quad \textbf{(2)}$$

$g_{p,q}$, $b_{p,q}$ and $u_{p,q}$ are the amount of good, bad and uncertain opinion that are interpreted from the past respectively. $g'_{p,q}$, $b'_{p,q}$ and $u'_{p,q}$ are the amount of new good, bad and uncertain opinion respectively which are obtained based on either from direct and indirect opinion. In this method, the uncertain opinion is considered as bad opinion. $g'_{p,q}$, $b'_{p,q}$ and $u'_{p,q}$ are computed in terms of direct and indirect opinion which is explained in section c.

Positivism:

Positivism treats uncertainty as good opinion based on the nature of trusting more. The trust value is computed by

$$T_{p,q}^{posi} = \frac{g_{p,q} + u_{p,q} + g'_{p,q} + u'_{p,q}}{g_{p,q} + b_{p,q} + u_{p,q} + g'_{p,q} + b'_{p,q} + u'_{p,q}} \quad (3)$$

In positivism, the probability of a node for transmitting the message is high because uncertainty is taken as positive opinion so trusting the node and passing the message is high.

In the above two calculation, the uncertainty is used for the calculation of trust value.

Practivism:

In practivism, uncertainty is not considered for trust calculation. The trust calculation is only based on opinion that is available during that time. The trust can be calculated as follows,

$$T_{p,q}^{prac} = \frac{g_{p,q} + g'_{p,q}}{g_{p,q} + b_{p,q} + g'_{p,q} + b'_{p,q}} \quad (4)$$

In practivism, it will not update the trust if the new opinion is not available.

Hybrid:

By using the above three schemes, hybrid method is proposed in which the uncertain opinion is dealt based on historical patterns on the amount of evidence. It is computed as

$$T_{p,q}^{hyb} = \begin{cases} T_{p,q}^{neg} if\,(g_{p,q} < b_{p,q}) \\ T_{p,q}^{pos} if\,(g_{p,q} > b_{p,q}) \\ T_{p,q}^{prac} if\,(g_{p,q} == b_{p,q}) \end{cases} \quad (5)$$

Thus, the trust calculated depends on the ratio of amount of good and bad opinion based on the trust estimation using positivism, negativism and practivism. The node p will entirely depend on direct observation towards node q' s behavior to collect new opinion at time t during their encounter. The indirect trust evaluation can be done only when node p is a DN. The node p will depend on the original message to calculate the trust of the node q.

Trust Calculation:

In the below section, we discuss how to calculate the value of trust for each trust property based on either direct opinion or indirect opinion.

Direct Opinion:

The new opinion $g'_{p,q}$, $b'_{p,q}$ and $u'_{p,q}$ is computed based on direct opinion when the two nodes p and q encounter each other. The direct trust value is computed as follows:

Direct Accessibility trust:

It is calculated by whether a node is available in the network truly to transmit the message to ensure connectivity. Accessibility of a node can be checked by examining any MC in the network having ID specified in the HI. If MC is having ID specified in HI then $g'_{p,q}$, $b'_{p,q}$ and $u'_{p,q}$ is set as (1, 0, 0) else (0, 1, 0).

Direct Rectitudinous trust:

It is calculated based on the attacks exhibited by MC

- Identity attack
- Message Modification attack.

Identity attack is checked by examining the ID specified in HI. The malicious MC can modify or use fake ID to deliver the message.

Message Modification attack is identified by examining whether the original message sent by source and the message passed to next MC is the same or not.

To avoid these attacks, the source and the destination obtain a same pair of keys from trusted authority (TA). Source node encrypts the message using key and generates key1=F (key). Source node dictates the next MC to use key1 for encrypting the message. This process continues until the message reaches the destination node. A MC does not know the HI of the previous MC's HI encryption key. So, it cannot decrypt the HI of the previous MC. When the DN receives the message, it can check the message using the key received from trusted authority. DN can properly decrypt all HIs by tracking back the chain of symmetric keys, if there is no modification of keys occurs along the path. Each exhibiting attack behavior is counted as opinion, resulting in ($g'_{p,q} + b'_{p,q} + u'_{p,q}$) = 3. If any of the attack is exhibited by the MC, the opinion is given based on the severity of the attack. The uncertain opinion is set when the MC is not in the range of next MC. For secure delivery of messages MD5 hashing algorithm is used.

Direct Proficiency trust:

It is accessed by the MC's energy status and cooperativeness behavior and is measured based on two pieces of opinion with $g'_{p,q} + b'_{p,q} + u'_{p,q} = 2$. Energy represents the remaining lifetime of the node to do the basic routing function. Cooperativeness behavior is estimated by the behavior of correct delivery of messages to other MC or destination. The node p will not monitor if q has forwarded a packet since it is impractical to monitor packet forwarding. If node q is not available within the range of p, uncertain opinion is given (i.e) ($g'_{p,q}$, $b'_{p,q}$, $u'_{p,q}$) = (0, 0, 2). The good opinion is given to the nodes having high life time and good cooperativeness behavior.

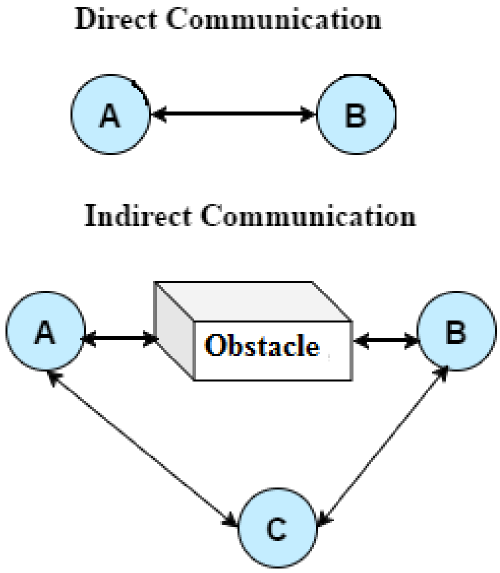

Fig 3: Direct and indirect opinion collection between A and B

Indirect Opinion:

When nodes p and q are far away from each other without any direct communication, if the node q is the destination node, it will rely on HI passed along with the delivered mission message in order to derive indirect opinion. Here indirect accessibility, rectitudinous and proficiency is calculated as follows:

Indirect Accessibility trust:

It is calculated based on the algorithm given below:

Algorithm for Indirect Accessibility Trust Calculation

```
Input (Msg (MM,HI))
    if p's id in HI
        if p's id = p's id in next MC
            TrustMC = Calculate_trustI(PreviousMC)
            if  TrustMC > Tmin Then
                (g'p,q, b'p,q, u'p,q) is set as (1,0,0)
            else
                (0,1,0)
        else
            Discard
    else
        (0,0,1)
```

Indirect Rectitudinous trust:

It is estimated based on whether it encounters attacks such as ID modification and message modification. It is calculated in the same way as the direct rectitudinous trust, but the trust of each MC will be checked against trust threshold. If it is greater than the threshold it is given good opinion otherwise it is given the bad opinion. Based on the opinion, trust will be given to each MC.

Indirect Proficiency trust:

It is estimated based on remaining energy status and cooperativeness behavior. It is calculated similar to direct Proficiency trust, but the trust value is checked against the trust threshold as in indirect rectitudinous trust calculation.

III. INVESTIGATION OF EXPERIMENTAL OUTCOMES

Here we have used various trust factors and other baseline schemes against which the proposed model is compared, and the results obtained from this are used for analysis purpose.

A. Factors:

Here we have used various factors such as trust to evaluate the performance of the proposed model.

Trust Bias:

It is calculated by the difference between the trust of node '**q**' evaluated by the other node '**p**' at time **'t'** and the trust value of node '**q**' evaluated by all other nodes that encounter it along the path in time 't' which is averaged against the entire session time. The trust calculation is based on both good and bad opinion. Here N is the set of authorized or approved nodes in the network. The aggregated trust bias is calculated as follows.

$$T_B = \frac{\sum_{t=0}^{NT} T_B(t)}{LT} \tag{6}$$

TB (t) is calculated by

$$T_B(t) = \frac{\sum_{p,q\in N, p\neq q} | T_q^R(t) - T_{p,q}^R(t) |}{(| N | -1)^2} \tag{7}$$

Here $T_q^R(t)$ is the overall truth value of node **'q'** which is determined by all nodes in the path by direct opinion at **'t'**. $T_{p,q}^R(t)$ is the trust of node **'q'** evaluated by node **'p'** at time **'t'** in the property R.

$$T_p^R(t) = \frac{g_q^R(t)}{g_q^R(t) + b_q^R(t)} \tag{8}$$

Here $g_q^R(t)$ and $b_q^R(t)$ are the gathered good and bad opinion until time t.

Message Correctness (X):
It refers to the ratio of no of packets that reaches the destination node correctly over the total no of messages that are transmitted from the source node during the session time NT. The correctness of the message received by the DN is affected by the honesty or truthfulness of the intermediate MC. The message correctness is calculated by

$$X = \frac{\sum_{m\in M} \prod_{y\in Y} X_{y,m}(t)}{|M|} \tag{9}$$

$$X_{y,m}(t) = \begin{cases} 1 \text{ if MC } y \text{ did not modify } m \\ 0\, otherwise. \end{cases}$$

Delay (D):
It denotes the average time for the message to be delivered from the source node to the destination node. It is calculated by

$$D = \sum_{m\in M} \frac{D_m}{|M|} \tag{10}$$

Here the time taken for the message m to be received by the destination node is denoted as Dm and the set of the message to be sent from the source node to the destination node is denoted by M.
Relay rate (C):

It refers to the cost involved in the transmission of the message from the source node to the destination node. It is calculated in terms of number of messages associated with trust calculation E(t) and the cost for the delivery of message from SN to DN F(t) for the whole session time. It is computed using

$$C = \frac{\sum_{t=0}^{NT} E(t) + F(t)}{NT} \tag{11}$$

B. Comparison of Trust Bias:

In this section, Trust bias for a node is evaluated based on accessibility, rectitudinous and proficiency for four variants of the proposed model.

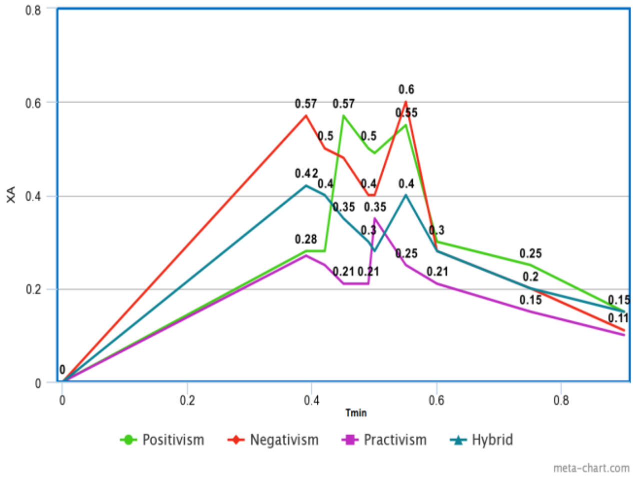

Fig. 4: Accessibility Trust Bias

The figure 4 shows the trust bias introduced by measuring accessibility plotted against the corresponding trust threshold of a node for Hybrid, Negativism, Positivism and Practivism. It shows that practivism has less trust bias followed by hybrid in accessibility than other three variants because the difference between ground trust value and measured trust value is less in practivism. Trust bias should be low for nodes that does not exhibit any attack behaviors.

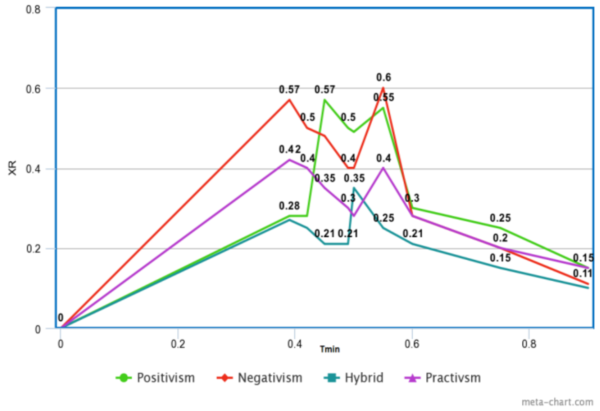

Fig. 5: Rectitudinous trust bias

The figure 5 shows the trust bias introduced by measuring rectitudinous plotted against the corresponding trust threshold of a node for Hybrid, Negativism, Positivism and Practivism. It shows that hybrid has less trust bias followed by practivism. Negativism and practivism has high difference between ground trust value and measured trust value so their bias is high.

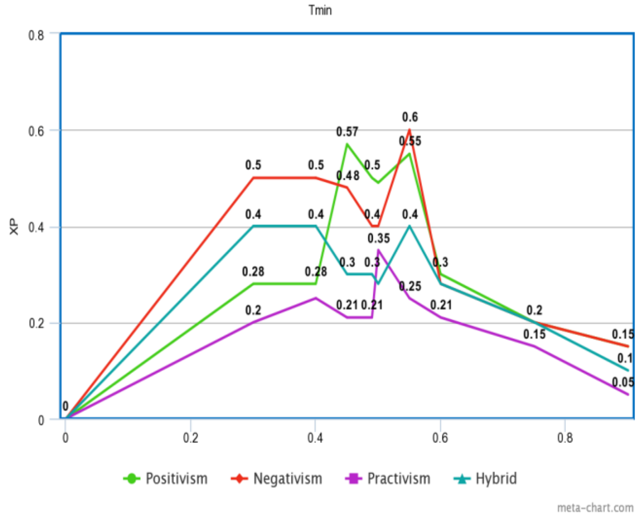

Fig. 6: Proficiency Trust Bias

The figure 6 shows the trust bias introduced by measuring proficiency plotted against the corresponding trust threshold of a node for Hybrid, Negativism, Positivism and Practivism. It shows that hybrid has less trust bias next to practivism.

C. Performance Comparison of Proposed Model:

In this section, we have compared all the four trust variants of the proposed model based on message correctness, Delay and Relay cost.

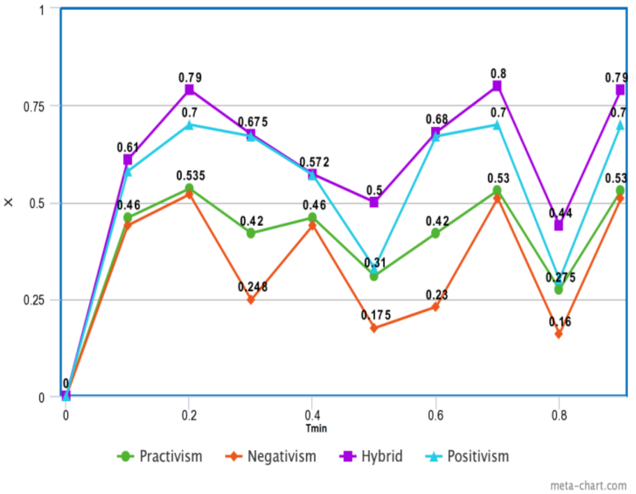

Fig. 7 Message Correctness

From figure 7, it is interpreted that the hybrid has the highest ratio of delivering the packet correctly to the destination node when compared to other variants because it takes the best of other three variants. The Negativism takes the uncertain opinion as bad opinion. So it ignores the node whose opinion is uncertain. This is the reason for less delivery ratio in Negativism. The positivism takes uncertain opinion as the positive one and it will trust the node more and send the message.

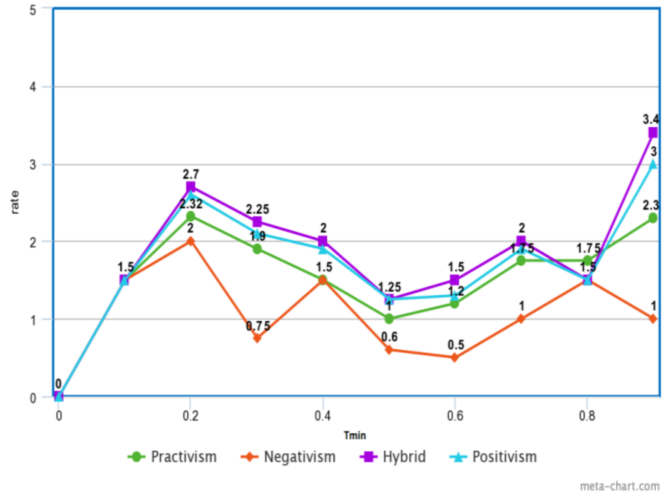

Fig. 8 Relay Rate

In figure 8, we compare the relay rate for the four variants. It is found that the relay rate of negativism is less among the other three variants. It is followed by practivism and positivism. The hybrid has highest relay rate. This is because; increase message delivery ration will lead to increase in relay rate. Here negativism has lowest relay rate because it will not trust most nodes so message delivery ratio is low.

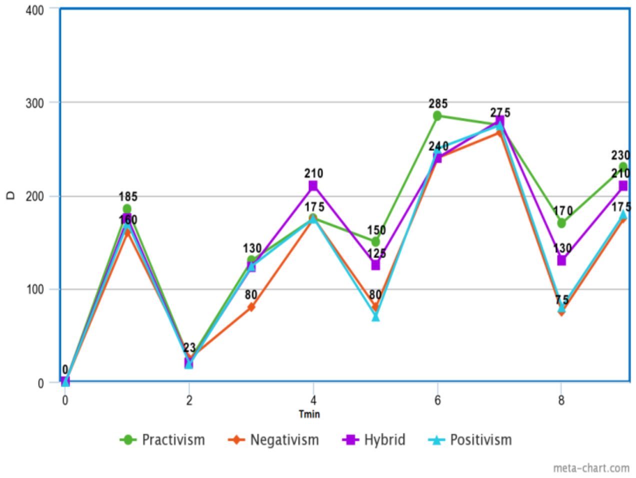

Fig. 9. Delay

In figure 9, we compare the delay for the message delivery for our proposed model. Here positivism performs well because uncertain opinion is taken as positive so the underestimated has the chance to deliver the messages quickly.

IV. PERFORMANCE ANALYSIS USING FUZZY LOGIC

We have analysed the performance of our proposed model using fuzzy logic. In this we have used four membership functions such as trust bias, relay rate and trust threshold and distance between the source and destination i.e. the location of the node to evaluate the performance of positivism, negativism, practivism and hybrid. The defuzzified value is plotted in the form of the graph for analysis of the proposed model. The inputs for the fuzzification function are trust bias, trust threshold, relay rate and location of nodes of each node. We have used center of gravity method for fuzzification. After fuzzification, defuzzification is done. The value obtained after defuzzification is plotted as the graph for analytic purpose. In the rule block, we have considered trust as the most important criteria. If the trust is low, the performance will low. If trust is not low, the other factors will be considered for analyzing the performance. We have chosen relay rate as one of the inputs for analysis because relay rate is one of the main factors in determining the performance of the network in resource constrained environment. Here distance also places a major role because if two nodes are within the range of contact, they can participate in direct communication. If they are not then, they have to go for other option indirect communication. This leads to extra overhead like high cost and increase in delay. The table 1 shows how fuzzy rules are formulated based on four factors to analyze the performance of four variants such as positivism, negativism, practivism and hybrid.

Table 1: Rule Block for Fuzzy Logic

Bias	Cost	Trust	Distance	Performance
Low	Cheap	Min	Near	Bad
Low	Cheap	Medium	Near	Ok
Low	Cheap	Max	Near	Good
Low	Moderate	Min	Near	Bad
Low	Moderate	Medium	Near	Ok
Low	Moderate	Max	Near	Good
Low	Expensive	Min	Near	Bad
Low	Expensive	Medium	Near	Bad
Low	Expensive	Max	Near	Good
Medium	Cheap	Min	Near	Bad
Medium	Cheap	Medium	Near	Ok
Medium	Cheap	Max	Near	Good
Medium	Moderate	Min	Near	Bad
Medium	Moderate	Medium	Near	Bad
Medium	Moderate	Max	Near	Good
Medium	Expensive	Min	Near	Bad
Medium	Expensive	Medium	Near	Bad
Medium	Expensive	Max	Near	Ok
High	Cheap	Min	Near	Bad
High	Cheap	Medium	Near	Bad
High	Cheap	Max	Near	Good
High	Moderate	Min	Near	Bad
High	Moderate	Medium	Near	Ok

High	Moderate	Max	Near	Ok
High	Expensive	Min	Near	Bad
High	Expensive	Medium	Near	Bad
High	Expensive	Max	Near	Bad
Low	Cheap	Min	Far	Bad
Low	Cheap	Medium	Far	Ok
Low	Cheap	Max	Far	Good
Low	Moderate	Min	Far	Bad
Low	Moderate	Medium	Far	Ok
Low	Moderate	Max	Far	Good
Low	Expensive	Min	Far	Bad
Low	Expensive	Medium	Far	Bad
Low	Expensive	Max	Far	Good
Medium	Cheap	Min	Far	Bad
Medium	Cheap	Medium	Far	Ok
Medium	Cheap	Max	Far	Good
Medium	Moderate	Min	Far	Bad
Medium	Moderate	Medium	Far	Bad
Medium	Moderate	Max	Far	Good
Medium	Expensive	Min	Far	Bad
Medium	Expensive	Medium	Far	Bad
Medium	Expensive	Max	Far	Ok
High	Cheap	Min	Far	Bad
High	Cheap	Medium	Far	Bad
High	Cheap	Max	Far	Good
High	Moderate	Min	Far	Bad
High	Moderate	Medium	Far	Ok
High	Moderate	Max	Far	Ok
High	Expensive	Min	Far	Bad
High	Expensive	Medium	Far	Bad
High	Expensive	Max	Far	Bad

During fuzzification, the bias is defined as low if the value is between 0 and 0.3. It is medium if it ranges between 0.3 and 0.6. It is high if it is between 0.6 and 1. Figure 9 shows the membership function for trust bias B(x).

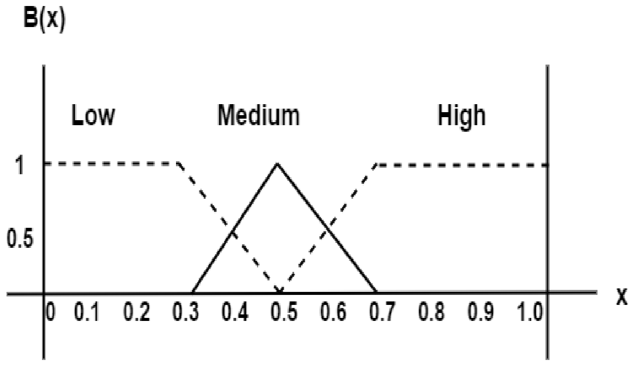

Fig. 9 Membership Function for Bias

Figure 10 shows the membership function for relay rate. It is cheap when it ranges between 0 and 15 and it is moderate if it ranges between 15 and 35 and expensive if it is above 35.

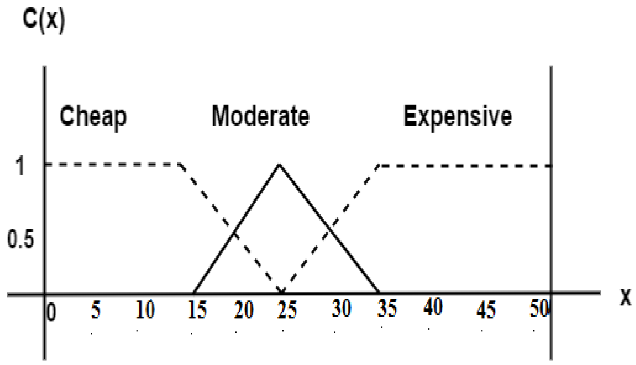

Fig. 10 Membership Function for Relay Rate

Likewise, if the trust is between 0 and 0.3 it is minimum and if it is between 0.3 and 0.6 it is medium and if between 0.6 and 0.9 it is termed maximum. Figure 11 depicts the membership function for trust.

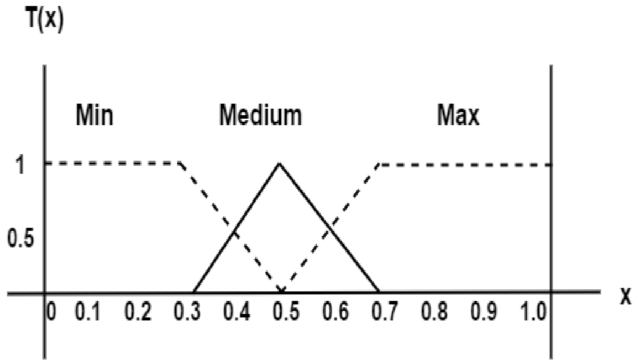

Fig. 11 Membership Function for Trust

Figure 12 shows the membership function for distance. If the distance between two nodes is in the range of 0 to 40 units it is near or else it is far.

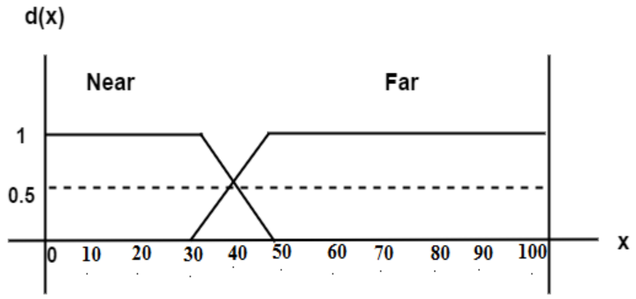

Fig. 12 Membership Function for distance

During defuzzification we define the value 0 to 0.3 if the performance is bad, OK as 0.3 to 0.6 and 0.6 to 1.0 for good performance.

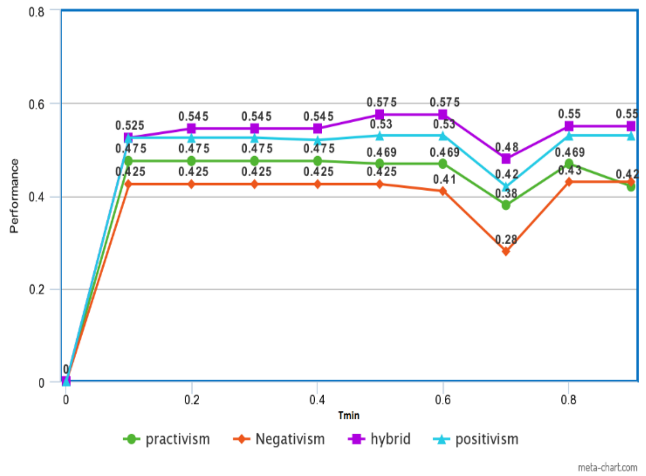

Fig. 13 Performance of proposed model using Fuzzy

Figure 13 is obtained after applying defuzzification process. From the graph, it is shown that performance of the hybrid and positivism is better when compared to negativism and practivism. This is because in hybrid, we have taken the best of other three methods and in positivism, the uncertainty is taken as good opinion. So, trusting the node and the delivering the messages is high. The lowest point in the graph shows that the malicious nodes hinder the performance of the network when compared to good nodes. Message delivery in hybrid is high when compared to Negativism because uncertainty of a node is considered as bad opinion. So, the trust of node is almost bad in negativism. It will decrease the message delivery ratio.

Table 2 : Design Parameters and Their Meanings

Notation	**Meaning**
NT	Lifetime of a node
SN	Source node
DN	Destination node
N	Number of legitimate node
Ks,t	Symmetric key is given by trusted authority
MC	Message Carrier i.e The node in between SN and DN
Tmin	Trust threshold
HI	History of information about the past node
Hi,k	HI provided by the node i with the opinion of previous MC k.
$T_q^R(t)$	Trust value of node q on trust metrics X at time t
$T_{p,q}^R(t)$	Overall trust value of node q assess by node p for trust metrics X at time t
$g_{p,q}$, $b_{p,q}$	Number of good and bad opinion towards q assessed by p
k	Number of MC involved for message delivery
T_p^{enc}	Time taken for node pto encounter node q
C	Communication cost also called relay rate to deal with E(t) and F(t) during NT
OM	Original Message
E(t)	Cost of trust evaluation.
F(t)	Cost of message delivery
X	Number of packets accurately received by DNs over number of messages transmitted by SNs during NT
D	Delay incurred for a message during NT
Dm	Delay obtain for message m to deliver to a
DN M	Total number of messages
Op,j(t)	P's direct opinion about attack behaviour of j at time t
TA	Trust authority

V. COMPARATIVE ANALYSIS

In this section, we have compared our proposed model with other existing models such as PRoPHET, encounter-based and epidemic based on message correctness, Delay and Relay cost.

Figure 14 shows the comparative analysis based on message correctness. Here our proposed model has the highest probability of delivering the correct messages from source to destination followed by encounter based. The epidemic has the least role in delivering the correct message. This is because the epidemic will pass the message to whoever it encounters so the malicious node may drop the message. Hybrid has the capacity to pass maximum number of correct messages over the network,

when compared to other routing protocols.

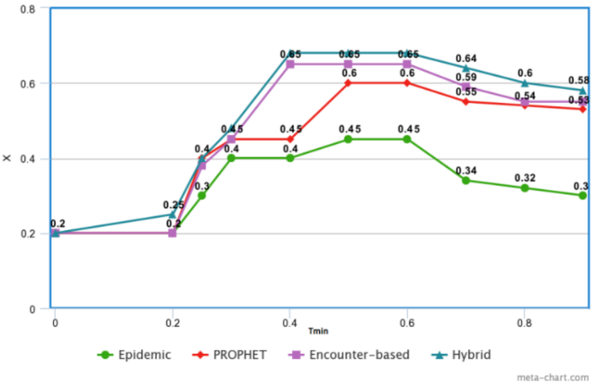

Fig. 14 Message Correctness

The figure 15 shows the comparative analysis based on relay rate. Here hybrid has the lowest relay rate for transmission of messages. This is because it will pass the message only to the trusted node, so the dropping of messages is reduced. It does not depend upon direct encounter for opinion collection. Here epidemic has the highest cost for delivery because the number of copies of message is high.

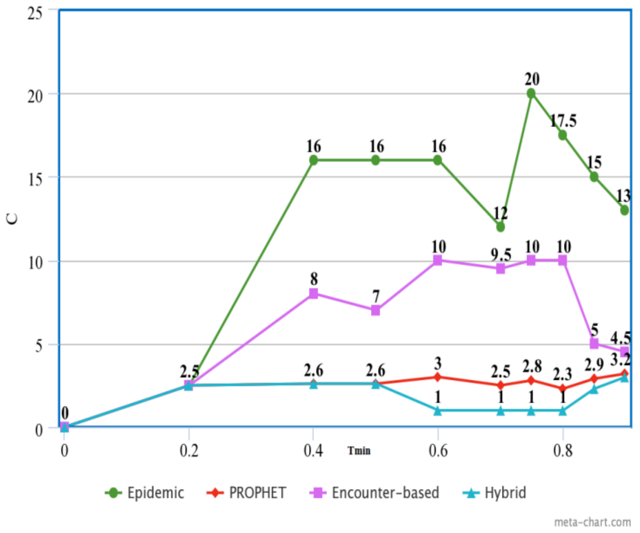

Fig. 15 Relay rate

Figure 16 shows the comparative analysis based on the delay incurred for the delivery of messages from the source node to the destination node. Here epidemic has the lowest delay time. This happens because in epidemic, it will send the message to whoever it encounters; this causes the message to be delivered to the destination quickly. It is followed by encounter-based, PRoPHet, and hybrid. Hybrid incurs high delay because it will transmit the messages only to the trusted member.

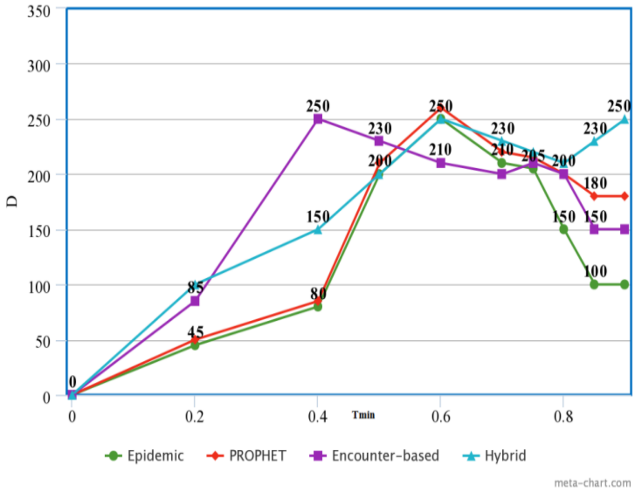

Fig.16 Delay

From this analysis it is shown that hybrid performs better than other three routing models

VI. EXPERIMENTAL SETUP

We conducted simulation using Java programming language based on the data obtained from ONE simulator. In this, we have used the table 3 for defining the default values for the parameters used in the experiment. We use 104 nodes i.e n=104. In this, each node communicates with the other node within the coverage area of 100m. The speed of each node is between 7 to 10 km/hr. We use the wkt file for describing the movement of nodes and for assigning other values. Here we use one event generator. We use Message event generator as the class of the first event generator. We have selected 25 to 35 seconds as the creation interval for one new message i.e one new message is created for every 25 to 35 seconds. We have defined 500 KB to 1 MB as the message size. The range of message source or destination address is between 0 to 126. We have used 1 as the seed for the movement model's pseudo random number generator. The world size for the Movement model without implicit size is 4500 width and 3400 height. The time to move hosts in the world before real simulation is 1000 ms. We have used 4 map files for road, main roads, pedestrian paths and shops.

The length of the warm-up period in simulated seconds is set to 0. The granularity for energy level report is set to 1. The number of nodes we have used for energy level report ie n=104. We have used 5% of the total nodes as the malicious node. If the message is passed to one of the malicious nodes it may perform ID modification attack or message modification attack on that message with probability p_f. Based on the probability of attack intensity the malicious node will perform attack on the received message if it is selected as message carrier. If the malicious node is selected as the message carrier it will provide the fake opinion towards the previous message carrier. It will cause the reputation of good message carrier to be decreased to bad message carrier and the bad message carrier's reputation is increased to good message carrier. Thus decreasing the delivery probability of correct messages from source node to destination node.

Table 3: Key Default Design Parameter Values

Parameter	**Values**
|N|	5, 10, 15
Tmin	0 – 1.0
M	50,100
NT	99,000 sec
Speed	[1 – 15] m/s
Recharge Energy	3000
Random Energy	0 – 1000
Scan Energy	0.92,1
Transmit Energy	0.08
Receive Energy	0.08
Wait time	10 – 30
Granularity	100

VII. CONCLUSION AND FUTURE WORK

In this work, we have proposed a trust model, which evaluates the trust value of the previous message carrier. It is based on the history of ownership of information which is collected through indirect opinion collection during message transmission. This is done by the intermediate message carriers between the source and destination nodes. In this model we have designed four variants practivism, negativism, positivism and hybrid. The negativism, positivism deals with the unavailability and uncertainty of evidence. The hybrid method integrates the advantages of both positivism and negativism by using history of information. This is extremely useful in case of bad nodes when the opinion available is uncertain. We used fuzzy logic to analyze the performance of proposed model in order to find the best among the four variants. We compared the performance of our proposed model with other existing models like PRoPHET [2], Epidemic [1] and Encounter-based [5]. Our history of information-based approach reduces relay rate, delay and increases the fraction of delivery of correct messages when compared to Epidemic, PRoPHET and Encounter-based.

In future work, we planned to identify and control outsider attack and further decreasing delay and relay rate for passing the message and to increase the ratio of delivery of correct message to be delivered from source to destination.

VIII. REFERENCES

[1]. A. Vahdat and D. Becker, “Epidemic routing for partially connected ad hoc networks,” Duke Univ., Durham, NC, Tech. Rep. CS-200006, 2000.

[2]. A. Lindgren, A. Doria, O. Schelen, “Probabilistic routing in intermittently connected networks,” ACM SIGMOBILE Mobile Comput. Com- mun. Rev., vol. 7, no. 3, pp. 19–20, Jul. 2003.

[3]. E. Ayday and F. Fekri, “An iterative algorithm for trust management and adversary detection for delay-tolerant networks,” IEEE Trans. Mobile Comput., vol. 11, no. 9, pp. 1514–1531, Sep. 2012.

[4]. Y. Zhu, B. Xu, X. Shi, and Y. Wang, “A survey of social-based routing in delay tolerant networks: Positive and negative social effects,” IEEE Commun. Surv. Tuts., vol. 15, no. 1, pp. 387–401, Jan.-Mar. 2013.

[5]. I.-R. Chen, F.Bao, M. Chang, and J.-H. Cho, “Trust management for encounter-based routing in delay tolerant networks,” in Proc. IEEE Global Telecommun. Conf., 6-10 Dec. 2010, pp. 1–6.

[6]. U. Lee, S. Y. Oh, K.-W. Lee, and M. Gerla, “RelayCast: Scalable multicast routing in delay tolerant networks,” in Proc. IEEE Int. Conf. Netw. Protocols, 2008, pp. 218–227.

[7]. M. Musolesi and C. Mascolo, “CAR: Context-aware adaptive rout- ing for delay-tolerant mobile networks,” IEEE Trans. Mobile Comput., vol. 8, no. 2, pp. 246–260, Feb. 2009.

[8]. P. Costa, C. Mascolo, M. Musolesi, and G. Picco, “Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks,” IEEE J. Sel. Areas Commun., vol. 26, no. 5, pp. 748–760, Jun. 2008.

[9]. Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, “Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks,” IEEE Commun. Lett., vol. 24, no. 12, pp. 2472–2481, Nov. 2010.

[10]. W. Gao and G. Cao, “User-centric data dissemination in disrup- tion tolerant networks,” in Proc. IEEE INFOCOM, 10-15 Apr. 2011, pp. 3119–3127.

[11]. L. Gao, M. Li, A. Bonti, W. Zhou, and S. Yu, “Multidimensional routing protocol in human-associated delay-tolerant networks,” IEEE Trans. Mobile Comput., vol. 12, no. 11, pp. 2132–2144, Nov. 2013.

[12]. Y. Wang, W.-S. Yang, and J. Wu, “Analysis of a hypercube-based social feature multipath routing in delay tolerant networks,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1706–1716, Sep. 2013.

[13]. T.Abdelkader, K. Naik, A.Nayak, N. Goel, and V. Srivastava,“ SGBR: A routing protocol for delay tolerant networks using social grouping,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 12, pp. 2472–2481, Dec. 2013.

[14]. Z. Li and H. Shen, “SEDUM: Exploiting social networks in utilitybased distributed routing for DTNs,” IEEE Trans. Comput., vol. 62, no. 1, pp. 83–97, Jan. 2013.

[15]. H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, “A probabilistic mis- behavior detection scheme toward efficient trust establishment in delay-tolerant networks,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.

[16]. S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The eigentrust algorithm for reputation

management in P2P networks," in Proc. 12th Int. Conf. World Wide Web, 2003, pp. 640–651.

[17].S. Buchegger and J. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in Proc. 2nd Workshop Econ. Peer-to- Peer Syst., 2004, pp. 1–11

[18].R. Hasan, R. Sion, and M. Winslett, "Introducing secure prove- nance: Problems and challenges," in Proc. ACM Workshop ACM Workshop Storage Security Survivability, 2007, pp. 13–18.

[19].U. Braun, A. Shinnar, and M. Seltzer, "Securing provenance," in Proc. 3rd Conf. Hot Topics Security, 2008, pp. 1–5.

[20].R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in Proc. 7th Conf. File Storage Technol., 2009, pp. 1–14.

[21].X. Wang, K. Zeng, K. Govindan, and P. Mohapatra, "Chaining for securing data provenance indistribute dinformation networks,"inProc. IEEE Mil. Commun. Conf., 2012, pp. 1–6.

[22].L. Gadelha and M. Mattoso, "Kairos: An architecture for securing authorship and temporal information of provenance data in gridenabled workflow management systems," in Proc. IEEE 4th Int. Conf. eSci., 2009, pp. 597–602.

[23].R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[24].S. Rajbhandari, I. Wootten, A. Ali, and O. Rana, "Evaluating provenance-based trust for scientific workflows," in Proc. 6th IEEE Int. Symp. Cluster Comput. Grid, vol. 1, 16-19 May 2006, pp. 365–372.

[25].E. Bertino, C. Dai, D. Lin, and M. Kantarcioglu, "An approach to evaluate data trustworthiness based on data provenance," in Proc. 5th VLDB Workshop Secure Data Manage., Aug. 2008, vol. 5159, pp. 82–98.

[26].B. Yu, S. Kallurkar, and R. Flo, "A demspter-shafer approach to provenance-aware trust assessment," in Proc. Int. Symp. Collaborative Technol. Syst., May 2008, pp. 383–390.

[27].J. Golbeck, "Combining provenance with trust in social networks for Semantic Web content filtering," in Proc. Int. Conf. Provenance Annotation Data, 2006, vol. 4145, pp. 101–108.

[28].W. Zhou, E. Cronin, and B. T. Loo, "Provenance-aware secure networks," in Proc. IEEE 24th Int. Conf. Data Eng. Workshop, 2008, pp. 188–193.

[29].L. Koczy, K. Hirota, "Interpolative reasoning with insufficient evidence in sparse fuzzy rule bases", Inf. Sci., vol. 71, no. 1/2, pp. 169-201, 1993.

[30].Z. C. Johanyak, S. Kovacs, "Fuzzy rule interpolation by the least squares method", Proc. Int. Symp. Hung. Researchers Comput. Intell., pp. 495-506, 2006.

[31].S. M. Chen, S. H. Cheng, Z. J. Chen, "Fuzzy interpolative reasoning based on the ratio of fuzziness of rough-fuzzy sets", Inf. Sci., vol. 299, pp. 394-411, 2015.

[32].L. Yang, Q. Shen, "Adaptive fuzzy interpolation", IEEE Trans. Fuzzy Syst., vol. 19, no. 6, pp. 1107-1126, Dec. 2011

[33].P. Angelov, R. Buswell, "Automatic generation of fuzzy rule-based models from data by genetic algorithms", Inf. Sci., vol. 150, no. 1/2, pp. 17-31, 2003.

[34].S. Wu, M. Joo, "A fast approach for automatic generation of fuzzy rules by generalized dynamic fuzzy neural networks", IEEE Trans. Fuzzy Syst., vol. 9, no. 4, pp. 578-594, Aug. 2001.

[35].D. Tikk, P. Baranyi, "Comprehensive analysis of a new fuzzy rule interpolation method", IEEE Trans. Fuzzy Syst., vol. 8, no. 3, pp. 281-296, Jun. 2000.

[36].T. D. Gedeon, L. T. Koczy, "Conservation of fuzziness in rule interpolation", Proc. Symp. New Trends Control Large Scale Syst., pp. 13-19, 1999

Cite this article as :

Santhana Lakshmi M, Hemaanand M, "Opinion Based Trust Model for Delay Tolerant Networks using Fuzzy Logic ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 1, pp. 113-130, January-February 2021. Available at
doi : https://doi.org/10.32628/CSEIT217125
Journal URL : http://ijsrcseit.com/CSEIT217125