A Trust Model Based on Grey Relational Analysis and Cooperative Computing in Opportunity Networks

Jian-Bo Xu, Dan-Ping Shou
School of Computer Science and Technology, Hunan University of Science and Technology Xiangtan, China
E-mail: jbxu@hnust.edu.cn, shoudanp@foxmail.com

***Abstract*-The existence of selfish nodes and malicious nodes pose a significant threat to the complex environment of opportunistic network. In order to improve the transmission security in bad environment, a multi-dimensional trust model GRATM(Grey Relational Analysis Trust Model) based on gray relational degree and cooperative computation is proposed which may improve the success rate and reduce the delay during the process of transmission. GRATM adopts multi-dimensional parameters, the parameters are fused and updated dynamically, and the total trust value is calculated by direct interaction combine with other nodes recommendation trust value. GRATM is based on gray relational analysis, the weight coefficients of the direct trust value are reasonably distributed, and the recommendation trust value is calculated by the neighbor nodes. Trust information is sent to other nodes and exchanged with each other through regular sending package. Compared with Direct, MaxProp, and Direct Delivery, GRATM has the advantages of balanced transmission success rate, transmission delay and performance.**

Keywords-opportunity network; trust model; grey correlation degree; cooperative computing

I INTRODUCTION

Opportunistic network is characterized by the lack of infrastructure which is store - carry - forward routing mode to achieve the communication between nodes [1]. Selfish and malicious nodes are mixed with network nodes, posing a threat to opportunistic network security because information thieves disguised as selfish nodes and malicious nodes can enter the network to steal data. Selfish nodes utilize network resources as much as they can to achieve the purpose of access to information, occupy only resources, do not make any contributions. This behavior receives and then discards information instead of transmitting. Malicious nodes are to undermine the operation of the network, through improving their own high and fake trust value, by offering high trust value to defraud normal nodes trust, so that the message is forwarded to it, and then discarding these messages when their purpose is achieved. Serious selfish and malicious attacks will lead to paralysis of the network. It can be seen that the opportunity network is vulnerable to selfish nodes and malicious nodes attack. Using trust management technology to improve the security of the network is necessary at present.

Trust is defined as a degree of subjective confidence about the behavior for a particular entity [3]. The current trust model can be divided into direct trust model and cooperative computing trust model. The trust relationship of direct trust model is based on separate decision of evaluated node, which may easily result in inaccurate decision-making. While cooperative computing trust model cooperating with other nodes and jointly accounting degree of trust among the nodes is a mature program.

In this paper, a trust model is established to overcome selfish node and malicious node existing in the network, ensures the timely transmission of the message to the destination node, and improves data rates and shortens the delay of data transfer on the basis of reducing consumption of node s energy and ensuring protective network safety. Combining the characteristics of node in opportunistic network with attack patterns of selfish and malicious node, multi-dimensional trust attribute is proposed to be an evaluation parameter in trust model. And node is divided into single pattern and encounter pattern according to its motor pattern. Single pattern refers to its own status information including nodes energy, storage and other parameters. Encounter pattern refers to status information among the encountering nodes. It also includes lots of parameter such as contact intimacy, deliver reliability and location intimacy. The total trust value of being evaluated node is calculated by direct trust value and recommended trust value. Then, comparing the total trust value with threshold value is to determine whether send the message to being evaluated node. The calculation of direct trust value is adjusted dynamically with Grey Relation Theory, which can accurately reflect the characteristics of the network and update trust model in real time. The calculation of recommended trust value adopts recommendations trust provided by neighbor node to achieve cooperative computing among the nodes.

II RELATED WORK

Many scholars have advanced segments of trust models, these models have caused a certain amount of attention in the field of opportunistic network security, but the search for an effective mechanism to eliminate or mitigate the selfish and malicious behaviors on the opportunities network remains an enormous challenge.

Shabut [6] made an effective defense in mobile ad - hoc networking based on trust model, which uses the dynamic clustering technology to filter out malicious nodes' insincere trust value and isolate malicious insincere recommendation trust issued by malicious node, but it overlooks the importance of multi-dimensional trust model of direct trust property. [4] Scholars have put forward an trust management strategy applied to the secure routing. Comparative analysis was used to set the running environment of trust models and set parameters, maximizing routing performance and reduce trust bias. That paper is not a good combination of direct trust and recommendation trust, ignored the role of direct trust in the opportunistic network. [5] proposed a mobility models based on multi-dimensional evaluation of human movement, analyzing the impact factors of human movement regulation on opportunistic network. It provided a new method modeling multi-dimensional property, but did not take into account the selfish and malicious nodes, and ignored the collaborative computing in nodes, it s insufficient.

Most of the trust models above mentioned rely on a simple parameters to calculate the values of trust, lack of consideration of selfish and malicious nodes in the network, collaboration between nodes are ignored as well. On opportunistic network, building trust model to defend selfish and malicious nodes, direct trust combining with how trust is the common use of the trust model.

III TRUST MODEL

A Multi-dimensional Trust Parameters

Due to the large number of selfish and malicious nodes in the network, selection of trust properties should have a certain deterrent to selfish and malicious behavior of the network. Just to select a single dimension of trust properties is one-sided and doesn t reflect overall performance. Using the multi-dimension trust properties can limit the selfish and malicious nodes from multiple aspects.

In this paper, state of nodes in the network can be divided into individual pattern and encounter pattern. Individual pattern refers to the node s status (such as energy, storage space, CPU processing capacity etc.), and it s a series of indices to measure the node itself. Encounter pattern refers to descriptive approach that nodes interaction with other nodes or to participate in the network transmission. This paper pick up two important attributes in individual pattern, namely, energy and storage space. Encounter pattern select Contact intimacy value, Delivery reliability value, Location intimacy value.

Definition 1 Contact intimacy value: Intimating degree of the current node's direct interaction (or contact) with the Sink, Sink is the base station of the opportunistic network model. the communication coverage of Sink is the whole of the opportunistic network. The goal of normal nodes is to forward messages to Sink, the more direct interaction between current nodes and Sink, the higher the contact intimacy value. The calculation shows below.

$$V_C = \frac{C_S}{C} \tag{1}$$

Where Vc is Contact intimacy value, CS (Contact frequency with Sink) is frequency of current node contact with the Sink, C (Contact frequency) indicates that the frequency of current node contact with all the nodes in the network running time.

Definition 2 Delivery reliability value: The credible degree of nodes in message transmission. High frequency of packet dropout shows that delivery reliability is low, otherwise, delivery reliability is high. It is represented by VD.

$$V_D = \frac{C_P}{R_P} \tag{2}$$

Where VD is the delivery reliability value, Cp is the number of node transfer packages, Rp is the total number of packets nodes receive from other nodes.

Definition 3 Location intimacy value: The position relationship degree between current node and Sink Nodes composed of handheld devices, the movement way has the characteristics of people's behavior. The smaller the distance node from the Sink, node movement is more partial to the Sink, the greater the probability of its encounter with Sink is. And the probability of transmission increases. The calculation shows below:

$$V_L = 1 - \frac{D_S}{S} \tag{3}$$

VL is Location intimacy value, DS is the distance of current node from Sink. S represents the entire perimeter of the communication range. The paper using multi-dimension trust property to construct the basic parameters of the model, having considered the versatility of the network.

B. Trust Property Integration Mechanism

The paper presented a trust model for restraining selfish and malicious nodes. Trust model using a combination of direct trust and recommendation trust, and calculating the total value of trust by combination of cooperative computing between current node with neighbour nodes to avoid incorrect decisions of the individual making.

Opportunistic network implements the transmission of the message through the contact and cooperation with neighbor nodes, interaction between nodes are usually used as standard to estimate whether nodes are selfish or malicious nodes. Because some malicious nodes posing as normal nodes in the network, only calculating direct trust value is not comprehensive. A part of trust value need to be obtained from other nodes, that is recommendation trust. Total confidence value formulas shows in (4):

$$T_{i,j} = T_{i,j}^{direct} + T_{i,j}^{\mathrm{recom}} \tag{4}$$

Where T is the total value of trust, i and j are nodes in opportunistic network, where i represents the evaluating node, j represents the node being evaluated. Ti, j is the total trust values for i evaluating j. Ti, jdirect is direct trust value of node i to j, Ti, jrecom represents the recommend trust values of node i to j.

The formula of direct trust value computation is:

$$T_{i,j}^{direct} = \beta_1 V_C + \beta_2 V_D + \beta_3 V_L \qquad (5)$$

1, 2, 3 are the weight coefficients of Contact intimacy value, Delivery reliability value, Location intimacy value, 1 + 2 + 3 = 1. Contact intimacy value, Delivery reliability value, Location intimacy value is different factor affecting the system. They change over time and different node object, this relevance called correlation. Grey Association analysis is a method through gray correlation degree to analysis and to determine the impact of system or master a way to measure the contribution of the system[6]. It applies to different capacity and the irregular of the samples, and a small amount of calculation, the time complexity of the algorithm is low. Grey incidence analysis steps are as follows:

1) First to determine the data series of characteristic reflecting trust model's behavior on opportunities network. This article selects as sequence for a reference.

2) Determines the contrast sequence -- x0 = {VC0, VD0, VL0} Data sequences of factors affecting the behavior of the system [6]. Selecting time series of contact intimacy value, Delivery reliability value and Location intimacy value as a reference sequence.

$$\begin{aligned} x_1 &= \{V_C^k, V_C^{k-1}, V_C^{k-2}\} \\ x_2 &= \{V_D^k, V_D^{k-1}, V_D^{k-2}\} \\ x_3 &= \{V_L^k, V_L^{k-1}, V_L^{k-2}\} \end{aligned} \qquad (6)$$

Which VCk, VDk, VLk respectively are the contact intimacy value, Delivery reliability value, the Location value at k moment of intimacy.

Calculating grey correlation coefficient (xi) of reference sequence and comparision sequence. Calculation of the correlation coefficient compare sequence relative to the reference sequence at various points in the curve shows as (7):

$$\xi(x_i) = \frac{\Delta(\min) + \rho\Delta(\max)}{\Delta_{oi}(k) + \rho\Delta(\max)} \qquad (7)$$

Where is the identification coefficient, generally take between 0 and 1, and second minim-um differential denoted as (min), (max) is the largest maximum differential. Absolute differences of every point on the curve at series of comparison sequence Xi and each point on the curve of reference series X0 denoted as Oi (k) [4].

4) Relevancy degree. Correlation coefficients are the correlation value of comparison sequence associated with the reference sequence in all moments, there are much value, and information too scattered are not convenient to compare integrity [4]. Therefore it is necessary to concentrate correlation coefficient to a value each time (that is, all points in the curve) Correlation degree is calculated as (8):

$$r_i = \frac{1}{N}\sum_{k=1}^{N} \xi_i(k) \qquad (8)$$

To calculate 1, 2, 3 according to the correlation degree as(9):

$$\beta_i = \frac{r_i}{r_1 + r_2 + r_3} \qquad (9)$$

Grey correlation reflects the influence of various factors affect the performance to the network trust model, it assigned the proper weight coefficient for the direct trust value distribution in the model, optimized the model performance. Recommend trusted values calculated by evaluating node together with neighbor nodes. When node i evaluating node j, node i request on the surrounding neighbor nodes. After node i receiving the request from neighbor nodes, node j sends the trust value to node i in the form of a package. Trust value will be integration collected by node i, then obtaining a total value of recommendation trust, that is Ti, jrecom as (10).

$$T_{i,j}^{\text{recom}} = \frac{\Sigma_{m\in R}\{T_{i,m}(t)\times T_{m,j}(t)\}}{\Sigma_{m\in R} T_{i,m}(t)} \qquad (10)$$

Where R is the assembly of recommend nodes, and m is random recommend node of assembly, node m and i make collaborative decision. Ti,m(t) is the trust value of node i evaluate node m, Tm, j (t) is the trust value of node m evaluate node j. Ti, m (t), Tm, j (t) obtained by formula (4).

C. Update and Decision-Making of Trust Value

The trust value must be periodically updated to meet the Dynamic Characteristics of network nodes. For selecting the updating period, the length of the period should be firstly taken into consideration to accurately reflect the changes of nodes' state or not, therefore it should not be too long. If it's too short, the trust value's updating needs to calculate the data collected, but frequent period's update will lead to the waste of node energy and storage space and other resources. The node takes updates through periodically sending a package containing trust value information to its neighbor node. Nodes updating trust value by periodically sending a package containing trust value information to its neighbor nodes.

TABLE I. ALGORITHM OF DATA FORWARDING

```
Node i obtain assembly of neighbor nodes M (I)
IF M(i)=
{
    IF life cycle of package over
        Dropping package
    Else node i continue moving
}
Else
{
    Update M(i), Collect information about trust}
    Calculate trust parameters as in Eqs (2) (3) (4)
    Calculate as in Eqs (4)~(6)
    Calculate $T_{i,j}^{\text{recom}}$ as in Eqs (10);
    Calculatea $T_{i,j}$ s in Eqs (4)
}
IF $T_{i,j}>$ $_{\text{T}}$ send package to j
Else Compare with other neighbor nodes
END
```

The time complexity of Ti,j is based on Ti,jrecom and Ti,jdirect, due to the length of reference sequence is just three, according to the formula (6), the time complexity of Ti,jdirect is a constant. The time complexity of Ti,jrecom is is linearly to the number of recommended nodes. The time complexity of Ti,j is O(n).

IV PERFORMANCE ANALYSIS OF TRUST MODEL

A. *Comparison of Simulation Parameters*

The existence of selfish and malicious node on the network has a great threat to the performance of opportunistic network. Selfish nodes do not forward message to the nodes that are not familiar, greatly reduced the success rate of transmission in the network. Malicious nodes generate false confidence value for the nodes, then nodes will send the message to the wrong next-hop node according to the wrong trust value, that increasing the routing cost of opportunistic network, and extending the message delivery time. GRATM aims at the following three aspects generated by selfish and malicious nodes.

1) Transmission rate: The ratio of the total number of data packets successfully reaches its destination node and the total number of packets issued by the source node transmission within a certain time [5].

2) Transmission delay: the time of data packets from the source node to destination node, average transmission latency is often used to evaluate [6].

3) Routing overhead, the total number of nodes forward data grouping within a certain time, is generally evaluated by the overhead ratio. The Network Overhead = (the total number of messages that are under transmission the number of messages that have been successfully submitted) / the number of messages that have been successfully submitted.

B. *Simulation Environment Settings*

In order to verify the effectiveness of GRATM on improving the network performance, the simulation using ONE simulator, an open-source simulator designed to support research in opportunistic networking. It's from Finland simulation platform developed by Nokia Research Center. The platform is based on the Java environment. We make the comparison of GRATM with Epidemic, MaxProp, Direct Delivery routing algorithms. Epidemic can maximize the success rate of packet transmission to reduce transmission delay and can be used as standards contrast of transmission rate and delay. MaxProp algorithm is an algorithm based on schedule strategy, it can be used as a comparative benchmark of predicting the forwarding decision making. Direct Delivery is an algorithm based on forwarding strategy, to minimize energy consumption, it can be used as a comparative benchmark in terms of energy consumption. Simulation parameter settings shown in the table 2.

In the design of experiments, setting 50 selfish nodes and 50 malicious nodes in the simulation environment. the selfish node identifiers packets from other nodes then discarded after it. The malicious node attacts the oppotunistic network will interfere with the network running. This experiment need to considered the influence of selfish and malicious node.

TABLE II. NETWORK SIMULATION PARAMETERS

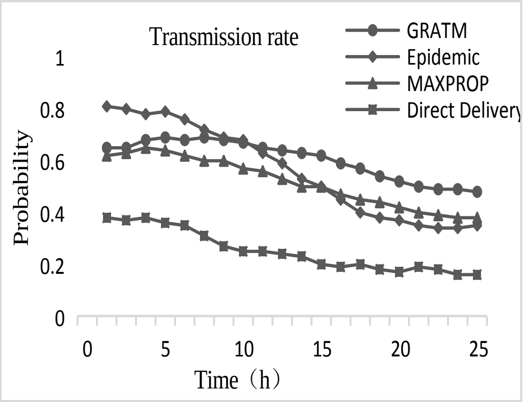
Parameters	***value***
Number of normal nodes	300
Number of selfish nodes	50
Number of malicious nodes	50
Number of Sink	1
Simulation area	5000m 5000m
Node movement speed	1~2m/s
transmission rate	200KB/s
cache size	5MB
Packet Size	500~800KB
Message generated frequency	30~45s
communication radius of normal nodes	20m
communication radius of Sink	Simulation area
The updating cycle of trust t	3.5min
mobility models	SPMBM

C. *Analysis of Simulation Result*

In this section compares GRATM with three classical routing algorithms that ONE bringing in the simulator. If the proposed GRATM success improve in transmission success rate, transmission delay and routing cost, GRATM is illustrated to have certain effect on curbing selfish and malicious nodes.

As shown in Fig. 1, with the increase of operation time, the network resources consumption, the transmission rate of this routing algorithm overall decline. Epidemic has the highest success rate of transmission, but with the increase in simulation time, transmission rate dropped sharply, its transmission performance is inconsistent. GRATM adopts multi-dimensional trust parameters, comprehensive consideration of various factors affecting the transmission in the network, the computed trust value of selfish nodes is small in general compared with normal node confidence value. Nodes send the message to next hop nodes, the next hop nodes' trust value is greater than certain threshold value.

GRATM effective identification of selfish nodes in the network. Direct Delivery routing algorithm is poor in transmission, because it s single-copy transfer. In the figure 1, transmission rate of GRATM is higher than MaxProp, Direct Delivery and it can verify this theory.



.

Figure 1. Comparison chart of network delivery rate.

In Figure 2 The average transmission delay of GRATM is the smallest, followed by MaxProp. Direct, Delivery is the largest. For MaxProp algorithm, if the number of nodes is large, transmission delay would be small. Multiple copy of transmission in Epidemic can be used to greatly increasing transmission delay in message grouping. Direct Delivery routing algorithm, only one copy of the message in the network, and requires a lot of delay time forwarding the package to the destination node. GRATM simplifies the decision-making process, transmission delay is relatively small. GRATM trust model combining with the current routing list for computing trust value, transmission delay is relatively decrease by simplifying the decision-making process.

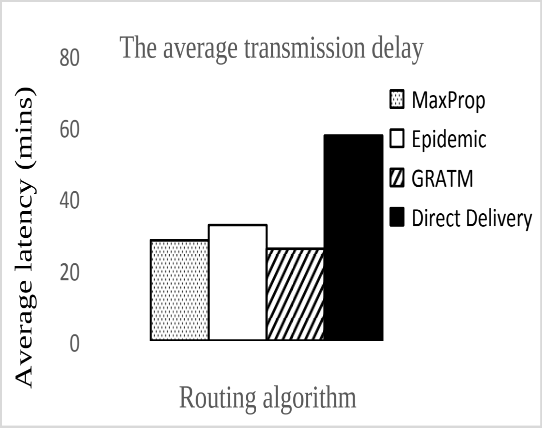


Figure 2. Comparison of the average delay.

Figure 3 shows the node routing overhead, Direct Delivery routing's transmission has only one copy in the opportunistic network, it's routing overhead is negligible. MaxProp determining the priority of the packet is based on the transmission overhead. GRATM eliminated most of selfish and malicious nodes, a small part of higher trust value node is selected as the next hop, it reduces network overhead greatly.

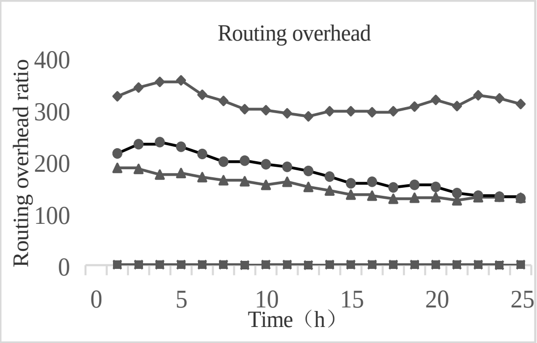


Figure 3. Comparison chart of network overhead ratio.

To sum up, on opportunistic network, GRATM Trust model has succeeded in improving the rate of transmission, at the same time, to control the transmission delay and network overhead effectively, It is an preferably algorithms on combination property. Compared to other routing algorithms, GRATM can effectively defend against selfish and malicious nodes .

D. Cost of the GRATM

Opportunistic networks are characterised by scarcity resources in terms of communication, The memory usage and computational complexity requirements [5]. The size of data is very small because the direct trust of GRATM provides just three parameters of Contact intimacy value, Delivery reliability value and Location intimacy value and the length of reference sequence in direct trust vaule is just three. The memory consumption in which the GRATM consumes more memory to store direct trust parameters and little memory consumption on the side of the recommend trust. An additional cost by the time consumption which is more than the traditional routing like Epidemic, MaxProp, Direct Delivery routing algorithms which uses single copy of the transmission.

V CONCLUSION

The paper gives an effective design of trust model to the selfish nodes and hostile nodes. It uses nodes motion modes to select multidimensional trust parameter from single mode and encounter mode. The total trust value is determined by calculation of direct trust value and recommend trust value. Comparing the total value of trust and the preset threshold, it determines whether to send messages to nodes.

According to the dynamic allocation weight coefficient of gray correlation, the direct trust value optimizes the role of various attributes to trust model, then to calculate the recommend trust value through collaborative methods, which contains calculation of trust value with neighbor nodes collaboration. It asks dynamically updating trust value in accordance with the trust updating period. Finally, it improves the network performance of GRATM model, which improves the success rate of transmission and reduces the energy consumption of the network under the reduction of average delay. Considering the impact of selfish nodes and malicious nodes for recommend trust and avoidance of false recommendation, this model should be continuously improved to establish a better network in the near future.

ACKNOWLEDGMENT

This work is supported by Project supported by Hunan Provincial Natural Science Foundation of China, 2016JJ2058.

REFERENCES

[1] Fu, Hao, et al. "Optimal System Maneuver for Trust Management in Social Networks." (2016).

[2] H. Cho, a. j. - Swami, and r. Chen, "A survey on trust management for mobile AD hoc networks," IEEE Commun. Surveys Tuts. vol. 13, no. 4, pp. 562-583, 4 th Quarter 2011.

[3] Shabut, Antesar M., et al. "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs." IEEE Transactions on Mobile Computing 14.10(2015):2101-2115.

[4] Chen, Ing Ray, et al. "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing." IEEE Transactions on Parallel & Distributed Systems 25.5(2014):1200-1210.

[5] Thakur, Gautam S., and A. Helmy. "COBRA: A framework for the analysis of realistic mobility models." Proceedings - IEEE INFOCOM12.11(2013):3351-3356.

[6] Roselina Sallehuddin, Siti Mariyam Hj. Shamsuddin, Siti Zaiton Mohd Hashim, Grey Relational Analysis and Its Application On Multivariate Time Series. The Journal of Applied Mathematics Volume 2014 (2014), Article ID 56869.