

A trusted routing algorithm based on D-S evidence theory combined with physical layer security

Lin Ma[†], Chong Tan, Jun Pan and Kai Yu

*Broadband Wireless Communications Lab,
Shanghai Institute of Microsystem and Information Technology,
Chinese Academy of Sciences, Shanghai, China, 200050*

[†]*E-mail: lin.ma@mail.sim.ac.cn*

With the rapid development of the communication technology, the traditional routing algorithms which only consider functional QoS metrics are difficult to meet the needs of applications. In this paper, we propose a trusted routing algorithm to overcome this problem. First, we propose a trust evaluation model of service instances based on the Dempster-Shafer theory combined with physical layer security, and then the trusted routing algorithm is proposed by using this model to improve the traditional routing algorithms. The simulation results show that the proposed trusted routing algorithm can effectively improve the success rate of routing and the performance of the QoS metrics.

Keywords: Trusted routing; Dempster-Shafer Theory; Trust Evaluation Model

1. Introduction

The distributed routing technology has been more and more widely used in various fields, such as cloud computing, service-oriented computing, MANETs, etc. The distributed routing technology uses various scheduling algorithms to generate new complex services, which are composed of many single services. The computing resources, information resources and communication resources distributed in different nodes can be composed in this way to meet the various QoS requirements of the applications. With the development of wireless communication technology, a lot of research introduce the physical layer security technologies to improve the routing effect, and these have become a hot topic of research in recent years[1][2][3]. In this paper, we try to propose a trusted routing algorithm to improve the success rate of routing and the performance of the QoS metrics[4].

Routing algorithm is well studied in recent years[5], Related researches are done by QUEST[6][7], LIAC[8], MCDM[9]. The purpose of these related researches is to find an appropriate route under certain measurement. These researches usually use a linear function to aggregate the QoS metrics, which are mainly refers to the function QoS metrics, such as delay, cost and link

bandwidth, etc. In practical environments, due to the uncertainty of the service instances, the execution of the services instances may failed, and it can seriously reduce the QoS performance of the whole composition process. To overcome this shortcoming, Gu [7] adds the service reliability indicators into the QoS metrics, but she only considers the direct interaction between two service instances to evaluate service reliability. In fact, this method only considers the direct interaction is usually inaccurate, it should consider the interaction between awaiting service instance and other service instances[10]. Hu[11] uses D-S Theory to calculate the reliability of the path level, but it doesn't detailed discuss the weight of the recommendation. Zhu[12] proposes a dynamic trust evaluation model under distributed computing environment, they use Shapley entropy and the honesty of nodes to calculate the weight of each node, and then use D-S Theory to combine all belief functions. But this model does not obtain an accurate reliability values, which is the probability domain mapped from the belief interval, this model does not consider the phenomenon that services have been composed step by step, so this model can't be directly used to evaluate service reliability. From the above analysis, the traditional routing algorithms do not consider the issues of service reliability in depth, and some information fusion algorithms are difficult to directly evaluate service reliability. In order to evaluate service reliability more accurately, we consider the weight of each service by analyzing the degree of conflict among belief functions, then use D-S Theory to combine the belief functions.

We present a trusted routing algorithm based on D-S Evidence Theory. and we note the uncertainty of service may seriously reduce the QoS performance, and present a trust evaluation model of service instances based on the Dempster-Shafer theory and the Pignistic transformation theory, and then the trusted routing algorithm is proposed by using this model to improve the traditional routing algorithms. We also verify in simulations that the proposed algorithm can improve the success rate of routing and the performance of the QoS metrics.

The rest of the paper is organized as follows. Section 2 presents the preliminaries. Then in Section 3, we present a trust evaluation model. In Section 4, we present the trusted routing algorithm. The experiment study is present in Section 5. Finally, in Section 6, we conclude the paper.

2. Preliminaries

In this section, to facilitate understanding of the trust evaluation model and the trusted routing algorithm, we briefly review some necessary foundation of evidence theory considered in our work. These necessary foundation theories include D-S theory and the Pignistic transformation theory. For more details, please refer to [13],[14],[15], [16]and [17].

2.1. Dempster-shafer evidence theory

Let Ω be a finite set called the frame of discernment. The elements of Ω are assumed to be mutually exclusive and exhaustive. The power set of Ω is denoted by $2^\Omega = \{A \mid A \subseteq \Omega\}$. The measure functions commonly used in evidence theory include mass function, belief function and plausibility function and so on.

Definition 1: Let Ω be the frame of discernment. A basic belief assignment (BBA, also called mass function) is a mapping $m: 2^\Omega \rightarrow [0,1]$ defined by

$$\sum_{A \subseteq \Omega} m(A) = 1, m(\emptyset) = 0 \quad (1)$$

Definition 2: Let Ω be the frame of discernment and a BBA m defined on it, the belief function (bel) and plausibility function (pl), both derived from m , are defined respectively as

$$bel(A) = \sum_{B \subseteq A} m(B) \quad \forall A \subseteq \Omega \quad (2)$$

$$pl(A) = \sum_{A \cap B \neq \emptyset} m(B) \quad \forall A \subseteq \Omega \quad (3)$$

When A is a set with single element, $bel(A)=m(A)$. The main difference between them is that $bel(A)$ represents the sum of masses committed to the subsets of A , whereas $pl(A)$ corresponds to the sum of masses committed to the subsets that do not refute A . Absolutely, $pl(A) \geq bel(A)$, and the belief interval $[bel(A), pl(A)]$ represents the uncertainty of A .

Definition 3: Let Ω be the frame of discernment, m_1 and m_2 are two distinct BBAs defined on it, the Dempster's combination rule can be defined as

$$\begin{cases} m_{12}(\emptyset) = 0; \\ m_{12}(A) = \frac{1}{1-K} \sum_{B \cap C = A} m_1(B)m_2(C) \quad (A \neq \emptyset) \end{cases} \quad (4)$$

Here, $K = \sum_{B \cap C = \emptyset} m_1(B)m_2(C)$ reflects the whole degree of conflict between the two BBAs, and $\sum_{B \cap C = A} m_1(B)m_2(C)$ corresponds to the conjunctive rule of combination.

2.2. Evidence distance

A principled metric distance between two BBAs is given by Jousselme [18]. m_1 and m_2 are two BBAs defined on the set Ω , and \bar{m} is a $2^{|\Omega|}$ -dimensional column vector with row names $(\emptyset, \{\theta_1\}, \{\theta_2\}, \{\theta_3\}, \dots, \{\theta_1, \theta_2\}, \dots, \Omega)$, where $|\Omega|$

denotes the cardinality of Ω . They define the evidence distance $d_{BBA}(m_1, m_2)$ between m_1 and m_2 as

$$d_{BBA}(m_1, m_2) = \sqrt{\frac{1}{2}(\overline{m_1} - \overline{m_2})^T D(\overline{m_1} - \overline{m_2})} \quad (5)$$

Where $(\overline{m_1} - \overline{m_2})$ stands for vector subtraction and $(\overline{m_1} - \overline{m_2})^T$ is the transpose of $(\overline{m_1} - \overline{m_2})$, and D is a $(2^{|\Omega|} \times 2^{|\Omega|})$ -dimensional matrix with elements in the form

$$D(i, j) = \frac{|A \cap B|}{|A \cup B|} \quad \forall A, B \subseteq \Omega \quad (6)$$

Jousselme et al. show that this distance satisfies the metric axioms and is an appropriate measure of the dissimilarity between two BBAs. In this paper, we choose it to measure the dissimilarity between two BBAs.

2.3. Pignistic transformation

In the theories of belief functions, the mapping from the belief to the probability domain is a controversial issue. A classical transformation is the so-called pignistic probability, denoted BetP, and BetP is defined as

$$BetP(A) = \sum_{B \subseteq \Omega} \frac{|A \cap B|}{|B|} \cdot \frac{m(B)}{1 - m(\emptyset)} \quad \forall A \subseteq \Omega \quad (7)$$

3. Trust Evaluation Model

In this section, we propose the trust evaluation model (TSM) to evaluate service reliability accurately. TSM can be divided into three phases: (1) direct evaluation phase, (2) general evaluation phase, (3) accurate evaluation phase. By running this model periodically, we can get the relatively accurate evaluation result, and this result is the service reliability.

3.1. Direct evaluation phase

In the distributed routing scenario, the prior service instance can evaluate the direct reliability of the posterior service instance, and the direct reliability is called the local reliability in some cases. The direct reliability can be obtained from the interaction history of service instances in adjacent service group. Here we take two service instances for example; A_i indicates the i -th service instance in SGA, B_j indicates the j -th service instance in SGB, SGA and SGB are two

adjacent service groups. The evaluation period is set to τ . Let I_{ij} represents the total number of interactions between A_i and B_j within the time interval τ , S_{ij} represents the number of successful interactions, and F_{ij} represents the number of failed interactions, then t_{ij} represents the direct reliability between A_i and B_j , it can be expressed as follows:

$$\begin{cases} t_{ij}(T) = S_{ij} / I_{ij} \\ t_{ij}(-T) = F_{ij} / I_{ij} \\ t_{ij}(T, -T) = 1 - t_{ij}(T) - t_{ij}(-T) \end{cases} \quad (8)$$

The calculation process in direct evaluation phase is relatively simple, and the direct reliability can be achieved by putting the direct interaction results into the above formula. By the definition of t_{ij} , we can easily know that t_{ij} is a BBA (mass function), so we can conduct general evaluation by using Dempster-Shafer Theory to combine all the BBAs.

3.2. General evaluation phase

After direct evaluation phase, we can get the direct reliability between every two service instances in adjacent service groups, and then each service instance in the same service group broadcasts its direct evaluation of the posterior service instance. Here we assume that the number of service instances in each service group is n , and then the direct reliability matrix is defined as

$$M = \begin{bmatrix} t_{1j} \\ t_{2j} \\ \dots \\ t_{nj} \end{bmatrix} = \begin{bmatrix} t_{1j}(T) & t_{1j}(-T) & t_{1j}(T, -T) \\ t_{2j}(T) & t_{2j}(-T) & t_{2j}(T, -T) \\ \dots & \dots & \dots \\ t_{nj}(T) & t_{nj}(-T) & t_{nj}(T, -T) \end{bmatrix} \quad (9)$$

In the matrix M , j denotes the j -th service instance in the posterior service group to be evaluated. t_{ij} is the direct reliability of the j -th service instance in the posterior service group, which is evaluated by the i -th service instance in the prior service group. When j is fixed, t_{ij} can be written as t_i . There are n BBAs in the matrix M obviously, and all these BBAs are combined in general evaluation phase.

Usually these BBAs are not equally important in a distributed routing scenario, and we consider that the importance of each BBA may be different. We can get the importance by using evidence distance $d_{BBA}(t_i, t_j)$, which can describe the degree of conflict between two BBAs. The higher degree of conflicting with other BBAs, the less important it will be. Suppose the distance

between two BBAs can be calculated by Formula 3, The similarity measure S_{ij} between two BBAs is defined as:

$$S(t_i, t_j) = 1 - d_{BBA}(t_i, t_j) \quad (10)$$

So the total similarity measure of the BBA t_i is defined as:

$$Total_S(t_i) = \sum_{j=1, j \neq i}^n S(t_i, t_j) \quad (11)$$

The weight of each BBA t_i is defined as:

$$w_i = \frac{Total_S(t_i)}{\sum_{i=1}^n Total_S(t_i)} \quad (12)$$

It is obviously that $\sum w_i = 1$, so we can use w_i as the weight of each BBA, then we use w_i to transform t_i as follows:

$$\begin{cases} t_{ij}(T) = w_i \bullet t_{ij}(T) \\ t_{ij}(-T) = w_i \bullet t_{ij}(-T) \\ t_{ij}(T, -T) = 1 - t_{ij}(T) - t_{ij}(-T) \end{cases} \quad (13)$$

Then we can use Dempster's rule to combine the transformed direct reliability, and get three effective reliability intervals, namely $ct_j(T)$, $ct_j(-T)$ and $ct_j(T, -T)$.

3.3. Accurate evaluation phase

In this section, we present the accurate evaluation of the reliability, we use Pignistic Theory to transform the interval-valued belief degree into precise probability. This transformation can help us evaluate the reliability and decision-making.

In real system, Traditional pignistic transformation such as the Smets pignistic probability (BetP) usually more biased towards a smaller interval. Some improved pignistic transformation with the larger stability measured by probabilistic information content or the lower entropy are more proper to be used in decision procedure, but in our scenario, what we need is the precise service reliability, rather than the decision-making. The PrPI method can achieve more precise evaluation results, the simplest form of PrPI method is defined as:

$$f(T)=m(T)+\frac{PI(T)}{PI(T)+PI(-T)}m(T,-T) \quad (14)$$

Have substituted the reliability intervals into Formula 3, what we have desired is $f(T)$, this is the service reliability. In real system, we can achieve the posterior service reliability by running this evaluation model periodically.

4. Trusted Routing Algorithm

In this section, we will add service reliability into the traditional routing algorithm smoothly to improve the performance. Service reliability is useful for different types of routing algorithms, such as shortest path algorithm, multi-objective optimization and linear programming. For simplicity, we only consider the implementation of the sequence process, complex processes such as parallel, pick and while process, can refer to the discuss in more specialized articles. We consider three properties for the QoS model without loss of generality, These properties are delay, security capacity and service cost, which are the most important attribute for routing. In this paper, the shortest path algorithm has been chosen to compose service instances, we introduce service reliability to improve the performance of the QoS metrics.

Traditional routing algorithms, either centralized or distributed, they only consider the functional QoS metrics. These algorithms calculate the QoS aggregation metrics, and then choose an appropriate path with the minimum QoS aggregation metrics. In the real environment, normally the service instance may have the uncertainty or malicious nature, this nature may lead to the failure of the execution, as a result of the transaction mechanism, the service instance will be executed until successful, it will result in unexpected cost, the traditional algorithms are difficult to obtain satisfactory results. We add precise service reliability (r) into routing algorithm, and then $1/r$ denotes the expected number of calls, we use the expected value of QoS aggregation metrics (EQAM) to measure the composition paths, and select the appropriate path with the minimum EQAM. The trusted routing algorithm is described as follows:

Algorithm1. Trusted routing algorithm

```
public Path calMinPath(){
//SGNum is the number of SG, SGSize is the size of SG
//d[i] denote the evaluation results of i-th service instance
for(int i=0;i<SGSize;i++){
    a[i]=start.score[i]/start.d[i];
    b[i]=MAX;
}
for(int k=1;k<SGNum;k++){
//orderly traversal
for(int i=0;i<SGSize;i++){
for(int j=0;j<SGSize;j++){
if(a[j]+nextSG.ws[j].score[i]/d[i]<b[i])
```

```

        {
            b[i]=a[j]+nextSG.ws[j].score[i]/d[i];
            c[k-1][i]=j;//Record every step of the path for the latter calculation
        }
    }
}
for(int i=0;i<SGsize;i++){
    a[i] = b[i];//EQAM
    b[i] =MAX;
}
}
t<--min(a[i]); //calculate the path with the minimum EQAM.
minPath<--(i,c[k-1][i]);//minPath is the optimal path.
}

```

5. Experiments

In order to test and verify the performance of the trust evaluation model and the trusted routing algorithm, a simulation environment has been built. The process has been designed in four service groups, and each service group is consist of 20 service instances. All service instances can be classified into three types in accordance with good performance (85%-90%), random performance (40%-60%) and poor performance (10%-15%). The number in parentheses is the probability of the service instance to be successful.

In the simulation experiment, we set the number of direct interaction between two service instances is 50, and then we can get the direct reliability, by calculating the ratio between the successful number and the number of interactions. The algorithm proposed in [7] firstly adds the service reliability indicators into the QoS metrics and this algorithm is generally considered to be more effective than others, so we choose this algorithm as the only control group representing the traditional algorithm. The trusted routing algorithm and the traditional algorithm have been tested 20 periods, all service instances work well in the first 10 periods, and then we set the half service instances perform randomly, the other half service instances are still as good performances. Both trusted routing algorithm and traditional algorithm have been executed 50 times in a period, and then we calculate the average execution time and the success rate in a period.

It can be seen from Fig.1, in the condition with all service instances perform well in the first 10 periods, the trusted routing algorithm performs a litter better than the traditional algorithm in execution time and the success rate. In the last 10 periods, since half of the service instances performs randomly, the execution time of traditional algorithm increases rapidly, and the success rate is also decline rapidly, while the performance of trusted routing algorithm decline more slowly than traditional algorithm. So our trusted routing algorithm performs better than other routing algorithms.

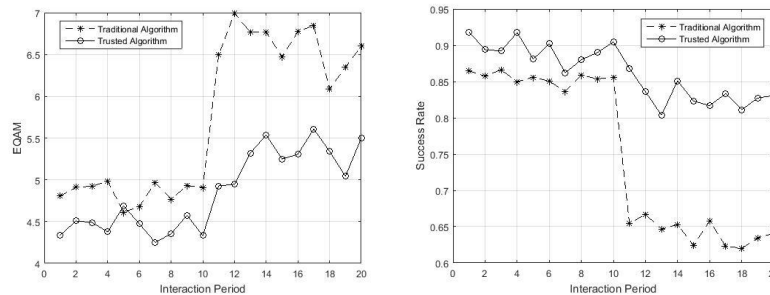


Figure 1. Contrast between traditional algorithm and trusted routing.

6. Conclusion

In this work, we analysis the problem of applying trust evaluation to routing algorithm. Based on Dempster-Shafer evidence theory, evidence distance and physical layer security theory, we propose a trust evaluation model of service instances, and this model can evaluate service reliability accurately, and then we propose the trusted routing algorithm by using this trust evaluation model. The experimental results confirm the advantages of our work in the success rate of routing and the performance of the QoS metrics.

Acknowledgement

This research was supported by the National High Technology Research and Development Program of China (863 Program) SS2015AA011306 and NSFC grants No. 61401445.

References

1. S Biswas, T Nag, S Neogy, Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET, in Proc *Applications and Innovations in Mobile Computing (AIMoC)* (Kolkata, India, 2014).
2. MMEA Mahmoud, X Lin, X Shen, Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 26(4),(2015).
3. IR Chen, F Bao, MJ Chang, JH Cho, Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 25(5),(2015).
4. Thomas Repantis, Xiaohui Gu, Vana Kalogeraki. QoS-aware shared component composition for distributed stream processing systems, *IEEE Transactions on Parallel and Distributed Systems*. Vol20(7),(2009).

5. Juan Du, Daniel Dean, Yongmin Tan, Xiaohui Gu, Ting Yu, Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds, *IEEE Transactions on Parallel and Distributed Systems*, Vol.25(25), (2014).
6. Gu Xiao-hui, Klara Nahrstedt, Rong Chang et al. SpiderNet: An integrated peer-to-peer service composition framework, in Proc *IEEE international Symposium on High-Performance Distributed Computing(HPDC)* (Hawaii, USA, 2004)
7. Gu Xiao-hui, Klara Nahrstedt. On composing stream on parallel and distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, Vol17(8),(2006)
8. Raman B, Katz R H. Load balancing and stability issues in algorithms for service composition, in Proc *IEEE INFOCOM* ,(California, USA,2003)
9. Angus F.M. Huang, Ci-Wei Lan, Stephen J.H Yang. An optimal QoS-based Web service selection scheme, *Information Science*, Vol179(19) ,(2009).
10. Yuan Chen, Lin Ma, Min Zheng, Kai Yu, A Trust Routing Protocol Based on D-S Evidence Theory in Mobile Ad Hoc Network, in Proc *IEEE/CIC International Conference on Communications in China (ICCC2014)*, (ShangHai, China, 2014)
11. Hu Chun-hua, Wu Min, Liu Guo-ping. QoS scheduling based on trust relationship in web service workflow, *Chinese Journal of Computers*. Vol32(1),(2009).
12. Zhu You-wen, Huang Liu-sheng, Chen Guo-liang, et al. Dynamic trust evaluation model under distributed computing environment, *Chinese Journal of Computers*, Vol34(1),(2011).
13. Dempster A. Upper and lower probabilities induced by multivalued mapping, *Annals of Mathematical Statistics*, Vol38(2),(1967)
14. Shafer G. A Mathematical Theory of evidence, (Princeton, NJ: Princeton University Press, 1976)
15. Shapley S. A value for n-person games, *Annals of Mathematical Statistics*, Vol28(1953).
16. Yager R. A class of fuzzy measures generated from a Dempster-Shafer belief structure, *International Journal of Intelligent Systems*, Vol114(12),(1999).
17. Yager R. On the entropy of fuzzy measures, *IEEE Transactions on Fuzzy Systems*, Vol8(4),(2000).
18. AL Jousselme, D Grenier, Éloi Bossé, A new distance between two bodies of evidence, *Information Fusion*, Vol 2(2),(2001).