International Journal of Grid Distribution Computing
Vol.8, No.2 (2015), pp.247-258
http://dx.doi.org/10.14257/ijgdc.2015.8.2.22

A CPN-based Trust Negotiation Model on Service Level Agreement in Cloud Environment

Hongwei Chen, Qiuxia Chen and Chunzhi Wang

School of Computer Science, Hubei University of Technology, Wuhan, China
chw2001@sina.com

Abstract

The negotiation process of the Service Level Agreement (SLA) in cloud environment is an interaction process of access control rules and credentials. Due to the mass of credentials in cloud environment, the negotiation efficiency is not high. To address the problem, this paper proposes an Automated Trust Negotiation (ATN) model based on Colored Petri Net (CPN), which exists a legitimate occurrence sequence and a reachable state space graph. A Minimal Credential Path Searching (MCPS) algorithm is proposed to find a minimum credential disclosure set in the reachable marking graph. The results show that the algorithm can effectively improve the negotiation efficiency.

Keywords: *Cloud Computing, Service Level Agreement, Automated Trust Negotiation, Credential set, Colored Petri Net*

1. Introduction

In cloud environment, the Cloud Service Consumer (CSC) can use resources elastically on their demand and Pay-Per-Use or Pay-As-You-Go; the ATN method [1-3] on SLA provides a new access control way to respond the dynamic resource request by requesting and disclosing digital certificates gradually between the Cloud Service Providers (CSP) and the CSC, finally to establish the mutual trust relationship. However, in the process of the actual SLA negotiation in cloud environment, each cloud service resources' acquisition requires mass of attribute credential to disclose, the complex access control rules and the large number of negotiation handshakes, which make the negotiation efficiency not high during the ATN process. Therefore, it is necessary to study the minimum disclosure credential set to control the ATN process on SLA in cloud environment, which reduces unnecessary credentials to disclose and improve the negotiation efficiency.

With the advantages of graphic intuitionism and understandability, the CPN [4] is an effective formal modeling and analysis tool to generate a secure and credible credential disclosure set on SLA in cloud environment. Especially for a complicated model with a large amount of data, the ATN strategies can be expressed in disjunctive normal form in the CPN, which can simplify greatly in cloud environment. In this paper, places represent credentials between two negotiation parties, and transitions represent the clause of access control policies.

The essence of ATN is that two strange negotiation parties exchange a series of credentials to establish trust relationship. In fact, the process of ATN is to search a credential disclosure sequence between the resource provider and resource requester in distributed network [5]. To improve the attributes security of user's identity during trust negotiation, Federica Paci [6] puts forward a minimum certificate sequence method that two parties only need to exchange the necessary property credentials.

In this paper, we provide an ATN example on SLA in cloud environment, build a CPN-based model in terms of the example, and analyze the CPN-based model according to legitimate credential sequences, which make resource request reachable. A reachable

ISSN: 2005-4262 IJGDC

state space graph can be mapped from the CPN model, and an algorithm for searching minimum credential disclosure set is put forward On the basis of the reachable graph.

This paper is organized as follows: Section 1 introduces the related research on ATN in cloud environment. Section 2 proposes architecture of ATN on SLA in cloud environment and describes the function of each component briefly. Section 3 gives a concrete ATN example on SLA in cloud environment, and presents access control strategies between CSC and CSP according to the example. Section 4 mainly describes the CPN model and the reachable state space graph according to the example. Then, Section 5 puts forward an algorithm for searching the minimum credential disclosure set and analyzes this algorithm, and the simulation results show that the algorithm can effectively improve the negotiation efficiency. Finally, Section 6 concludes the work.

2. Architecture of ATN on SLA in Cloud Environment

In cloud environment, it is dynamic for the CSC to use cloud resources, so the CSP needs a standard SLA document to manage cloud resources with the CSC. An SLA document can provide the CSC with different service levels, so the CSC and the CSP need negotiate for generating the SLA successfully before the CSP provide cloud resources and services for the CSC in terms of the SLA. During the process of trust negotiation, the two negotiation sides disclose credentials and access control policies gradually to establish trust relationship. This section describes the architecture of ATN on SLA and the function of each component during the process of trust negotiation. The proposed architecture of ATN on SLA is shown in Figure 1, which mainly includes three components: the SLA document, cloud resources, and the ATN module.

The SLA document contains many negotiation clauses, which mainly include service level, service pricing, QoS indicator and monitor management, *etc*. The CSC can start trust negotiation in terms of different cloud service level, which is corresponding to different service pricing and QoS indicator. After successful negotiation, the CSP will deploy cloud services and provides the cloud resources to the CSC according to the SLA document.

The CSP own cloud resources and provides cloud services by broadcasting their service type and service content to the CSC via resource catalogs. Currently, cloud services are divided into three categories [7], namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The ATN module mainly includes access control policies, credentials, negotiation strategies and negotiation protocol. Credential and access control policies have played an important role in protecting sensitive information together. Both negotiation sides who process credentials can access certain resources by the disclosure of the credentials. In order to guarantee successful ATN on SLA, confidence interval is introduced to choose the most credible credential to establish trust relationship [8]. Only when trust values of the credentials fall into the corresponding confidence interval, the credential can disclose. Credentials usually contain some sensitive information, such as the ID of cloud service application, the resource type and access control policies, trust value and various control parameters. Both negotiation sides hope to disclose as little information as possible to reach an SLA contract for cloud service. Negotiation strategy decides how to release certificates and access control policies [9-11]. This paper adopts the cautious negotiation strategy, namely the negotiation side provide the relevant credential only when the access control policy request the certain credential. In order to improve the negotiation efficiency, it's necessary to find a set of minimum credentials. The negotiation protocol is responsible for negotiation sequences of both sides on the basis of negotiation strategy.

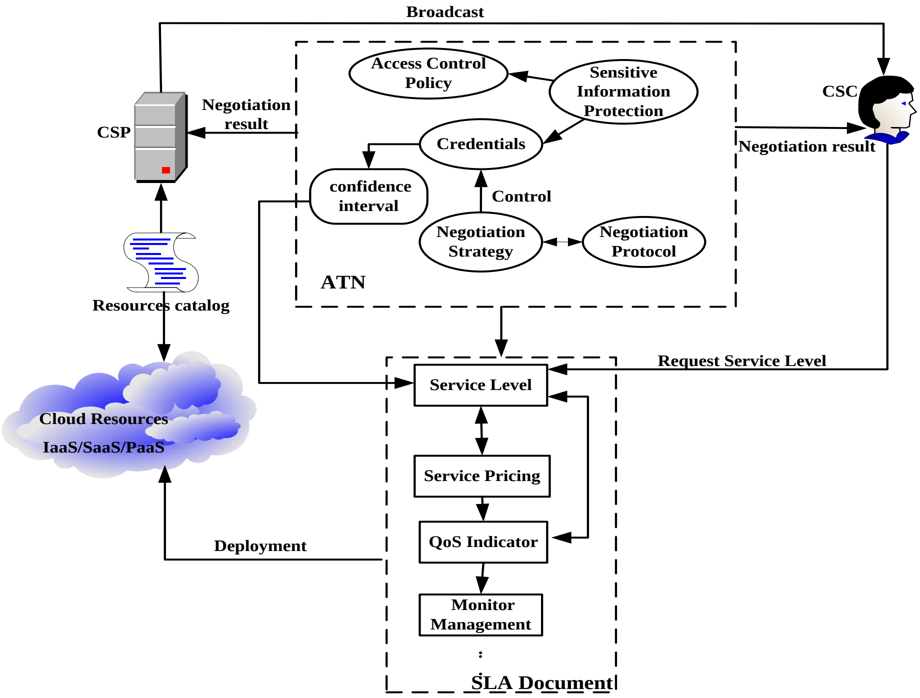

Figure 1. The Architecture of ATN on SLA in Cloud Environment

3. Access Control Policies on SLA in Cloud Environment

The access control policy on SLA in the paper uses disjunctive normal formula, $R \leftarrow D_1 \vee D_2 \vee \ldots \vee D_k$, $D_i = C_1 \wedge C_2 \wedge \ldots \wedge C_m$, $i \le k$. C_i represents the credentials that both negotiation sides need disclose.

In this paper, we give a example, and the scene is as follows. A regular CSC wants to rent a online management software in the cloud, and the CSP provides a discount ($Discount(i)$)to the regular CSC or those who rent the cloud service (execution time T) for more than 3 years. In order to protect their own interests, it is necessary to carry out an ATN to make a SLA document before renting this service. The CSC as a resource requestor starts the SLA-based trust negotiation process. In order to avoid being deceived and improving safety, first of all, both negotiation sides need disclose their identity information. The CSP need disclose the certificate of the relevant permits (*CSP.c*), and the CSC need disclose the registered certificate (*User.ID* and *password*) and propose the service parameters about this management software such as reliability($Rel(i).level$), availability ($Av(i).level$),and service time(T) to get a services discount. According to the architecture of figure 1, the cloud service in the example belongs to the application of SaaS, then the SLA trust negotiation between both sides mainly focus on the following aspects:

(1) Safety of the CSC and the CSP. Before negotiating service parameters, both sides need verify the authorization of the service and permission, such as the $User.ID$ and $Password$.

(2) The service pricing. The budget of the cloud service is calculated as certain principles, such as discount, service level (level) and service execution time T.

(3) Credibility of cloud resources. The credibility of the service properties can be divided into three levels: trust, unknown and distrust. The CSC chooses the service level they want, and the credibility is evaluated by the overall trust value in a period of time.

(4) Reliability of cloud resources, such as availability, reliability, and mean time to restoration (MTTR).

Figure 2 is access control policies for the CSC and the CSP according to above example.

Access Control Policies for the CSC:

$User.ID \leftarrow CSP.c \wedge E_{ID}(f)$

$Password \leftarrow CSP.c \vee R \wedge E_{password}(f)$

$N(i).price \leftarrow Bc \wedge Discount(i) \wedge E_{N(i).price}(f)$

$Av(i).level \leftarrow AV(i) \wedge E_{Av(i).level}(f)$

$Rel(i).level \leftarrow REL \wedge E_{\mathrm{Rel}(i).level}(f)$

$t(i).level \leftarrow T \wedge E_{t(i).level}.(f)$

Access Control Policies for the CSP:

$CSP.c \leftarrow User.ID \wedge Password \wedge E_{CSP.c}(f)$

$Service(i) \leftarrow (N(i).price \wedge Av(i).level) \vee (Rel(i).level \wedge t(i).level) \vee Mttr(i).level \wedge E_{Service(i)}(f)$

$AV(i) \leftarrow N(i).price \wedge Av(i).level \wedge E_{AV(i)}(f)$

$REL(i) \leftarrow N(i).price \vee Rel(i).level \wedge E_{REL(i)}(f)$

$Bc \leftarrow True$

$R \leftarrow True$

$MTTR(i) \leftarrow Mttr(i).level \wedge E_{MTTR(i)}(f)$

$T \leftarrow True$

$Discount(i) \leftarrow User.ID \vee ((T > 3) \wedge R))$

Figure 2. Access Control Policies for the CSC and the CSP

4. The CPN Model for ATN on SLA in Cloud Environment

4.1. Mapping from Access Control Policies to the CPN Graph

When a CPN graph is mapped to access control policies, places represent the limited access resources or credentials, and transitions represent the disclosure of credentials, which is a clause of access control policies. With Boolean operation expression, the logical relationship between places and transitions is defined as follows:

(1) The flow relationship from transitions to places is denoted as : $R \leftarrow D_1 \vee D_2 \vee \ldots \vee D_k$;

(2) The flow relationship from places to transitions is denoted as: $D_i = C_1 \wedge C_2 \wedge \ldots \wedge C_m$;

(3) The initial unprotected credential is expressed as: $C_i \leftarrow True$.

Figure 3 shows the mapping from access control policies to the CPN graph with the CPN tool [12], and $C(p) = \{C_S, C_C\}$ denotes the color set of credentials from both negotiation sides.

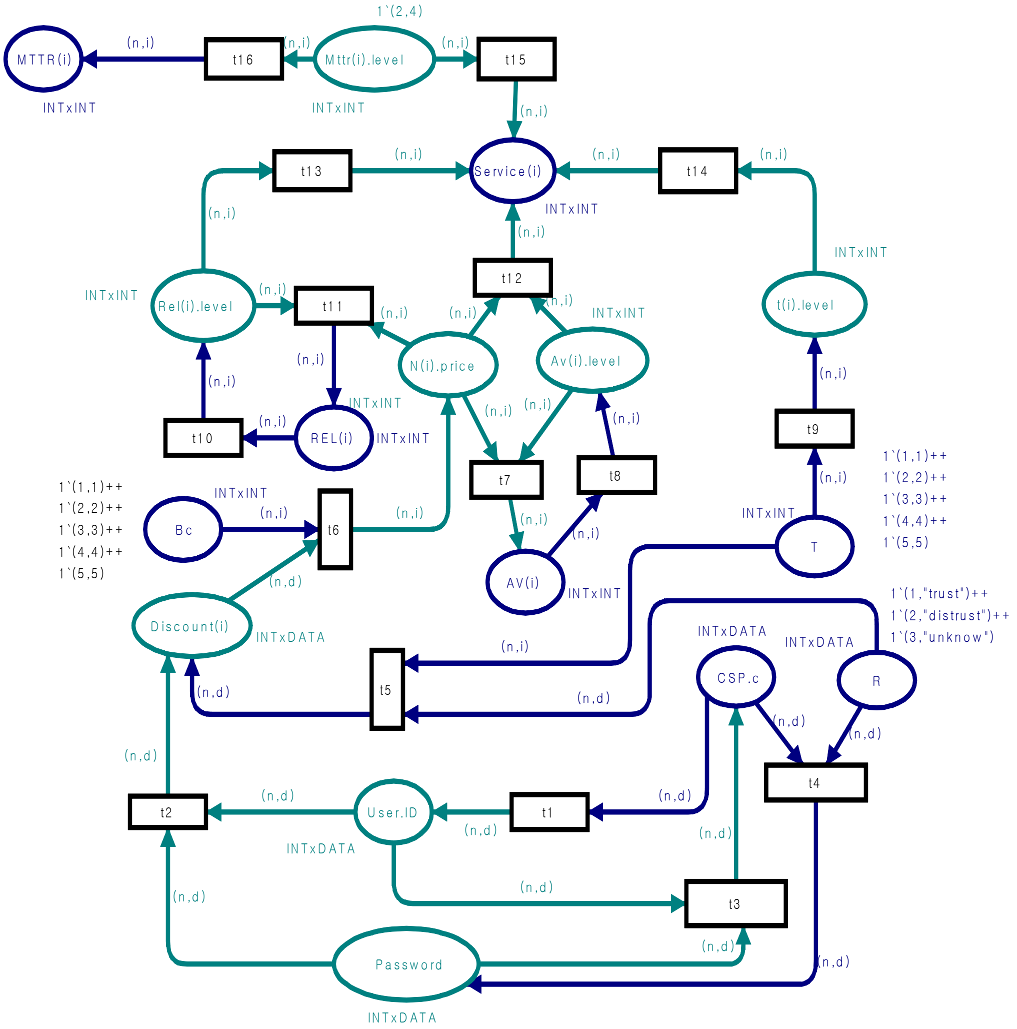

Figure 3. Mapping from Access Control Policies to the CPN Graph

$C_S = \{CSP.c, Bc, REL(i), AV(i), R, Discount(i), MTTR(i), T\}$ is a credential set for service level i. Bc denotes the color set of different service levels' budget to the CSC. The CSC should meet the demand of service budget in order to access a certain level of cloud service. The place R represents the color set which shows the trust level of cloud resources. The initial trust level can be obtained directly by broadcasting. T denotes the color set of the execution time.

$C_C = \{User.ID, Password, N(i).price, Av(i).level, Rel(i).level, Mttr(i).level, t(i).level\}$ corresponds to the credential set which the CSC need disclose to access the cloud service i in the process of negotiation, such as ID verification($User.ID$, $Password$), signed service price certificate($N(i).price$), and the service level i of availability($Av(i).level$), reliability($Rel.level$), mean time to restoration($Mttr(i).level$), execution time($t(i).level$) and discount ($Discount(i)$). Of which, $Mttr(i).level$ denotes the color combination of mean time to restoration, and the credential accession is not restricted.

$C(Utility) = \{(n,i)\}$ is an application function, which represents a threshold function or a Boolean expression to decide whether disclosing the access control policy during the trust negotiation. The application function can make the place changed and transfer negotiation to the next credential, only when the trust value of the certificate meets the demand of confidence interval. The application function varies with different negotiators, and the negotiated information is $C_S \times C_C \times C(t) \times C(Utility)$.

4.2. Reachability Analysis of the CPN Model

In order to find a credential disclosure set for accessing the requested cloud resources, it is necessary to analyze the above CPN model. Due to the boundedness of the CPN, there exists one or more legitimate reachable sequences δ . If a sequence from the initial marks M_0 to the end marks M_F exists, that is $M_F = M_0[\delta >$, and the sequence is reachable.

In Figure 4, all states and changes can be seen from a reachable marking graph. There are 3375 nodes in the state space mapping from the CPN model, so Figure 4 is only a part of reachable marking graph from the above CPN model. Each node represents a reachable marking, and each arc represents the occurrence of a binding element from source node to destination node. The reachable marking graph records all changes of places and transitions in the CPN model, and expresses the logical relationship among various events. Each node's information about the number of subsequent nodes and the precursor nodes is given in the graph, such as the "1" node "0:10" denotes it has 10 subsequent nodes and no precursor node. When negotiation process starts, the enabled marking place makes a transition, while other places are in waiting state. If an arc function meets the requirements of a transition, then the place marking conveys to the other place. The reachable marking graph in Figure 4 demonstrates the feasibility of the CPN model.

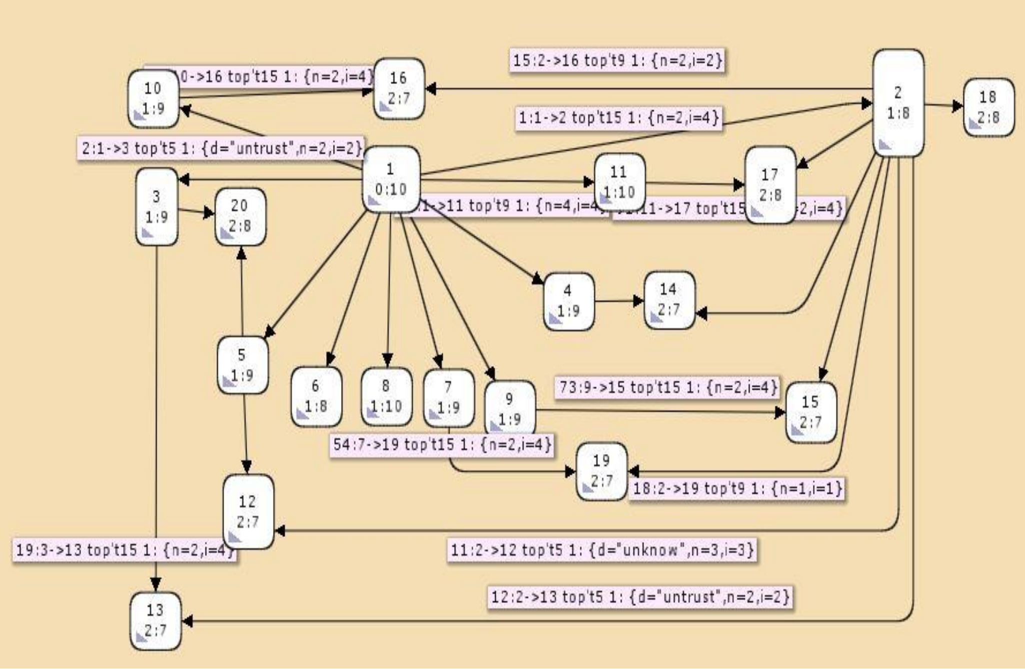
0->16 top't15 1: {n=2,i=4}
15:2->16 top't9 1: {n=2,i=2}
10
1:9
16
2:7
2
1:8
18
2:8
1:1->2 top't15 1: {n=2,i=4}
2:1->3 top't5 1: {d="untrust",n=2,i=2}
1
0:10
11
1:10
17
2:8
3
1:9
20
2:8
1->11 top't9 1: {n=4,i=4
11->17 top't15
2,i=4}
4
1:9
14
2:7
5
1:9
6
1:8
8
1:10
7
1:9
9
1:9
73:9->15 top't15 1: {n=2,i=4}
15
2:7
54:7->19 top't15 1: {n=2,i=4}
19
2:7
18:2->19 top't9 1: {n=1,i=1}
12
2:7
19:3->13 top't15 1: {n=2,i=4}
11:2->12 top't5 1: {d="unknow",n=3,i=3}
12:2->13 top't5 1: {d="untrust",n=2,i=2}
13
2:7

Figure 4. Part of Reachable Marking Graph from the CPN Model

5. The Algorithm for Minimum Credential Disclosure Set

5.1. The Minimal Credential Path Searching Algorithm

In the process of actual trust negotiation on SLA in cloud environment, each acquisition for cloud service requires disclosure of many attribute credentials to the other party. Both negotiations sides wish to disclose as little information as possible to achieve successful trust negotiation on SLA in cloud environment, including some sensitive information or unnecessary credentials. In an example like the one illustrated above, there are 14850 arcs and 3375 nodes. The more nodes, the more complicated CPN model, so it is necessary to find the shortest path to reach the target node service (i) that is to find a minimal credential disclosure set. The following is the pseudo code of the Minimal Credential Path Searching (MCPS) algorithm for minimum credential disclosure set:

Table 1. The Minimal Credential Path Searching (MCPS) Algorithm

Algorithm 1: *The Minimal Credential Path Searching Algorithm*

```
$OPEN = \{S\}; CLOSED = \phi;$
$while(!OPEN)\{$
    $n = get\_min\_evaluation(OPEN);$
    $if\ (n == Service\ (i))$        //Service(i) is the target node
        $break;$
    $for(each\ child\ u\ from\ n)\{$
        $gu = evaluate(u);$
        $if\ (u \in OPEN)\ \{$
            $fo = calculate\_evaluation(OPEN);$
            $if(gu < fo)\ \{$
                $u.parent \leftarrow n;$
                $fo = update\_evaluation(OPEN);$
            $\}$
        $\}$
        $else\ if\ (u \in CLOSED)$
            $continue;$
        $else\ \{$        $// u \notin OPEN\ \&\&\ u \notin CLOSED$
            $u.parent \leftarrow n;$
            $OPEN = OPEN \cup \{u\};$
        $\}$
    $\}$
    $CLOSED = CLOSED \cup \{n\};$
    $sort\_evaluation(OPEN);$
    $min\_path = update\_path(OPEN);$
    $min\_dist = update\_distance(OPEN);$
$\}$
```

The MPCS algorithm in this paper is on the basis of the heuristic searching algorithm A*, which is used to find optimal path. A successful SLA negotiation needs kinds of service quality property and identity information to establish trust relationship for cloud service. As many credentials exist in the process of SLA negotiation in cloud environment, credentials will be mapped into the CPN model as many nodes. The MCPS algorithm evaluates nodes which need to be extended, and chooses the best node; then continues to extend the node, until to find the target node service (i). In the process of trust negotiation in cloud environment, many credentials need to be classified to reduce the state space and improve the efficiency. In fact, classification is a clustering problem [13-14], so this paper also carries on the cluster analysis for states of nodes.

According to the characteristic x_i of each node in state space graph, the initial samples are builded. The original data matrix has n samples and m dimensions, and the matrix form is as shown in Formula (1):

$$X = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{bmatrix} \tag{1}$$

Formula (2) is the standardization of standard deviation result from Formula (1).

$$x'_{ij} = \frac{x_{ij} - \frac{1}{n}\sum_{i=1}^{n} x_{ij}}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_{ij} - \frac{1}{n}\sum_{i=1}^{n} x_{ij})^2}} \quad (i = 1,2,\dots,\ n,\ j = 1,2,\dots m) \tag{2}$$

Calculating the similarity r_{ij} between the sample i and the sample j , and constructing the fuzzy similarity matrix R ,

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1m} \\ r_{21} & r_{22} & \dots & r_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ r_{n1} & r_{n2} & \dots & r_{nm} \end{bmatrix},\ r_{ij} = 1 - c\sum_{k=1}^{m}\left|x_{ik} - x_{jk}\right| \tag{3}$$

In Formula (3), c is a proper selective parameter, and the matrix R is a symmetric matrix. We can judge whether an unclassified node belongs to the $i-th$ node by means of the following function,

$$x_{ij} = \begin{cases} 0, & r_{ij} < \beta \\ 1, & r_{ij} \geq \beta \end{cases} \tag{4}$$

,in which β_i is the neighbor threshold. So, when traversing the graph, the known $i-th$ classification threshold λ_i satisfies $I = (\sum_{i=1}^{n} x_{ij})/n$. If $I \geq \lambda_i$, the node belongs to the category.

5.2. Simulation Results and Analysis

In order to verify the validity and reliability of the Minimal Credential Path Searching algorithm, we conduct simulation test according to the above example. There exist 15 kinds of credentials in the example, so the trusted nodes and the negotiation goal (Service (i)) can classify 15 categories. According to the algorithm, first of all, 3600 nodes are generated randomly, then a similarity matrix is created, and different categories represent different attributes of trusted nodes, such as reliability, cost budget, *etc*.

In Figure 5, it is about 15 kinds of trusted nodes' classification diagram, trusted nodes' value falls into different confidence interval after normalization of the trust value, it is convenient for the CSC to search directly from a class to choose a eligible trusted node and turn into the next class of trusted nodes quickly.

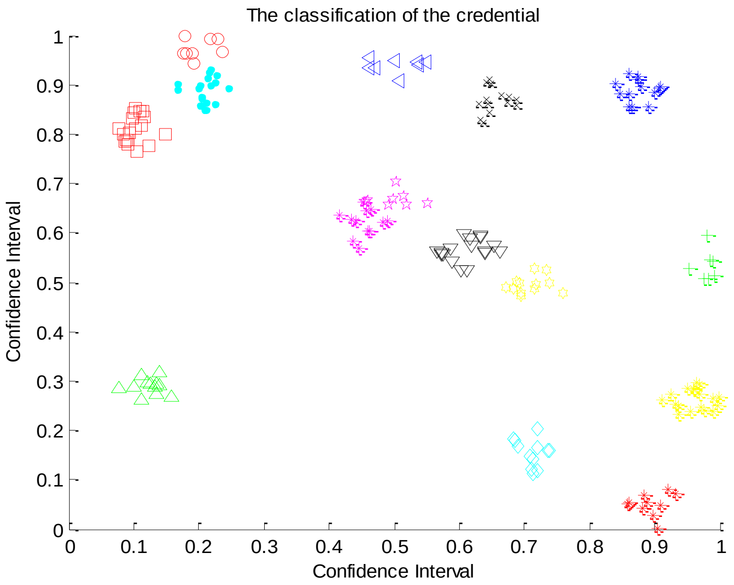

Figure 5. Trusted Nodes Classification Diagram based on the MCPS Algorithm

With the increasing of nodes, the arc number and interaction of nodes become more complicated, and classification time raises sharply, thus classification needs in a large number of nodes condition when traversing nodes. We increase the number of nodes gradually and record the elapse time that different number of nodes to be classified. The simulation result is shown in Figure 6. From the simulation result, we can see that with the increase of trusted nodes, the classification time increases when using the MCPS algorithm to traversal all trusted nodes. When the number of the nodes is small (<600), the classification time is short, and the classification time rises observably when trust nodes become large gradually.

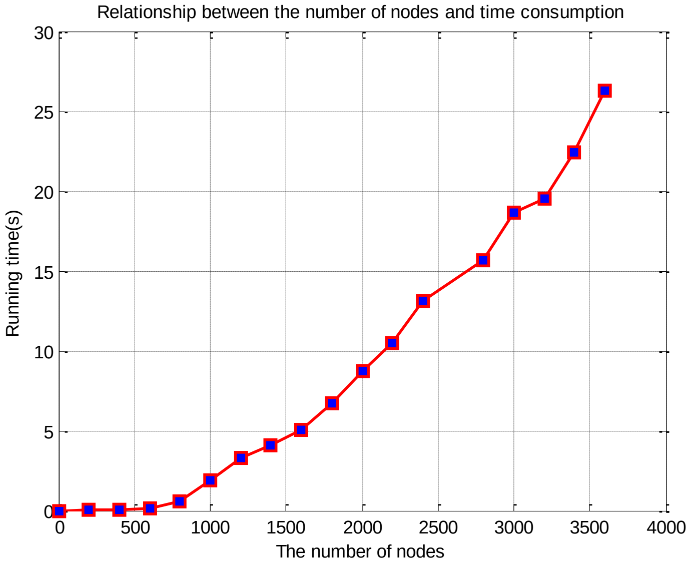

Figure 6. Relationship Diagram between the Number of Nodes and Time Consumption

With the increase of trusted nodes, the shortest distance both grow when using the MCPS algorithm with classification and the BFS [15] algorithm with no classification. The MPCS algorithm for searching the shortest distance is less than the latter. Figure 7 shows comparison between the MCPS algorithm and the BFS algorithm in shortest distance.In Figure 7, the shortest distance equals to the shortest path to service (i) that means the least credential exchange. In cloud environment, on the same condition of the same number of nodes, the length of shortest path generated by the MCPS algorithm is less than that by the BFS algorithm.

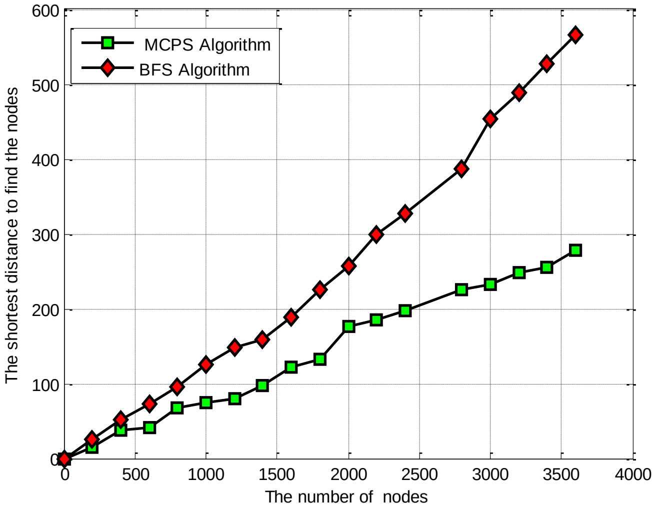

Figure 7. Comparison between the MCPS Algorithm and the BFS Algorithm in Shortest Distance

6. Conclusions

This paper we propose a CPN-based trust negotiation model on SLA in cloud environment. In the CPN model, a credential is regarded as a trusted node, and the credential with a trust value falling into confidence interval determines the corresponding service level. In cloud environment, there are a large number of credentials need to be exchanged, which make the trust negotiation efficiency not high. Therefore, we need simplify the complex model and disclose the minimum credentials. The reachable marking graph is the main measure for qualitative analysis and quantitative analysis in the CPN model, which is also the foundation of related properties analysis. A Minimal Credential Path Searching algorithm is proposed to find a minimum credential disclosure set in the reachable graph. The results show that the algorithm can effectively improve the negotiation efficiency. In the future, we will make a further extension for the proposed architecture of this paper, and build the layered CPN model on SLA, that adapts to the complex cloud environment better.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 61170135, No. 61202287, No.61440024), and the General Program for Natural Science Foundation of Hubei Province in China (No. 2013CFB020, No. 2013CFA046).

References

[1] A. V. Dastjerdi and R. Buyya, "An Autonomous Reliability-Aware Negotiation Strategy for Cloud Computing Environments", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, **(2012)**, pp. 284-291.

[2] A. C. Squicciarini, F. Paci and Elisa Bertino, "Trust establishment in the formation of Virtual Organizations", Computer Standards & Interfaces, vol. 33, no. 1, **(2011)**, pp. 13-23.

[3] D. Zou, S. Du, W. Zheng and H. Jin, "Building Automated Trust Negotiation architecture in virtual computing environment", The Journal of Supercomputing, vol. 55, no. 11, **(2011)**, pp. 69-85.

[4] P. Katsaros, "A roadmap to electronic payment transaction guarantees and a Colored Petri Net model checking approach", Information and Software Technology, vol. 51, no. 2, **(2009)**, pp. 235-257.

[5] C. A. Ardagna, S. De C. di Vimercati, S. Foresti, S. Paraboschi and P. Samarati, "Minimizing disclosure of client information in credential-based interactions", International Journal of Information Privacy, Security and Integrity, vol. 1, no. 2, **(2012)**, pp. 205-233.

[6] F. Paci, D. Bauer, E. Bertino, D. M. Blough, A. Squicciarini and A. Gupta, "Minimal credential disclosure in trust negotiations", Identity in the Information Society, vol. 2, no. 3, **(2009)**, pp. 221-239.

[7] I. Muttik and C. Barton, "Cloud security technologies", Information security technical report, vol. 14, no. 1, **(2009)**, pp. 1-6.

[8] Q. Han, Y. Lin, R. Zhang, H. Wen, Y. Xie, X. Zhu, Y. Jiang and X. Guo, "A P2P recommended trust nodes selection algorithm based on topological potential", 2013 IEEE Conference on Communications and Network Security (CNS), IEEE Press, **(2013)**, pp. 395-396.

[9] X. Dongmei, Z. Guosun, H. Yu and B. Yu, "Analysis of Automated Trust Negotiation Policy", 2010 2nd International Conference on e-Business and Information System Security (EBISS), IEEE Press, **(2010)**, pp. 1-4.

[10] C. Ke, Z. Huang and M. Tang, "Supporting negotiation mechanism privacy authority method in cloud computing", Knowledge-Based Systems, vol. 51, **(2013)**, pp. 48-59.

[11] A. V. Dastjerdi and R. Buyya, "An Autonomous Reliability-Aware Negotiation Strategy for Cloud Computing Environments", Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012) , IEEE Press, **(2012)**, pp. 168-171.

[12] L. Yonghao and L. Yun, "Research on Modeling of Multiparty Trust Negotiation Based on Coloured Petri-net in P2P Network", 2010 Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), IEEE Press, **(2010)**, pp. 437 - 441.

[13] P. Jiang and M. Singh, "SPICi: a fast clustering algorithm for large biological networks", Bioinformatics, vol. 26, no. 8, **(2010)**, pp. 1105-1111.

[14] M. Polczynski and M. Polczynski, "Using the k-Means Clustering Algorithm to Classify Features for Choropleth Maps", Cartographica: The International Journal for Geographic Information and Geovisualization, vol. 49, no. 1, **(2014)**, pp. 69-75.

[15] M. Kurant, A. Markopoulou and P. Thiran, "Towards unbiased BFS sampling", IEEE Journal on Selected Areas in Communications, vol. 29, no. 9, **(2011)**, pp. 1799-1809.

Authors

Hongwei Chen, in 2006, he graduated from Nanjing University of Posts & Telecommunications and received PHD degree in China, majored in Communication and Information System. He is an associate professor at School of Computer Science in Hubei University of Technology, Wuhan, China. From August of 2013 to February of 2014, he was an academic visiting scholar at Temple University in USA. Now his major study field is Peer-to-Peer Computing, Cloud Computing and SDN.

Qiuxia Chen, She is from Guangxi Province of China, and a master candidate at School of Computer Science in Hubei University of Technology, interested in Cloud Computing.

Chunzhi Wan, She is from Hubei province of China, PHD, professor and dean at School of Computer Science, in Hubei University of Technology. She is interested in Peer-to-Peer Computing and network security. She is a member of CCF, ACM and IEEE.