Group Analysis and Evaluation Method of Enterprise Competitiveness Based on Law of Logic Partial Order

Xin Wang

School of Taxation and Public Administration, Jiangxi University of Finance and Economics, Nanchang 330038, Jiangxi China

Abstract
The node in the network of enterprise competitiveness is possible to receive service and information with poor quality from the other nodes. Group analysis and evaluation is a common method to solve this problem. The calculation mechanism of enterprise competitiveness based on score feedback has the following disadvantages: unable to distinguish the difference between malicious evaluation and error evaluation given by honest nodes; need second evaluation on the score credibility, which slows down the computing speed of competitiveness; the method of using number to express the node reputation is not natural. In fact, the use of group analysis and evaluation is to determine the relative order of node credibility. Therefore, a kind of reputation based law of logic partial order (RLPO) was proposed. The mathematical modeling and theoretical analysis were conducted based on RLPO and its malicious attacks. Results show that the influence of non-malicious error of RLPO decreases with the exponent of law of logic partial order number; generally, the effect of malicious attack on RLPO decreases with the polynomial of law of logic partial order number; for the collusion attack by design, the malicious attacks were effectively neutralized because RLPO must introduce the right information. Therefore, RLPO no longer feeds back rating information. So there is no group analysis and evaluation problem caused by score feedback (such as no need of second evaluation for the credibility of feedback information).

Key words: Enterprise Competitiveness, Group Analysis and Evaluation, Law of Logic Partial Order, Collusion Attack.

1. INTRODUCTION
Due to the less control of node into the network of enterprise competitiveness network, a lot of enterprise competitiveness systems even do not conduct any control. For such open systems, there will inevitably appear plenty of selfish, malicious, or not able to provide certain service ability of nodes. These nodes will seriously affect the overall performance of the system. This influence performs much obviously in enterprise competitiveness e-commerce system, such as the Lightshare. In such system, whether the service provider is honest and trustworthy or not will directly determine the quality of received service for customers, and determine the system availability. For the enterprise competitiveness file sharing and enterprise competitiveness streaming media system, the existing lowperforming nodes can also cause serious decrease of the system availability. Group analysis and evaluation are suitable methods to solve the basic problem. The basic method is to find low-performing nodes through the calculation of reputation, so as to avoid exchange with these nodes in the information exchange (Li and Chang, 2007; Chalmeta, Campos and Grangel, 2001; Kalpic and Bernus, 2002).

Take the present method of enterprise competitiveness reputation mechanism as the foundation (Li and Chang, 2007; Chalmeta and Campos and Grangel, 2001; Kalpic and Bernus, 2002): first according to the search conditions, request the node \( r \) to search found the target node set \( G \) to meet the requirements; for each node \( g \) in \( G \), the reputation value of \( g \) should be obtained before the service exchange of node \( r \) and \( g \); then, according to the size of the node reputation value, rank the nodes in \( G \) and return to the users of enterprise competitiveness; finally, determine to choose which node to complete the service exchange by the user (Li and Chang, 2007). The group analysis and evaluation of \( g \) is the core of this process. The common method of node \( r \) in the calculation of \( g \) reputation value is that, the node \( r \) first selects witness set \( W = \{ w_1, w_2, ..., w_k \} \), each of \( w \in W \) will produce an evaluation value \( t_w \) for \( g \). Based on the group analysis and evaluation value, the credibility can be calculated by \( r \) through the aggregation function.

At present, the majority of group analysis and evaluation mechanism of enterprise competitiveness calculates \( T_g \) based on Formula (1) (Chalmeta, Campos and Grangel, 2001; Kalpic and Bernus, 2002; Chrysaﬁadi and Virvou, 2013):
Herein, $I$ is the credibility evaluation obtained from the direct interaction experience, $R$ is the result after the feedback aggregation of recommended node. When calculating $R$, $C_w$ means the recommended credibility evaluation of the given recommended reputation value $r_{wg}$ from the node $r$ to node $w$ (namely the credibility of feedback in the literature (Praznik, Butala and Senegačnik, 2013)). By using the recommended credibility as weight to combine the reputation feedback value, the global reputation value of node $g$ can be obtained. Except for the above literatures, many researches of enterprise competitiveness reputation management (Praznik and Butala and Senegačnik, 2013; Yim and Kim and Seong, 2013; O’Neill and McDonald and Deegan, 2015; Stanton and Nielsen and Tamsir, 2014) also regard Formula (1) as the basis. They usually synthetically consider other factors on the basis of Formula (1). For example, literature (Praznik, Butala and Senegačnik, 2013) provides the idea of combining the node similarity in considering the feedback. Literature (Yim, Kim and Seong, 2013) found and applied the power-law distribution characteristics of reputation feedback when collecting reputation feedback. And the literature (Neill, Donald and Deegan, 2015) considers the differences of node credibility in different areas. In addition, although some other research work of enterprise competitiveness reputation (Camci, Medjaher and Zerhouni, 2013; Bhowmik, You and Salahuddin, 2014; Power, Klassen and Kull, 2015) did not directly study the calculation of $T_{g}$, they finally acted on $T_{g}$. For example: the literature (Camci, Medjaher and Zerhouni, 2013) gives that how to build the appropriate incentive strategy on the basis of reputation, and the calculation of competitiveness took Formula (1) as the foundation; the RETM method put forward in the literature (Power, Klassen and Kull, 2015) is to first filter the useless and misleading recommended data before the aggregation of reputation feedback, so as to improve the accuracy of the results.

The group analysis and evaluation method based on Formula (1) has the following problems: (1) needs to evaluate the rater and recommendation credibility, namely the $c_w$ in Formula (1). In the open environment like enterprise competitiveness, it is difficult to correctly evaluate the recommendation credibility; (2) the $T_{g}$ and the recommended value $r_{wg}$ in Formula (1) are scores. So the group analysis and evaluation method becomes a function on the numerical, and only relies on number as reputation feedback is not able to carry more meanings. In addition, there exist problems like unified standard for evaluation by using scores as the group analysis and evaluation.

In fact, the node reputation value is to be used for information exchange of selected high credibility nodes. Therefore, the basic purpose of group analysis and evaluation is to confirm the relative order of node reliability. On this basis, reputation based law of logic partial order (RLPO) was proposed in this paper. In RLPO, the witness node $w$ feedback a node sequence for the target node $g$:

$$R_r(w,g) = \{p_1, p_2, \ldots, p_m\}$$

Herein, $\exists j \in \{1, \ldots, m\} \cdot g = p_j, R_r$ is a sequence descending ranking with the node credibility (so it is called law of logic partial order competitiveness calculation method). Now the group analysis and evaluation method of enterprise competitiveness is shown in Figure 1.

![Figure 1. The group analysis and evaluation method of enterprise competitiveness based on RLPO](image-url)

(1) The node $r$ searches the node set $G$ that can respond to service requests in enterprise competitiveness network;
(2) Each node \( w \) that received \( Q \) returns a feedback sequence \( R_j(w,Q) \) descending ranking with the node credibility;

(3) The node \( r \) conducts group analysis and evaluation (namely operates RLPO) according to the received sequence set;

(4) The node \( r \) selects partial nodes \( O \subseteq G \) for information exchange according to the RLPO results.

The input of RLPO is \( |P| \) sequences of \( R_j \), and the output is the sequence \( \{r_1, r_2, ..., r_k\} \) formed from \( k \) highest reputation nodes in \( G \).

Obviously, in the process of calculating \( \{r_1, r_2, ..., r_k\} \) according to \( R_j \), RLPO only needs the node sequence information, instead of the second evaluation for recommendation credibility and the introduction of node reputation value (score). At the same time, \( R_j \) has more meanings, which avoids the two problems of group analysis and evaluation based on Formula (1). The theoretical analysis and simulation results show that:

1. RLPO performs better than the current group analysis and evaluation method of enterprise competitiveness in dealing with the uncertainty of trust relationship and improving the convergence speed of competitiveness;
2. RLPO shows better performance against malicious attacks on reputation;
3. RLPO does not generate score consistent problem. Therefore, the proposed competitiveness computing method based on law of logic partial order can better solve it.

2. THE COMPETITIVENESS COMPUTING METHOD BASED ON LAW OF LOGIC PARTIAL ORDER

2.1. The Global RLPO Method

For the convenience of analysis, first suppose that for any query \( Q \) initiated from, any node in enterprise competitiveness \( p \in P \) can return to a \( R_j(p,Q) \). And this sequence contains all the nodes in \( P \). So it is called the global RLPO method. Now, \( r \) will receive \( n = |P| \) feedback sequences:

\[
\begin{align*}
R_j(1) = & \{p_{11}, p_{12}, ..., p_{1n}\} \\
R_j(2) = & \{p_{21}, p_{22}, ..., p_{2n}\} \\
& \vdots \\
R_j(n) = & \{p_{n1}, p_{n2}, ..., p_{mn}\}
\end{align*}
\]  

(2)

Malicious nodes lead to \( R_j(i) \) contain intentional errors. The uncertain trust relationship will make \( R_j(i) \) occur the non-malicious error. Both of them will lead to erroneous group analysis and evaluation. The following k-Ranks RLPO group analysis and evaluation method algorithm is first used to eliminate the non-malicious errors in the group analysis and evaluation information.

Definition 1(k-Ranks RLPO). For \( R_j(1), R_j(2), ..., R_j(n) \), denote the \( j \) item in \( R_j(i) \) as \( R_j^i(i) \). The \( R_j^i(1) \) returned from \( k\)-Ranks RLPO is the \( R_j^i(m) \) item with the most frequency in sequence \( \{R_j^i(1), R_j^i(2), ..., R_j^i(n)\} \).

The work effects of k-Ranks RLPO. If each \( R_j(i) \) in Formula (2) can correctly give the reputation ranking sequence of node, here all the \( R_j(i) \) are exactly the same, then k-Ranks RLPO apparently returns the correct result. Now analyze that, when some random errors (namely the non-malicious error caused by uncertain information) occur in \( R_j(i) \), the work efficiency of k-Ranks RLPO.

Theorem 1. k-Ranks RLPO can effectively eliminate the non-malicious error in \( R_j(p,Q) \).

Prove: The meaning of containing uncertain \( R_j(p,Q) \) is that the nodes obtain complete information will give a correct evaluation result, while other nodes will give the evaluation containing random errors because of the incomplete information, and these random errors are independent. The essential difference with malicious attack is that in malicious attacks, these errors are related, or synergistic.

From the formal point of view, the uncertainty in \( R_j(p,Q) \) refers to \( R_j(i) \) is in the \( j \) position or right, or contains independent random errors. We can assume that the correct evaluation \( C_j^i \) of sequence \( \{R_j^i(1), R_j^i(2), ..., R_j^i(n)\} \) has \( \alpha \) proportion, then the number of random error evaluation \( E_j^i(i) \) is \((1-\alpha)n\). The
independent random errors show that the probability such as \( E_j'(i) \) (the probability is \( 1/(n-1) \)) selected the nodes in \( P/\{C_j'\} \).

According to the definition 1, the returned \( r_j \neq C_j' \) of k-Ranks RLPO algorithm, if and only if the times of the identical nodes occurred in \( E_j'(i) \) is not less than \( \alpha n \), the probability of the event occurrence equals to the probability that choose the same items with \( \alpha n \), and other items can be selected arbitrary from \( E_j'(i) \) with the number of \((1-\alpha)n\) (thus contains the condition with more than \( \alpha n \) identical items (including the fact that random errors are independent of each other in \( R_j'(i), 1 \leq i \leq n \)):

\[
\left( \frac{1}{n-1} \right)^{(n-1)} = \left( \frac{1}{n-1} \right)^{\alpha n-1}
\]

This probability value multiplies \((1-\alpha)n\) combinatory numbers with \( \alpha n \) items from \( E_j'(i) \) is the probability of \( r_j \neq C_j' \):

\[
p_r(r_j \neq C_j') = \left( \frac{(1-\alpha)n}{an} \right)^{\alpha n} \leq \left( \frac{((1-\alpha)n)^{\alpha n}}{(an)^{\alpha n-n}(n-1)^{\alpha n-1}} \approx \frac{1}{a^{\alpha n-n}} \times \frac{1}{(n-1)!} \right)
\]

Therefore, as long as \( \alpha \) is a constant (not \( O(1/P(N)) \)), \( P_i (r_j \neq C_j') \) is a number of 0 with \( n \) exponential order. This shows that as long as the k-Ranks RLPO algorithm receives certain scale of law of partial order, it will be able to return to the correct ranking \( r_j \), \( 1 \leq j \leq n \) with significant probability. If there is no malicious attack in \( R_j (p, Q) \), and only exists uncertainty of information, the assumption of \( \alpha \) be a constant is reasonable; but even \( \alpha \) is very small, due to the exponential decay existing in \( r_j \neq C_j' \), k-Ranks RLPO will soon return to the correct result, with the increasing number of collected law of partial order. QED.

Theorem 1 shows that k-Ranks RLPO can effectively eliminate the uncertainty of the information in group analysis and evaluation. But in order to resist malicious attacks, namely when collaborative error occurred caused by collusion attacks in \( R_j (p, Q) \), k-Ranks RLPO needs further improvement. The prove process of Theorem 1 shows that the fundamental difference of the random errors caused by malicious attack and uncertain information is that, \( E_j'(i) \) in malicious attack is no longer independently selecting nodes in \( P/\{C_j'\} \) with equal probability, but once \( E_j'(i) = e \) in \( i \), some \( R_j'(c) \) given by common nodes \( c \) no longer select other nodes independently, while choosing \( e \) with the probability much larger than \( 1/(n-1) \) (the probability is actually closer to 1), that is

\[
\exists (c \in p \Lambda e \neq i) \Pr(E_j'(c) = e | E_j'(i) = e) \gg \frac{1}{n-1}
\]

Formula (2) gives the mathematical meaning of collusion attack different from the uncertain error. On this basis, it can describe the malicious attacks that k-Ranks RLPO cannot deal with.

Definition 2 (the collusion attack of RLPO). If there exists \( j \), making the highest occurrence frequency \( R_j'(m) \neq C_j' \) in sequence \( \langle R_j'(1)R_j'(2)\ldots R_j'(n) \rangle \), then call there exists collusion attack in \( \langle R_j'(1)R_j'(2)\ldots R_j'(n) \rangle \). Suppose the correct ranking of \( R_j'(m) \) is \( j' \), namely \( R_j'(m) = C_j' \). If \( j > j' \), then it is called collusive boost attack (CBA); if \( j < j' \), then it is called collusive denigration attack (CDA).

The working principle of RLPO is produced after the comprehensive analysis of multiple \( R_j(i) \). So the malicious praise and malicious slander of a single node has no effect on RLPO, and k-Ranks RLPO can effectively eliminate (results of Theorem 1), which has no difference with the error caused by the uncertainty of information. In fact, they both should have no difference. Due to incomplete information, the honest nodes may also come to the same conclusion with the malicious nodes, which is an improvement of RLPO to the traditional enterprise competitiveness reputation mechanism based on score. In a word, the given collusion attack in Definition 2 is the only attack that RLPO needs to deal with.

Theorem 2. The method of k-Ranks RLPO used in independently observe each line in Formula (3) cannot manage the given collusion attack in Definition 2.
Therefore, weighted k means other nodes; \( p \) means that \( p \) node ranks in the wrong (right) position, here, the law of logic partial order without "*" is the feedback given by collusion attack.

\[
\begin{array}{c|c|c}
 j & j^* \\
 \hline
 \ldots & \ldots & \star \ldots \star \\
 \ldots & \ldots & \star \ldots \star \\
 \vdots & \vdots & \vdots \\
 \begin{array}{c}
 \ldots \\
 \ldots \\
 \end{array} & P & \begin{array}{c}
 \ldots \\
 \ldots \\
 \end{array} \\
 \hline
\end{array}
\quad
\begin{array}{c|c|c}
 j^* & j \\
 \hline
 \ldots & \ldots & \star \ldots \star \\
 \ldots & \ldots & \star \ldots \star \\
 \vdots & \vdots & \vdots \\
 \begin{array}{c}
 \ldots \\
 \ldots \\
 \end{array} & P & \begin{array}{c}
 \ldots \\
 \ldots \\
 \end{array} \\
 \hline
\end{array}
\]

(a) A case of CBA  (b) A case of CDA

\textbf{Figure 2.} The collusion attack in RLPO

The calculation of \( r_j \) finished by k-Ranks RLPO is only on the basis of the \( j \) line and \( j^* \) line in Fig. 2. For the two cases given in Fig. 2, due to the existence of \( j^* \), so as long as reverse the position, the \( j \) line and \( j^* \) line in Fig. 2(a) is identical to the \( j \) line and \( j^* \) line in Fig. 2(b). But when k-Ranks RLPO finishing the calculation, it is independent of the position of law of logic partial order in Formula (3).

Therefore, k-Ranks RLPO cannot distinguish a CBA and a CDA, so it cannot deal with collusion attacks. QED.

The proving process from Theorem 2 shows that: in the calculation \( r_j \), if only observe \( R_j(1)R_j(2)\ldots R_j(n) \), then k-Ranks RLPO cannot handle the collusion attack; and even a conflict \( r_j = r_j \) was observed when observing another sequence \( R_j(1)R_j(2)\ldots R_j(n) \), k-Ranks RLPO is still unable to handle the collusion attack. The fundamental reason of this results is that the independent observation of every line in Formula (3) of k-Ranks RLPO, making no difference of the \( j \) line and \( j^* \) line in Fig. 2(a) and the \( j \) line and \( j^* \) line in Fig. 2(b) to k-Ranks RLPO. This requires that when calculating \( r_j \), it needs to comprehensively observe every ranking position of \( R_j(i) \), namely the influence of whole \( R_j(i) \) on \( r_j \). This kind of influence can be reflected from the weight \( W(R_j(i)) \) associated with \( R_j(i) \). For the two case of Fig. 2, if we can design a reasonable algorithm to ensure to associate significant different weights with the lines having "*" and not having "*", then, the location of the \( j \) line and \( j^* \) line in Fig. 2 can no longer be reversed. So the CDA and CBA can be distinguished, which can resist collusion attack.

Definition 3(weighting k-Ranks RLPO). Using the number in \([0,1]\) to describe the weight of law of logic partial order \( R_j(i) \), namely \( W(R_j(i)) \in [0,1] \), and define a \textit{score}(\( R_j(i) \)) for each \( R_j(i) \):

\[
\text{score}(R_j(i)) = \sum_{R_j(i)\neq R_j(w)} W(R_j(w))
\]

The returned \( r_j \) \((1 \leq j \leq k)\) by weighted k-Ranks RLPO is the largest \( R_j(i) \) of score value.

The weight of \( R_j(i) \) in Definition 3 is \( W(R_j(i)) \in [0,1] \). Its meaning is, regarding \( R_j(i) \) as \( n \) possible events, and describe the accuracy (credibility) of law of logic partial order \( R_j(i) \). The meaning of \( W(R_j(i)) \) is identical with the value \( c_m \) in Formula (1), but has essential difference with \( c_m \). \( W(R_j(i)) \) is a number induced from the analysis of Formula (3), which is inherent containing of Formula (3) and does not need storage and maintenance.

Obviously, when each of the \( W(R_j(i)) \), \( 1 \leq i \leq k \) in Formula (5) have the same value, equal value, the weighted k-Ranks RLPO is k-Ranks RLPO, and k-Ranks RLPO is a special case of weighted k-Ranks RLPO. Therefore, weighted k-Ranks RLPO can also satisfy Theorem 1, which can effectively eliminate the uncertainty.
of information. At the same time, due to the introduction of weight, the weighted k-Ranks RLPO can effectively treat collusion attack. The effective resist to collusion attack embodies in the definition of $W(\mathbf{R}_f(i))$. Formula (6) gives a simple calculation method:

$$W(\mathbf{R}_f(w)) = \frac{1}{n} \sum_{t=1}^{n} \left( \sum_{x' \in \mathcal{X}} \sum_{x' \in \mathcal{X}} \mathbf{P}(x \in \mathcal{X}) \mathbf{R}_f(t) \frac{1}{n} \right)$$ (6)

The Formula (6) calculates the occurrence times of item $R_f(i)$ in all $R_f(w)$, $1 \leq w \leq n$. The number of times shows the consistency degree of evaluation of $R_f(i)$ at $k$ position and the other evaluation of $R_f(w)$ given in the same position; then, accumulate the consistency degree of all position $(1 \leq k \leq n)$, reflecting the overall consistency degree of $R_f(i)$ and other law of logic partial order. This value can describe the credibility of $R_f(i)$.

2.2. RLPO in the Local Law of Logic Partial Order

The above conclusions are aimed at the global RLPO method, but for the actual large-scale enterprise competitiveness network, the global RLPO hypothesis exists the following two disadvantages: (1) For the reputation query $Q$ of $r$, not all nodes $p \in P$ will give the law of logic partial order $R_f(p, Q)$; (2) The law of logic partial order given by nodes usually cannot contain all the nodes. For the disadvantage (1), since $r$ receives law of logic partial order given by some nodes, the RLPO input at $r$ is $n||P|$ law of logic partial order. But the proofs of Theorem 1-4 do not need $n=||P||$ condition. So this locality has no substantial impact on RLPO, and the latter experimental data are obtained from collecting part of law of logic partial order. For the disadvantage (2), when the RLPO input $R_f$ only includes partial nodes, $R_f$ cannot correspond in the ranking position. The vertical rectangle in Fig. 2 will lose its significance, and the RLPO algorithm is not correct anymore. This is the main effect of local logic partial order on RLPO. When $R_f$ is the rank of partial nodes in $P$, the main problem of RLPO is the alignment problem of ranking position (APoLR):

Definition 4 (APoLR (align problem of local RLPO)). The APoLR on a given law of logic partial order $R_f = \{p_1, p_2, \ldots, p_n\}$, including partial nodes is to search a law of logic partial order $R_f = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ including all the nodes in $P$. Herein, $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ is a substitution in set $P/\{p_1, p_2, \ldots, p_n\}$ and makes the largest weight of $R_f$ on weighted k-Ranks RLPO.

The basic requirement of APoLR is to fill $R_f$ as $R_f$, in the premise that the filled position does not affect the original credibility evaluation of $R_f$. So the introduced filled nodes in $R_f$ should not affect the credibility evaluation of other rankings. Therefore, $(a_1, a_2, a_3, a_4, a_5)$ in Definition 4 does not need to be the actual node, which only needs to occupy these positions. These positions can be replaced by placeholder “#”. “#” participates in RLPO calculation according to the following method: for the ranking with “#”, “#” means that it is not consistent with any node at the same position, and the obtained count is 0. So, when solving the ApoLR of Definition 4, it needs to fill “#” in the appropriate position on the ranking $R_f$, making the modified local ranking $R_f$ has conformity assessment in the ranking position as far as possible (reflects aligned meaning). Fig. 4 shows an example of APoLR problem and the alignment results.

![Figure 3](image-url) An APoLR example

Obviously, APoLR is the multiple sequence align (MSA), as long as the MSA gene, corresponding to the same evaluation in APoLR, then the two problems are exactly the same. So, like MSA, APoLR is also a NPC
problem. For the local ranking with ranking length of, the algorithm complexity of finding the optimal alignment result is usually

\[ O(k_1 \times k_2 \times \ldots \times k_n) \approx O(k^n) \] 

Although only the law of logic partial order given by part of nodes has no influence to RLPO in essence, in the local ranking set the possibility to appear in the CSCA (shown as Fig. 6) increases. We can control the acquisition process of to resist CSCA. Due to a node is usually localized within the collection than random network the selected sets are more likely to form collusion, on this assumption that the node can control () query in the following method: (1) each “local group” only collects fixed number of (such as 1) can receive multiple (such as ) law of logic partial order returned from different “local group”.

3. EXPERIMENTAL VALIDATION OF RLPO

3.1. Experimental Platform

In this paper, we use the NetLogo simulation tool to verify the RLPO experimentally. Because of some typical cluster analysis and evaluation mechanism has been implemented in NetLogo and in-depth analysis(Siuti, Yazbek and Lu, 2013), so the use of NetLogo as the experimental platform can be conveniently compared with those of the typical RLPO computer system of enterprise competitiveness. In this paper, an agent of NetLogo is used to simulate the behavior of a peer, which divides the time into several simulation periods. In each simulation cycle:

(1) 50% (This is a tunable parameter in the simulation experiment, but this parameter has little effect on the experimental results, so this paper only takes 50%) randomly selected nodes in the network initiate queries to the nodes in the network;

(2) Start a cluster analysis and evaluation mechanism and select a trusted node to perform service interaction according to the calculation result;

(3) The requesting node gives an evaluation of the interaction after the interaction and writes the transaction record in its history list.

The core of the enterprise competitiveness reputation mechanism is to find out the trusted nodes to carry out the service invocation in the enterprise competitive network with a large number of malicious nodes. Thus, the ratio of successful interactions to the total number of interactions is a direct performance of the reputation mechanism. In this paper, the ratio will be used as the basic experimental evaluation parameters. Definition is the number of successful services in the simulation process, is the number of failed services, and the effect of group analysis evaluation is defined as

\[ R_e = \frac{\eta_e}{\eta_e + \eta_h} \]

3.2 RLPO Group Analysis and Evaluation Results

Fig. 5 compares and analyzes the evaluation methods of the competitive power group of the 3 kinds of representative enterprises in the same simulation experiment, and selects the 1000 peer to form the network structure of the enterprise. Among them, 20% (corresponding to adjustable parameters, abbreviated as) nodes are bad nodes (Total reply failed service), other nodes return to the probability of successful service is set to 0.6 to 1.0 evenly distributed random number (Reflecting the good nodes in the provision of certain types of services on the ability of differences). Among them, the recommended node rate for giving bad reputation feedback (If the malicious node according to the historical interaction information to get the target node transaction confidence as [0,1], gives the reputation feedback) is set at 20% (Corresponding to adjustable parameters, referred to as). Among them, each node can correctly evaluate the recommendation credibility with the probability of 0.8 (corresponding adjustable parameter) (according to the transaction results, right adjustment of in Formula (1) is conducted. Due to the lack of ability of some honest recommenders, the reputation feedback giving errors will lead to the mistake of adjustment. The simulation parameter 1- is used to indicate the possibility of the occurrence of such situation).

Fig. 5 (a) shows the effect of typical group analysis and evaluation method based Formula (1) that proposed in literature (Wang, Lu and Willner, 2014). c_m evaluates the recommended capacity of rater. The adjustment method is . Herein, [-1,1] means the consistency of the deal results and the recommended values of . Fig. 5 (b) shows the with the mean cluster analysis and evaluation methods given in literature (Siuti, Yazbek and Lu, 2013; Williges, Lilliestam and Patt, 2010). The core idea is to use to replace the calculation in Formula (1). Fig. 5 (c) is presented for RLPO group analysis of the evaluation result, and is part of the node form logic (i.e. local law partial order ranking section 1.3 describes the input after the RLPO) and the effects after this. Because, let the system of the 1000 nodes are involved in the RLPO operation is not the fact there is
no significance. In this experiment, we selected 10 recommended nodes from the node collection form law of logic partial order, analysis and evaluation of the logical group node partial alignment after the implementation of law RLPO. The following RLPO experiments have been carried out in the same way, and the length of $\text{is set to } 10$.

As can be seen from Fig. 5, WRA and AVG have substantially the same successful service ratio, but the correct recommended number of AVG is significantly higher than the WRA. This result shows that in the open environment of enterprise competitiveness, the recommended nodes can give malicious and "goodwill" error information, and the open environment cannot effectively distinguish it. The results show that the competitiveness of enterprises in such open environment, the recommended node will give malicious and "good faith" false recommendation information, and open environment is unable to distinguish, so WRA in polymerization to recommend a reputation rather than the average weight of AVG polymerization will lead to error evaluation more.

Fig. 5 shows the evaluation of WRA, AVG and RLPO reputation of the three types of aggregation methods and working mechanism. It can be seen that RLPO shows a better performance than WRA and AVG in this typical experimental environment. Figure 6 compares the parameters of the three methods in various experimental settings. The results show that RLPO can work well in a variety of situations, especially in the presence of a large number of failed service nodes and malicious nodes (Blind in the figure is the result of not using the reputation mechanism, indicating that the network can provide a successful service node ratio, Scilicet, R. For the $\text{=0.6 shown in Fig. 6, is only 30% when the Blind mechanism is employed; And when RLPO is used, is 80% or more, which indicates that RLPO can effectively discover the nodes with high credibility in the network).
4. CONCLUSION

In this paper, a method of RLPO based on logical partial order law is proposed to evaluate and evaluate the enterprise competitive power group. RLPO is different from the existing enterprise competitiveness group analysis and evaluation mechanism in two aspects: (1) the reputation feedback given by the recommendation node is no longer a score, but a ranking sequence. Compared to a number, the logical partial order law carries a richer meaning. It can make the enterprise competitive cluster analysis and evaluation mechanism to effectively deal with the complex environment of enterprise competitiveness and the existence of various types of malicious attacks; (2) In the process of reputation aggregation, we only need to deal with the logical partial order law given by the recommended nodes. It is not necessary to evaluate the reliability of the recommended nodes and maintain the information of the recommended nodes. The feedback information given by the recommended nodes only plays a role in this cluster analysis and evaluation. For the open network environment, this kind of history independent calculation is superior to the efficiency and performance. TFT in BT embodies the same idea.

In this paper, the ability of RLPO to deal with random errors is modeled and analyzed theoretically. On this basis, we define a series of malicious attacks against the reputation of enterprise competitiveness: CBA, SCA, CSCA, which are different from random errors. And the RLPO framework is designed to deal with these malicious attacks. Mathematical modeling and theoretical analysis of these methods show that the effect of random errors in RLPO is exponentially decaying with the number of logic partial orders. The influence of CBA on RLPO decreases with the polynomial of the number of logic partial orders. SCA can be effectively neutralized in RLPO due to the need to introduce the correct information to RLPO. In a word, RLPO has the ability to deal with the complex factors of the open network environment and resist the malicious attacks, which is superior to the other enterprises in the analysis and evaluation of the competitiveness of the group. The simulation results are also validated. In addition, for the partial RLPO and logic partial order law which can only be collected in the real environment, this paper also gives the detailed processing method.
REFERENCES


