IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received August 23, 2020, accepted September 8, 2020, date of publication September 18, 2020, date of current version October 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3024590

Risk Analysis of Cash on Delivery Payment Method by Social Network Analysis and Fuzzy Petri Net

LEI YU[1,2], QINGZHI LIU[1], RONG HUA[2], AND YOU FU[2]
[1]Institute of Finance and Economics, Shandong University of Science and Technology at Tai'an, Tai'an 271019, China
[2]College of Computer Science and Engineering, Shandong University of Science and Technology at Qingdao, Qingdao 266590, China
Corresponding author: You Fu (fuyou@sdust.edu.cn)

ABSTRACT Cash on delivery is one of the payment methods provided to customers by the enterprises. In this article, the links of cash on delivery transactions were decomposed and divided into detailed nodes. Based on the survey data, the qualitative and quantitative analysis on risks associated with the cash on delivery process were carried out using the social network model. The influential risk factors of cash on delivery were precisely narrowed in scope. Fuzzy Petri Net was then used in identifying the dynamic risk factors, analyzing the correlation between dynamic risk factors and subsequent nodes, and establishing risk matrix to analyze the relationship between risk index grade, risk size and risk level. Finally, the two methods were combined and a reasonable and effective risk evaluation index system was obtained. The presented work was expected to serve as reference for the e-commerce platforms to reduce the risks and improve the service quality in the cash on delivery transactions.

INDEX TERMS Cash on delivery, risk, social network analysis, fuzzy petri net.

I. INTRODUCTION

The development of e-commerce is significant worldwide, especially in China, where a large number of e-commerce platforms have emerged. With convenient and fast services, these platforms have imperceptibly changed the consumer behaviors of users, such as the type of payment. Generally speaking, in the e-commerce scenario, payment can either be online or offline. In Europe and many developing countries such as Thailand, India and Bangladesh, one of the most popular offline payment methods is cash on delivery (COD) [1], [2]. The option of COD payment would help the online sellers expand the market and gain more profits. In addition, the risk, brought by the uncertainty of quality and demand, would actually be shared by enterprise and consumers. There are also some disadvantages with the COD payment that the seller needs to wait for a period of time to receive the money from the customer, which reduces current income [3]. For the consumers, the concerns about financial security and privacy would be relieved by use of the COD payment method. Viktória *et al.* [4] discussed the relationship between the choice of payment methods and the information security of users and considered COD as the safest way but with the highest cost.

However, in actual practice, there are still risks associated with the COD payment which need to be investigated. Generally, risk is observed in various fields and refers to a kind of measurable uncertainty, which could be quantified by means of probability or other methods [5]. Risk identification is a process of analyzing, identifying, classifying and evaluating various risks that may or have occurred in the process of a project [6]. Risk identification consists of two parts: risk perception and risk analysis. Risk analysis is the analysis on various factors that cause the risk accidents, and it is the key to identify a certain risk [7]. The risk factors from the previous link would have a continuous impact on the follow-up links, and change the overall risk level [8]–[10]. Therefore, it is important to consider risk measurement from an early perspective.

Tanimoto *et al.* [11] applied the risk analysis in evaluating the risk of sharing economy, where the researchers counter-measured the risk factors, comprehensively extracted the risk factors by risk decomposition structure, and put forward the countermeasures using the risk matrix method. The method of Analytic Hierarchy Process (AHP) is widely used in measuring the risk of e-commerce [12]. It provides

The associate editor coordinating the review of this manuscript and approving it for publication was Zhiwu Li.

a comprehensive and reasonable framework for constructing a decision problem, representing and quantifying its elements, linking these elements to the overall goal, and evaluating alternative solutions [13]. For e-commerce enterprises, the AHP method serves in the decision-making that how to effectively analyze the influencing factors of payment risk, so as to adjust and meet the needs of consumers on risk aversion [14]. However, there are qualitative tendency in the calculation of weight, and some qualitative indexes cannot be assigned accurately when assigning values to indexes [15].

COD is a typical dynamic and complex process, involving multiple participants. The risk assessment of influencing factors on the process is different from that on a static equipment or a fixed process. For the risk analysis of COD, the operational risk analysis could be referred [16]. Operational risk analysis is completed by an expert group including operators, supervisors and managers who are familiar with the operation process. The basic steps are as follows: for a certain operation activity or process, the operation process is first decomposed into several connected sub processes; second, the potential risk factors of each sub process are identified, and the risk level of each sub process is evaluated; and finally, the corresponding risk control measures are formulated according to the evaluation results. A fuzzy probability model was proposed in the operational risk analysis [17]. The Fuzzy Petri Net is used to express the knowledge of system fault diagnosis, and the result antecedent relationship between the performance of risk diagnosis knowledge and the antecedent is deduced by using the maximum algebraic iterative algorithm [18]. With the expansion of the knowledge base and the complexity of rules, the constructed Petri net model tends to become redundant where various types of risk factors and complex relationships are presented and how to simplify the existing models has become a key problem to be solved [19]. At present, there are few studies on the influencing factors of COD transaction risk and their relationships, and they tend to conduct qualitative analysis. They have certain limitations and cannot identify potential risks well.

Previous studies on the theory and application of Petri net have formed a mature system, but few of them have applied it to the risk analysis. Many people do not realize that the risk of payment on arrival is the key in restricting the development of e-commerce platform especially in the early stage, and in affecting the relationship between business and customer. Therefore, the research on the risk of COD is carried out in order to reveal the mechanism of COD risk and its related factors.

Aiming at the analysis of risk influencing factors in COD payment, this article firstly constructed the risk factor model of COD transaction by social network analysis on basis of the questionnaire, and established the risk factor adjacency matrix to identity the main risk factors. Fuzzy Petri Net was then used for matrix representation of key risk factors of COD, and Fuzzy Petri Net model was stratified to quantitatively analyze on key factors. For the first time, Fuzzy Petri net was also combined with social network analysis in identifying the risk in business transactions. The combination of these two methods can identify key influencing factors of transaction risks more accurately and can improve the business judgment and decision making.

The rest of the paper is organized as follows. The second part is that social network analysis was applied in constructing the risk analysis model of COD where risk factors were analyzed and identified. The third part put forward a stratified fuzzy reasoning Petri net risk assessment method where the matrix representation and quantitative risk assessment algorithm of the net model were presented. In the fourth part, Fuzzy Petri Net was applied for risk analysis where risk factors in chapter II were included. The conclusion was presented in the fifth part.

II. BACKGROUND: SOCIAL NETWORK ANALYSIS MODEL AND FUZZY PETRI NET

A. SOCIAL NETWORK ANALYSIS (SNA) MODEL

Social network analysis was originated from sociological research and has been used in analyzing the structure of research objects and their interaction from the perspective of network. The method has played a very important role in fields of economics, management and sociology. With the increase of difficulty and complexity of the project, social network analysis methods have been increasingly applied in risk management for qualitative, quantitative and visual analysis. For example, researches identified and analyzed the risk factors of various stakeholders by the use of social network analysis method [20]–[22].

Centrality is a very important structural measure index in SNA analysis. It indicates the status and control of the nodes in the network and influences the relationship between them. The higher the centrality of a risk factor, the stronger its capability would be, and the influence of network location is greater. At present, there are three central indicators in SNA researches including Degree centrality, Betweenness centrality and Closeness centrality. In this article, the degree centrality index and center centrality index were used to measure the direct impact relationship of a specific risk factor and the control ability of the risk factor on other nodes.

Definition 1 (Degree Centrality Analysis): Degree centrality is an index to measure the frequency of a node's connection with other nodes. According to the directivity of the relationship, the degree centrality includes two aspects: in-degree and out-degree. The point in degree refers to the total number of points directly pointing to the point in the network. The point out degree refers to the total number of other points in the network pointed by the point. The adjacency matrix was constructed based on related data. In this adjacency matrix, i represents the element in the row, and j represents the element in the column. S_{ij} represents the strength of the relationship between element i and element j. Out-degree (O) and In-degree (I) are indicators to measure the relative strength of each factor and were calculated as follows:

$$O = \sum\nolimits_{i=1}^{n} S_{ij}, \tag{1}$$

$$I = \sum_{j=1}^{n} S_{ij}, \quad (2)$$

The penetration degree and the occurrence degree of the points are analyzed to find out the risk factors that located at the core and periphery of the network. A larger risk factor indicates that the interaction between the risk factor and other risk factors is more significant. It shows that the risk factor is highly objective and is not easy to be influenced by other risk factors. Therefore, in a specific relationship network, if the risk factor is higher and the entry point is low, it means that the node impacts more on other nodes and is little influenced by the other nodes.

Definition 2 (Closeness Centrality Analysis): In order to analyze the importance of all risk factors in the whole network and accurately identify them, Ucinet 6.0 software was used to analyze the centrality of the factors in the network. Proximity centrality (also called the overall centrality) is an index indicating the degree of short distance between a node and other nodes in the network, and measures the degree that the node is not affected by other nodes. It is the sum of the shortcut between the risk factor and other risk factors in the network, calculated as Equation (3).

$$D(i) = \sum_{j,k} \frac{N_{jik}}{N_{jk}}, \quad (3)$$

N_{jk} represents the number of shortest paths from node j to node k(j,k≠i), N_{jik} represents the number of shortest paths from node j to node k passing through node I. If there is a unique and shortest path between node i from node j to node k (j,k≠i), under this condition, node i has the highest degree of betweenness centrality, which also means that at this time, node i has the greatest degree of control over other nodes and the greatest degree of control over risk transmnoion.

If the number of nodes in a network is n, the maximum value of betweenness centrality is $n^2 - 3n + 2$, so the mathematical expression for the betweenness centrality can be converted to

$$D_s(i) = \frac{2D(i)}{n^2 - 3n + 2}, \quad (4)$$

B. FUZZY PETRI NET(FPN)

Petri net was first proposed by Carl Adam in the 1960s. It is a scientific method with strong representation ability for discrete parallel systems. Due to the its advantages including scientific mathematical expression and intuitive graphical representation, Petri net was applied to the field of Internet science. Many types of Petri nets have been developed in different directions and for solving different problems [23].

A standard Petri net is composed of Places, Transitions, Arcs and Tokens. In this article, places are represented by circles and transitions are represented by rectangles. They jointly represent two different nodes in Petri net. Directed arc is the connection line between places and transitions, including two types: one is the directed arc from places to transitions; the other is the directed arc of transition to the repository. The flow of Petri net means the flow with solid black spots and is represented with a token. The flow of token also includes two types: one is from the input to the warehouse to the transition and the other is the transition to the output repository. In a research of system, places represent system resources; transitions represent the relationships between system resources; the tokens in the repository are the number of system resources and the tokens are triggered and the tokens will flow from the original repository to the target repository; the condition for a transition trigger is that all the initial repositories have tokens and that the tokens in the target repository flow after the transition is triggered [25].

Definition 3 (Petri Net): A Petri net can be represented as a six-tuple, PN= (P, T; F, W,M,K), where P is a finite set of places, $P=\{p_1,p_2,p_3,\ldots,p_n\},n\geq 0$; T is a finite set of transition, $T=\{t_1,t_2,t_3,\ldots,t_m\},m\geq 0$, and $P\cup T\neq\emptyset$, and $P\cap T\neq\emptyset$, $F \subseteq (P \times T) \cup (T \times P)$ $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs; W is the weight of the arc, W(p,t)≥1, W(t,p)≥1; M is an identifier for the number of tokens in the place; M(p) represents the number of tokens in the place P;K represents the capacity of the place. The place is represented by a circle, a black dot for token, a black vertical line for transitions, and an arrow for arcs, as shown in figure 1 [24]. When there is transition trigger in Petri net, token will move and M will change.

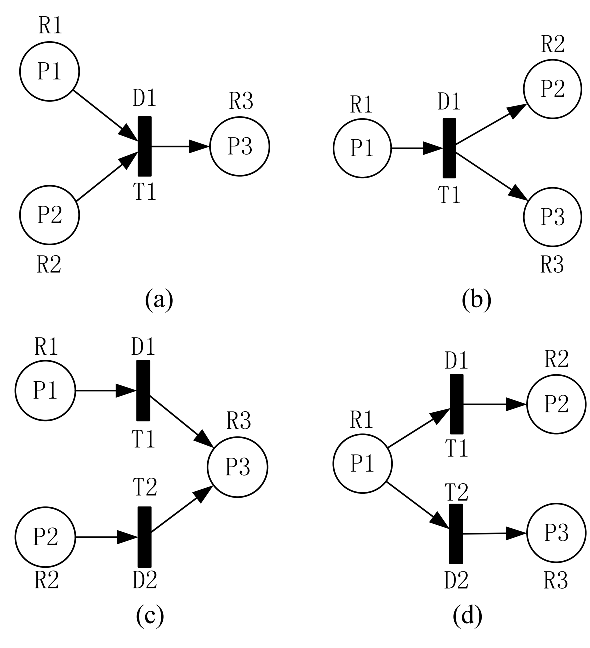

FIGURE 1. Four types of basic Petri net structure [28].

Trigger rules:

(1) The transition $t \in T$ is enabled if and only if $\forall p \in {}^{\cdot}t$: $M(p) \geq 1$,denoted as M[t >;

(2) After the change t is triggered by the action of the mark M, a new mark M' can be obtained, which is recorded as

M[t > M,and then:

$$M^{\cdot}(p) = \begin{cases} M(p)+1 & \text{if } p \in t^{\cdot} - {}^{\cdot}t, \\ M(p)-1 & \text{if } p \in {}^{\cdot}t - t^{\cdot} \\ M(p) & \text{otherwise.} \end{cases}$$

Definition 4 (Fuzzy Petri Net(FPN)): FPN = (P, T, I, O, D, C)

(1) P={p_1,p_2,…,p_n} is a finite set of all places in a Fuzzy Petri Net. The library in this article represents transaction risk.

(2) T={t_1,t_2,…,t_n} represents the set of all transition nodes in the Fuzzy Petri Net, and transition represents the basis of rule realization. The transition in this article represents the transition rule.

(3) I defines a fuzzy relationship between place and transition, which represents the closeness of the relationship between place and transition. The value range is: $0<I(p_i, t_j) \leq 1$.

(4) O indicates the tightness of the connection from transition to place, and the value range is $0<O(p_i, t_j) \leq 1$.

(5) D is defined as truth degree, D= $(D_{P1}, D_{P2},\ldots, D_{Pj})^T$ is a matrix of i*j, indicating the truth degree of a proposition.

(6) C is a triangular matrix, which represents the truth degree of transition.

For the quantitative calculation of Petri net [26], the method of truth degree is used to express the strength of transaction risk judgment, and risk is quantitatively calculated so as to more accurately represent the situation of risk. The main idea of truth degree method is that the truth value of the combination of fuzzy propositions takes the minimum value of the truth value of each sub formula, and the truth value of the disjunction of fuzzy propositions takes the maximum value of the truth value of each sub formula [27].

(1) $\oplus$:a$\oplus$b=c, a, b, c is n-dimensional vector, if $a_i \in a$, $b_i \in b$, $c_i \in c$, $c_i = \max(a_i, b_i)$;

(2) $\otimes$: A is n×m-dimensional vector, b is m-dimensional vector, d is n-dimensional vector, if $b_i \in b$,$d_i \in d$, $a_{ik} \in A$, $1 \leq k \leq m$, $d_i = \max(a_{ik}, b_k)$;

$\oplus$ is an addition operator, which outputs a larger value after comparing two elements; $\otimes$ is the multiplication operator, which multiplies the two elements and outputs the larger value of the product; · is the multiplication of two matrices; k≥0, k is a positive integer.

According to the definitions of (1) and (2), let neg be the operator and VK be the intermediate variable

$$\text{negD}_k = 1 - D_k, \tag{5}$$

k is the number of reasoning steps, and negD_k is one-dimensional vector, D= {D_1,D2,D3,…, Di}, 1≤i≤m

$$V_k = I^T \otimes (\text{negD}_k) = I^T \otimes \overline{D_k D_k}, \tag{6}$$

$$\theta_k = \text{negD}_k = \text{neg}(I^T \otimes (\text{negD}_k)) = \overline{(I_k^T \otimes \overline{D_k})}, \tag{7}$$

V_k is n-dimensional vector, θ_k is m-dimensional vector.

Therefore, the formula for calculating the next state of place Pi is:

$$D_{k+1} = D_k \oplus \left[(O_k \cdot C_k) \otimes \overline{(I_k^T \otimes \overline{D_k})}\right], \tag{8}$$

If $D_{k+1} = D_k$, out of calculation.

Based on the standard Petri net, combined with the basic structure and rules of the knowledge representation domain, the basic structure and fuzzy rules of FPN are defined as follows:

(a) IF R1 AND R2 THEN R3, means that risks R1 and R2 occur simultaneously and will cause risk R3. The truth degree of risks R1, R2 and R3 are P1, P2 and P3, respectively, and the truth degree of transfer rule T1 is D1.

(b) IF R1 THEN R2 AND R3, means that risk R1 occurs, which will cause risks R2 and R3 to occur simultaneously.

(c) IF R1 OR R2 THEN R3, means that as long as at least one of risks R1 and R2 occurs, it will trigger risk R3. The truth degree of the transfer rule T1 is D1, and the truth degree of T2 is D2.

(d) IF R1 THEN R2 OR R3, means that risk R1 occurs, it will lead to risk R2 or risk R3, but not necessarily at the same time.

The correspondence between these types of Petri net and each set of input matrices and output matrices are expressed as follows:

$$I_{(a)} = \begin{vmatrix} 1 \\ 1 \\ 0 \end{vmatrix} \quad O_{(a)} = \begin{vmatrix} 0 \\ 0 \\ 1 \end{vmatrix}$$

$$I_{(b)} = \begin{vmatrix} 1 \\ 0 \\ 0 \end{vmatrix} \quad O_{(b)} = \begin{vmatrix} 0 \\ 1 \\ 1 \end{vmatrix}$$

$$I_{(c)} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{vmatrix} \quad O_{(c)} = \begin{vmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{vmatrix}$$

$$I_{(d)} = \begin{vmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{vmatrix} \quad O_{(d)} = \begin{vmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{vmatrix}$$

Because of the strong uncertainty of risk, the use of the classic Fuzzy Petri Net may lead to a lack of structural and hierarchical analysis of risk analysis, and thus affect the intuition of risk analysis. Therefore, we propose a layered Fuzzy Petri Net to achieve quantitative analysis of different levels of risk and provide more intuitive suggestions for solving risk problems [29]–[31].

For specific FPN, the principle of layering is

(1) Calculates the number of transitions from the initial places to the termination places.

(2) If the transition corresponding to place is one-to-one, put the input places with the same number of transitions, the transition corresponding to the place, and the output places into the same layer.

(3) If there are more than one transition for the same place, add an auxiliary place and an auxiliary transition that

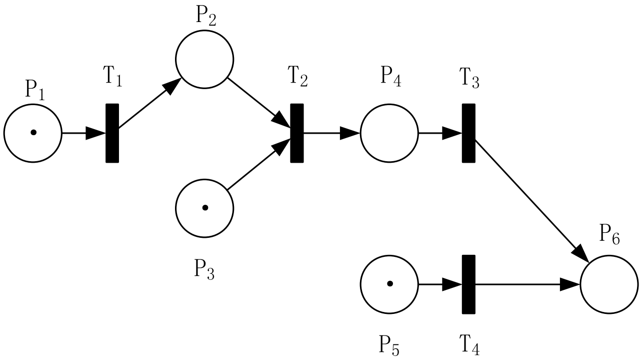

FIGURE 2. An example of standard Petri net.

have no actual physical meaning to fulfill the requirements of (2). The basic rule of addition is that the value of the auxiliary place is the same as its adjacent place value, and the truth degree of the auxiliary transition is always 1.

The Petri net on the graph is analyzed. P_1 is the starting place of the whole network. P_6 is the terminating place. The paths from P_1 to P_6 have two: $P_1 \longrightarrow P_2 \longrightarrow P_4 \longrightarrow P_6$ and $P_1 \longrightarrow P_6$. In order to ensure the layered structure of the network, as suggested by the above layering principle, it is necessary to add auxiliary place P' and auxiliary transition T' between P_1 and P_6.

The Petri net can be divided into three layers after stratification. The first level is P_1, T_1, P_2, P_3; the second level is P_2, P_3, T_2, P_4; the third tier is P_4,P_5,P',T_3,T_4,T', as shown in Figure 3.

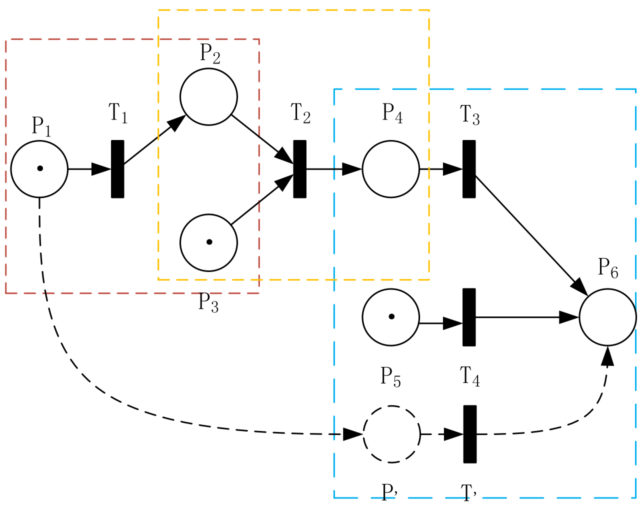

FIGURE 3. A layered Petri net.

The place in Petri net corresponds to the cause of the accident or risk. The direct cause and root cause of the failure event can be directly identified from the layered Petri net: P_1 represents the root cause, P_4, P_5, P'(or P_1) represent the direct cause, and the other places represent the middle cause. Therefore, from the point of view of cause analysis, the layered Petri net can directly distinguish the direct cause and the root cause. So that the model is more structured.

In addition to graphical representation, in order to adapt to the layered model, the original calculation formula (5) needs to be corrected. In layered Petri net, the computation steps only depend on the number of layering. For each Petri net, the truth degree vector is calculated according to formula (6):

$$D_k = D_{k-1} \oplus \left[(O_{k-1} \cdot C_{k-1}) \otimes \overline{\left(I_{k-1}^T \otimes \overline{D_{k-1}}\right)} \right] \quad (1 \leq \text{k} \leq \text{n}), \qquad (9)$$

Among them, the variable k is a positive integer, and n is the number of divided Petri net. The specific algorithm is as follows:

(1) According to knowledge representation rules, Petri net is expressed in combination with specific fuzzy rules;
(2) Use the layering principle in the layered Fuzzy Petri Net for layering, identify special situations, and add necessary auxiliary places and auxiliary transitions as needed;
(3) If k=1, according to the formula D1;n=1;
(4) If k=2, according to the formula D2;n=2;
(5) If k=n, calculate Dn;
(6) If Dk−1= Dk,means that the probability of occurrence of all propositions will not change, the calculation is terminated, the state of the place is obtained, and the risk is evaluated.

III. CASH ON DELIVERY RISK ANALYSIS

A. THE CONSTRUCTION OF SOCIAL NETWORK ANALYSIS MODEL FOR CASH ON DELIVERY TRANSACTIONS

When COD was optioned as a payment method, the users' perception and experience of the service providers largely affect their choice. In the perspective of the service provider, the cost and safety of COD payment were mainly considered to improve the user experience and attract existing and potential users.

In this article, JD and Tmall e-commerce platforms in China were investigated on their COD service. The risk factors associated with the COD process were divided into five categories: credit risk, security risk, payment risk, distribution risk and environmental risk. Each sub risk factor was analyzed in detail, as shown in Figure 4.

According to Figure 4, a questionnaire was designed and 0, 1, 2 and 3 were used to indicate the degree of direct influence. The 0 showed no direct impact. 1 showed a direct impact on the relationship. 2 showed a direct impact on the relationship. 3 showed a strong direct impact. A total of 267 questionnaires were distributed, and 256 responses of them were valid. The adjacency matrix of risk factors for COD was established as formulas (1)-(4) and was shown in Table 1.

As shown in Table 1, most of the risk factors have larger degree of occurrence and degree of penetration, indicating that most of the risk factors have an influence on each other. In order to identify the risk factors more accurately, the social network analysis software Ucinet 6.0 is used to analyze the

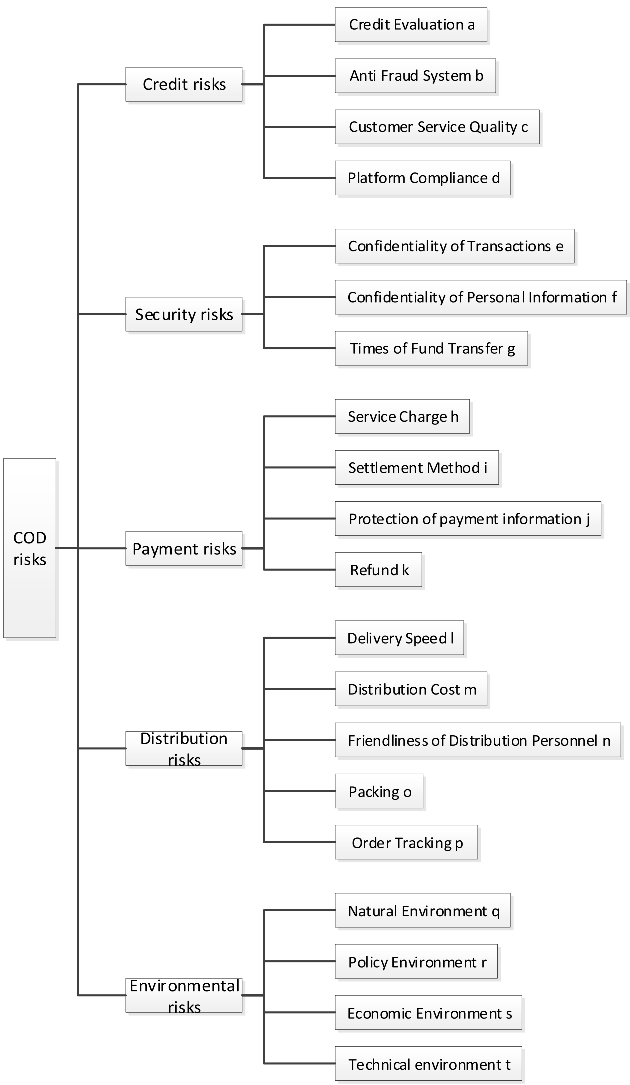

FIGURE 4. **Cash on delivery risk factors. COD is short for Cash On Delivery.**

internal and external centrality of all the risk factors. The results of analysis are shown in Table 2.

Based on the results, 10 key risk factors were determined including platform compliance, service charge, settlement method, distribution cost, friendliness, packaging, order tracking, natural environment, policy environment, and economic environment.

B. QUANTITATIVE EVALUATION OF COD BASED ON FPN

Quantitatively, Fuzzy Petri Net was used for evaluation on the risk of delivery. 5 risk categories were analyzed including credit risk, payment risk, distribution risk and environmental risk. Risk factors were encoded, as shown in Table 3, in order to facilitate modeling.

According to the method of truth degree determination [32] and with expert knowledge and experience considered, the specific truth degree was specified for each risk evolution rule. Petri net was used to express the key risk factors of COD, as shown in Figure 3.

TABLE 1. **Adjacency matrix of COD risk factors.**

Influencing factors	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	Out-degree
a	0	3	2	0	1	2	0	0	0	3	1	0	0	0	0	0	0	0	1	2	15
b	3	0	1	1	0	0	0	0	0	2	0	0	0	0	1	0	0	0	2	2	12
c	3	3	0	2	0	2	0	0	0	2	0	3	1	3	2	3	0	0	2	2	28
d	2	3	1	0	3	3	0	0	0	3	3	3	1	3	2	2	0	0	1	3	33
e	3	2	3	3	0	3	0	0	0	3	0	0	0	1	3	1	1	0	0	2	25
f	3	2	3	3	3	0	0	0	1	3	0	0	0	0	0	0	0	0	0	2	20
g	0	1	0	3	0	0	0	0	0	2	3	0	3	0	0	0	0	0	0	1	13
h	1	1	0	3	0	0	1	0	3	0	2	0	3	0	0	0	0	0	0	0	14
i	1	1	2	1	2	2	0	2	0	2	3	0	2	0	0	0	0	0	2	2	22
j	3	1	3	3	3	3	0	0	0	0	0	0	0	1	0	0	0	0	0	0	17
k	3	2	3	2	1	1	0	0	2	1	0	0	3	0	0	0	0	0	0	1	19
l	2	0	3	2	0	0	0	0	1	0	0	0	2	0	0	0	0	0	2	2	14
m	1	1	2	2	0	0	1	0	3	2	1	0	0	1	3	1	0	0	0	2	20
n	1	0	3	1	0	0	0	0	0	0	0	2	0	0	0	0	0	1	1	1	10
o	2	1	2	2	1	0	0	0	0	0	0	0	2	0	0	0	3	1	1	1	16
p	1	1	3	2	1	0	0	0	1	0	0	0	1	0	0	0	0	0	1	2	13
q	0	0	1	0	0	0	0	0	1	0	0	3	3	2	2	1	0	2	2	2	19
r	1	3	3	3	3	3	0	0	1	3	0	3	1	1	3	3	0	0	3	3	37
s	3	3	3	3	3	3	3	1	1	3	0	3	3	3	2	0	0	3	0	1	41
t	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	3	3	2	3	0	54
In-degree	36	31	41	39	24	25	8	6	17	32	16	20	28	17	20	14	7	9	21	31	

According to the principle of stratification of Fuzzy Petri Net, the key risk factors of COD were divided into two layers, as shown in Figure 5. $P_2 \longrightarrow P_{13}$ was a special case and for consistency, P' and auxiliary transition D' between P_2 and P_{13} were added, and its truth degree was set to 1. The new formed Petri Net was shown in Figure 6.

Based on the Petri Net COD's key risk factors, the truth degree of the initial place is:

$$|P_1, P_2, P_3, P_4, P_5| = |0.4, 0.7, 0.8, 0.5, 0.4|$$

And the truth degree of transition is:

$$|T_1, T_2, T_3, T_4, T_5| = |0.65, 0.85, 0.80, 0.65, 0.55|$$

The truth degree vector of the network at the first level is:

$$\begin{aligned} D_0 &= |P_1, P_2, P_3, P_4, P_5, P_8, P_7, P', P_9, P_{10}|^T \\ &= |0.4, 0.7, 0.8, 0.5, 0.4, 0, 0, 0, 0, 0|^T \end{aligned}$$

$$I_0 = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{vmatrix}$$

TABLE 2. Closeness centrality analysis of risk factors for COD.

Risk factor category	Sub factors of risk	External approach centrality	Internal approach centrality	Key factors or not
Credit risks	Credit evaluation	0.63333	0.90476	N
	Anti-fraud system	0.79167	0.90476	N
	Customer service quality	0.73077	0.90476	N
	Platform compliance	1	0.90476	Y
Security risks	Confidentiality of transactions	0.61290	0.86364	N
	Confidentiality of personal information	0.73077	0.76000	N
	Number of fund transfers	0.57576	0.76000	N
Payment risks	Service Charge	0.86364	0.73077	Y
	Settlement method	0.70370	0.70370	Y
	Protection of payment information	0.63333	0.67857	N
	Refund	0.73077	0.67857	N
Distribution risks	Speed of delivery	0.61290	0.65517	N
	Cost of distribution	0.67857	0.65517	Y
	Friendliness of distribution personnel	0.61290	0.61290	Y
	Packing	0.67857	0.61290	Y
	Order tracking	0.65517	0.61290	Y
Environmental risks	Natural environment	0.82609	0.55882	Y
	Policy environment	0.59375	0.54286	Y
	Economic environment	0.67857	0.52778	Y
	Technical environment	0.57576	0.52778	N

$$O_0 = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

$$C_0 = \mathrm{diag}(T_1, T_2, T_3, T_4, T_5) = \mathrm{diag}(0.65, 0.85, 0.80, 0.65, 0.55)$$

The calculated value of D_1 is:

$$D_1 = |0.4, 0.7, 0.8, 0.5, 0.4, 0.52, 0.38, 0.7, 0.55, 0.63|^T$$

Results showed that the truth degree of P_8, P_7, P_9 and P_{10} in the betweenness repository were 0.52, 0.38, 0.55 and 0.63, respectively. The calculations implied that order tracking was related to the timeliness of delivery to a certain extent and affects the satisfaction of users to a greater extent.

The similar processes and the same method were used in analysis of network at the second level. The truth degrees of P_{11}, P_{12}, P_{13} and P_{14} are 0.61, 0.45, 0.73 and 0.42, respectively. The results showed that the risk of delivery was greater than other risk categories when consumers purchase their orders. To a large extent, distribution risk factors would determine consumers' overall consumption experience. Therefore, the e-commerce platforms should improve their service

TABLE 3. Key risk factors coding for COD.

Code	Risks	Code	Risks
P_1	Service Charge	P_8	Settlement method
P_2	Friendliness of distribution	P_9	Cost of distribution
P_3	Packing	P_{10}	Order tracking
P_4	Policy environment	P_{11}	Payment risks
P_5	Natural environment	P_{12}	Credit risks
P_6	Economic environment	P_{13}	Distribution risks
P_7	Platform compliance	P_{14}	Environmental risks

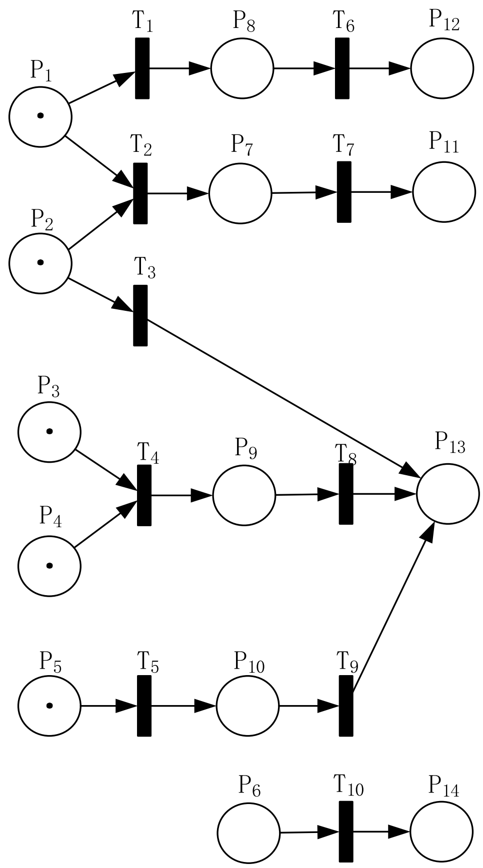

FIGURE 5. Petri net of the key risk factors of COD.

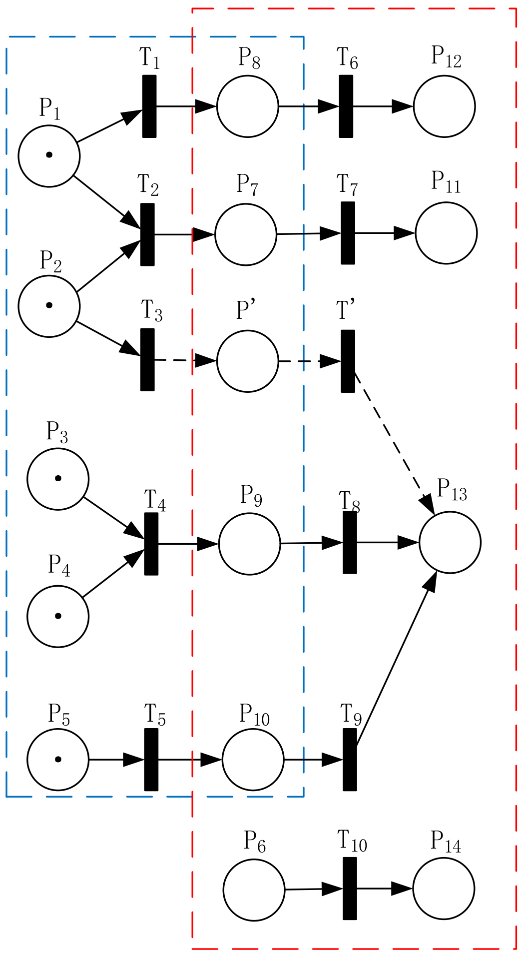

FIGURE 6. The layered Petri Net of key risk factors for COD.

quality and management in the distribution to better meet consumers' demand.

According to the above analysis, it can be seen that high occurrence of payment risks of COD is caused by the quality of order tracking and the cost of distribution, which also affect the occurrence of distribution risks ultimately.

Therefore, when merchants provide customers with COD services, they should pay special attention to improving the traceability of orders and reduce the cost of distribution. On one hand, merchants should better use the existing management information system and provide consumers with constant information on location and personnel of the commodity distribution. This would improve the interaction between merchants and consumers in this link and enhance the consumer experience. On the other hand, merchants could also use more environmentally friendly packaging of lower cost, construct neighboring warehouses for potential consumers or apply other methods that reduce the cost of distribution. Only when businesses pay attention to these risks can they gain the trust of consumers and effectively reduce the regret rate and finally achieve a win-win situation for both sides.

IV. CONCLUSION

With the development of Internet applications, especially in field of e-commerce, people pay more and more attention to online shopping and consumption. The development of e-commerce depends greatly on the payment where every step of payment will definitely affect the quality of the consumption experience of the consumers. COD is one of the payment services provided by many e-commerce platforms for the convenience of consumers. Risk analysis on the COD payment method is meaningful in improving the response of e-commerce platforms to various risks and their service quality.

In this article, social network analysis and Fuzzy Petri Net are used to analyze the risk of COD transaction. In comparison to traditional risk analysis methods, this article analyzed the risk factors in a comprehensive manner and determined the key ones using social network analysis; Fuzzy Petri Net and stratified thinking were applied to model and quantify the key factors; and a more accurate risk identification was achieved. In addition, risks of COD transaction were assessed using the combination of the social network analysis and Fuzzy Petri Net.

However, there are some limitations with the paper. One is that the risk evaluation index of the COD payment was relatively rough in the paper and it was suggested that a more complete, scientific and applicable index system can improve the reliability of risk evaluation results. The other one is that the model is only considered from the risk assessment of COD transaction, but not from other more aspects, which still needs to be further improved.

REFERENCES

[1] J. Zhang, B. Niu, and J. Li, "Optimal pricing and inventory policy with order cancelations under the cash-on-delivery payment scheme," *J. Syst. Sci. Complex.*, vol. 27, no. 5, pp. 970–992, Oct. 2014.

[2] M. H. Junaidi and M. S. M. lam, "Online buying behavior among university students: A cross cultural empirical analysis," *J. Inf. Technol. Manage.*, vol. 12, no. 2, pp. 26–39, 2020.

[3] Y. Chen, S. Ray, and Y. Song, "Optimal pricing and inventory control policy in periodic-review systems with fixed ordering cost and lost sales," *Nav. Res. Logistics*, vol. 53, no. 2, pp. 117–136, Mar. 2006.

[4] T. Pencarelli, V. Škerháková, V. A. Taha, and T. Valentiny, "Factors determining italian online shoppers' preference of cash on delivery: Empirical analysis," *Polish J. Manage. Stud.*, vol. 18, no. 2, pp. 245–258, Dec. 2018.

[5] F. Knight, "Risk, uncertainty and profit," Social Ence Electron. Publishing, Tech. Rep., vol. 4, 1921, pp. 682–690.

[6] V. Venkatasubramanian, "Systemic failures: Challenges and opportunities in risk management in complex systems," *IEEE Eng. Manage. Rev.*, vol. 57, no. 1, pp. 2–9, Jan. 2011.

[7] Y. Y. Haimes, S. Kaplan, and J. H. Lambert, "Risk filtering, ranking, and management framework using hierarchical holographic modeling," *Risk Anal.*, vol. 22, no. 2, pp. 383–397, Apr. 2002.

[8] J. Rasmussen, "Risk management in a dynamic society: A modelling problem," *Saf. Sci.*, vol. 27, nos. 2–3, pp. 183–213, Nov. 1997.

[9] J. Luo, S. Ba, and H. Zhang, "The effectiveness of online shopping characteristics and well-designed websites on satisfaction," *MIS Quart.*, vol. 36, pp. 1131–1144, Dec. 2012.

[10] K. S. Almberg, L. S. Friedman, D. Swedler, and R. A. Cohen, "Mine safety and health administration's part 50 program does not fully capture chronic disease and injury in the Illinois mining industry," *Amer. J. Ind. Med.*, vol. 61, no. 5, pp. 436–443, May 2018.

[11] S. Tanimoto, K. Chiba, H. Sato, and A. Kanai, "A study of risk assessment for sharing economy based on a user's viewpoint," in *Proc. IEEE 8th Global Conf. Consum. Electron. (GCCE)*, Oct. 2019, pp. 240–242.
[12] L. T. Saati, "The analytic hierarchy process for decision in a complex world," *Energy Policy*, vol. 32, no. 10, pp. 1151–1158, 1980.
[13] B. Boudreau-Trudel and K. Zaras, "Comparison of analytic hierarchy process and dominance-based rough set approach as multi-criteria decision aid methods for the selection of investment projects," *Amer. J. Ind. Bus. Manage.*, vol. 02, no. 1, pp. 7–12, 2012.
[14] D. Liang, D. Liu, W. Pedrycz, and P. Hu, "Triangular fuzzy decision-theoretic rough sets," *Int. J. Approx. Reasoning*, vol. 54, no. 8, pp. 1087–1106, Oct. 2013.
[15] G. Tian, N. Hao, M. Zhou, W. Pedrycz, C. Zhang, F. Ma, and Z. Li, "Fuzzy grey choquet integral for evaluation of multicriteria decision making problems with interactive and qualitative indices," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Apr. 12, 2019, doi: 10.1109/TSMC.2019.2906635.
[16] J. Jehring and H. W. Heinrich, "Industrial accident prevention: A scientific approach," *Ind. Labor Relations Rev.*, vol. 4, no. 4, p. 609, Jul. 1951.
[17] M. Amiri, A. Ardeshir, and M. H. Fazel Zarandi, "Fuzzy probabilistic expert system for occupational hazard assessment in construction," *Saf. Sci.*, vol. 93, pp. 16–28, Mar. 2017.
[18] G. Tian, H. Zhang, Y. Feng, H. Jia, C. Zhang, Z. Jiang, Z. Li, and P. Li, "Operation patterns analysis of automotive components remanufacturing industry development in China," *J. Cleaner Prod.*, vol. 164, pp. 1363–1375, Oct. 2017.
[19] K.-Q. Zhou, A. M. Zain, and L.-P. Mo, "A decomposition algorithm of fuzzy Petri net using an index function and incidence matrix," *Expert Syst. Appl.*, vol. 42, no. 8, pp. 3980–3990, May 2015.
[20] S. Pryke, "Analyzing construction project coalitions: Exploring the application of social network analysis," *Construct. Manage. Econ.*, vol. 22, no. 8, pp. 787–789, 2004.
[21] P. Chinowsky, J. Diekmann, and V. Galotti, "Project organizations as social networks," *J. Construct. Eng. Manage.*, vol. 136, no. 4, pp. 452–458, 2010.
[22] J. R. Yang and X. W. P. Zou, "Stakeholder-associated risks and their interactions in complex green building projects: A social network model," *Building Environ.*, vol. 73, pp. 208–222, Mar. 2014.
[23] M. Silva, "50 years after the PhD thesis of carl adam Petri: A perspective," *IFAC Proc. Volumes*, vol. 45, no. 29, pp. 13–20, 2012.
[24] H.-C. Liu, J.-X. You, Z. Li, and G. Tian, "Fuzzy Petri nets for knowledge representation and reasoning: A literature review," *Eng. Appl. Artif. Intell.*, vol. 60, pp. 45–56, Apr. 2017.
[25] X. Guo, S. Liu, M. Zhou, and G. Tian, "Disassembly sequence optimization for large-scale products with multiresource constraints using scatter search and Petri nets," *IEEE Trans. Cybern.*, vol. 46, no. 11, pp. 2435–2446, Nov. 2016.
[26] Y. Xu, Y. Du, L. Qi, W. Luan, and L. Wang, "A logic Petri net-based model repair approach by constructing choice bridges," *IEEE Access*, vol. 7, pp. 18531–18545, 2019.
[27] G. Meimei and W. Zhiming, "Fuzzy reasoning Petri net and its application in fault diagnosis," *Autom. J.*, vol. 26, no. 5, pp. 677–680, 2000.
[28] S. Wang, D. You, and C. Seatzu, "A novel approach for constraint transformation in Petri nets with uncontrollable transitions," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 8, pp. 1403–1410, Aug. 2018.
[29] L. Jian-Gang, G. Jie, and W. Ming-Zhe, "Fuzzy Petri net and its application in uncertain reasoning," *Comput. Simul.*, vol. 21, no. 11, pp. 152–154, 2004.
[30] H. Guangqiu, Z. Huaping, and Z. Yangquan, "Research on fuzzy analysis of fault tree based on fuzzy Petri net," *J. Hunan Univ. Sci. Technol.*, vol. 21, no. 2, pp. 34–39, 2006.
[31] G. S. Hura and J. W. Atwood, "The use of Petri nets to analyze coherent fault trees," *IEEE Trans. Rel.*, vol. 37, no. 5, pp. 469–474, Dec. 1988.
[32] H. Ni, A. Chen, and N. Chen, "Some extensions on risk matrix approach," *Saf. Sci.*, vol. 48, no. 10, pp. 1269–1278, Dec. 2010.

LEI YU is currently pursuing the Ph.D. degree with the College of Computer Science and Engineering, Shandong University of Science and Technology at Qingdao, Qingdao, China. He is currently a Lecturer with the Institute of Finance and Economics, Shandong University of Science and Technology. His current research interests include behavioral analysis, web security, and data mining.

QINGZHI LIU is currently a Full Professor with the Institute of Finance and Economics, Shandong University of Science and Technology, China. His research interests include internal control and risk management, and big data processing.

RONG HUA is currently an Associate Professor with the College of Computer Science and Engineering, Shandong University of Science and Technology, China. His research interests include high-performance computing, artificial intelligence, and big data processing.

YOU FU was a Visiting Scholar with the Karlsner Institute of Technology (KIT), Germany, from November 2006 to November 2007. She is currently a Full Professor with the College of Computer Science and Engineering, Shandong University of Science and Technology, China. Her research interests include high-performance computing, distributed computing, and intelligent computing.