Measurement and Control of Operational Risk of Banking Industry based on Complex Network

Xiaoling Hao [1,2] Songqiao Han [1,2]
[1]School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai, 200433, China
[2]Key Laboratory of Financial Information Technology of Shanghai City, Shanghai, 200433, China
Emails: haoxiaolingsh@163.com, hansq@gmail.com

***Abstract*—Operational risk has been great challenges of commercial banks and financial institutions since losses caused by operational risk have been significantly greater than ever before. In order to control and manage operational risk better，clear awareness of the operational risk conduction mechanism is helpful to further understand the whole dynamic process of the risks affecting the business. Traditional researches focus on the method to measure the risk more accurately, but few studies took into account the conduction mechanism of operational risk. This paper constructs operational risk network to simulate the contagion process of operational risk and put forward new measurement model based on complex network. First, properties of the operational risk network is analyzed, and risk spreading process in the network is described. Then, a load model is established to explain the conduction mechanism of operational risk factors. Next, a new measurement method of operational risk based on BA model is presented to make Monte Carlo simulation and calculate the amount of operational risk losses in the operational risk network. Also, this model is used to simulate the affecting factors in the operational risk network. The simulation results show that the degree of operational risk network as well as the selection of initial node plays an important role on losses, and thus some control recommendations based on the simulation results is given. Finally, a framework of operational risk management system is designed to apply this research result into practice.**

***Index Terms*—Operational Risk, Scale-free Network, BA Model, Monte-Carlo Simulation**

I. INTRODUCTION

In recent years, operational risk has given rise to widespread concern in the financial industry. Losses caused by operational risk in many financial institutions have been significantly greater than that of market risk and credit risk. Therefore, the international financial and regulatory organizations are committed to the exploration and construction of operational risk management techniques, methods and organizational frameworks, and made significant progress. Most studies have concentrated on how to measure operational risk loss; however, studies on the conduction mechanism and the cumulative effect of operational risk are relatively scarce.

This study is to evaluate the conduction mechanism of an operational risk loss events caused by the failure of the associated processes. We use the complex network theory to describe the conduction mechanism of operational risk network, and construct a load model to represent evolutionary dynamic behavior. Simulations were conducted to make operational risk measurement based on scale-free network. Then, we use Monte-Carlo simulation to calculate the total losses of network nodes with BA network. Next, we analyze the impact of node-degree on the operational risk loss, and make a comparison between the random selection and target selection mode on initial collapse of the nodes. Afterwards, we put forward control countermeasures of operational risk. Finally we improve the design scheme of operational risk management system to apply this research result into practice.

II. RELATED WORK

There are three main academic perspectives on research of operational risk: measurement or estimation methods and algorithms of operational risk, control and management methods of operational risk, and mechanism explanation of operational risk.

A. Measurement or Estimation Methods of Operational Risk

Since the approval of new regulatory guidelines known as Basel II for banking, quantitative operational risk studies become popular. The accord includes a regulatory capital charge for OR, under which Banks should adequately manage their OR in order to assume lower levels of capital.

Cruz, Coleman, Salkin(1998) introduced the parameter estimation method in statistics and actuarial measurement method into operational risk, and put forward the concept of Value of Risk (VaR). Coral Alexander (1999) used Bayesian network measurement and management of operational risk to provide an analytical model for operational risk control. A.Frachot, P.Georges, T.Roncalli (2001) utilized the loss distribution approach (LDA) combined with Monte Carlo simulation method to calculate the commercial bank operational risk VaR, and operational risk calculations should be allocated capital according to the VaR. They compared the internal measurement method (IM) published by BIS and LDA, and found that LDA is also suitable for operational risk.

doi:10.4304/jsw.9.4.820-828

Miro Powojowski, Hans Tuenter (2002) used covariance to describe the interaction of different operational risk sources, and considered their relations. However, since such a relationshp is relatively simple, it can not reflect dynamic characteristics of operational risk events. Jack King (2003) presented a Delta-EVT model, and analyzed how to use Delta factor to measure peak risk of "high frequency but low severity" event losses, combined with the extreme value theory in the measurement of tail events advantage, and provided scientific methods for banks to precisely calculate operational risk capital. Based on QIS2 data collected by the Basel Committee Marco Moscadelli (2004), summarized and compared the previous methods of operational risk measurement, and found that the use of extreme value theory based on the generalized Pareto distribution (EVT) can best capture characteristics of thick tail of operational risk events.

Recent studies on the financial industry pay more attention to the combination of qualitative and quantitative models for operational risk. Petersand Sisson (2006) extended the range of models admissible for Bayesian inference under the LDA model, as it provided a mathematically rigorous paradigm to combine observed data and expert opinion. Dominik et al. (2009) proposed a new approach based on the Bayesian inference method, to combine these three sources of information to estimate the parameters of the risk frequency and severity distributions. Cheng et al.(2005) proposed a methodology modeling operational risk based on business process models. By connecting the generation of a probabilistic network with the business process model, this approach enables changes in the operational risk model according to the changes of different aspects of the business process in the financial institution. Mittnik, Stefan (2011) presented an econometric model which uses the Copula connection function and correlation coefficient with no parameter to describe the relationship between the operational risks, and exploits the Monte Carlo simulation method to calculate operational risk VaR, and make further calculation to allocate capital.

B. Control and Management Methods of Operational Risk

Suh, Han(2003) improved the IS risk analysis approach based on business model, which adds organizational investigation to traditional risk analysis, and uses quantitative approach to measure the value of IS assets from the viewpoint of operational continuity. Alter, Sherer (2004) presented a general, but broadly adaptable model of system-related risk, which encompasses goals and expectations, risk factors and other sources of uncertainty, the operation of the system or project whose risks are being managed, the risk management effort, the possible outcomes and their probabilities, impacts on other systems, and the resulting financial gains or losses. Muehlen, Rosemann(2005) addressed the topic of risk management in the context of business process management, and presented a taxonomy of process related risks and discussed how this taxonomy can be applied in the analysis and documentation of business processes. Jordan (2005) set up an integrative IT risk governance model that meets the wider needs of corporate governance. WorrellBush (2007) surveyed the perceptions of 13 information technology risk factors, among which “lack of organizational alignment between businesses” is relatively high. Salmela (2008) adopted the business process analysis approach to analyze the business losses caused by information system risk, which associated information systems availability with potential losses. Most of these methods are based on theoretical analysis without experimental observations or data analysis, and thus they can’t support the cost-benefit decision.

C. Mechanism Analysis of Operational Risk

Kuhn, Neu(2003) proposed a dynamic model to describe the operational risk generation mechanism using the lattice gas model in physics. This model uses the lattice gas liquefaction into liquid process to describe the process where business process failure eventually led to the collapse of the whole system. A breakthrough of this model is considering the dynamic relationship between business processes in the measurement of operational risk.

From the literature review, we find that most studies concentrated on how to measure operational risk loss based on the new Basel Capital Accord. Many researchers introduced more sophisticated methodologies based on mathematics and statistics in order to accurately calculate the capital charge. Some literature advances risk analysis and management method, but doesn’t give specific information on how to use the method in real situation. Moreover, few studies considered the impact of conduction mechanism on measurement and the cumulative effect of operational risk. Therefore, we should deepen the study of conduction mechanism and find root cause of operational risk, which can provide meaningful, repeatable and consistent result in the future.

III TRADITIONAL MEASUREMENT OF OPERATIONAL RISK

There are three approaches to set capital charges for operational risk: (1) The Basic Indicator Approach, (2) The Standardized Approach and (3) The Advanced Measurement Approach. Each approach requires a greater investment in processes and procedures than the one that precedes it. One of advanced approach is Internal Measurement Approach (IMA) , under which the capital to be allocated is computed as a quantile (expected loss + unexpected loss) but rather than modeling losses to a particular distribution. Another advanced approach is Loss Distributional Approach (LDA). The idea of LDA is to fit severity and frequency distributions over a predetermined time horizon, typically annual. Popular choices include exponential, weibull, lognormal, generalized Pareto, and g-and-h distributions (Dutta et al. 2006), then the best fitting models are used to produce compound processes for the annual loss distribution, from which VaR and capital estimates may be derived.

According to a data sample collected from 2000 to 2010, the loss events of the operational risk and according loss is listed in table 1 , in which the internal

fraud events account for the largest proportion, more than 69%.

The statistical results showed that the most common operational risk of commercial banks of China is internal and external fraud, which means that bank staffs can easily take advantage of higher authority to illegally make profit owing to the loopholes of internal management in commercial banks.

TABLE I.

DATA COLLECTION OF SOME OPERATIONAL RISK INCIDENTS OF CHINESE COMMERCIAL BANK DURING 2000-2010

Event type	Frequency	Ratio（%）
Fixed assets destroyed	3	1.30
employment policy and the workplace	1	0.43
Clients, products and business operation	26	11.30
Internal fraud	160	69.57
External fraud	34	14.78
Business disruption and system failure	4	1.74
Execution, delivery and process management	2	0.87

Here we use LDA method to simulate the distribution of annual total amount of loss with the data sample. Using data fitting method, we know that the loss event frequency obeys Poisson distribution with parameter of 7.3, loss severity obeys lognormal distribution with parameter (9.4, 4.6). The simulation procedure is as follows:

- Random generation of loss event number M according to the loss distribution of event frequency
- Random generation of annual loss according to the loss event intensity distribution, M random number is generated, each with $L_{11}, L_{12}, ..., L_{1M}$
$$Loss_1 = \sum_{n=1}^{F_1} L_{1n}$$
- Calculate total annual loss.
- Repeat the above steps N times, N=10000.
- Calculate the VaR, and draw the histogram.

Using Matlab to make simulation, the program is as follows.

```
N=10000;
n=1;
lamda=5;
miu=5;
sigma=3;
tLossTable(1:N)=0;
while n<=N
   lossFrequency=poissrnd(lamda);
   f=fix(lossFrequency);
   tLoss=0;
   flag=1;
   while flag<=f
      lossSeverity=lognrnd(miu,sigma);
      lossValue=log(lossSeverity);
      tLoss=tLoss+lossValue;
      flag=flag+1;
   end;
   tLossTable(n)=tLoss;
   n=n+1;
end;
tLossTable=sort(tLossTable(1:N));
n=1000;
while(n>0)
   fprintf('%d\n',tLossTable(n));
   n=n-1;
end;
hist(tLossTable,1000),title('Total Loss Distribution');
Nq=N*0.999;
quantile=tLossTable(Nq);
fprintf('99.9quantile is %d\n',quantile);
```

According to simulation result, the 99.9quantile is 1.883431e+002 VaR1 is188.3, as shown in figure 1.

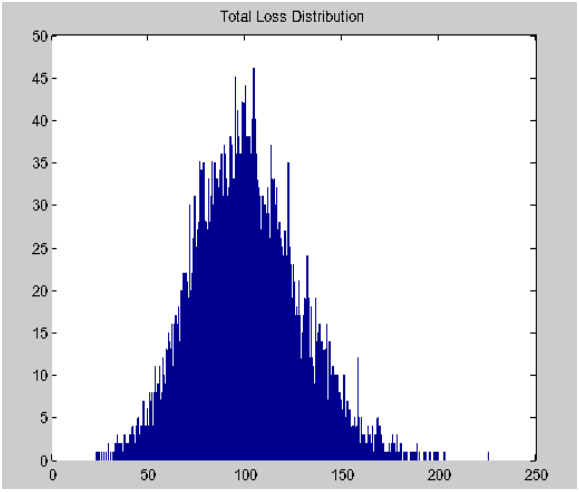

Figure 1. Distribution of annual total amount of loss

IV CHARACTERISTICS OF OPERATIONAL RISK NETWORK

According to Basel II, operational risk is caused by the following sources: the failure of the associated process, internal people, breakdown of information system, or external incidents. The four different types of operational risk factors form the nodes of the network of operational risk. These nodes contact each other through information flow, or capital flow, or the interflow of goods and materials, and they build up the carrier of the operational risk, the links between the risk sources, the network of operational risk is then formed.

For example, in the network of commercial banks operational risk, there are a large number of nodes; some links exist among these nodes and the contact mode among them are not the same. Some of the network nodes have a high degree of contact, such as certain key employees and key system module. The degree of other nodes is relatively low, such as most of the customers. Various risk factors in the network of operational risk are also interrelated and interacted, for instance, loopholes in information system nodes or some internal or external deliberate attacks can cause the failure of the system

[1] According to BCBS(2001b) guidelines, the confidence level is 99.9% to calculate the VaR.

nodes. When more nodes join the business network, the network will grow quickly and become more complex. The newly added node is actually priority selectivity. For example, customers that handle basic business deposit and loan apparently increases much more than those apply for specialized financial business unit. In this case, clients tend to choose more skilled staff or client managers, which reflect the priority selectivity.

With two typical features: network growth and priorities selectivity, operational risk network will develop into a scale-free network after a period of evolution. Studies by Barabasi and Albert (1999) have shown that preferential attachment characteristics and continuous growth of the network did eventually develop into a scale-free network, and node distribution follows the power-law distribution. Therefore, we can abstract operational risk network into a complex network, specifically, a scale-free network.

V. Conduction Mechanism of Operational Risk Network

The conduction dynamics on complex networks originated in the spread of infectious diseases. Researchers constructed a variety of models according to different groups and spread patterns, mostly based on the SIS model and SIR model.

Similar to the spread of infectious disease process, the nodes in the network can be divided into three states during the spread period of operational risk through the network:

- Health state, also known as the susceptibility status (susceptible). That is, the node is currently healthy, but it is connected with other infected nodes. Such node is a potential risk.
- Infection state (infected). Nodes in infection status are the sources of risk; they can infect the susceptible node.
- Immune state, also known as the removed state (removed). Nodes in the immune status have low possibility of infection due to control measures.

The spread of operational risk in business processes can be described with the SIS model. There are two states in the SIS model: infection state (I) and susceptible state (S). Without human interference, operational risk network is in line with the SIS process. With the spread of operational risk, a node may come into infected state from the susceptible state, or return to the susceptible state.

Effective transmission rate is defined as follows:

$$\lambda = \gamma / \delta \tag{1}$$

γ means the probability of infection status (I) from the susceptible state (S); δ means the probability of return from the infection status (I) to the susceptible state (S).

We can assume that $\delta = 1$, because in a long time period, the node will usually return to the susceptible state from the infected state.

The risk threshold of the effective transmission rate is defined with λ c. It is used to determine whether the risk can spread across the network with the effective transmission rates. If $\lambda > \lambda$ c, risk will continue to spread in decline into a steady state; if $\lambda < \lambda$ c, infected individuals will gradually decay, the risk can not be large-scale transmission. To simplify the study, the operating risk network is regarded as a BA network. The BA network is a scale-free network with the characteristics of growth and priority selectivity. Then we use these two features to derive the threshold of operational risk.

First we define the propagation probability. $\rho_k(t)$ is the probability of infection the node with Degree k, $\theta(\rho_k(t))$ indicates the probability of connection between any given side and the node in infection state. Suppose the steady-state value of $(\rho_k(t)$ is ρ_k, let the left side of above equation equals to 0, we can get:

$$\rho_k = \frac{k\lambda\theta(\lambda)}{1 + k\lambda\theta(\lambda)} \tag{2}$$

The result indicates: higher the degree of nodes results in higher probability of infection.

Next step is to calculate the value of $\theta(\lambda)$, through mathematic inference, we can get

$$\theta(\lambda) = \frac{1}{< k >} \sum_k kP(s)\rho_k \tag{3}$$

As we know the distribution of the degree of BA network is P（k）=2m2k-3, distribution of <k> and average P (k) is substituted into above equation, we can get:

$$\theta(\lambda) = m\theta(\lambda)\ln[1 + \frac{1}{m\lambda\theta(\lambda)}]$$

$$\theta(\lambda) = \frac{e^{-\frac{1}{m\lambda}}}{\lambda m}(1 - e^{-\frac{1}{m\lambda}})^{-1}$$

$$\rho = 2e^{-\frac{1}{m\lambda}} \tag{4}$$

The above equation is valid only if λ =0. So the threshold value of network transmission of operational risk is λ c=0. This conclusion means that the network of operational risk, as long as the effective transmission rate of risk spread is greater than 0, can be spread in the network until a stable state. Therefore, the operational risk network is a very fragile network. If risk points are

left unchecked, they can easily lead to operational risk events.

VI Load Model of Operational Risk Conduction

Similar to the other network, operational risk begins to conduct from a risk source to the adjacent node, if adjacent node control is weak, it will be infected, and become a new source of infection, and continues to spread. Otherwise, the node is still in a state of health. As long as the effective transmission rate of a risk factor is greater than 0, without enough efforts to control operational risk, the entire network will fail, leading to loss events. We can use a load model to describe the process of risk conduction.

Model description is as follows:

Suppose any node i in the network can withstand a certain load, the threshold value of Ci, it is consistent with the distribution P (Ci), indicating the strength of its internal control. If more efforts are put into this node control, it will have more anti-attack capability. Each node i has the initial load of Li, if the node suffers a hit over its load, it will crash into the infected state. Suppose the load intensity of all nodes in the network follow certain distribution P (Ci) .

When the impact of a node exceeds its endurance limit, this node will collapse, its function will fail. Original impact within its endurance limit will be sub-allocated to all adjacent nodes, which accords with the rule of priority selective of the scale-free network. That is, the possibility of allocation load to node j is Pij , which originally

assigned to node i, the probability Pij. Node J receives from node i to pass over the additional load ΔLji.

$$\Delta L_{ij} = L_i \frac{k_j}{\sum_{n \in \Gamma_i} k_n} \tag{5}$$

Where, Γ_i represents complete sets of adjacent nodes with i nodes, as shown in Figure 2:

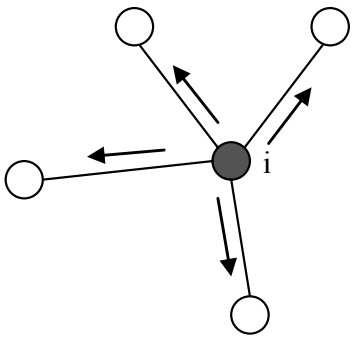

Figure 2. The conduction of risk between the nodes

As shown above, the n nodes adjacent to i-node have the same degree of 1, so, after the collapse of node i, its original load will be evenly distributed to the adjacent n nodes.

For the receiver node, its total additional impact is the sum of all the impact of the nodes passed over by the adjacent crash nodes, as shown in Figure 3. In this example, we can calculate the impact of four nodes A, B, C, D, received from node 1, 2, 3, 4, Through the calculation of this example, a better understanding of the load model. Point A only receives the shocks coming from Node 1, Node 1 is adjacent to the A, B, The degree of A is 2 and degree of B is 5. Based on the above model, A received additional shocks from 1.

Point B receives the impact from 1, 2, 4. The degree of node 1 is 2, and the degree of node 2 is 3, and the degree of node 4 is 2, B-node degree is 5, but all of the adjacent three nodes has failed and can not spread the risk of shock. In accordance with the method of calculating the A-node, B receives the additional shocks from 2 and 4.The same method can apply to the additional shocks of point C.

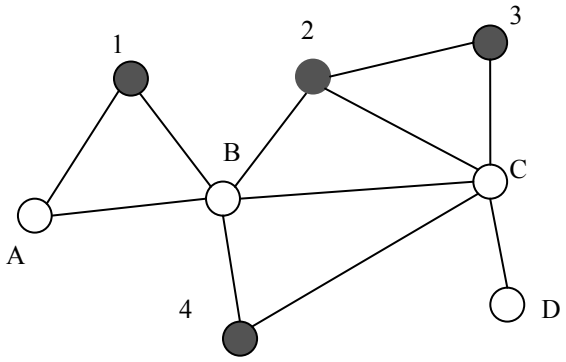

Figure 3. Example of risk conduction

In this example, point D which is not directly adjacent to any node has crashed, so it does not receive any additional losses, so LD=0. It explains the impact on the adjacent nodes when node i collapse. Kj is the degree of node j, means the degree that the node is affected. According to priority selectivity of scale-free network, the node with higher degree has greater probability of being affected. Therefore, the total load of the node is:

$$TL_i = L_{ij} + L_i \tag{6}$$

If the total load of node j exceeds its threshold C_j, node j will become a state of collapse, and become a new risk source and affect the neighboring nodes.

VII. Operational Risk Measurement Based on Scale-free Network

Operational risk loss events arise from daily operations of the banks business process. An error of a node in the network of operational risk led to its collapse, it then spreads to adjacent nodes, and eventually gives rise to an operational risk events. Therefore, the source of operational risk events is the collapse of a number of nodes in the network of operational risk. The degree of the nodes determine its impact the network, if a node has higher degree, if will suffer more impact and cause higher amount of loss.

From the perspective of operational risk network, after a period of conduction process, the network will be in a stable state. The total amount of losses will not change no matter which path it spreads without considering the external disturbances. So in the end, the measurement of operational risk losses does not have to consider the spread path of risk. Calculation of operational risk losses is similar to the Loss Distribution Approach (LDA), we still use the Monte Carlo simulation method, but add the parameter node-degree to describe the degree of importance of the node. Higher degree of nodes means higher importance of the nodes in the network.

The calculation of the specific steps is as follows:

- The initial node number of M is randomly generated, according to the frequency distribution of loss events;
- The initial amount of loss of node number of M is randomly generated, according to the severity distribution of loss events; they are L11, L12, L1M, respectively.
- Since the random number that obey a power law distribution is not directly and easily generated, we first simulate a BA network with degree n, the node degree is power-law distribution, so each step randomly selected from the storage network node degree vector M value of K11, K12, the K13, ... K1M;
- In this model, the impact of node degree is a multiple of the form of performance, because during a longer time period, the collapse of a node will lead to the collapse of the adjacent node. Then a node with a higher degree will play a role in amplification in operational risk spread. So the total loss in this process for

$$Loss_1 = \sum_{n=1}^{M} L_{1n} k_{1n} \tag{7}$$

- Repeat above steps N times, then draw a histogram of the total amount of loss, and take the amount of loss in the 99.9% confidence level as the output. Assuming that the initial collapse of the number of nodes is in line with the parameters of Poisson distribution, the loss distribution of a single node is in line with the parameters of lognormal distribution. The network average degree <k> = 4, the amount of operational risk distribution is shown in Figure 4.

The code that simulates the process is shown as follows.

```
n=500; a=zeros(n,n);
m=6.5;
n0=7;
p0=0.8;
for i=1:n0
   for j=i+1:n0
      if rand(1,1)<p0
         a(i,j)=1;
         a(j,i)=1;
      end
   end
end

for i=1:n0
   deg(i,1)=sum(a(i,:));
end

for i=n0:n-1
    b=zeros(m,1);
   [b]=scalefree(i,m,deg);
   for j=1:m
      a(b(j,1),i+1)=1;
      a(i+1,b(j,1))=1;

deg(b(j,1),1)=deg(b(j,1),1)+1;
   end
   deg(i+1,1)=m;
end

Function scalefree ():
function [b]=scalefree(ni,m,de)
b=zeros(m,1);
dp=zeros(ni+1,1);
sk=0;
for i=1:ni
   sk=sk+de(i);
end
dp(1,1)=0;
for i=1:ni
   dp(i+1,1)=dp(i,1)+de(i,1);
end
is=1;
while is<=m
r=rand(1,1);
r=fix(r*sk+1);
for i=1:ni
   if r>dp(i,1)&r<=dp(i+1,1)
      it=i;
   end
end
pd=0;
for j=1:is
   if it==b(j,1)
      pd=1;
   end
end
if pd==0
  b(is,1)=it;
  is=is+1;
else
   is=is;
end
end
```

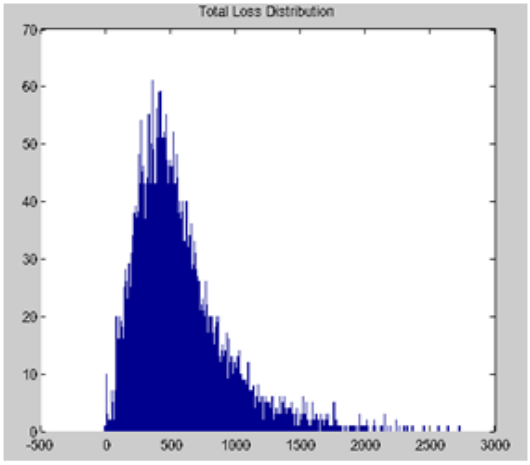

Figure 4. LDA Simulation with BA network

Output: 99.9quantile is 2.2387651e +003, generated in the process of operational risk value loss of $ 2.23 X-103. The size of this figure is not important, because the banks can be adjusted according to their own internal data collected to calculate the operational risk losses.

From the distribution figure, we can clearly see that it is the left deviation, suggesting that the loss amount for the vast majority of operational risk events will not be large, but this kind of events accounts for a large proportion of the total, occurred in the relatively high frequency. It also shows that the operational risk loss distribution tail dragged on very long, which shows that probability of the events that caused large amount loss is small, but they can lead to huge loss, so accurate measurement of operational risk loss of the tail is very meaningful for banks.

VIII The Impact of Node Importance and Selection Mode on Loss

In operational risk Network, the greater the degree of a node, the greater impact it will exert on other nodes in the time of collapse, thus it will bring greater impact on the operational risk network. For internal personnel node, the

node with higher degree shows that in the process of banking operations, the staff will have more contact with other employees, or with higher privileges, or can handle many types of business, or have more access to the internal multi-kinds of data. For information system node with higher degree, it means the node may be the hub of the local network; it will exchange data with many modules. The failure of this module will lead to the failure of the adjacent module. In short, the network with higher average degree will take more risks and is not conducive to bank operational risk management without effective countermeasures. We use LDA method to calculate the operational risk losses under different network average degree <k>, as shown in figure 5.

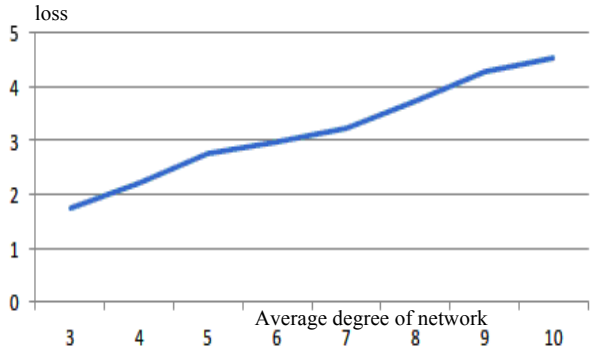

Figure 5. Influence of Average degree of network on loss

From Figure 5, the calculation results are consistent with the theoretical results. It can be seen that the network average degree have positive impact on the amount of operational risk: greater average degree of will bring about more operational risk losses.

The size of the resulting loss of operational risk is determined by the initial collapse. So the selection mode of initial node will also affect the final operational risk losses. We can select the initial collapse of the nodes in two ways: random selection and target selection.

A. Random Selection.

In this mode, initial collapsed node is randomly selected from the operational risk network, since the degree of nodes obey the power law distribution, most of the nodes in the network node degree is not high, so the low-degree nodes have larger probability to be selected. Operational risk event under random-selection mode occur more frequently in the process of business operations due to personnel errors or system failures, and other reasons. Such events are caused by the business disruption and system failures, execution, delivery and process management, customers, products and business operations, employment policies and workplace safety and other unintentional violations or attacks. Such loss events are due to the people, processes or system errors, rather than deliberately caused.

B. Target Selection.

Target selection means selecting the initial collapsed node with relative higher degree. Operational risk events generated in this way is mostly due to the artificially illegal operations or the intentional use of the loopholes in the system to obtain benefits. Target selection corresponds to the event type of internal fraud and external fraud. They are usually caused by their own economic interests knowingly take advantage of loopholes in the internal control by the bank's internal operational risk event. Many cases of operational risk events showed that the internal fraud is usually implemented by senior management personnel or system administrators, and the amount of loss caused by these events is enormous.

In theory, the target selection is initiated against the key nodes, so the loss of entire network is much greater than random selection. The amount of loss under random selection method and the target selection one is shown as figure 6:

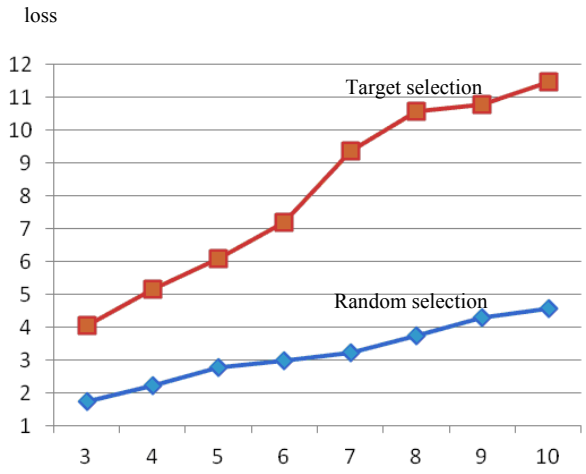

Figure 6. Comparison of target selection and random selection

From Figure 6, we can see that under the condition of the same average degree of operational risk, target selection method caused losses far greater than a randomly selected. With the growth of average degree, these two methods produces bigger gap. The simulation results are in line with the theoretical assumptions.

From the simulation results, we can get the inspiration as follows: In the actual business operations of banks, operational risk shows an obvious fat-tail shape. The amount of loss caused by the majority of loss events is small; the bank will not cause substantial harm, such as the teller data entry errors. This kind of operational risk can be reduced by enhancing internal control. Operational risk in the tails, which is characterized by very low probability of occurrence, but cause a great deal of loss, such as the Barings incident, which eventually leading to bank failures. Control cost to cover this operational risk is often high, due to the extremely small probability of occurrence, control measures will not seem so important. This kind of operational risk event needs specialized provision for capital funds or insurance to cover.

Because the network's average degree of operational risk directly affects the amount of operational risk.

Internal control measures should be taken to minimize average degree of the network without affect normal business operation. Under the same situation of internal control measures, target selection tends to cause more loss than random selection, so these nodes with higher degree should be monitored and managed more effectively.

IX Design of Operational Risk Management System

Based on above research, we design an operational risk management framework, which consists of the following four layers: management and control layer, report layer, simulation and analysis layer, data layer, as shown in figure 7.

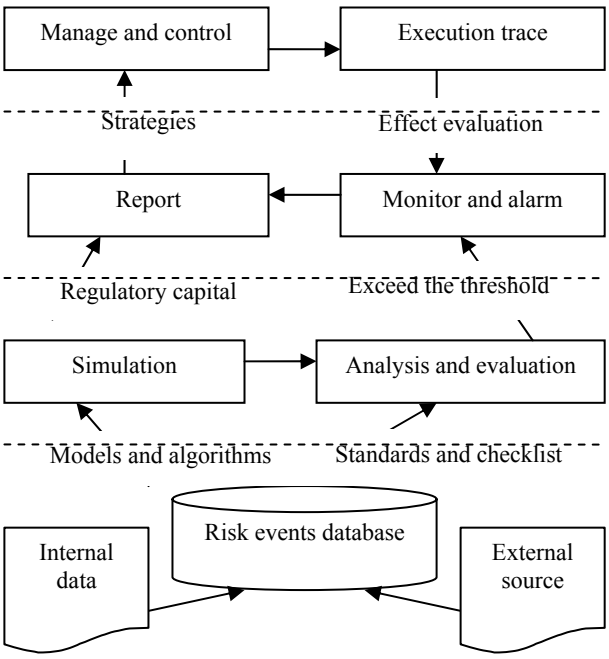

Figure 7. Design framework of OR management system

Data layer is the bottom layer to build the underlying database, which includes OR index database: and OR loss event database. External and internal operational risk loss events, events causes, as well as the loss type, amount, business lines, time and other attributes are collected, recorded and classified.

Simulation and analysis layer mainly provide a variety of operational risk analysis model, including: risk assessment model, operational risk index detection model, operational risk loss analysis model, operational risk level evaluation model, operational risk capital measurement model. At the same time, the simulation algorithm described in this paper is embedded to the module. Through the establishment of operational risk measurement model based on complex networks, by adjusting the parameters, the simulations of operational risk VAR value under different scenarios (different network nodes, the initial attack) is calculated. We can also set the loss threshold, and make early warning according to the setting threshold about some indexes.

Report layer provides multiple report analysis function for the user, including: operational risk assessment report, improvement measures of operational risk reporting, inspection report, test report, key risk indicators of operational risk loss event reporting, operational risk capital measurement report. This can be arranged or displayed systematically in table form or graphic form.

Management and control layer includes development of operational risk measures and controls, such as operational risk identification, assessment, risk control, management of key risk indicators, risk decision making and processing, control execution, risk tracing plan, etc. The goal is to provide operational risk management platform for user. Then the execution is traced and effect evaluation is made to check the validity of the plan, tracking and action plan, which forms another recycle of risk management.

X Conclusion

In this work, the risk source and carrier are summed up to abstract network model, on the basis of the definition and characteristics of operational risk and loss data, which lay the theoretical foundation for the study. Then SIS model of risk conduction is introduced. As long as critical value is more than 0, risk can reach a steady state in the network. We describe the conduction mechanism of operational risk in the scale-free network. Then the load model was established, and used to study the risk sources of influence on its neighboring nodes, thus explaining the conduction mechanism of operational risk in the network.

Based on the operational risk of the network, we propose a method of measuring operational risk losses; this method takes into account the different nodes of the network with different importance. We then use Monte Carlo for measurement of operational risk loss amount with this method, which can well capture the operational risk tail events. With this measurement method of operational risk losses using the BA model in this paper, we take into account the effects of node importance as well as selection of the initial node of attack in the network. This research result has management implications to guide financial institutions to execute internal control of the operational risk. We finally advance the design scheme of operational risk management system to help us to apply this research result into practice.

Acknowledgments

The authors wish to thank Xin Zhou, who has made an contribution to this work by making the simulation experiments. This work was supported in part by Shanghai Natural Science Foundation (Grant No 11ZR1411900), and National Science Foundation of China (Grant No 61003022 and 71001058).

REFERENCES

[1] A. Barabási, R. Albert. Emergence of Scaling in Random Networks. Science(1999) 286:509-512

[2]]A.Frachot, P.Georges, T.Roncalli, Loss Distribution Approach for operational risk, working paper, 2001.4

[3] D.Dominik, Lambrigger, et al., The Quantification of Operational Risk using Internal Data, Relevant External Data and Expert Opinions.The Journal of Operational Risk 2(3), (2007)3-27

[4] H. Dahen, G. Dionne, Scaling models for the severity and frequency of external operational loss data, European Journal of Political Economy, l25(3)(2009) 311-326

[5] Y. Moreno et al. Instability of free-scale networks under node-breaking avalanches,Europhys. Lett. 58(4)(2002):630-636

[6] P. Embrechts. Copulas: A Personal View, Journal of Risk and Insurance. l76(3)(2009) 639–650

[7] R. Kuhn, N. Peter. Functional correlation approach to operational risk in banking organizations. Physica A. 322 (2003): 650–666

[8] R. Cohen, S. Havlin. Scale-Free Networks Are Ultrasmall, Physical review letters, (2003) 90(5), 058701.

[9] B. Suh, I. Han. 2003. The IS risk analysis based on a business model. Information & Management. 41(2):149-158

[10] D.D.Lambrigger, P.V.Shevchenko, M.V. Wüthrich. 2007. The Quantification of Operational Risk using Internal Data, Relevant External Data and Expert Opinions, Journal of Operational Risk. 2(3), pp.3-27

[11] K.Dutta, and J.Perry, 2006. A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital. Working Paper:Federal Reserve Bank of Boston, No 06-13.

[12] F. Cheng, D.Gamarnik, N. Jengte, W. Min, Bala Ramarchandran. 2005. IBM Research Report: modeling operational risk in business processes, RC23672(W0507-148)

[13] G. V. Post, J.D. Diitz. 1986. A stochastic Dominance Approach to Risk Analysis of Computer Systems. MIS Quarterly. (12):363-375

[14] H.H.Salmela. 2008. Analysing business losses caused by information systems risk: a business process analysis approach, Journal of Information Technology (Palgrave Macmillan). 23(3):185-202.

[15]]J.L. Worrell. A.A. Bush. 2007. Perceptions of Information Technology risk: a Delphi study. Conference of AMCIS.

[16] M.Muehlen, M.Rosemann. 2005. Integrating Risks in Business Process Models. 16th Australasian Conference on Information Systems Integrating Risks in Business Process Models.

[17] P.V. Shevchenko, M.V. Wüthrich. 2006. The Structural Modeling of Operational Risk via Bayesian inference: Combining Loss Data with Expert Opinions. The Journal of Operational Risk 1(3): 3-26.

[18] G.W.Peters, and S. A.Sisson, 2006. Bayesian inference, Monte Carlo sampling and operational risk. Journal of Operational Risk .1(3): 27–50.

[19] [S.Halliday, K.Badenhorst, R.Solms. 1996. A business approach to effective information technology risk analysis and management. Information Management & Computer Security. 4 (1):19-31

[20] S.Sherer, S. Alter .2004. Information system risks and risk factors: Are they mostly about information systems? Communications of the AIS . 1 4 (1): 29-64.

[21] S.Alter, S.Sherer. 2004. A general, but readily adaptable model of information system risk, Communications of the Association for Information Systems .14(1):1-28

[22] X. K. Dimakos, K.Aas. Integrated Risk Modelling, NR Report, Norwegian Computing Center, Applied Research and Development.

[23] X.Bai, Design of Risk Management Strategies in Business Process Information Flow, Risk Workshop SAMSI

[24] R. Albert, A. Barab´asi, Statistical Mechanics of Complex Networks, Rev. Mod. Phys. (2002) 74, 47–97

[25] R.Pastor-Satorras, A. Vespignani, Epidemic spreading in scale-free networks. Physical review letters, (2001),86(14), 3200-3203.

Xiaoling Hao is an Associate Professor at School of Information management and Engineering, Shanghai University of Finance and Economics, China. She was born in 1975. She received her B.S. degree and M.S. degree from Jilin University in Changchun, China, in 1998 and 2001, respectively. She received Ph.D degree in management science from Tongji University in 2004. She worked as a Visiting Scholar at Washington University in 2009. At present, she also works in Key Laboratory of Financial Information Technology of Shanghai City. She has (co-)authored three books and over 30 scientific papers. Her current research interests include operational risk management, data mining, and etc.

Songqiao Han is a lecturer at School of Information management and Engineering, Shanghai University of Finance and Economics, China. He received the Ph.D degree in computer science from Shanghai Jiaotong University in 2008. He works as a Visiting Scholar at Northwestern University in 2013. He has (co-)authored over 20 scientific papers. His research interests are in ubiquitous computing, mobile and wireless ad hoc networks, data mining.