Analysis of Network Risk System Based on Non-optimum Factor Assessment

Jin LI [a], Ping HE[b]

Department of Information, Liaoning Police College, Dalian, 116036, China

[a]email: lnpolice@126.com, [b]email:heping2000@163.com

Keywords: non-optimum category of network security; risk and non-optimum; risk-born relationship; trusted assessment

Abstract. The formation of non-optimum factors serves as the basis for existence of network risk system in uncertainty. Besides, the various characteristics and functions of the network security can be measured from the assessment of the non-optimum factor. By summing the practice, this paper has also come at non-optimum assessment principle in the risk analysis of network security, established the conception models of risk system and the risk management models based on the non-optimum category. At the same time, it also puts forward the non-optimum measurement of the network risk system along with non-optimum tracing and trusted management of the network risk systems. Based on the non-optimum analysis of the network risk system, it puts out the academic idea of the extension risk data. Meanwhile, it discusses about the general framework of the cooperative mapping of network risk systems. Finally, according to the previous practice of trusted measurement, kind of method has been developed to approach the network risk system from network non-optimum systems.

Introduction

Ever since nearly half a century, the risk analysis theory has undoubtedly contributed extensively every branch of information science and management science. It is because of its wide use that people find out it is far from actual requirements. People wonder whether ideal model analysis can solve real risk problems. Furthermore, it is very hard to build up a mathematic model for many of the actual risk analysis problems. Especially when the risk measurement of the system is uncertain, man can only limply build up the model, but can hardly get its solution. Although there are a lot of approximate methods and theories of solving, they are far from satisfaction.

As the reach of today’s network system has become global, they have become the focus of arguments over the values that should govern their development. However due to the complexity of network system, there are numbers of unknown and uncertain factors, longitudinal and transverse relationship of things, people’s networks behavior. Especially as the network systems heads to the orderly dynamic condition, some of the hidden troubles are not exposed, the achieved most optical modes are in unstable states. This implies that the recognition and practice of mankind is featured by the exploration and pursuit not only in an optimum category, but also, under many conditions, in a non-optimum category. That is to say when people are faced with urgent problems, they need not only to find out the most optimum mode or realize the most optimum aim, but also, more importantly, to get rid of the vicious influences of non-optimum accidents effectively as well as control the non-optimum factors of the network system. In reality, every network system belongs to the non-optimum category [1]. It meets the recognition and realization of mankind to analyze the causes of network system and the ways to reach risk from the viewpoint of non-optimum category. This way of thinking is abbreviated as risk assessment theory based on non-optimum analysis. The objective of this paper is to analyze the non-optimum factor on the network system and to discuss a method for risk analysis based on measurement of non-optimum factor.

This paper is structured as follows: The second section introduces the non-optimum concepts of network systems and related research reviews theoretical principles relevant to network risk system like factors of non-optimum, analysis on technology acceptance model. The third section network risk system models architecture studies based on non-optimum cooperative mapping. Finally, conclusion puts forward the discoveries of this research and future research direction.

Basic Concept

Non-optimum Assessment of Network Security. Non-optimum analysis on system, as a technology with the fastest rate of development and application in all branches of business, requires adequate protection to provide high decision making level. [1] The aim of the non-optimum assessment applied on a risk analysis of network security is to identify and evaluate threats, vulnerabilities and non-optimum factors. Decision analysis assets are exposed to risk of damage or losses. In order to minimize losses, it is necessary to involve risk management and risk assessment in the areas of non-optimum system and operational risks. Non-optimum assessment is the most important parts of risk analysis of network security. But most experts accept that assessment of non-optimum factor involves analysis, planning, implementation, control and monitoring of implemented measurements, and non-optimum assessment, as part of non-optimum system. It consists of several processes: (1) Non-optimum attributes identification of network system. (2) Non-optimum factors evaluation of network system.

Non-optimum system recognizes, accesses non-optimum, and takes measures to reduce non-optimum, as well as measures for non-optimum maintenance on an acceptable level. The main aim of non-optimum assessment is to make a decision whether a system is acceptable, and which measures would provide its acceptability. For every organization using non-optimum analysis in its business process it is significant to conduct the non-optimum assessment. Numerous threats and vulnerabilities are presented and their identification, analysis, and evaluation enable evaluation of non-optimum impact, and proposing of suitable measures and controls for its mitigation on the acceptable level.

The policy of the analysis of non-optimum system has changed in the last years. From checklists for identifying specific events, the evaluation and analysis has risen onto a higher level, i.e. the policy and strategy consider threats and weaknesses of the business environment.

In the process of non-optimum factor identification, its sources are distinguished by a certain event or incident. In that process, the knowledge about the organization, both internal and external, has an important role. Besides, past experiences from this or a similar organization about non-optimum issues, are very useful.

We can use many techniques for identifying non-optimum factors: checklists, experienced judgments, flow charts, brainstorming, Hazard and Operability studies, scenario analysis, etc. In order to assess the level of non-optimum factor, likelihood and the impact of incidental occurrences should be estimated. This estimation can be based on experience, standards, experiments, expert advice, etc.

Since every event has various and probably multiple consequences, the level of non-optimum is calculated as a combination of likelihood and impact. Non-optimum analysis or assessment can be quantitative, semi quantitative, and qualitative.

Risk Analysis Based on Non-optimum Factors. Non-optimum factors are very important problem in risk assessment. However due to the complexity of mankind’s practice, there are numbers of unknown and uncertain factors, longitudinal and transverse relationship of things, people’s behavior. Especially as the system heads to the orderly dynamic condition, some of the hidden troubles are not exposed, the achieved behavior aim is in unstable states. This implies that the recognition and practice of mankind is featured by the exploration and pursuit not only in an optimum category, but also, under many conditions, in a non-optimum category. That is to say when people are faced with urgent problems, they need not only to find out the optimal model or realize the optimal aim, but also, more importantly, to get rid of the vicious influences of non-optimum effectively as well as control the risk factors of the system [2].

As to every kind of uncertainty problem, there are the individual non-optimum factors as well as the common non-optimum factors. The so-called individual non-optimum factors are decided by the characters of the network system, while the common non-optimum factors are an objective entity.

In fact, every risk exists in a non-optimum category, thus, network risk system is an uncertainty system with the non-optimum factors. The real actions of the network system tell its risk factors. Generally speaking, these risk factors are included in the non-optimum factors. The key to analyze and research the network system's risk lies in how to build up non-optimum factors of the system. First of all, finding out the non-optimum factors of the past is the prerequisite. In the different stages of the past, the size of the non-optimum factors might be different. Therefore, in the non-optimum category, it is important to find out the non-optimum factors that caused the changes of the network system's risk, which possess a stable region. Thus, the risk analysis of the network system is composed of these non-optimum factors.

Since the risk factors research is rather complex, it takes on certain unclear factors under any condition. The unclear factors are unknown things possessed by the risk factors, which are decided by the complexity of the risk in numerical value. For example, the economic risk model is much more complicated than the physical risk model. Therefore the unknown thing of economic risk factors is much more than physical risk factors. These unclear attributes cause the non-optimum factors of the risk system. For example, in the risk analysis of economic systems, the non-optimum factors of the economic systems of the past play an important role in analyzing the current risk analysis of economic system. In reality it is very difficult to analyze all the non-optimum factors of the past, sometimes even not possible under certain conditions. If we could find out the time period when the important changes happened in the economic system, search for the non-optimum factors during that time, and analyze which factors were the major non-optimum ones causing the economic fluctuations, we can then tell the risk factors in the stable region of the actual economic system.

There are two factors that need to be paid attention during the formation of the risk analysis of the network system: one is non-optimum procedure, and the other is non-optimum result. The decrease of the network system's risk degree is actually the decrease of the system's non-optimum degree, which explains the decrease of the system's uncertain factors at the same time. Thus the decrease of the system's non-optimum factors reflects the improvement of controllability and observability of the network risk system. From the viewpoint of the network risk system's own characters, the minimization of the non-optimum factors is the qualification of creating the minimization of the network system's risk. From the viewpoint of the network risk system's environment, the decrease and the increase of the non-optimum factors decides the direction of the changes of the risk's factors. Furthermore, if the network system's risk is increasing, the reasons of it lie in two aspects: one is the increase of the system's non-optimum degree.

The groundwork of the risk analysis theory of the system is the systematic non-optimum analysis doctrine. For any system, whether it has entered the risk category or gone out of risk category are judged through non-optimum analysis. In order to hold the system in the optimum category under certain degree and stage, we have to recognize and control the risk factors of the system through non-optimum analysis. As we know, the non-optimum factors of the system are not only dynamic, but also evaluative. In order to measure the degree of the evolution of the system's non-optimum factors, the criteria of evolution have to be set up (non-optimum criteria). Generally speaking, from the viewpoint of the inner structural organization of the risk system, entropy and relevant parameters can be used as criteria, e.g. entity of the entropy, upper-entity of the entropy, and negative entropy. As is explained in the statistics of entropies, the value of the entropy proves how much chaos there are in the system and when the system achieves the thermodynamic balance, the entropy reaches maximum. Therefore, the direction, where the entropy decreases is called, as the direction where the system evolves. That is to say the decrease of the entropy, the difference of the entropy and the maximum entropy can be taken as the measurement of the risk degree. From the viewpoint of the relationship of the optimum and the non-optimum, there exist criteria of capacity and function. For example, the sub-optimum degree can represent the risk within the system as well as the relationship between the optimum and non-optimum. Therefore, the sub-optimum degree can be used as a characteristic reference of the evolution of the risk systems. Except for the above two criteria of the basic risk analysis, different risk evaluation criteria can be chosen depending on the different natures of systems.

Assessment Methods of Network Security

Thresholds Analysis and Minimum-risk Index. The uncertainty decision arises during balancing that optimum and non-optimum attributes. Thus, if an attribute has optimum and non-optimum factors at same time, it is called sub-optimum factor. In traditional optimization theory, the standards of optimum factor are expressed by mathematical models. Although theoretic researches and its applications have been deep developed, it is still difficult to solve the realistic decision problems. The primary cause is uncertainty of optimum attribute and the existence of non-optimum ones. The decision process is based on the comparison of optimum and non-optimum. We can give the following definition:

Definition 3.1 [3] Let $P=\{p_1,p_2,\cdots,p_n\}$ is a factors set of the objects set X , and the optimum degree of the factors p_i is $\mu_O(p_i)\in[0,1]$, the non-optimum degree of the factors p_i is $\mu_{\bar{O}}(p_i)\in[-1,0]$ $(p_i\in P(i=1,\cdots,n))$, then there be a coordinate-optimal (sub-optimum relationship) $R_{o\times\bar{o}}(p_i)\in[-1,1]$ based on optimum degree and non-optimum degree, and $R_{o\times\bar{o}}(p_i)$ be also called the risk feature index of p_i in X , without loss of generality, we have

$$I_R(p_i)=R_{o\times\bar{o}}(p_i)=\frac{1}{2}\{1-(\mu_O(p_i)+\mu_{\bar{O}}(p_i))\}.$$

The definition with nature comes to following:

(1) If $\mu_O(p_i)=1,\mu_{\bar{O}}(p_i)=0$, then $R_{o\times\bar{o}}(p_i)=0$ that is to say, the p_i is the factors of complete optimum (or complete certainty) ;

(2) If $\mu_O(p_i)=0\ \mu_{\bar{O}}(p_i)=-1$, then $R_{o\times\bar{o}}(p_i)=1$, that is to say, the p_i is the factors of complete non-optimum, thus, $R_{o\times\bar{o}}(p_i)=1$ is also called the complete risk;

(3) If $-1<\mu_O(p_i)+\mu_{\bar{O}}(p_i)<1$, then the p_i is the uncertainty factors with different optimum degree and non-optimum degree ;

(4) If $\mu_O(x)=\mu_{\bar{O}}(x)$, then the X with basic uncertainty.

In the actual analysis, under certain optimum degree of aims and results, the premise is to find out the correspondent non-optimum degree. Thus sub-optimum relation $R_{o\times\bar{o}}(p_i)$ is decided by differences the optimum degree and non-optimum and if the results of decisions fall in this trusted classification, we can call them trusted $R_{o\times\bar{o}}(p_i)$, which decide the optimum degree and the non-optimum of the system. For example, in the strategic analyses of a system, we need to go through aim-cause and result-choice procedures. The conventional methods of theoretical researchers are to build up choice thresholds, obtain analysis results through thresholds index and the aim of trusted sub-optimum analysis is to build up its quantitative express methods.

Definition 3.2 [4] Let λ is an index set of optimum degree in R_m , and $\lambda=\{\lambda_1,\cdots,\lambda_L\}$, then

$$\mu_O^{\lambda_j}(p_i)=\{\mu_O(p_i)\geq\lambda_j:\lambda_j\in\lambda>0,p_i\in P,\}$$

is called λ -optimum if there is a minimum limitation.

Definition 3.3 Let η is an index set of non-optimum degree in R_m , and $\eta=\{\eta_1,\cdots,\eta_K\}$, then

$$\mu_{\bar{O}}^{\eta_j}(p_i)=\{\left|\mu_{\bar{O}}(p_i)\right|\leq\eta_j:\eta_j\in\eta>0,p_i\in P\}$$

is called η -non-optimum if there is a maximum limitation.

The sub-optimum relationship $R_{o\times\bar{o}}(p_i)$ observes a lower and upper-bound for threshold analysis. The thresholds λ and η provide the value for inclusion into the optimum, non-optimum, and boundary regions. Thus, a method of reducing the boundary region materializes from the modification of the sub-optimum analysis. Utilizing game theory to analyze the relationships between optimum and non-optimum, and the modification of optimum and non-optimum degree, we can provide the decision-maker with a means for changing their uncertainty.

Definition 3.4 Let $P=\{p_1,p_2,\cdots,p_n\}$ is a factors set of the objects sets X , effect function $\mu_O(p_i)$, $\mu_{\bar{O}}(p_i)$ of optimum and non-optimum is homeomorphism mapping in X for any $p_i \in P$ (decision making), and there are maximum optimum degree and minimum non-optimum degree to $\mu_O(x)$ and $|\mu_{\bar{O}}(x)|$ in X , then we can give the following model of the minimum-risk index

$$I_R(p_i)=\frac{1}{2}\{1-(\max\{\mu_O^{\lambda_j}(p_i)\}+\min\{\mu_{\bar{O}}^{\eta_j}(p_i)\})\}.$$

This minimum-risk index gives us a foundation in which to classify objects into approximation regions. They give us the ability to not only collect decision rules from optimum attribute and non-optimum frequent in many sub-optimum set applications, but also the calculated risk that is involved when discovering (or acting upon) those index.

Framework of Network Risk System. A network system always functions within an environment of uncertainty to achieve its objectives. The uncertainty prevailing in the environment has the chance of something happening, and that happening may be optimum system or non-optimum system. In this situation, risk can be viewed as happening of something in non-optimum system, which has negative impact upon the objective of a system.

Every network risk systems (NRS) exist in a non-optimum system. Due to the needs of the NRS, certain conducts and functions of the NRS come into being, which are confirmed by the non-optimum system? The real actions of the system tell its non-optimum characteristics. Generally speaking, these non-optimum characteristics are included in the non-optimum system, but it is not always the case. If the system has developed a great deal on its former basis or the actual actions of the system differentiate a great deal from the past, most risk factors of the actual system are then not embodied in the non-optimum characteristics system and still have things to do with the characteristics [5].

Since the NRS is rather complex, it takes on certain unclear factor under any condition. The unclear attributes are unknown things possessed by the system, which are decided by the complexity of the system in numerical value.

The key to analyze and research non-optimum systems lies in how to build up NRS. First of all, finding out the non-optimum factors of the past is the prerequisite. In the different stages of the past, the size of the non-optimum factors might be different, yet non-optimum factors is not at all losses of network system. Therefore, in the non-optimum analysis, it is important to find out the non-optimum factors that caused the changes of the network system’s actions, which possess a stable region. Thus, the risk system are a comparison of these non-optimum factors and systematic losses [6-10].

Conclusions

The formation of non-optimum factors serves as the basis for existence of NRS in uncertainty. Besides, the various characteristics and functions of the NRS models can be measured from the sub-optimum system. By summing the practice, this paper has also come at non-optimum assessment principle of the NRS, established the conception models of risk system and establishes the risk management models based on the non-optimum category of the NRS. At the same time, it also puts forward the non-optimum measurement of the risk system along with non-optimum tracing and trusted management of the NRS. Based on the non-optimum assessment of the NRS, it puts out the academic idea of extension optimum. Meanwhile, it discusses about the general framework of sub-optimum. Finally, according to the previous practice of optimization, kind of method has been developed to approach the risk system from non-optimum systems.

The key issues of network security are effective recognition and evaluation for non-optimum of the system. Depending on all above studies, we can identify security attributes of network systems by using non-optimum assessment methods of systems. Thereby we can control the security of network system. Because there are various uncertainty attributes of information security. For example, the random of non-optimum occurrence, the fuzzy of behaviors judgments, the unascertained of security attributes. Due to the limit of space, the detailed algorithm and computer program, which is about recognition and evaluation system, will be introduced in another paper.

From the non-optimum assessment, it can be concluded that people need the controllable order of the network system, and non-optimum can also be non-risk. From the risk reference system, the transit of the system from risk into non-risk as well as the requisites of the transit can be estimated. The Self-organization of NRS based on non-optimum assessment will be widely used in the decision sciences. It can often transform people’s experiences into scientific means and might set up reference models with behavior attributes in the control network system. This kind of model can marry the experiences and the theories, and can make actual judges to the running path of the risk management.

Acknowledgments

The authors are grateful for the support given by National Natural Science Foundation of China (Grant No. 61272170). We also thank reviewers for insightful and helpful suggestions.

References

[1] Zengtang Qu, Ping He, Method of Non-optimum Analysis on Risk Control System, Journal of Software, 2009, Vol.4, No. 4, 374-381.

[2] Libo Hou, Ping He. Approach of Non-optimum Analysis on Information Systems Security, IEEE Computer Society, IITA International Conference on Control, Automation and Systems Engineering, 2009, 225-228.

[3] He Ping, The Method of Non-optimum Analysis on Risk Management System In: Bartel Van de Walle, ed, proc. of the Int’l conf. 2007, ISCRAM, 604-609.

[4] He Ping, Qu Zengtang, Theories and Methods of Sub-Optimum Based on Non-optimum Analysis, ICIC Express Letters, An International Journal of Research and Surveys. 2011, Vol.4, No.2, 441-446.

[5] Tao Weidong, He Ping, Measurement of Network Security Based on Sub-optimum Degree, ICTM 2009, 457-460.

[6] Qu Zengtang, He Ping, Self-organizing of Network Security System Based on Non-optimum Analysis, 2010, 389-393.

[7] He Ping, Qu Zengtang, Comparison Computing Based on Sub-optimum Analysis: A Guide System of Network Security, Journal of Networks, 2009, Vol.4, No.8, 779-786.

[8] Teng Ping, He Ping, Characteristics of Network Non-optimum and Extensionality Security Mode, Third International Symposium on Intelligent Information Technology and Security Informatics, IEEE Computer Society,2010,439-443.

[9] Qu Zengtang, He Ping, Self-organization Theory and Surveillance of Network Anomalous Behaviors. The 2nd IEEE International Conference on Advanced Computer Control, 2010, 466-469.

[10] He Ping, Characteristics Analysis Of Network Non-Optimum Based On Self-Organization Theory, Global Journal of Computer Science and Technology, 2010, Vol.10, No.9, 67-72.