Risk Assessment of Network Security Based on Non-Optimum Characteristics Analysis

Ping He
Liaoning Police Academy
No.260, Yingping Road, Dalian, China

***Abstract*—This paper discusses in detail the theory of non-optimum analysis on network systems. It points out that the main problem of exploring indefinite networks' optimum lies in the lack of non-optimum analysis on the network system. The paper establishes the syndrome and empirical analysis based on the non-optimum category of the network security. At the same time, it also puts forward the non-optimum measurement of the network security along with non-optimum tracing and self-organization of the network systems. The formation of non-optimum network serves as the basis for existence of optimum network. Besides, the level of network security can be measured from the non-optimum characteristics analysis of network systems. By summing the practice, this paper has also come at the minimum non-optimum principle of the network security optimization, established the relationship between risk and non-optimum, and put forward evaluation method about trust degree of network security. Finally, according to the previous practice of network security risk management, a kind of network security optimization has been developed to approach the relationship of non-optimum and risk.**

Keywords—network security; non-optimum analysis; risk assessment; maximum and minimum limitation; ARS

I. INTRODUCTION

Network security, as a technology with the fastest rate of development and application in all branches of business, requires adequate protection to provide high security. The aim of the safety analysis applied on an information system is to identify and evaluate threats, vulnerabilities and safety characteristics. To cope up the mode of the network security management in the research and application field of computer science is still a challenge. Many literatures [1-4] research shows that the objective of network security management is optimized for network security. In fact, Optimization involves Operations Research techniques that have been used for years in designing networks, transportation system, and manufacturing systems also can be applied to optimizing network security. The objective of this problem is to minimize the Tost Cost of Ownership is the sum of capital and operating over the life of the network security assets [1].

One of motives of traditional optimization theory is to express mankind seek perfection of things. Practice has showed that people could not have an accurate judgment for the perfection. The previous system analysis committed that it is impossible to realize optimum under a limited condition of time and resources. At the same time, behind the optimum, there is definitely a series of hypotheses, middle-way decisions, and predigesting of data. Under most conditions, the hypotheses of optimum do not exist. Although people have generalized this method to many fields, the results obtained can be only temporary, and sometimes cannot achieve the final goals [5]. Thus limitations of traditional optimization theory are to be reflected.

However due to the complexity of network's practice, 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.

The objective of this paper is to analyze the self-organization characteristic on the network system and to discuss a method for network security analysis based on measurement of non-optimum characteristics.

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 system like characteristics of non-optimum, analysis on technology acceptance model. The third section RAS architecture studies based on non-optimum analysis. Finally, conclusion puts forward the discoveries of this research and future research direction.

II. THEORY AND METHODS

A. A New System Self-organization Theory

In the research of the self-organization theory of systems, the transmission of order and non-order is a core question. The Theory of Dissipation Structure (I. Prigogine, 1977), Synergetic Theory (H. Haken, 1979) and Chaos Theory contribute a great deal to it. According to the theory of Dissipation Structure, as long as the system is open, the non-equilibrium state may become the source of ordered system. So non-optimum is the source of non-ordered system. Only when the system goes out of the non-optimum category, can it come into the ordered stage, where we are to seek the optimization.

In fact, their individual theories include non-optimum theory of the system [6]. Because the major character of the self-organization of the system is to perfect the running of the system, develop its goals, they have to experience from non-optimum to optimum, and from optimum to non-optimum. If the system is not featured with this non-optimum, it doesn't need self-organization either. Analysis shows that systems always stay on the transmission of optimum and non-optimum, and the aim of self-organization is to bring the system from the non-optimum to the optimum

System non-optimum analysis is one of the youngest branches of information science; it is not ten year s old. The date of its birth can, with certainty, be considered to be the appearance in 2003 of the by now classical work of He Ping [6]. In the following years, the research of systems' non-optimum has developed very fast, both in theory and in practice, which involves non-optimum recognition of systems, evaluation of the optimum and non-optimum solutions, the non-optimum measurement of systems, the non-optimum differentiation and instruction of systems in the engineering areas. In reality, every system belongs to the non-optimum category. It meets the recognition and realization of mankind to analyze the causes of non-optimum system and the ways to reach optimum from the viewpoint of non-optimum category. This way of thinking is abbreviated as non-optimum tracing theory, and the theory of researching and tracing non-optimum is called non-optimum analysis theory of system.

Network security systems (NSS), a synthetic product of computer science and communication technology, came into being in the 1980's. It abstracts a security system of network into a model and searches for the most optical solution systematically under restrictions. However due to the complexity of network, there are numbers of unknown and uncertain factors, longitudinal and transverse relationship of networks, people's networks behavior. Especially as the network heads to the orderly dynamic condition, some of the hidden troubles are not exposed, the achieved modes of the network security are in unstable states. This implies that the recognition and practice of network security is featured by the exploration and pursuit not only in known security mode, but also, under many conditions, in many unknown security mode. That is to say when network system are faced with urgent problems, they need not only to find out the trust mode or realize the most trust aim, but also, more importantly, to get rid of the vicious influences of non-trust accidents effectively as well as recognition the non-trust factors of the network system.

The groundwork of the security analysis theory of the network system is the systematic self-organization doctrine. For any network systems, whether it has entered the optimum category or gone out of non-optimum category are judged through self-organization theory. Because a network has to go through three attributes: dynamic, uncertainty and invented, it is characterized by the alternating occurrence of trust, non-optimum, optimum, and so on. In order to hold the network security in the optimum category under certain degree and stage, we have to recognize and control the non-optimum factors of the network through self-organization function. As we know, the self-organization system is not only dynamic, but also evaluative. In order to measure the degree of the evolution of the system's self-organization, the criteria of evolution have to be set up (self-organization criteria). Different schools have different choice of the criteria and different opinions have to be applied in different systems. Generally speaking, from the viewpoint of the inner structural organization of the network system, network entropy (NE) and relevant parameters can be used as criteria, e.g. entity of the NE, upper-entity of the NE, and negative NE. As is explained in the statistics of entropies, the value of the network entropy proves how much chaos there are in the network system and when the network system achieves the thermodynamic balance, the entropy reaches maximum. Therefore, the direction, where the entropy decreases is called, as the direction where the network security optimization. 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 organization (the measurement of the trust network). From the viewpoint of the relationship of the network and the outside, there exist criteria of capacity and function. For example, the order references of the network system can represent the organization within the network as well as the relationship between the network and its outside. Therefore, the order reference can be used as a characteristic reference of the evolution of the self-organizing system. Except for the above two criteria of the basic self-organization, different self-organization criteria can be chosen depending on the different natures of network action systems [7].

B. The Relationship of Risk and Non-optimum

The purpose of any risk analysis is providing decision-makers with the best possible information about the probability of loss. As a result, it is important that decision-makers accept the risk analysis method used, and that information resulting from the analysis should be in a useful form.

A 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.

Risk universe is the overall non-optimum environment of system. The future is uncertain, therefore the future system is non-optimum, that is, and risk is prevailing everywhere. Especially, in the context of system, we can sort out some items or the risk universe based on empirical characteristics of non-optimum system, which includes the following:

- Functioning risk of system. This type of risk arises due to functioning of system. In business system, the non-optimum impact of unwise pricing and distribution policy of product (where unwise pricing and distribution are two non-optimum factors) on the overall revenue of the business system can be cited as an example of the risk.
- In the analysis of the business environment risks, three are the risks imposed by market scenario. The loss of market share due to introduction of new competitive forces and the functioning of illegal forces in market are all non-optimum factors of business environment risk.

- Risks arising out of the structure of the management system include non-optimum factors in management decision making, for example, delay in implementation of projects, hierarchy ego, wrong placement of personnel etc.

Every risk assessment systems (RAS) exist in a non-optimum system. Due to the needs of the RAS, certain conducts and functions of the RAS 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 (See figure1).

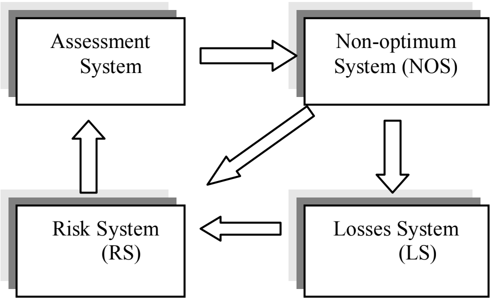

Fig. 1. Relationship of risk and non-optimum

Since the RAS is rather complex, it takes on certain unclear attributes 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.

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 system. Therefore, in the non-optimum analysis, it is important to find out the non-optimum factors that caused the changes of the system's actions, which possess a stable region. Thus, the risk system is a comparison of these non-optimum factors and systematic losses [8, 9].

III. Non-Optimum Analysis Of Nss

A. Basic Structure of Networks Security Non-optimum Analysis

In fact, every networks system exists in a non-optimum category. The future security of societies that depend increasingly on networks is contingent upon how our complex human and technical systems evolve. New network technologies including the Internet favor fragmentation into many loosely connected open and closed communities governed by many different principles. As the reach of today's networks has become global, they have become the focus of arguments over the values that should govern their development.

A key issue is the relationship between trust and non-optimum. Some of the factors non-optimum the evolution of networks and the feasibility of various non-optimum prevention measures are considered in this note. The development of networks, or 'cyberspace' as it is sometimes called, raises issues that are fundamental to individual and collective human safety and security. Analysis of the potential non-optimums to human safety and security in a pervasive network environment is complicated by uncertainty about how people will perceive its associated non-optimums, whether or not they perceive it as trustworthy, and whether they behave as if it is trustworthy.

According to the non-optimum analysis of the system (He Ping, 2003), the important thing in the management of network system as a new effort is not a problem of optimizing. Rather, it is one of eliminating threaten and keeping away risk and detours as possible.

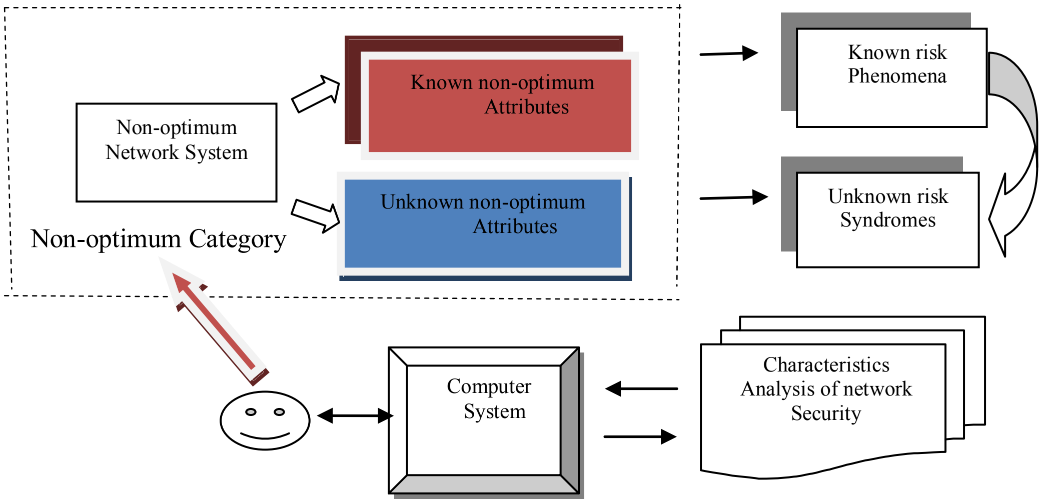
Non-optimum Network System
Non-optimum Category
Known non-optimum Attributes
Unknown non-optimum Attributes
Known risk Phenomena
Unknown risk Syndromes
Computer System
Characteristics Analysis of network Security

Fig. 2. Basic structure of networks security analysis based on non-optimum category

Even if some model of network management is considered optimum under the present circumstances, it is hard to be a stable one because it is in the midst of a dynamic process with quite a few hidden threats lurching and many horizontal or vertical relations between factors and their specific laws unknown. The so-called optimum model on network system is only at a system optimum state. So, if we try to set goals for the network system, make plans and take measures and advocate some optimum models simply following the optimum thinking methods out of blind subjective wish, we'll be actually putting the network system on an unreliable and unrealistic basis.

So we say that the non-optimum thinking and the methods of system non-optimum measurement with risk-avoiding as its basic aim are based on the non-optimum facts with its special ways of thinking, network gathering, analyzing and processing, and with the setting up of non-optimum network system, these methods seek to eliminate threaten and risk, thus providing a new way of scientifically summarizing past lessons and making them lamppost for the future. Figure 1 shows the basic structure of networks security analysis based on non-optimum category [10].

The security of the network system emerges and develops in non-optimum category. Every security attributes exists in a non-optimum category, and the non-optimum characteristics of the real actions tell its risk attributes of networks systems. Generally speaking, these risk phenomena are included in the non-optimum category of network system, but since the network system is rather complex, it takes on certain unclear attributes under any condition. The unclear attributes are unknown things possessed by the risk system of network security, which are decided by the complexity of the risk system in numerical value. For example, the risk analysis of the network system is much more complicated than the physical system. Therefore the unknown things of a network system are much more than a physical system. These unclear attributes cause the risk factors of the network system.

The concept of non-optimum is quite comprehensive in network security system. From the viewpoint of networks system' software, non-optimum means unfeasible and unreasonable; from the viewpoint of human' network behavior, it means non-trust; from the viewpoint of networks' capacity, it means ineffective and abnormal; from the viewpoint of networks' change, it means obstacles, disturbance and influence. There exists a serious of non-optimum problem from the entity of the network system to the change of the network system, which causes non-optimum category. As to every kind of networks security problems, there is the individual non-optimum category as well as the common non-optimum category. The so-called individual non-optimum category is decided by the characters of the networks relationship system, while the common non-optimum category is an objective entity of networks behavior. At present, most security analysis is designed manually based on past experience of their networks behavior. Since the number of possible optimization model very large for realistic applications of reasonable complexity, security analysis modeling designed manually may not work well when applied in new problem instances. Further, there is no systematic method to evaluate the effectiveness of security designed manually. For these reasons, a "cooperative" method for discovering the proper security decision for a particular application is very desirable. This leads to the development of our method for extensionality security model (ESM) of non-optimum category.

B. A Basic Theorem of Network Security Attributes Limitation

In network system, the factors of network security has optimum characteristics and optimum characteristics, as well as the evolution relationship between these characteristics, therefore, we can set up a state space of network security based on these characteristics and relationships [11].

Definition 3.1 Let $S = (X, O, \overline{O}, R(o,\bar{o}))$ be a state space of network security, where $X = \{x_1, \cdots, x_L\}$ be a set of the network security factor, $O = \{o_1, \cdots, o_n\}$ be a set of optimum characteristics of the network security factor, $\overline{O} = \{\bar{o}_1, \cdots, \bar{o}_m\}$ be a set of non-optimum characteristics of the network security factor, $R(o,\bar{o})$ be a relationship between O and $\overline{O}$, and $R(o,\bar{o}) = \{< o,\bar{o} >| o \in O \wedge \bar{o}\overline{O}\}$.

Definition 3.2 Let $\mu_O(x) = \{\mu_{O_1}(x), \cdots, \mu_{O_n}(x)\}$ is the optimum degree set of O, $(\mu_O(x) : X \to [0,1])$ and exist index set λ of optimum degree in $S = (O, \overline{O}, R(o,\bar{o}))$,

$\lambda = \{\lambda_1, \cdots, \lambda_l\}$, then $O_\lambda = \{\mu_O(x) \geq \lambda : \lambda > 0, x \in X\}$ is called λ -optimum if there is a minimum limitation.

Definition 3.3 Let $\mu_{\overline{O}}(x) = \{\mu_{\overline{O}_1}(x), \cdots, \mu_{\overline{O}_m}(x)\}$ is the non-optimum degree set of $\overline{O}$ ($\mu_{\overline{O}}(x) : X \to [-1,0]$), and exist index set η of non-optimum degree in $S = (O, \overline{O}, R(o,\bar{o}))$, $\eta = \{\eta_1, \cdots, \eta_l\}$, then $O_\eta = \{| \mu_{\overline{O}}(x) | \leq \eta : \eta > 0, x \in U\}$ or $O_\eta = \{| \mu_{\overline{O}}(x) | \geq -\eta : \eta > 0, x \in U\}$ is called η -non-optimum if there is a maximum limitation.

Theorem 3.1 (Attributes Limitation Theory) Let X is a closed set definition in metric space, effect function $\mu_O(x)$, $\mu_{\overline{O}}(x)$ of optimum and non-optimum is homeomorphism mapping in X for any $x \in X$ (network security factor), and there are maximum optimum degree and minimum non-optimum degree to $\mu_O(x)$ and $| \mu_{\overline{O}}(x) |$ in X , then we have $M(R)$ is called network security optimization with minimum risk model, that is

$$M(R) = \max\{< \mu_O(x), \min | \mu_{\overline{O}}(x) |>: \\ x \in \mu_O^{-1}(O_\lambda) \cap \mu_{\overline{O}}^{-1}(O_\eta) \subset X\}$$

Proof: Let $\mu_O(x)$ and $| \mu_{\overline{O}}(x) |$ have maximum and minimum respectively in X :

What is called the minimum risk analysis, in the can support range of risk analysis, is that if the maximum of corresponding to optimum characteristics values is chose from the minimum absolute value of non-optimum characteristics values. Meanwhile if it has a corresponding value in O_{λ}, there exists the minimum risk value in the corresponding decision-making project. According to the known condensations, it exist the minimum value to $|\mu_{\overline{O}}(x)|$ in X, and the minimum value is in $\overline{O}_{\eta}$, then we will prove that it existed the minimum risk analysis in O_{λ}

According to the literature [11], we have the minimum value of $|\mu_{\overline{O}}(x)|$, and $O_{\eta}=\{|\mu_{\overline{O}}(x)|\leq\eta:\eta>0,x\in U\}$

Suppose that it there exists a minimum value at least in $\overline{O}_{\eta}$. Let X be a closed set, according to the literature [11] Lemma1, $O=\mu_{o}(X),\overline{O}=\mu_{\overline{o}}(X)$ are all closed sets, we know $O_{\lambda},\overline{O}_{\eta}$ are closed sets of $O,\overline{O}$, respectively. $\mu^{-1}_{\overline{O}}(\overline{O}_{\eta})$, $\mu^{-1}_{O}(O_{\lambda})$, are closed sets from Lemma 2 of literature [11], so $\mu^{-1}_{\overline{O}}(\overline{O}_{\eta})\bigcap\mu^{-1}_{O}(O_{\lambda})$ is a closed set.

Suppose $x_0\in\mu^{-1}_{\overline{O}}(\overline{O}_{\eta})$ and $|\mu_{\overline{O}}(x)|$ is a minimum value in $\overline{O}_{\eta}$, the optimum attribute value $\mu_{O}(x_0)$ is existed in corresponding to the minimum $|\mu_{\overline{O}}(x)|$ from Definition 1. Assume that the minimum $|\mu_{\overline{O}}(x)|$ have a sequence $\{\mu_{\overline{O}}(x_n)\}$, $(n\in N)$, satisfy $\mu_{\overline{O}}(x_n)\to\mu_{\overline{O}}(x_0)$, $(n\to\infty)$; because $\mu^{-1}_{\overline{O}}$ is continuous, we obtain:

$$\mu^{-1}_{\overline{O}}(\mu_{O}(x_n))=x_n\to x_0=\mu^{-1}_{\overline{O}}(\mu_{\overline{O}}(x_0)).$$

As μ_{O} is continuous, and has a corresponding sequence $\{\mu_{O}(x_n)\}$ in O_{λ}, satisfying $\mu_{O}(x_n)\to\mu_{O}(x_0)$, because O_{λ} is a closed set, we have $\mu_{O}(x_0)\in O_{\lambda}$, at the same time O_{λ} is a homeomorphism mapping, we obtain, $x_0\in\mu^{-1}_{O}(O_{\lambda})$ hence, $x\in\mu^{-1}_{\overline{O}}(\overline{O}_{\eta})\bigcap\mu^{-1}_{O}(O_{\lambda})$, therefore, the minimum risk model of network security optimization is as follows:

$$M(R)=\max\{<\mu_{O}(x),\min|\mu_{\overline{O}}(x)|>:$$
$$x\in\mu^{-1}_{O}(O_{\lambda})\bigcap\mu^{-1}_{\overline{O}}(\overline{O}_{\eta})\subset X\}$$

C. Risk Assessment Method Based on $M(R)$

In fact, the $M(R)$ is a relationship between optimum attributes and non-optimum in network security, thus, this relationship can be represented by a table where each row $x_i\in X(i=1,2,\cdots,m)$ represents the factor of network security, for instance, physical factor, software factor, management factor as well as man-made factor and so on. Every column represents a relationship of optimum attributes and non-optimum for every network security factors (See table 1).

TABLE I. BASIC INFORMATION TABLE OF $M(R)$

	$<o_1,\overline{o}_1>$	$<o_2,\overline{o}_2>$	$\cdots$	$<o_n,\overline{o}_n>$
x_1	$<o_{11},\overline{o}_{11}>$	$<o_{12},\overline{o}_{12}>$	$\cdots$	$<o_{1n},\overline{o}_{1n}>$
x_2	$<o_{21},\overline{o}_{21}>$	$<o_{22},\overline{o}_{22}>$	$\cdots$	$<o_{2n},\overline{o}_{2n}>$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
x_m	$<o_{m1},\overline{o}_{m1}>$	$<o_{m2},\overline{o}_{m2}>$	$\cdots$	$<o_{mn},\overline{o}_{mn}>$

Thus, we can be set up a method of network security optimization, which is risk assessment method based on Attributes Limitation Theory (ALT). According to basic principle of network security management [11], we have

Can be determined acceptable level value of every $x_i\in X$ If $S(R)\to\min(Risk)$ [12].

$$S(R)=\min(\sum_{i}^{m}\sum_{j=1}^{n}<\mu_{jo}(x),\mu_{j\overline{o}}(x)>x_i)$$

Subject to
$$M(R)=\max\{<\mu_{O}(x),\min|\mu_{\overline{O}}(x)|>:$$
$$x\in\mu^{-1}_{O}(O_{\lambda})\bigcap\mu^{-1}_{\overline{O}}(\overline{O}_{\eta})\subset X\}$$

Every network security problems exists in a non-optimum category. Due to the needs of the network security optimization, certain conducts and functions of the networks come into being, which are confirmed by the non-optimum category? The real behavior of the network tells its security problem. Generally speaking, these security problems are included in the non-optimum category, but it is not always the case. If the network has developed a great deal on its former basis or the actual actions of the network differentiate a great deal from the past, most network security factors of the actual network are then not embodied in the non-optimum attribute and still have things to do with the attribute.

IV. THE DESIGN OF RISK ASSESSMENT SYSTEM (RAS)

Since the network security is rather complex, it takes on certain unclear attributes under any condition. The unclear attributes are unknown things possessed by the network system, which are decided by the complexity of the network in numerical value. The key to analyze and research network security systems lies in how to build up non-optimum sets of the network system.

First of all, finding out the non-optimum category of the past is the prerequisite. In the different stages of the past, the size of the non-optimum set might be different, yet non-optimum set is not at all non-optimum characteristics. Therefore, in the non-optimum set, it is important to find out the non-optimum characteristics that caused the changes of the network's actions, which possess a stable region. Thus, the security degree of the system is composed of these non-optimum characteristics.

So the non-optimum cases under condition of different network security are difference. Analyzing the general laws behind the system's movement, in the ARS, we can sum up three different types of non-optimum characteristics (or attributes):

1) RAS formed from the changed states of the networks' old self in the process of system movement. The former constraint conditions are no longer in keeping with the operating conditions of the new systems, because the systems now operate in the non-optimum.

2) RAS formed because of changes in constraint factors and new constraints can no longer satisfy the operation of the networks.

3) RAS formed from changes in both the network's own states and their constraints, operating in new conditions and thus making it impossible to determine their laws. Then the systems move in the non-optimum category.

There are three attributes (non-optimum characteristics) of the recognition to the risk information, experience, intuition and knowledge. The attribute of experience reflects the recognition to the characteristics of the crisis's behavior. The attribute of intuition reflects the fuzzy recognition to the characteristics of the risk's behavior. The attribute of knowledge reflects the definite recognition to the characteristics of the risk's behavior. Here the selection of the factors of the risk information is discussed from the experience attribute's viewpoint [13-15].

The experience of non-optimum recognition provides risk syndrome for the RAS. When the recognitions are different, the risk syndromes are different as well. The tracing to the non-optimum conditions of the past can propose a risk syndrome. In an artificial system, different people have different behaviors and stories, thus different experiences. Sometimes experiences are called a kind of ideology; but as the level of ideology is different, the ideology of the risk is also different. The degree of the risk is selected and decided by the ideology of the non-optimum, and the reasonability of the risk's ideology selection is also a meaningful question for discussion. For example, the increase of the recognition and control function of the non-optimum can reduce the risk degree, and the changes of the network's non-optimum characteristics can cause new risk factors of network security, which change with the non-optimum of the RAS. Thus the RAS structure of the actual network security is composed of non-optimum recognition, attributes classifiers, the evaluation of non-optimum, as well as non-optimum information analysis, the amount of non-optimum information changes and the potential non-optimum syndrome. Below is figure 3, with show the structure of RAS.

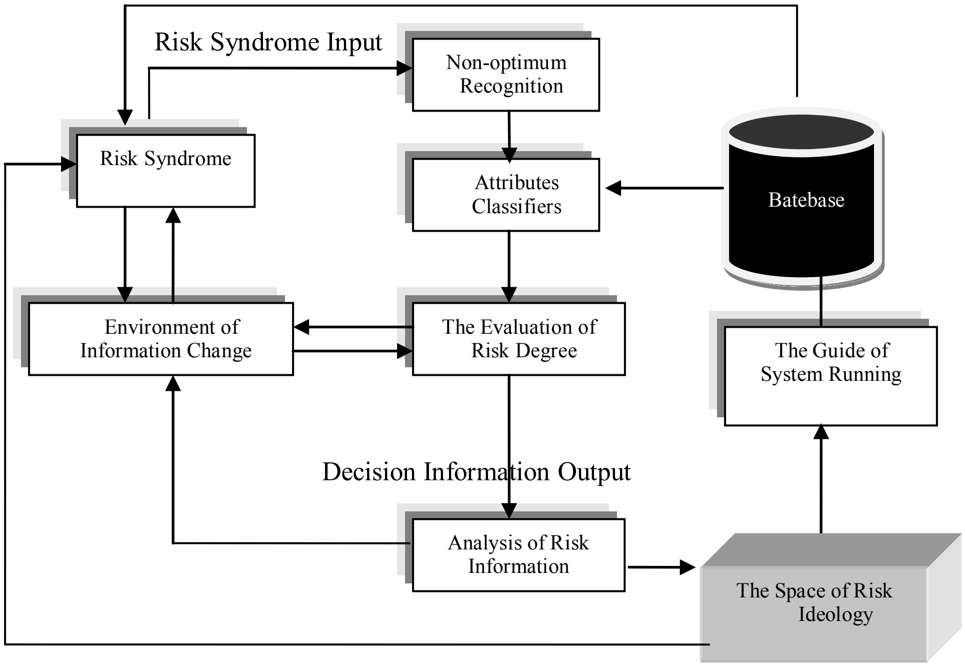
Risk Syndrome Input
Non-optimum Recognition
Risk Syndrome
Attributes Classifiers
Batebase
Environment of Information Change
The Evaluation of Risk Degree
The Guide of System Running
Decision Information Output
Analysis of Risk Information
The Space of Risk Ideology

Fig. 3. The structure of RAS

The main aim of Risk Assessment based on non-optimum analysis is to make a decision whether non-optimum characteristics are acceptable, and which measures would provide its acceptability. For every RAS using non-optimum analysis in its network management process it is significant to conduct the risk assessment. Numerous threats and vulnerabilities are presented and their identification, analysis, and evaluation enable evaluation of non-optimum characteristics impact, and proposing of suitable measures and controls for its mitigation on the acceptable level.

V. Conclusions

The key issues of network security management are effective recognition and evaluation for non-optimum characteristics of the network system. Depending on all above studies, we can identify security attributes of network systems by using non-optimum analysis 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 analysis, it can be concluded that people need the controllable order of the 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 Network Security System based on non-optimum analysis 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 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.

There is profound potential for putting the non-optimum thinking into use in Chinas network security management, and in other country's practice. Take the non-optimum guiding system for example; it can be employed in the network security management of the country's macro policies, financial system as well as decision analysis. To be sure, the establishment of this non-optimum guiding system with computer as its means with information processing techniques as its foundation is no easy task.

Acknowledgment

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] Prabhat Kumar Vishwakarma, Optimization and Analysing the Effectiveness of Security Hardening Measure Using Various Optimization Techniques as well as Network Measurement Model Giving Special Emphasis to Attack Tree Model, *International Journal of Network Security & Its Applications*, 2011, Vol.3, No.4, pp.100-109.

[2] Gupta, M., Rees, J., Chaturvedi, A., and Chi, J, Matching Information Security Vulnerabilities to Organizational Security Policies: A Genetic Algorithm Approach, 2006, *Decision Support Systems*, vol.41, no.3, pp. 592-603.

[3] Jeremy Cicurel, Information Security Process Optimization: Efficient Management of IT Security, Practice Director, CIO Advisory, 2012, www.kurtsalmon.com.

[4] He Ping, A Guiding System for Non-optimum Recognition, *Control and Decision,* 1989, vol.6, no.3, pp.18-21.

[5] He Ping, Theories and Methods of Non-optimum Analysis on systems, *Journal of China Engineering Science*, 2003, vol.5, no.7, pp.47-54.

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

[7] Božo Nikolić, Ljiljana Ružić-Dimitrijević, Risk Assessment of Information Technology Systems, *Informing Science and Information Technology,* 2009,Vol.6, pp.595-615.

[8] He Ping, The Method of Non-optimum Analysis on Risk Management System， In: Bartel Van de Walle, ed, proc. of the Int'l conf ISCRAM, 2008, pp. 604-609.

[9] Zengtang Qu, Method of Non-optimum Analysis on Risk Control System, JOURNAL OF SOFTWARE, 2009, Vol. 4, no. 4, pp.374-381.

[10] Ping He, Maximum Sub-Optimum Decision-Making Based on Non-Optimum Information Analysis, *Advanced Science Letters*, 2012, vol.5, no.1, pp.376-385.

[11] Arjen Lenstra, Tim Voss, Information Security Risk Assessment, Aggregation, and Mitigation, ACISP 2004, LNCS 3108, pp. 391–401.

[12] Emil BURTESCU, The Network's Data Security Risk Analysis, *Revista Informatica Economică,* 2008, Vol.48, No.4, pp. 51-53.

[13] Ping He, The Idea of Non-Optimum and It's Research Methods, 2011 International Conference on Agricultural and Natural Resources Engineering, *Advances in Biomedical Engineering*, 2011, Vol.3-5, 296-301.

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

[15] Ping He. The method of attribute analysis in non-optimum to optimum. Journal of Liaoning Normal University.2008, Vol.31, no.1, pp. 29-33. (Chinese)

Authors Profile

He Ping is a professor of the Department of Information at Liaoning Police Academy, P.R. China. He is currently Deputy Chairman of the Centre of Information Development at Management Science Academy of China. In 1986 He advance system non-optimum analysis and founded research institute. He has researched analysis of information system for more than 20 years. Since 1990 his work is optimization research on management information system. He has published more than 200 papers and ten books, and is editor of several scientific journals. In 1992 awards Prize for the Outstanding Contribution Recipients of Special Government Allowances P. R. China.