Detection and Prevention of Cyber Crime Based on Diamond Factor Neural Network

Jin Li, Ping He
Liaoning Police College, No.260, Yingping Road, Dalian China

ABSTRACT. The purpose of this paper is to provide a quantitative analysis method for cybercrime research, and also provide a new mathematical research method for network behavior analysis. Firstly, a novel factor space research method is established by using the "medium scale". On this basis, the concept of factor discovery of cybercrime behavior is proposed, and the corresponding cybercrime behavior analysis model is established, namely the criminal factor neural network. Secondly, the learning mechanism of network behavior neural network is discussed by using the factor discovery principle. At the same time, a network behavior learning algorithm based on diamond thinking is obtained. Finally, factor discovery thought, factor neural network learning system are applied to the research of cybercrime model analysis and prevention strategy to provide guiding decision support and problem solution for public security departments.

1. INTRODUCTION
Cybercrime diagnosis and measurement is the most basic means to fully understand and correctly understand the Internet by characterizing network behavior and crime patterns and quantifying various indicators. Network measurement is the most effective way to understand cybercrime and is the basis for controlling and guiding the Internet. In the measurement of cybercrime, the neural network method has been applied greatly and has an important position in data processing. Nowadays, the development of cybercrime measurement technology has taken user behavior analysis as an important field. Therefore, intelligent technology represented by various neural network methods will play an important role in crime behavior analysis and research [1].

Through the understanding of the public security department's reconnaissance and combating the basic situation of cybercrime, it is found that the most prominent problem at present is that there is no corresponding mathematical theory and lack of data analysis methods composed of criminal factors. First, the high incidence and concealment of cybercrime urgently requires pattern recognition of cybercrime. Most cybercrime cases are accidentally discovered or reported by victims, and only a very small number of criminal acts are actively detected. The current cybercrime search system used by the police, because there is no mathematical method for effective analysis of records after the search, the complexity of the information, it is difficult to reflect the spatial logic and relationship of cybercrime [2]. Secondly, cybercrime has the characteristics of criminals, criminal acts and spatial separation of crime results. The scope of crimes is not restricted by location. Especially for a large number of concurrent crimes, multi-location coordinated crimes, and overseas criminal behaviors, it is very difficult to track and prevent. However, cybercrime itself often has strong mathematical characteristics
of spatial and temporal distribution [3]. At present, most studies on network management and control follow the ideas in architecture design, rely too much on experience and intuition, and there is no effective way to formalize intuition and experience, without fully emphasizing the importance of theoretical analysis, lack of generalization and description of universal conclusions and laws.

Based on the analysis of the current situation of cybercrime mathematics research, this paper discusses the cybercrime factor discovery and behavior pattern evolution characteristics by using factor neural network, and proposes a factor neural network model based on diamond thinking, which is established from the perspective of micro and macro collaborative analysis. Cybercrime detection mode and prevention strategy.

2. CONSTRUCTION OF NETWORK BEHAVIOR FACTOR SPACE

2.1 Research Background
To fundamentally solve the mathematical description of network behavior, realize the recognizability of network behavior and the task of big data analysis, factor space theory is a relatively complete methodology and tool. Factor space theory was proposed by Professor Wang Peizhuang in 1982 [4]. For more than 30 years, factor space theory has formed a preliminary framework in terms of concept representation, reasoning decision, neural network, information fusion, etc., and has achieved initial achievements in the application field. Liu Zengliang [5] proposed a factor neural network for military science. The attribute theory proposed by Feng Jiali [6] is also complementary to the study of factor space theory. The current research depth of factor space theory is not inferior to the development of foreign intelligent mathematics. It can be considered that the factor space gives an operable method of conceptual connotation and extension transformation. This is a revolutionary work. It should be pointed out that the previous methods, including the decision tree algorithm and the rough set algorithm, do not achieve the purpose of bidirectional conversion. The fundamental purpose of the network behavior factor space construction is to provide a universal framework for network information description. At present, it provides the basis for formalization and data analysis for the construction of mathematical models for cybercrime research. Great engineering effectiveness for building a network of human-computer cognitive bodies. The main content of the study of network behavior factor space is:

2.1.1 Background relationship of network behavior
In the current network relational database table, a network information system is a set of sample points of the network factor space. Therefore, the network factor space is the platform that carries its overall. First, the study of the network behavior factor space should use Codd to establish the general relationship of the relational library, and further define a specific relationship that is configured to reflect the attributes of the factors, called the network behavior background relationship. It must be able to reflect all the cognitive information contained in the network behavior itself. Secondly, the factor space is used to process the network relational database, and the purpose is to construct a cybercrime big data algorithm.

2.1.2 Find the algorithm
First, concepts are extracted from a given cognitive unit network data sample. The main content to be studied is: how to cultivate the network behavior data sample to make it close to the real concept of the mother, how to distinguish the primary and secondary of the network behavior factor in the behavior concept extraction, and extract from the given network cognitive unit data sample Causal reasoning rules between unit network factors. The main question is how to approach the maternal full reasoning knowledge through the network behavior data sample. How to compress this knowledge without being buried by big data. How to ensure the efficiency and rationality of the operation. How to distinguish the primary and secondary of network behavior factors in the extraction of inference rules.
2.2 Cybercrime Causality Based on Factor Discovery

The factor discovery thought is not only limited to the space of cybercrime factors, but also has universal and theoretical significance for the study of the factors of many behavioral analysis. In fact, factor selection is a key issue in the study of social choice theory. Therefore, in the research on the factors of network behavior and criminal behavior, we must complete the following research contents:

- Discover the criminal factors based on microscopic perspectives. The formation process of individual criminal behavior factors is reflected in the network is the characteristics of local cybercrime. Including the conditional factors, process factors and target factors generated by network behavior.

- Discover the criminal factors based on macro perspectives. The formation process of the overall criminal behavior factor is reflected in the overall cybercrime behavior. It includes the conditional factors, process factors and target factors generated by the overall form of network behavior.

On the basis of the discovery of cybercrime factors, it is necessary to conduct network crime causal analysis. For the crime factor space, individual factors and network environment factors can be defined as two background sets, and the background relationship is established under the fuzzy “medium scale” measure. In the actual research, it is necessary to explain how to obtain reliable knowledge from incomplete cybercrime information, and to control the correctness and reliability of the conclusions obtained from the sample operation through the probability distribution of criminal factors. The breakthrough point of the research is to establish a sample theory based on factor space.

The sample uncertainty has randomness of sampling and the ambiguity of state description. Because intelligent data analysis focuses on inference decision making, this study is to control the sample in the uncertainty of reasoning is the goal, and its methodology is fundamentally different from mathematical statistics. The artificial intuition factor neural network based on experience and knowledge is used to modify the mathematical model of network behavior and crime, and the reasoning model of network behavior factor learning is obtained.

Through the collection and input of the intuition characteristics of crime factors and behavior attributes, each sub-factor subspace is formed. Then, the intuition concept space is established, and the credibility of crime factors and behaviors is learned through human-computer interaction. Based on the intuitive learning, establish a fuzzy neural network model. The specific research plan is: According to the intuitive learning algorithm proposed in the literature [7], the membership degree of each attribute of the network behavior factor is studied, and then the behavior parameters of the established cybercrime dynamic model are corrected. This research method can reflect the mutual fusion of data analysis and human perception, overcome the deficiencies of finite rigidity of mathematics in describing human behavior characteristics, and introduce the advantages of perceptual soft description. This is the characteristics of this paper. As shown in Figure. 1:
3. FACTOR NEURAL NETWORKS BASED ON DIAMOND THINKING

3.1 Factor state body

It is assumed that the network behavior factor space is composed of finite behavior factors, each behavior factor has different states (attributes), and each behavior attribute has different reliability. Then, the uncertainty state of a behavior factor space can be described according to the overall characteristics of the information formed by the factors, the set of factor states and the set of state reliability, and the overall feature of the information is called the state body of the behavior factor space. Without loss of generality, there are the following definitions:

Definition 1. Let $\Omega = \{ f(u), R(u, X(f)) \}$ be a factor space of behavioral system, where $U$ is an object set, $f(u)$ is the factors set of the object, $A = X(f)$ is the state set of the factor (attribute set), and there is a distribution $V(A)$ of the credibility of the factor state (called the confidence set), then, can describe the factor state information structure of a factor space by $f(u) , A , V(A)$, said the information structure is a factor state body (referred to as state body), used to represent. [8].

\[ B(A) = (f(u), A = X(f), V(A)) \]

Each behavioral system object in a factor space corresponds to a factor coordinate frame, and the characteristics of different objects in the factor space are different. In addition, the factors of the object also have different attributes. Therefore, it can be used to recognize the patterns and characteristics of the system in the condition of the attributes of the object in the factor space. The object-factor relation is shown in Table 1.
Factors determine the scope and nature of an object, thus form a different nature and scope of a system. Furthermore, the order relationship table of each factor can be generated by factor coordinate frame. For example, the demographic factors space, or population information system is constituted by population and the relationship between population and various factors. The design content of this population factor space has the following aspects:

### Table 1. Object-Factor Relation

| Factors | $f_1$ | $f_2$ | ... | $f_k$ |
|---------|-------|-------|-----|-------|
| Objects |       |       |     |       |
| $u_1$   | $r(u_1,f_1)$ | $r(u_1,f_2)$ | ... | $r(u_1,f_k)$ |
| $u_2$   | $r(u_2,f_1)$ | $r(u_2,f_2)$ | ... | $r(u_2,f_k)$ |
| ...     | ...   | ...   | ... | ...   |
| $u_n$   | $r(u_n,f_1)$ | $r(u_n,f_2)$ | ... | $r(u_n,f_k)$ |

The traditional factor neural network is the modeling idea of factors as neurons. If the neural network model is established from the perspective of the factor state body, it has great value for the spatial analysis of the factors of the behavioral system. Since a network behavior information can be regarded as a combination of a network behavior state body or a state body, it is called a network actor [9].

Definition 1 gives a possibility subspace using the state of the factor to explore the behavioral characteristics of the object. In fact, for a set of factors $\mathbf{f}(u)\equiv\{f_1(u), f_2(u), \ldots, f_n(u)\}$ of a behavior object, there is an information structure of the state body of the Z layer, that is

$$\mathbf{B}(B_{01}, B_{02}, \ldots, B_{0n}) \rightarrow \mathbf{B}(B_{11}, B_{12}, \ldots, B_{1n}) \rightarrow \mathbf{B}_Z.$$

Taking the network actor (behavior state body) as the neuron, the factor state neural network with the diamond-shaped thinking process as shown in Fig. 3 can be obtained, which is referred to as the diamond factor neural network.

### Figure 2. Criminal factor coordinate frame

#### 3.2 Factor neural network with diamond thinking

The traditional factor neural network is the modeling idea of factors as neurons. If the neural network model is established from the perspective of the factor state body, it has great value for the spatial analysis of the factors of the behavioral system. Since a network behavior information can be regarded as a combination of a network behavior state body or a state body, it is called a network actor [9].

Definition 1 gives a possibility subspace using the state of the factor to explore the behavioral characteristics of the object. In fact, for a set of factors $\mathbf{f}(u)\equiv\{f_1(u), f_2(u), \ldots, f_n(u)\}$ of a behavior object, there is an information structure of the state body of the Z layer, that is

$$\mathbf{B}(B_{01}, B_{02}, \ldots, B_{0n}) \rightarrow \mathbf{B}(B_{11}, B_{12}, \ldots, B_{1n}) \rightarrow \mathbf{B}_Z.$$
In this model, the transformation from the input behavior state body to the implicit behavior state body reflects the divergence process of the behavior state body, and the transformation from the implicit behavior state body to the input behavior state body reflects the convergence process of the diamond shape thinking. Such a three-layer forward BP neural network can effectively represent the entire process of diamond thinking.

In the factor neural network of the behavior system, a behavioral state body is expressed as a knowledge unit, which is divided into two parts: the factor state and the structure chain. The structure chain bridges the knowledge unit (behavior state body), which reflects the behavior. The divergence and correlation of state bodies, using these divergence and correlation can form an effective strategy for behavioral reasoning, and each structure chain reflects a strategy [10].

If the knowledge units are treated as data structures, then these structure chains are the connecting arcs between the data structures. These arcs provide an effective way for the divergence and convergence reasoning of diamond thinking. Therefore, in the neural network of the factor of the network behavior system of diamond thinking, we define the structure chain as the constraint relationship of the variables (attributes) between the knowledge units, which can reflect the correlation described by the correlation function between the behavior state bodies.

3.3 Diamond learning algorithm

3.3.1 Network behavior learning sample

a. Enter a set of behavioral state bodies $B_i$ ($i = 1, 2, ..., l$).

b. Generate a behavioral state set $B_j$ ($j = 1, 2, ..., r$) based on the behavioral state body.

c. Determine the value of the associated function $K_{ij}^{(1)} = \{B_i, B_j\}$ based on the data and initial conditions of the network behavior information system.

d. Delete $B_j$ with $K_{ij}^{(1)} < 0$ to get the divergence system $\{B_i\}$.

e. The output behavior state body $B_i$ is determined by $\{B_i\}$ according to a certain rule, and a learning sample $(B_{in}, L, B_{in}, B_{out})$ of the behavioral system neural network is obtained.

3.3.2 Learning algorithm

For the model shown in Figure 2, a BP-like learning algorithm can be used for training learning. The vector expressing the state body in the network is still recorded as $B$, and the total error of the $P$ samples is:

$$E = \frac{1}{P} \sum_{k=1}^{P} (B_{out}^{(k)} - B_{2}^{(k)})^2 / 2$$

Where $B_{out}^{(k)}$ and $B_{2}^{(k)}$ are the actual output and the expected output $Z$ of the kth sample, respectively. The functions of the hidden layer and the output layer node are:
\[ g(z) = \frac{1}{1 + e^{-z}} \cdot f(z) \]

For any sample, the \( r \)th iteration of the hidden layer output and the network output are:

\[
B_{ij} = g(\sum_{i=1}^{n} W_{ij}^1(r)B_{in} + b_j(r)), \quad B_{out} = \sum_{j=1}^{m} W_j^2(r)B_{ij}(r)
\]

Where \( W_{ij}^1(r) \) and \( W_j^2(r) \) are the weights between the input layer and the hidden layer, the hidden layer and the output layer node of the \( r \)th iteration, \( b_j(r) \) is the threshold of the hidden layer node of the \( r \)th iteration, and \( m \) is the number of hidden layer nodes. The correction formula for \( W_{ij}^1(r) \) and \( W_j^2(r) \) is:

\[
W_{ij}^1(r+1) = W_{ij}^1(r) + \eta \delta_j(r)B_{ij}(r), \quad j = 1, L, m
\]

\[
W_j^2(r+1) = W_j^2(r) + \eta \delta_j(r)B_{in}, \quad i = 1, L, t, j = 1, L, m
\]

where

\[
\delta_j(r) = B_j - B_{out}(r), \quad \delta_j(r) = B_j(r)(1 - B_j(r))\delta(r)\sum_{j=1}^{m} W_j^2(r+1), \eta \in (0, 1)
\]

For the learning rate, the hidden layer node threshold is calculated as:

\[
b_j(r+1) = b_j(r) + \eta \delta_j(r) + \beta(b_j(r) - b_j(r-1))
\]

where \( \beta \in (0,1) \) is the momentum factor. After the above learning, \( W_{ij}^1(r), W_j^2(r), \ b_j(r) \) can be stable for all samples, and the optimal is achieved according to the MSE criterion.

4. CYBERCRIME PREVENTION AND CONTROL BASED ON COORDINATION STRUCTURE

4.1 Establishment of cybercrime factor base

Firstly, it analyzes the differences between the characteristics of the cybercrime factor base and the existing cybercrime database. Secondly, it studies the basic algorithm of the cybercrime factor library. Thirdly, it studies the manifestation of cybercrime potential factors and feature extraction. Finally, it establishes the police. Use the network to prevent human-computer cognitive bodies. Human-computer cognitive body of Police cybercrime prevention and control consists of cybercrime cognitive units. The specific research content is: set each unit name, composed of people and libraries. People are responsible for building the library, using the library and the library. The library is the factor vine formed by the knowledge package. It is also necessary to study the partial order relationship between the cognitive parts. To have a set of cognitive units can be combined into a new cognitive unit function according to the factor vine theory [12].

4.2 Correlation Analysis of Cyber Crime Based on Factor Discovery

The factor discovery thought is not only limited to the space of cybercrime factors, but also has universal and theoretical significance for the study of the factors of many behavioral analysis. In fact, factor selection is a key issue in the study of social choice theory. Therefore, in the research on the factors of network behavior and criminal behavior, we must complete the following research contents [13]:
● Discover the criminal factors based on microscopic perspectives. The formation process of individual criminal behavior factors is reflected in the network is the characteristics of local cybercrime. Including the conditional factors, process factor.
● Discover the criminal factors based on macro perspectives. The formation process of the overall criminal behavior factor is reflected in the overall cybercrime behavior. It includes the conditional factors, process factors and target factors generated by the overall form of network behavior. Tors and target factors generated by network behavior. On the basis of the research on the discovery of cybercrime factors, the causal analysis of cybercrime should be carried out. For the crime factor space, individual factors and network environment factors can be defined as two background sets, and the background relationship is established under the fuzzy “medium scale” measure. In the specific research, it is necessary to fully reflect the factor discovery is the premise of the network crime association analysis, and the core of the factor discovery is the network crime background relationship.

In the actual research, it is necessary to explain how to obtain reliable knowledge from the incomplete cybercrime information body, and to control the correctness and reliability of the conclusions obtained from the cybercrime sample operation through the probability distribution of factor discovery. The breakthrough point of the research content is to propose a new sample theory based on the factor space as the parent. The sample uncertainty has the randomness of sampling and the ambiguity of state description, but since the intelligent data analysis focuses on the reasoning decision.

5. CONCLUSIONS
The foundation of the cybercrime prevention and control system for cybercrime factors. There are two aspects in the research of cybercrime analysis and prevention: First, the deterministic attribute space and the uncertain attribute space based on (factor, behavior) are established. The method of the previous research is used to discuss how to determine the certainty and uncertainty of cybercrime behavior. Secondly, based on the certain degree and uncertainty of cybercrime, a neural network model based on diamond thinking is constructed. Through the learning process of relevance, the detection and recognition of cybercrime behavior is carried out. The study of diamond-shaped neural networks provides the necessary experience and rules for the learning and improvement of traditional network behavior models. In the research process, through the training and solving of the factor body, the rigidity of the network behavior dynamics model is continuously improved, and the closeness of the mathematical model and the actual behavior is enhanced to achieve a certain degree of credibility.

REFERENCES
[1] A. Adas. Traffic models in broadband networks. Communications Magazine IEEE, 2010, vol.31, pp.82-89.
[2] D. Mitra, Q. Wang. A model-based study of the impact of managed services and the spawning of applications in broadband networks. International Telegraphic Congress, 2012.
[3] J. Mavodza. The impact of cloud computing on the future of academic library practices and services. New Library World 2013, vol.114, pp.132-141
[4] Wang P Z, Sugeno M. The factor fields and background structure for fuzzy subsets. Fuzzy Math, 1982, vol.2, pp.45-54.
[5] Liu Zhengliang, Liu Youcai, Research on Factor Neural Network Theory and Implementation Strategy. Beijing Normal University Press, 1992.
[6] Feng Jiali, The theory of nature in thinking and intelligent science. Atomic Energy Press, 1990.
[7] Ping He, Kaiqi Zou, Research of Crime Inversion Fuzzy Neural Network Based on Factor Space. 2016, vol. 10, pp.1943-1950.
[8] P. Holme, and M. E. J. Newman. Nonequilibrium phase transition in the coevolution of networks and opinions. Physical Review E, 2006, vol.74, pp.56-70.
[9] L. Zhang, and Y. Liu. Network Structures and User Behavior Analysis Based Hot Topic Detection for Internet Forum. Journal of Internet Technology, 2008, vol.9, pp.1-6.
[10] Effros M. Optimal modeling for complex system design. IEEE Signal Processing Magazine, 1998, vol.15, pp.51-73.

[11] He Ping. Characteristics Analysis of Network Non-Optimum Based On Self-Organization Theory. Global Journal of Computer Science and Technology, 2010, vol.10, pp.67-72.

[12] He Ping, Zou Kaiqi. Fuzzy Meso-Optimum Sets and Trusted Optimum Analysis. ICIC Express Letters, Part B: Application. 2015, vol.6, pp.2079-2086.

[13] He Ping. A Discriminant model of Network Anomaly Behavior Based on Fuzzy Temporal Inference. International Journal of Advanced Computer Science and Applications, 2012, vol.3, pp.46-52.