Defense Strategy of Network Security based on Dynamic Classification

Jinxia Wei[1], Ru Zhang[1,2], Jianyi Liu[1], Xinxin Niu[1],Yixian Yang[1]
[1] Information Security Center, National Engineering Laboratory for Disaster Backup and Recovery
Beijing University of Posts and Telecommunications
Beijing, 100876, China
[e-mail: 13930320234@163.com]
[2] Key Laboratory of Trustworthy Distributed Computing and Service
Beijing University of Posts and Telecommunications
Beijing, 100876, China
*Corresponding author: Wei Jinxia

Received July 17, 2015; revised September 16, 2015; accepted October 4, 2015; published December 31, 2015

Abstract

In this paper, due to the network security defense is mainly static defense, a dynamic classification network security defense strategy model is proposed by analyzing the security situation of complex computer network. According to the network security impact parameters, eight security elements and classification standard are obtained. At the same time, the dynamic classification algorithm based on fuzzy theory is also presented. The experimental analysis results show that the proposed model and algorithm are feasible and effective. The model is a good way to solve a safety problem that the static defense cannot cope with tactics and lack of dynamic change.

Keywords: Dynamic classification defense, Fuzzy theory, Membership function, Security element, Membership matrix

http://dx.doi.org/10.3837/tiis.2015.12.021 **ISSN : 1976-7277**

1. Introduction

With the development of information technology, Internet is becoming the key infrastructure of national information. Current Internet and computers are constantly under various attacks: hackers' intrusion, port scan, distributed denial-of-service (DDoS) [1], virus and worm infection, e-mail spam, etc. Many defense methods and systems have been proposed [2-4]. Most research has focused on stationary network operation with fixed configurations. However, attack detection system have to face the rapidly changing network condition and attack intensity [5,6]. A variety of applications based on web are increasingly common, the network security is related to the fundamental interests of the state and society. At the same time, network in many fields has been developed rapidly, but the network security has gradually been broken. Therefore the defense mechanism technology of network security is turning to mature, how to protect the safety of network is becoming more and more important. The traditional passive defense mechanism of network security technology, such as firewall, intrusion detection, loophole, is not enough to cope with protean network attacks [7-10]. The inherent limitations of these means and methods are obvious. On the other hand, if we can't deal with the network reasonably, the network would become paralyzed. In order to cope with dynamic network attack efficiently, many researchers turn defense measures from passive to active, and defense mechanism from static to dynamic [11-16]. An ideal defense system should make a protection for all weaknesses or aggressive behavior, but this kind of defense is obviously unreasonable for its cumulative cost. Hence, we should take into consideration the applicability of protected system [7]. In the literature [7], Jiang put forward a new active defense model of network system security assessment - network attack and defense game model, including that a defender dispose network security and active defense to the optimal price, and providing a powerful guarantee for active defense.

However, the defensive strategy doesn't provide a real-time protection, its dynamic is weak. In the current complexity environment of large-scale network security equipment distribution, heterogeneity [17-20], we may lead to strategy resources issued blindly, cause the waste of resources. So as to deal with the challenges of network security, VPN, IDS, anti-virus system, identity authentication [21], data encryption, security audit and other security protection and management system have been widely applied. In terms of security equipment and security mechanism, we propose a dynamic classification defense of network security, which provides correct and complete security policies for network security defense system. At the same time, the security strategies can be executed smoothly. Such we would solve the degradation problem of network performance for security deployment, and improve efficiency of security products. At the present stage, the idea of the classification for network security defense has not been commonly developed at home and abroad, therefore the method is a signal that represents the network security defense stepping into a new stage.

Comparing with the existing work, the main contributions of our paper have: (1) We have taken into consideration the effectiveness of the network security defense strategy. Basing on dynamic classification of network security defense, we have established a defense strategy model, and proposed the network security elements and their classification standard. At the same time, a detailed dynamic classification algorithm combined with fuzzy theory is presented. (2) We have solved the strategy generation and distribution in the form of interaction. When some kind of network security defense strategy in database is missing in the generation phase, the database would make the default feedback in time to resource management module. Then the resource management module would provide the missing defense strategy for the database. (3)The system is able to generate and issue strategy to the strategy executive subsystem. When some executive equipment lacks security strategy parameters (without security strategy parameters, executive equipment would can't adopt the security strategy), the resource management module receives feedback from the strategy executive system, the resource of strategy parameters may be distributed to the executive equipment by resource management module. The main task of resource management module is to accept feedback, and to provide the information what other modules need.

2. Related Work

In this section, we simply introduce some basic concepts and functional expressions of the fuzzy theory which will be used to construct the dynamic classification algorithm. The level of each security element is divided by using a numerical interval, which is equivalent of the Fuzzy set in Fuzzy theory.

2.1 The basic definitions

Definition2.1.Fuzzy set [22] **:**Suppose that U is a domain(non-empty), the "Fuzzy set" A on the area of U refers to given a random $x \in U$, such that x belongs to A with degree of μ ($\mu \in [0,1]$), rather than $x \in A$ or $x \notin A$.

Definition2.2.Membership function and Membership degree [22]: Suppose that U is a domain, μ : $U \to [0,1]$, μ is called as a membership function of U, put all membership functions of U together and denote as SH(U). Given all Fuzzy sets of U as F(U), the relationship between SH(U) and F(U) is one to one. That is to say, for any $\mu \in$ SH(U), there exists unique Fuzzy set $\underset{\sim}{A} \in$ F（U）of U corresponding to μ. Denote μ as $\mu_{\underset{\sim}{A}}$, for any $x \in U$, then $\mu_{\underset{\sim}{A}}(x)$ is called as membership degree of x to $\underset{\sim}{A}$.

2.2 The expression of membership function

According to the definition of membership degree, a Fuzzy set correspond with a membership function. Similar to the distribution function in probability theory, if the domain is real number set, a parameter function on $\left[0,1\right]$, which is applied by all kinds of problems, called Fuzzy distribution function (that is, the membership functions). There are several commonly used membership function as follows [22]: 1. Normal distribution; 2. Half a trapezoidal distribution and trapezoidal distribution; 3. K parabolic distribution; 4. Cauchy distribution; 5. S distribution. Based on our paper data, we choose the half trapezoid distribution, the second type membership functions are introduced in details, and specific expressions are given by:

(1) the right trapezoid distribution

$$\mu_A(x;a,b) = \begin{cases} 1\,, & x \le a \\ \dfrac{b-x}{b-a}, & a < x \le b \\ 0, & b < x \end{cases}$$

where a, b are parameters, $b > a$ (see **Fig. 1**).

(2) The left trapezoid distribution
(3)

$$\mu_A(x; a,b) = \begin{cases} 0\ , & x \le a \\ \dfrac{x-a}{b-a}, & a < x \le b \\ 1, & b < x \end{cases}$$

where a, b are parameters, $b > a$ (see **Fig. 2**).

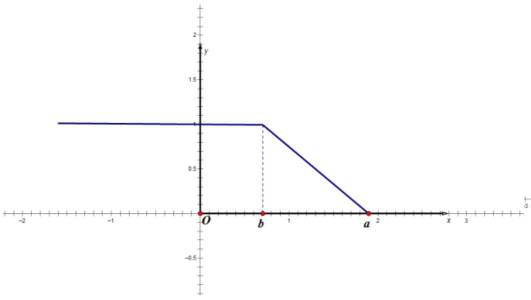

Fig. 1. right trapezoid distribution

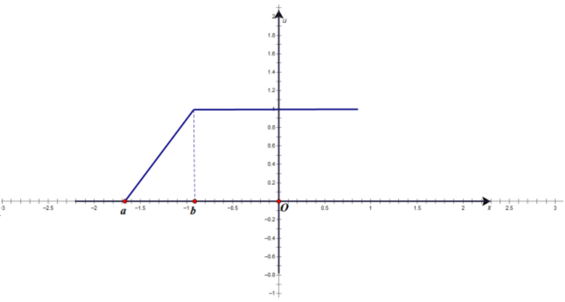

Fig. 2. left trapezoid distribution

3. The principle of the dynamic classification defense strategy of network security

In this work, we mainly introduce dynamic classification strategy system of network security. Based on the data of sensing from requirement system, strategy management system makes decision for network requirements by using safe grade matching and dynamic classification algorithm, and generate corresponding security strategy according to the decision content. Since some of safety equipment can't recognize strategy language, we establish a translation part, which converts strategy language appropriately by using the results from feedback of safety equipment. We should ensure that strategy is adopted by the corresponding equipment, send the ultimate security strategy to the strategy execution system. Finally, strategy execution system will be activated in turn according to the requirements. In order to understand the working principle of the strategy system, dynamic classification defense of network security system model is shown in **Fig. 3**.

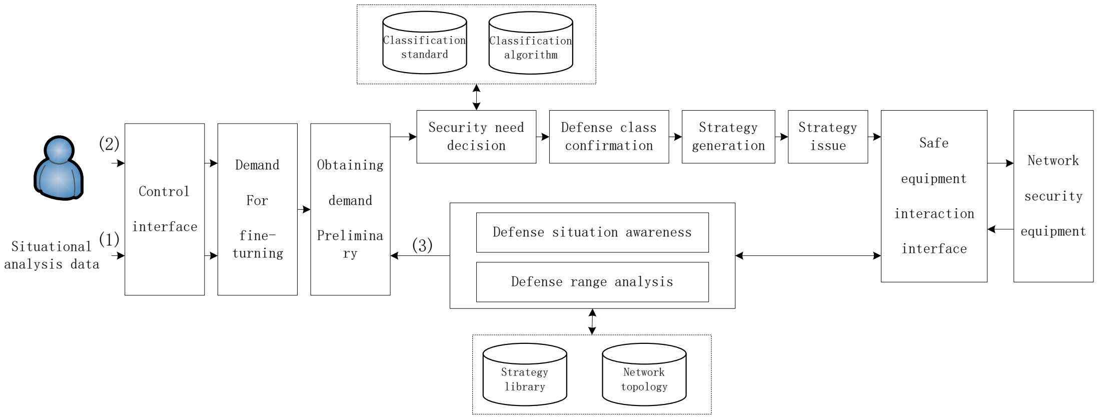

Fig. 3. Dynamic classification defense of network security system model

The input of system has three parts: (1) Situational analysis data for network monitoring information (by monitoring man); (2) User input data; (3) Current awareness of defense situation. When there are different security levels about input data(three parts input different data levels), we will select the highest security level data as defense needs, for we need ensure the network in a safety condition. The system executes defense situation awareness and defense range analysis using the implementation results of equipment, strategy library and network topology. Therefore, the data of implementation results of equipment, strategy library and network topology feed the defense situation awareness block.

The three parts implement fine-turning operation through control interface, and obtain the preliminary demand. Based on this preliminary demand, we apply classification algorithm and standard to generate security need decision. After generating the security need decision, we need to complete defense class confirmation with the network monitoring man and the user. When they agree with this securtiy need decision, defense strategy is generated. Then the strategy is issued to network security equipment through safe equipment interaction interface. In order to monitor equipment for strategy implementation, the system automatically executes defense situation awareness and defense range analysis according to strategy library and network topology, and gets current awareness of defense. He sends current awareness of defense to the preliminary demand module, and cooperates with the user and the network monitoring man to obtain the final preliminary demand. Then the three parts implement fine-turning operation again and repeat the above strategy generation and distributed operation.

We calculate the level of safety demand through dynamic network security classification algorithm. Finally, if the user agrees with performing the level strategy, the system begins to generate strategy. By establishing a dynamic classification strategy system model, we implement the dynamic strategy decisions, format conversion, generation mechanism, provide a guarantee for the security operation of the network in real time.

3.1 Dynamic classification defense strategy of network security

The system of dynamic classification defense strategy involves strategy decision unit, strategy generation unit, strategy issue unit, the resource management unit, equipment control unit and a variety of data base. Here, the strategy decision unit plays the most important role in strategy management sub system. The whole system is shown in **Fig. 4**.

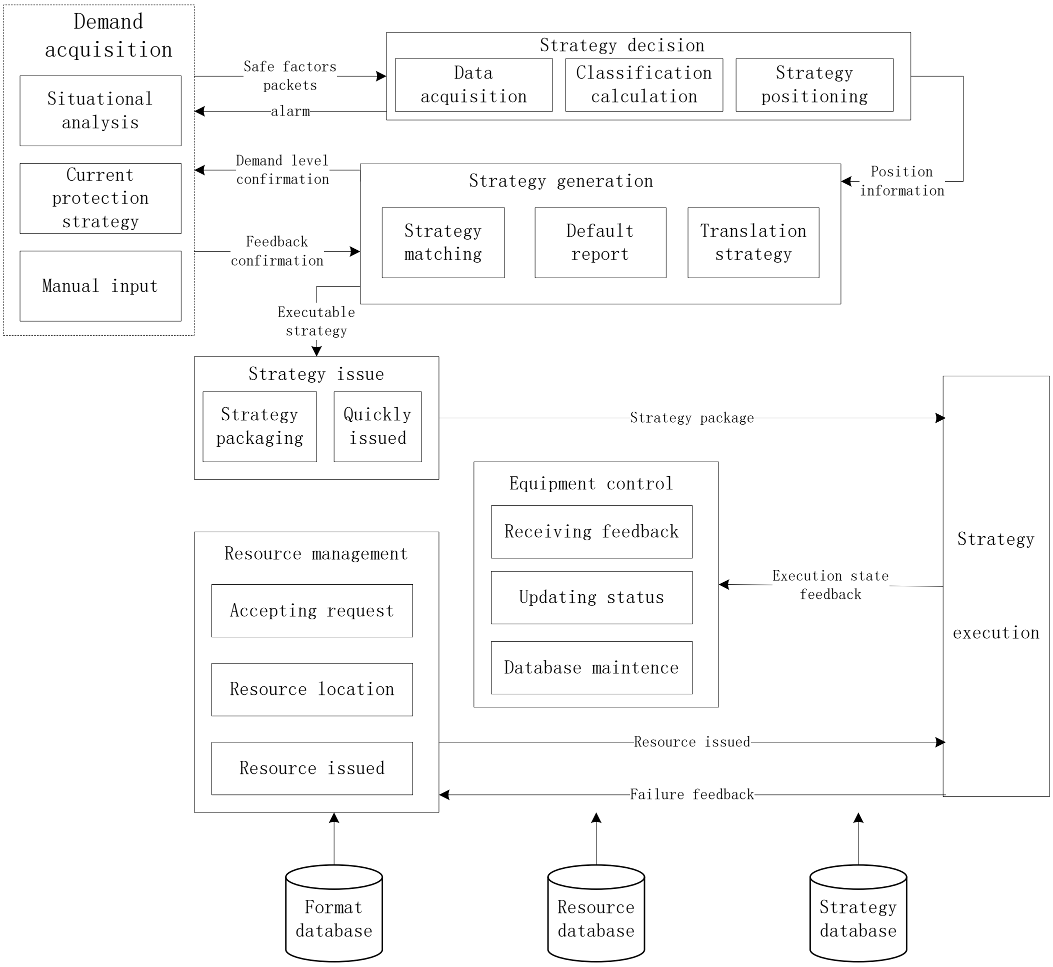

Fig. 4. Dynamic defense of network security system

As shown in **Fig. 4**, the system consists of eight modules: demand acquisition, strategy decision, strategy generation, strategy issue, equipment control, resource management, strategy execution and three databases. Demand acquisition module is a separate subsystem, it is not emphasis for our system. Therefore, we mainly introduce the function of other modules in details:

A) Strategy decision includes data acquisition unit, classification calculation unit and strategy position unit. After acquiring safe factor data, it generates the strategy information according to classification algorithm and standard which is proposed in Section 3.1.2 and 3.2. The proposed classification algorithm is based on membership function. At the same time, it also needs to get strategy position for implementing strategy distributed.

B) Strategy generation module receives the position information from decision module, and generates the final strategy. It includes three units: strategy match, default report and translation. Strategy match unit is responsible for confirmation of safe demand level, if the level of safe strategy satisfies requirement of three parts described in **Fig. 3**, it translates strategy into information which can be identified by safe equipment. If the level of safe strategy does not satisfy requirement of the three parts, it would produce a default report. Thus, the strategy would be regenerated until it satisfies the requirement of the three parts.

C) After receiving correct strategy from strategy generation module, strategy issue module packs safe strategy and sends it to strategy execution module which fulfils strategy execution.

D) In addition to execution, the strategy execution module is also responsible for status feedback. It sends the execution status to equipment control module for managing equipment.

E) The equipment control module receives status feedback from the strategy execution, and then updates equipment status. At the same time, it also takes on database maintenance.

F) When the equipment lacks some resource for performing the corresponding safe strategy, the strategy execution module will send a appropriate resource demand to resource management module. Once the resource management module receives this request, it will invoke an appropriate resources from database and send it back to strategy execution.

G) Format database, resource database and strategy database are the most important supporters for the whole system.

From **Fig. 3** and **Fig. 4**, we can see that the presentation in **Fig. 3** is a subsystem of the system in **Fig.4**. The strategy decision module, the strategy generation module and the strategy issue module shown in **Fig. 4** are detailed description for subsystem in **Fig. 3**. That is, the whole process in **Fig. 3** is strategy generation and issue, which extends to the strategy decision module, strategy generation module and strategy issue module presented in **Fig. 4**.

3.1.1 Safety factors of dynamic classification defense of network security

In this section, the selection of network security elements is the foundation of the whole dynamic classification defense of network security, since the network security elements are constructed by numerous correlative parameters which can reflect actual situation of network security. Liu and Zhang **[5]** have finished the research on defensive measure and safe factor in details. Wang Yulin proposed four network security factors in **[24]**, such as encryption, integrity, authentication and safe audit. However, these factors are not enough to reflect the change of safety level in a dynamic network environment. We make further analysis on the various aspects of network security parameters on the basis of their research. Combining with dynamic network environment and the experimental-derived QoS parameters presented in **[29-31]**, we introduce the traffic and access control, such as traffic filtration, access control, traffic protection and safe inspection. All these safe factors reflect the safe situation of the whole system. Consequently, we consider the following eight safe factors: traffic packet size, integrity, authentication, traffic packet rate, link frequency, traffic protection, safe inspection and safe audit, which are shown in **Fig. 5**.

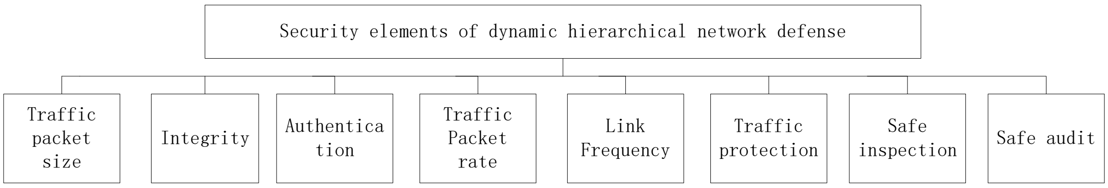

Fig. 5. The elements of dynamic classification defense for network security

3.1.2 The classification standard of safe factors

The classification criterion based on expert opinion and specific experimental environment is proposed. In the process of experiment, we take the load test for several times by setting different network load situations, and observe and record the specific value of various parameters obtained from the experiment, then analyze the relationship between values and the current situation of the network. For example, in normal and abnormal cases, the values of safe parameters are different. Thus we can see that the value of safe parameter is key to determine the scope of the levels of each parameter. We use the corresponding indicators to measure every security elements. Details are shown in **Table 1.**

Table 1. The level of network security factors

	Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**	**Level 7**	**Level 8**
Traffic packet size（bytes）	≤ 64	≤ 223	≤ 399	≤ 579	≤ 773	≤ 949	≤ 1149	> 1472
Integrity constraints rate（%）	≤ 20	≤ 40	≤ 50	≤ 65	≤ 70	≤ 80	≤ 95	> 95
Certification numbers(time)	≤ 1	≤ 2	—	≤ 3	—	≤ 5	≤ 6	> 6
Traffic packet rate(pps)	≤ 100	≤ 10100	≤ 25100	≤ 40900	≤ 55900	≤ 71846	≤ 86831	> 126500
Link frequency（GHz）	> 5	≤ 4.8	≤ 4.5	≤ 4.3	≤ 4	≤ 3.5	≤ 3	≤ 2.4
Loss rate of traffic packet（%）	> 4	≤ 4	≤ 2.4	≤ 2	≤ 1.5	≤ 1	≤ 0.5	≤ 0.2
Detection average response time（s）	> 5	≤ 5	≤ 4.5	≤ 4	≤ 3	≤ 2	≤ 1	≤ 0.5
Audit average response time（s）	> 10	≤ 10	≤ 8	≤ 6	≤ 3	≤ 2.5	≤ 2	≤ 1

Note: "—" denotes no.

Each level denotes the practical running status of all safe factors' indicators under different network environment. All the safe levels correspond to the change of network security status from unsafe to safe situations.

3.2 Dynamic classification algorithm based on fuzzy theory

In the dynamic classification defense strategy of network security, strategy decision is located at central position. We can obtain the current network security requirements through analyzing of network environment. We usually use the weighted average algorithm to calculate the comprehensive level of network security, the method has simple computational complexity and higher operation rate, but it cannot solve uncertain problems.

Due to the question in this paper is uncertain problems, we cannot regard dynamic classification of the network security as a certain object. Also we can't design a standard threshold, the network situation is good if they don't exceed in this threshold, and bad exceed. Therefore, the defense classification of network security should be regarded as a process of reasoning, which needs to make a comprehensive judgment by collecting information from different sources. According to the evaluation results, corresponding strategy are issued. For this problem, we solve the decision of security requirement using fuzzy theory, and obtain the strategy level.

The process diagram of the algorithm is shown in **Fig. 6.**

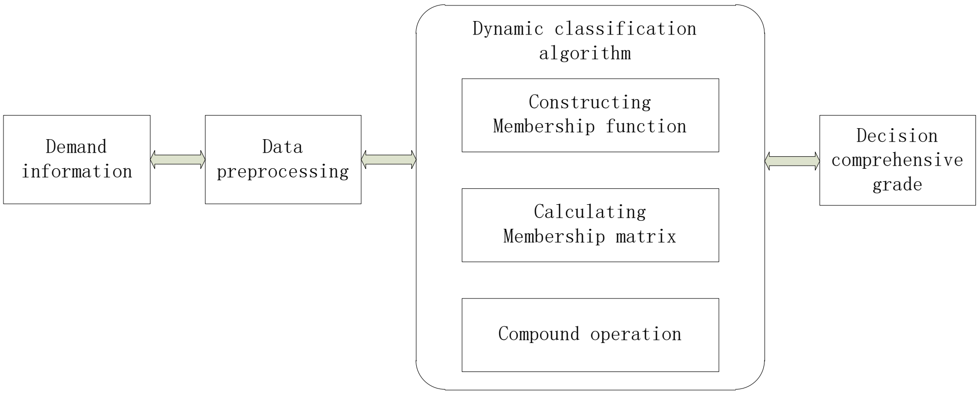
Demand information
Data preprocessing
Dynamic classification algorithm
Constructing Membership function
Calculating Membership matrix
Compound operation
Decision comprehensive grade

Fig. 6. Fuzzy theory algorithm process

Based on above process, data preprocessing module converts requirement information to the value of requirement for system, we can calculate the comprehensive security level by applying the dynamic classification algorithm.

The calculation process is given as following:

Step1：Construction of membership functions

On the basis of situational analysis information, user requirement and the current defense strategy , we have constructed the membership function. The level of classification defense of network security is divided into eight parts. Membership means that the situation of network security belongs to one level at some extent. Under normal circumstance, the membership value is greater , the possibility belonging to the corresponding level is greater. The specific standard of division needs to change with the specific network environment.

The method for establishing membership function is mainly based on distance between the actual data (monitoring to the current network data) and standard data (see**Table 1**). The specific expression is written as:

$$f(x)=\begin{cases}1 & x\le L_i \\ \dfrac{L_{i+1}-x}{L_{i+1}-L_i} & L_i<x\le L_{i+1} \\ 0 & x\ge L_{i+1}\end{cases} \tag{3-1}$$

where L_i denotes a standard value for the i th($1\le i\le 8$) level, L_{i+1} denotes a standard value for the $i+1$ th ($1\le i\le 8$) level.

Of course, in view of the standard of different parameters for safety factors, Eq. (3-1) needs to make some adjustment according to different situations.

Step2：Construction of the fuzzy matrix

Let U be a set of various safety factors, and V be a set of network security level. In terms of our system, U={ encryption, integrity,…, safety audit }, V={ level 1 , level 2, …, level 8 }. For each actual measured value x (monitoring data in current network) of safety elements, we calculate its membership for security level by using of membership function, and acquire judging matrix:

$$P = \begin{bmatrix} a_{1,1} & \cdots & a_{1,8} \\ \vdots & \ddots & \vdots \\ a_{8,1} & \cdots & a_{8,8} \end{bmatrix}$$

where a_{ij} denotes the membership (i is safe element, j is safe level, $1 \le i, j \le 8$). If some safe element level does not exist, then a_{ij} =0.

Step3: Calculation of the factor weight

Considering the actual situation, each security element plays a different role when different attacks exist on the network. For example, if the Internet is attacked by DDOS, the flow protection and control will play a more important role. We construct the weight calculation formula in double cases, the first case is that the tendency for changing of network safe elements is increasing from the level 1 to 8, the specific calculation formula is given by:

$$h_{\mathrm{i}} = \frac{\min(B_{\mathrm{i}}, B_{\max})}{\overline{B_{\mathrm{i}}}} \times \frac{B_{\max}}{B_{\min}} \tag{3-2}$$

The first case is that the tendency for changing of network safe elements is decreasing from the level 1 to 8, the specific calculation formula is given by:

$$h_i = \min\left(\frac{\overline{B_i}}{B_i}, \frac{\overline{B_i}}{B_{\min}}\right) \times \frac{B_{\max}}{B_{\min}} \tag{3-3}$$

where B_i denotes the actual value of the i th safe element, $\overline{B_i}$ denotes intermediate level value of the i th safe element, $B_{\max}$ denotes the maximum value of each security element classification standard, and $B_{\min}$ is the minimum value of each security elements classification standard.

We need to normalize the results, such that the sum of all weights is equal to 1. Formula for normalizing is as follows (h' denoted initial weight matrix):

$$h_i = h_i' \Big/ \sum_{i=1}^{n} h_i \qquad i = 1, 2, \ldots, 8 \tag{3-4}$$

Weighting matrix A is got, where $A = [h_i],\ i = 1, 2, \ldots, 8$.

Step4: Compound operation of matrix

Matrix A multiples matrix P (in this part, we adopt the multiplication from Fuzzy theory), the result is as follows:

$$A \circ P = [w_1\ ,\ w_2\ ,\ \cdots,\ \ w_8] \begin{bmatrix} a_{1,1} & \cdots & a_{1,8} \\ \vdots & \ddots & \vdots \\ a_{8,1} & \cdots & a_{8,8} \end{bmatrix} \tag{3-5}$$

$$=\left[c_1,c_2,\cdots c_8\right]$$

We normalize the result of $\left[c_1,c_2,\cdots c_8\right]$, such that the sum of all elements is equal to 1.

Step5: Decision

According to the results of the final vector to determine the comprehensive level, we choose the vector that has the largest value, and regard angle of it as the comprehensive level. If we regard C as the network safe level, and $C = \max\limits_{i=1,2,\cdots,8}\left\{c_i\right\}$. For example, c_5 is the largest one, we obtain the comprehensive level of network safety is level 5.

3.3 Dynamic defense system of network security

In terms of system function, strategy is some information which can be used to change the behavior of the execution. In terms of content, strategy is a series of rules, and they can control operation component of network.

In most cases, the network is a relatively stable state, we just make partial adjustment on required defense strategy. Most of the safe equipments are able to maintain safe strategy for themselves, only a small part needs to adjust. When strategy has been generated and distributed, system needs to establish a filtering mechanism, and it only sends necessary safe strategy which changes the execute component. Thus the resource can be distributed fast and efficiently. Strategy decision units, generating unit, strategy issued unit, resource management unit and equipment control unit play a unique function during the strategy generation, distribution and maintenance.

There exist interactive modes between strategy decision and generation and demand acquisition module, strategy decision and generation modules connect with demand acquisition module directly. When network security lies in a dangerous condition, demand acquisition subsystem will obtain an alarm from strategy system (see **Fig. 4**).

3.3.1 Strategy distribution and generation

Strategy generation unit accepts positioning information deriving from strategy decision unit. After the information confirmed by users, system will sent the selected strategy to the generation unit, and generate specific types of strategy. The default strategy information will be reported to the resource management module, then the resource management module deals with the default information. Strategy generation unit is a translation unit of system, it converts unified execution strategy description language into different language of executable equipment. Then strategy has been issued in the form of package.

3.3.2 Resource management

One of the most important tasks of resource management is receiving default information, the resource management would send the solution of the default information to strategy execution units.

Due to executive equipment is provided by different vendors, and they may adopt different protocols or standards. In order to ensure strategy can be executed by equipment smoothly, resource management unit provides all kinds of strategy implementation in details.When the strategy is issued to execution equipment, it will send a request to resource management unit if executive equipment isn't able to execute strategy. Resource management unit accesses to strategy resource database. According to the request above, the resource management searches strategy execution method in detail, and then sents it to executive equipment.

3.3.3 Equipment control

The main function of equipment control is to receive the execution status information that the execution equipment feedbacks regularly. According to the status information, the equipment control updates the equipment execution information in the database, at the same time also ensures maintenance of the database favorably.

4. The simulation and the analysis of experiment

We have presented how to design the dynamic classification defense of network security system. The system has not been existed before, therefore the method marks the beginning of dynamic classification defense. By comparing the safe level of two different network security, we illustrate the applicability of the method. We use network topology simulation shown in **Fig. 7**. The attack host is located in the external network, and a firewall separates target network from external network, firewall rules are shown in **Table 2**. The rest of system is made of a Web server with Win7 operating system, a file management server with Linux operating system and a database server with Win7 operating system.

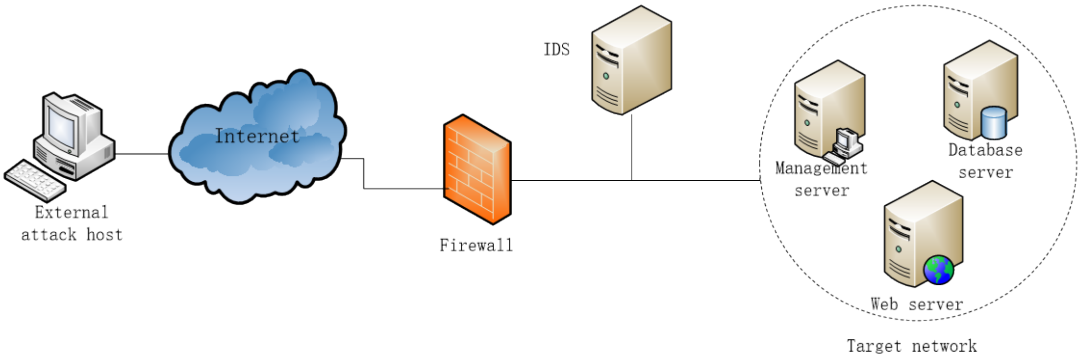

Fig. 7. Experimental environment of network topology

Table 2. Firewall rules

Original host	Target host	Server	Access strategy
All	Web server	Http	Allow
All	Web server	Ftp	Allow
All	Manage server	Ftp	Allow
Web server	Database server	Ftp	Allow
Manage server	Database server	Ftp	Allow

In order to illustrate rationality and applicability for the dynamic classification based on network security defense, we set up two experiments for comparing. The first experiment lies in a deteriorative Internet environment which is affected by the worm, and all measure indicator can not run normally. About the worm attack, we can refer research [25-28]. Now the safe server coefficient is falling, and the network resource is not enough to reply a large number of users request. The second lies in a normal operation, the safe level of various factors is kept in a high state, now situation of network security is very good. In this work, the precision of dynamic classification of network security defense is the dynamic classification algorithm. Strategy generation and distribution just follows with the design of system. So our main task is to prove the validity of the algorithm based on two different security environment above.

Experiment 1:

As we mentioned in the Section 3, the resource of safe elements has three parts: (1) Situational analysis data for network monitoring information; (2) User input data; (3) Current awareness of defense situation. We choose the lowest level data of them as our target data. In order to get the level of network security when the network is attacked by the worm, we should record the operation value of each safe element. Making use of these values and the algorithm given in Section 3.2, we obtain the comprehensive level of network security. The operation values of eight safe elements attacked by the worm are shown in **Table 3.**

Table 3. The actual measured value for safe elements

Traffic packet size（bytes）	Integrity constraint rate (％)	Certification numbers(time)	Traffic packet rate(pps)	Link frequency（GHz）	Loss rate of traffic packet (％)	Detection average response time（s）	Audit average response time（s）
100	79	3	20890	4.2	3.8	4.2	10

According to Eq.(3-1), we list the computational formula for membership function. Since the variation tendency of integrity constraints rate, certification numbers and average throughput is increasing. For the tendency is similar to the change of the traffic packet size, we just give the computational formula for membership function of the traffic packet size as following. The computational formulas of variation tendency of integrity constraints rate, certification numbers and traffic packet rate are similar to the traffic packet size membership function formula.

$$f_1(x)=\begin{cases}1 & x<64\\ \dfrac{223-x}{223-64} & 64<x<223\\ 0 & x\geq 223\end{cases}\qquad f_2(x)=\begin{cases}\dfrac{x-64}{223-64} & 64<x\leq 223\\ \dfrac{399-x}{399-223} & 223<x<399\\ 0 & x\leq 64, x\geq 399\end{cases}$$

$$f_3(x)=\begin{cases}\dfrac{x-223}{399-223} & 223<x\leq 399\\ \dfrac{579-x}{579-399} & 399<x<579\\ 0 & x\leq 223, x\geq 579\end{cases}\qquad f_4(x)=\begin{cases}\dfrac{x-399}{579-399} & 399<x\leq 579\\ \dfrac{773-x}{773-579} & 579<x<773\\ 0 & x\leq 399, x\geq 773\end{cases}$$

$$f_5(x)=\begin{cases}\dfrac{x-579}{773-579} & 579<x\leq 773\\ \dfrac{949-x}{949-773} & 773<x<949\\ 0 & x\leq 579, x\geq 949\end{cases}\qquad f_6(x)=\begin{cases}\dfrac{x-773}{949-773} & 773<x\leq 949\\ \dfrac{1149-x}{1149-949} & 949<x<1149\\ 0 & x\leq 773, x\geq 1149\end{cases}$$

$$f_7(x)=\begin{cases}\frac{x-949}{1149-949} & 949< x\le 1149\\ \frac{1472-x}{1472-1149} & 1149<x<1472\\ 0 & x\le 949, x\ge 1472\end{cases} \qquad f_8(x)=\begin{cases}\frac{x-1149}{1472-1149} & 1149<x<1472\\ 1 & x>1472\end{cases}$$

The variation tendency of the average response time of link frequency, packet loss rate, the average response time of detection, the average response time of auditing is decreasing, hence we give only the computational formula for membership function of the link frequency as following, the membership function of other safe element is similar to them.

$$f_1(x)=\begin{cases}1 & x>5\\ \frac{5-x}{5-4.8} & 4.8<x\le 5\\ 0 & x\le 4.8\end{cases} \qquad f_2(x)=\begin{cases}\frac{x-4.8}{5-4.8} & 4.8<x\le 5\\ \frac{4.8-x}{4.8-4.5} & 4.5<x\le 4.8\\ 0 & x\le 4.5\end{cases}$$

$$f_3(x)=\begin{cases}\frac{x-4.5}{4.8-4.5} & 4.5<x\le 4.8\\ \frac{4.5-x}{4.5-4.3} & 4.3<x\le 4.5\\ 0 & x\le 4.3\end{cases} \qquad f_4(x)=\begin{cases}\frac{x-4.3}{4.5-4.3} & 4.3<x\le 4.5\\ \frac{4.3-x}{4.3-4} & 4<x\le 4.3\\ 0 & x\le 4\end{cases}$$

$$f_5(x)=\begin{cases}\frac{x-4}{4.3-4} & 4<x\le 4.3\\ \frac{4-x}{4-3.5} & 3.5<x\le 4\\ 0 & x\le 3.5\end{cases} \qquad f_6(x)=\begin{cases}\frac{x-3.5}{4-3.5} & 3.5<x\le 4\\ \frac{3.5-x}{3.5-3} & 3<x\le 3.5\\ 0 & x\le 3\end{cases}$$

$$f_7(x)=\begin{cases}\frac{x-3}{3.5-3} & 3<x\le 3.5\\ \frac{3-x}{3-2.4} & 2.4<x\le 3\\ 0 & x\le 2.4\end{cases} \qquad f_8(x)=\begin{cases}\frac{x-2.4}{3-2.4} & 2.4< x\le 3\\ 1 & x\le 2.4\end{cases}$$

We get the membership degree matrix as follows

$$P=\begin{pmatrix} 0.7736 & 0.2264 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.1000 & 0.9000 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0.2807 & 0.7193 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.3333 & 0.6667 & 0 & 0 & 0 \\ 0 & 0.8750 & 0.1250 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.4000 & 0.6000 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We calculate the factor weight matrix by using Eq.(3-2)- Eq. (3-4), and normalize the results and achieve ultimate matrix

$$A=\begin{pmatrix} 0.1378 & 0.0427 & 0.1284 & 0.0687 & 0.1054 & 0.1936 & 0.1734 & 0.1500 \end{pmatrix}$$

Matrix A multiply P (“$\circ$”denotes the multiplication in fuzzy theory)

$$A\circ P=\begin{pmatrix} 0.1378 & 0.0427 & 0.1284 & 0.0687 & 0.1054 & 0.1936 & 0.1734 & 0.1500 \end{pmatrix}$$

$$\circ\begin{pmatrix} 0.7736 & 0.2264 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.1000 & 0.9000 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0.2807 & 0.7193 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.3333 & 0.6667 & 0 & 0 & 0 \\ 0 & 0.8750 & 0.1250 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.4000 & 0.6000 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$=\begin{pmatrix} 0.1378 & 0.1936 & 0.1734 & 0.1734 & 0.1054 & 0.0427 & 0 & 0 \end{pmatrix}$$

Normalizing the results above, we can get

$$\begin{pmatrix} 0.1667 & 0.2343 & 0.2098 & 0.2098 & 0.1276 & 0.0518 & 0 & 0 \end{pmatrix}$$

We can see that the largest number is 0.2343, which lies in the second position. Therefore, we know that the level of network security is level 2 when the network is attacked by the worm. Now the network is in a dangerous state.

Experiment 2:

The information of eight safe elements is given in **Table 4** by monitoring dynamically**.**

Table 4. The actual measured value for safe elements

Traffic packet size（bytes）	Integrity constraint rate (%)	Certification numbers (time)	Traffic packet rate(pps)	Link frequency（GHz）	Loss rate of traffic packet（%）	Detection average response time（s）	Audit average response time（s）
1130	81	7	70823	2.8	0.875	1.2	2.4

According to calculating steps in **Experiment 1**, the membership matrix is obtained:

$$P=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0.0950 & 0.9050 & 0 \\ 0 & 0 & 0 & 0 & 0.9333 & 0.0667 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0.0642 & 0.9358 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.3333 & 0.6667 \\ 0 & 0 & 0 & 0 & 0 & 0.7500 & 0.2500 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.2000 & 0.8000 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.8000 & 0.2000 & 0 \end{pmatrix}$$

We normalize the weight matrixrecalculatedas follows:

$$A=\begin{pmatrix} 0.3004 & 0.0733 & 0.1098 & 0.0308 & 0.0967 & 0.1801 & 0.1686 & 0.0403 \end{pmatrix}$$

The normalization form of final result is obtained:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0.1105 & 0.2714 & 0.4527 & 0.1654 \end{pmatrix}$$

The largest number is 0.4527 which locates in the seventh position, we draw a conclusion that the network safe is 7 level. The Internet is operating in good condition. But the result in experience 1 is terrible, we need to offer higher level strategy to defensive system. For example, the Internet may be in danger when the network safe is 2 level, we need to provide the 7 level strategies for the Internet and prevent the Internet from damaging. Referring to the classification standard and the membership degree matrix, we check each security elements level, then generate corresponding strategy for each security elements according to the level of each security elements. Thus the system achieves the distribution and execution of strategy. At the same time, every safe factor is promoted to a higher level of normal operation. When users want to change the execution state security element, the model can obtain security levels accurately.

It can be seen from the results of the validation that the dynamic classification algorithm to the network security factors is accurate, and the method has a clear physical meaning. Of course, we also know that the main advantage of this method is to solve the problem of current network performance degradation caused by the security arrangements, and improve the use efficiency of the security products.

5. Conclusion

Based on analyzing the research status of network security at home and abroad, we make a further study on network security defense knowledge. Considering the current network structure and the present condition of the network, we propose a dynamic classification defense policy model of network security, and discuss the possible problems and solutions on the basis of policy decision methods, strategies generation and issue. The model locates in the core position of whole network security active defense system. We put forward the feedback loop in strategy generation and distribution. The process helps the system issue and execute strategy successfully. The model reflects dynamic classification defense of network security directly. For a long time, most of the network security defense is based on static defense. If the system just considers the security technology, it isn’t able to solve the problem for changing of attack and defense completely. Compared with the literature [23], the model accomplishes the major function of the network security defense strategy, and has stronger adaptability and real-time performance.

Acknowledgements

The author thanks the editor and reviewers for their suggestions to improve the quality of paper. This work was supported by the NSF of China (U1433105) and the Beijing Higher Education Young Elite Teacher Project (YETP0448).

References

[1] Q. S. Wu, et al, "On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks," in *Proc. of the 2010 spring simulation multiconference. Society for computer Simulation International*, 2010. Article (CrossRef Link)

[2] K. W. Lye, J. Wing "Game strategies in network security," *School of Computer Science, Carnegie Mellon University, Pittsburgh: Technical Report CMU-CS-02-136*, May 2002. Article (CrossRef Link)

[3] C. Cliff Zou, Nick Duffield, Don Towsley, "Weibo Gong. Adaptive Defense Against Various Network Attacks," *IEEE Journal on Selected Areas in Communications*, vol.24, no.10, pp.1877-1887, 2006. Article (CrossRef Link)

[4] J. Xu, W. Lee, "Sustaining availability of Web services under distributed denial of service attacks," *IEEE Transactions on Computers*, vol.52, no.4, pp.195-208, 2003. Article (CrossRef Link)

[5] P. Liu, W. Zhang, "Incentive-based modeling and inference of attacker intent, objectives, and strategies," in *Proc. of the 10th ACM Computer and Communication Security Conference (CCS'03). Washington, DC*, pp. 179-189, 2003. Article (CrossRef Link)

[6] S. Northcutt, *Networking Intrusion Detection: An Analyst's Handbook*, 3rd Edition Indianapolis, Indiana, United States, New Riders Publishing, 1999. Article (CrossRef Link)

[7] W. Jiang, B. X. Fang, Z. H. Tian, and et al., "Evaluating network security and optimal active defense based on attack-defense game madel," *Chinese Journal of Computers*, vol.32, no.4, pp.817-827, 2009. Article (CrossRef Link)

[8] T. Spyridopoulos, G. Karanikas, T. Tryfonas, G. Oikonomou, "A game theoretic defense framework against DoS/DDoScyber attacks," *Computer & Security*, vol.38, pp.39-50, 2013. Article (CrossRef Link)

[9] A. Chonka, Y. Xiang, W. L. Zhou, A. Bonti, "Cloud security defense to protect cloud computing against HTTP-DoS and XML –DoS attacks," *Journal of Network and Computer Applications*, vol.34, no.4, pp.1097-1107, 2011. Article (CrossRef Link)

[10] U. Tariq, Y. Malik, B. Abdulrazak, "Collaborative Peer to Peer Defense Mechanism for DDoS Attack," *Procedia Computer Science*, vol.5, pp.157-164, 2011. Article (CrossRef Link)

[11] J. F. Xu, "A defense system for wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol.18, sup.2, pp.119-122, 2011. Article (CrossRef Link)

[12] Y. C. Jiang, Z. Y. Xia, S. Y. Zhang, "A novel defence model for dynamic topology network based on mobile agent," *Microprocessors and Microsystems*, vol. 29, no.6, pp.289-297, 2005. Article (CrossRef Link)

[13] W. M. Hong, "The technology research of dynamic network active defense in network management," *International workshop on information and electronics engineering(IWIEE)*, vol.29, pp.1584-1589, 2012. Article (CrossRef Link)

[14] S. Tripathy, S. Nandi, "Defense against outside attacks in wireless sensor network," *Computer Communications*, vol.31, no.4, pp.818-826, 2008. Article (CrossRef Link)

[15] J. A. Fitch III, L. J. Hoffman, "A shortest path network security model," *Computers & Security*, vol.12, no.2,pp.169-189, 1993. Article (CrossRef Link)

[16] N. Hoque, M. H. Bhuyan, R. C. Baishya, and D. K. Bhattacharyya, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, vol.40, pp.307-324, May, 2014. Article (CrossRef Link)

[17] G. Levitin, "Optimal defense strategy against intentional attacks," *IEEE Transactions on Reliability*, vol.56, no.1, pp.148-157, 2007. Article (CrossRef Link)

[18] H. Li, G. W. Rosenwald, J. Jung, and C. C. Liu, "Strategic power infrastructure defense," in *Proc. of The IEEE*, vol. 93, no.5,pp. 918-933, 2005. Article (CrossRef Link)

[19] R. L. Chen, J. M. Park, R. Marchany, "A divide – and – conquer strategy for thwarting distributed denial-of-service attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol.18, no.5, pp. 577-588, 2007. Article (CrossRef Link)

[20] O. P. Kreidl and T. M. Frazier, "Feedback control applied to survivability: A host-based autonomic defense system," *IEEE Transactions on Reliability*, vol.53 no.1, pp.140-166, 2004. Article (CrossRef Link)

[21] C. L. Cao, R. Zhang, M. Y. Zhang and Y. X. Yang, "IBC-based entity authentication protocols for federated cloud systems," *KSII Transactions on Internet and Information Systems*, vol.7, no.5, pp. 1291-1312, May 31, 2013. Article (CrossRef Link)

[22] Z. Z. Peng and Y. Y Sun, "*Fuzzy mathematics and its application*," 2nd Edition, Wu Han university press, China, pp. 4-10, 2007. Article (CrossRef Link)

[23] S. P. Yao, Y. Y. Gu, "Network security situation quantitative evaluation based on the classification of attacks in attack-defense confrontation environment," *2009 Chinese Control and Decision Conference*, pp. 6014-6019, 2009. Article (CrossRef Link)

[24] Y. L. Wang and G. F. Tian, "Network security technology and practices," *Tsinghua university press*, Beijing, China, pp. 65-67, 2013. Article (CrossRef Link)

[25] A. Dainotti, A. Pescapè, G. Ventre, "Worm Traffic Analysis and Characterization," *2007 IEEE International Conference on Communications (ICC 2007)*. Article (CrossRef Link)

[26] A. Dainotti, A. Pescapè, G. Ventre, "A cascade architecture for DoS attacks detection based on the wavelet transform," *Journal of Computer Security*, Volume 17, Number 6/2009, Pages 945-968. Article (CrossRef Link)

[27] M. Jo, L. Z. Han, N. D. Tan, and H. P. In, "A Survey: Energy Exhausting Attacks in MAC Protocols in WBANs," *Telecommunication Systems*, Vol. 58, No. 2 pp. 153-164, February 2015. Article (CrossRef Link)

[28] M. Jo, L. Z. Han, D. Kim, and H. P. In, "Selfish Attacks and Detection in Cognitive Radio Ad-hoc Networks," *IEEE Networt*, Vol.27, No.3 pp. 46-50, June 2013. Article (CrossRef Link)

[29] A. Botta, A. Pescapé, G. Ventre, "Quality of service statistics over heterogeneous networks: Analysis and applications," *European Journal of Operational Research* 101 (2008) 1075-1088. Article (CrossRef Link)

[30] R. P. Karrer, I. Matyasovszki, A. Botta, and A. Pescapé, "Experimental evaluation and characterization of the magnets wireless backbone," *WiNTECH'06*,September 29, 2006, Los Angeles, California, USA. Article (CrossRef Link)

[31] R. P. Karrer, I. Matyasovaszki, A. Botta and A. Pescapé, "MagNets-experiences from deploying a joint research-operational next-generation wireless access network testbed," in *Proc. of the 3rd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TridentCom 2007*. Article (CrossRef Link)

Jinxia Wei received the B.S. degree from Hebei Normal University in 2010 and M.S. degree from YanShan University in 2013. Her current research interesting include cryptography, network secrity, cloud storage security and its application, etc. Now, she is studying as a doctor in Beijing University of Posts and Telecommunications.

Ru Zhang was born in 1976 and received Ph.D. degree in Computer Application Technology in 2003. She is a Prof. at Computer College, BUPT. She researches on Information Security in the state key laboratory of networking and switching technology, BUPT. Her interests include digital watermark, cryptography and multimedia authentication. She was awarded a national second prize and two provincial prizes.

Jianyi Liu received the B.S. degree from Xi’an University of Posts and Telecommunications in 2000 and M.S. degree from Beijing University of Posts and Telecommunications in 2005. Her current research interesting include disaster backup, information retrieval, network secrity, and cloud storage security, etc. He has published more than 40 papers in International Journal.

Xinxin Niu is an professor of Computer Science and Technology at Beijing University of Posts and Telecommunications. She received the MS degree from Beijing University of Posts and Telecommunications in 1988, the PhD degree from Chinese University of Hong Kong in 1997. Her current research interests include network security, digital watermarking and digital rights management, etc.

Yixian Yang is a Professor of Computer Science and Technology at Beijing University of Posts and Telecommunications and also the director of the National Engineering Laboratory for Disaster Backup and Recovery of China. He received his MS degree in Applied Mathematics and Posts and Telecommunications in 1987 and 1988, respectively. His research interests include coding theory and cyrptography, information secrutiy and network security, disaster backup and recovery, signal and information processing, etc.