Conditions Using Genetic Algorithm.*Proc Conf. on Signal Processing*, Beijing,China,p.p.2502 -2505.
8. Ahmadi M. ,Shridhar M.(1995)Recognition of Handwritten Numerals with Multiple Feature and Multistage Classifier. *Pattern Recognition*,28(2), p.p.153-160 .
9. Otsu N. (1979)A Threshold Selection Method from Gray-level Histograms.*IEEE TransSystems. Man and Cybernetics*, 9(1), p.p.62-66.
10. Haralick R M. ,Shanmagam K. ,Dinstein I.(1973) Textural Features for Image Classification. *IEEE Transactions on Systems. Man and Cybernetics*,33(3), p.p.610-621.

Prediction of the trend of network attacks based on mechanism analysis method

Liya Wang

School of Mathematics and Information Science, Langfang Teachers University, Langfang065000, Hebei,China

Jiankun Shang*

Department of Antitank Missiles , Nanjing Artillery Academy, Langfang065000, Hebei,China

Yang Zhao

Department of Electronic and Information Technology, Jiangmen Polytechnic, Jiangmen 529090, Guangdong,China
**Corresponding author is Jiankun Shang, email:jkshang@sohu.com*

Abstract
With the development of Internet, network attacks are more and more.Network attacks have jeopardized all sectors, and even national security.The development trend of network attacks could be predicted through the mechanism of analysis.The model of network attacks was briefly built by principle analysis. Some experiment simulation were made by dealing with the data collected from the Internet,and the

corrected index was used for numerical simulation.Eventually the trends in data was found and predicted. Through the changes related data about the Internet could indirectly characterize the development of network attacks.Understanding network attacks and studying their development trends and grasping the latest developments in cyber attacks,which is benefit to maintain their own privacy and protect their own interests.

Key words: NETWORK ATTACKS,MECHANISM ANALYSIS,FIXED INDEX CURVE,BLOCK GROWTH MODEL .

1. Introduction

With the rapid development of new network applications and new technology in network, the Internet was faced with more serious security situation, especially including those of users interests incidents.It was not only a threat to personal safety, more serious would affect national security.Therefore, network attacks as a thorny issue should be attached and arouse the masses of attention. As a network attack vectors, Internet offered many opportunities to network attacks[1-2].Usually cyber attacks were certain steps. When attackers found suitable attack locations and certain targets after logging host and obtain account and password.They would be able to gain the initiative, and then control the host, steal information on the host.

A lot of scholars had studied for many years in this regard.Network attacks were immoral, and necessarily violated the law.Computer network attacks were related to the legal issues[3-5].Zichun Wang pointed out that cyber attacks should not only arouse concern of the domestic population,but also concern of the international peoples.Therefore, network attacks also violated international law.In addition,law and network attacks had necessarily linked[6-7].Xiaoxue Yang pointed out that in order to safeguard individual rights and the protect personal safety, people must understand international law and use the law to protect rights.There were many categories of cyber attacks.The characteristics of network attacks was different with classification criteria[8].Chunliang Li established a initial model of network attack systems through simulation and experimental simulation.Network attack technology was a critical component of a network attack system[9].Cong Wang conducted in-depth research on network attack techniques,and several typical attack techniques carried out impact assessment.

This article further predicted cyber attacks trends by analyzing the changes in Internet-related data.So it provided the foundation for restricting the development of cyber attacks and preventing network attacks.

2. Description of the mechanism analysis

Everything had its own law of development and the basic principles.Mechanism analysis was analyzed by the internal law of things, causes, mechanisms, and it discovered and summarized the scientific method which has some variation.The deductive method and the mechanism analysis as the two complement each other were able to use by studying on the mechanism of things[10].Thus the study of the mechanism for the things played a significant role.

In the physical sector, chemical industry, management community had all used the mechanism analysis[11].Especially in mathematical modeling,mechanism analysis method was widely used.Therefore, the mechanism analysis for the mathematical problem were more accurate and close to reality.

3. The establishment of the mathematical model

Internet was a basic network attacks as well as its source.In order to observe the development trend of network attacks,the relevant data could be look up through the national database on the Internet.In response to these statistics,mathematical models were used to carry on simulation experiments.Through the trends of below-mentioned data the development trend of network attacks could be indirectly forecast .Among them the increasing number of web sites and pages opened up a channel for the network attack which had a certain impact on the attack tools.So the trend of web sites and pages could indirectly forecast the development trend of network attacks.Popularity of the Internet, increasing number of Internet users,Internet international outlet bandwidth,Internet broadband access ports and Internet broadband access users directly showed the degree of automation of the network ,which enable network attacks more quick. So the trend of below data could also indirectly forecast the development trend of network attacks.

Thereby the simulation experiment was made about the above data.Finally the development trend of network attacks could be predicted. The NTES site for example, had been attacked for seven years by the survey which was found that the number of attacks had a rapid growth, shown in the table below:

Table 1. Internet-related data

Project	Years	
	2013	2014
The number of sites (ten thousand)	320.16	335.42
Number of pages (ten thousand)	15004076.3	16594758.6
Internet penetration (%)	45.8	49.4
Number of Internet users (million) Internet access		64875
Internet dial-up users (million)	485.10	502.26
Internet international outlet bandwidth (Mbps)	3406824.00	3629392.51
Internet broadband access ports (ten thousand)	35945.30	40105.40
Internet broadband subscribers (million)	18890.90	21059.78

Table 2. NTES sites have been attacks by distributed denial of service

year	2008	2009	2010	2011	2012	2013	2014
Times (a hund-million)	0.41	0.87	1.34	1.62	1.83	2.46	3.6

The line statistical figure was shown to find the relevant data.It was found that the number of times rose as the approximate index from this figure, so the simplest website attacked times growth model was set up without any external intervention.

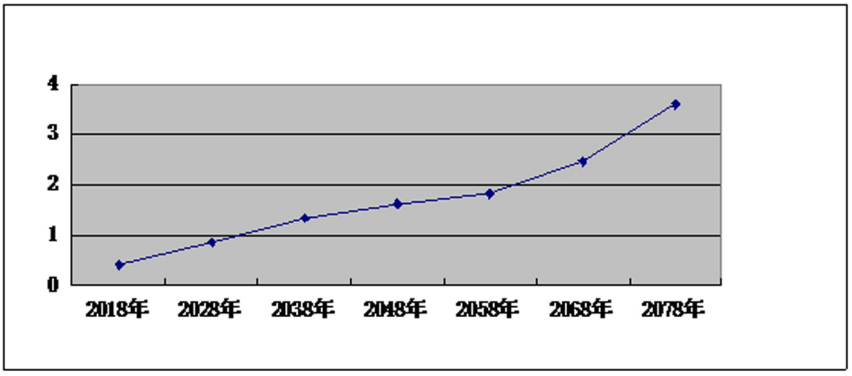

Figure 1. The number of NTES attacked in seven years

x_0 represented the attack times this year, x_k showed the attack times after k years, r was the rate of network attacked (constant).So it can be concluded,

$$x_k = x_0(1+r)^k \tag{1}$$

The hypothesis was put forward that the increase of NTES attacked times was proportional with the Internet users in per unit time,

$$r = \frac{x(t+\Delta t)-x(t)}{x(t)\Delta t} \tag{2}$$

where $x(t)--t$ was the number on the Internet, $x_0--t=0$ was the number of people online, $x(t)$ satisfied the differential equations of separable variables as follows,

$$\begin{cases} \dfrac{dx}{dt} = rx \\ x(0) = x_0 \end{cases} \tag{3}$$

$$x(t) = x_0 e^{rt} \tag{4}$$

when $r>0$, it showed that the number of attacked times was according to the index law of infinite growth in accordance with commonly used formula, when $r>0$, it showed that the number of attacked times was according to the index law of infinite growth in accordance with commonly used formula,

$$x(t) = x_0(e^r)^t \approx x_0(1+r)^t \tag{5}$$

The least squares method could be used to make a fitting.It was the main core idea that the least squares fitting method had a lot of curve fitting, which linear least squares method often was used ,

$$f(x) = a_1 r_1(x) + a_2 r_2(x) + \cdots + a_m r_m(x) \quad (6)$$

The relationship among sets of linearly independent function needed to be find out by characterization of $r_k(x)$ and the parameteris a_k $(k = 1,2,\cdots,m,m,n)$ be identified.when the sum of square of the distance δ_i between $f(x_i)$ and $y_i, i = 1,2,\cdots,n,$ is at minimum the least squares fitting criterion can be established and the least quotient a_k can be describted:

$$J(a_1,\cdots,a_m) = \sum_{i=1}^{n} \delta_i^2 = \sum_{i=1}^{n} [f(x_i) - y_i]^2 \quad (7)$$

J can be used when the least necessary condition of extremum is $\frac{\partial J}{\partial a_k} = 0 (k = 1,\cdots,m)$

so linear system of equations about $a_1,\cdots,a_m$ is as follows,

$$\sum_{i=1}^{n} r_j(x_i)[\sum_{k=1}^{m} a_k r_k(x_i) - y_i] = 0, (j = 1,\cdots,m) \quad (8)$$

$$\sum_{k=1}^{m} a_k [\sum_{i=1}^{n} r_j(x_i) r_j(x_i)] = \sum_{i=1}^{n} r_j(x_i) y_i, (j = 1,\cdots,m) \quad (9)$$

$$R = \begin{bmatrix} r_1(x_1) & \cdots & r_m(x_1) \\ \vdots & \vdots & \vdots \\ r_1(x_n) & \cdots & r_m(x_m) \end{bmatrix}_{n \times m}, A = [a_1,\cdots,a_m]^T,$$
$$Y = (y_1,\cdots,y_n)^T \quad (10)$$

$$R^T R A = R^T Y \quad (11)$$

The linear system of equations has only one condition ,that is, $\{r_1(x) \cdots, r_m(x)\}$ is linear independent so $R^{'}s$ list is full rank and $R^T R$ is reversible.

$$A = (R^T R)^{-1} R^T Y \quad (12)$$

The statistics the number of network attack would be obtain by calculation as follows:

Table 3. The statistics the number of network attack

	Actual times	Forecast times	Error
2008	0.41	0.50	0.09
2009	0.87	0.85	-0.02
2010	1.34	1.08	-0.26
2011	1.62	1.54	-0.08
2012	1.83	1.89	0.06
2013	2.46	2.52	0.06
2014	3.60	3.68	0.08

An available fitting curve can be get as follow:

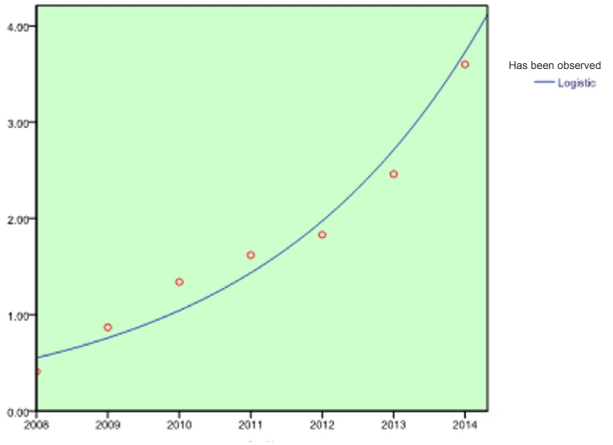

Figure 2. The attack frequency fitting

Upon examination, sig <0.05, test passed. However, in the long run, with the advent of cyber attacks, technical staff also prepared a growing number of anti-virus software, it can be assumed that the number of future attacks will be similar block model of population growth, the two will be in the dynamic balance.

4. The exponential curve based on mathematical model

The development of anything is a certain limit,-fixed exponential curve method overcomes the disadvantages that exponential curve in predicting the predicted value over time grow indefinitely.Forecast closer to the reality of things variation.Mathematical model exponential curve correction is fomula(13):

$$\hat{y}_t = K + ab^t \quad (13)$$

Among them, K, a, b are determined by using historical data.Modification index curve guiding ideology is that the initial rapid growth followed by accounts decreased gradually.

When $K > 0, a < 0, 0 < b < 1$, $t \to \infty, ab^t \to 0$, so $\hat{y}_t \to K$ .If the K value can determine, using the least squares method to determine the parameters of the model.If the K value can not be determined the below laws should be used.

m observations of the time series divided into three parts,Each section has m , $n = 3m$.

First part: $y_1, y_2, y_3, \cdots, y_m$;

The second part: $y_{m+1}, y_{m+2}, y_{m+3}, \cdots, y_{2m}$

The third part: $y_{2m+1}, y_{2m+2}, y_{2m+3}, \cdots, y_{3m}$

Among them, the tendency of each part is equal to the sum of the corresponding observed values, thereby giving parameter estimation, three legal steps observed for the sum of its parts were as follows:

$$S_1 = \sum_{t=1}^{m} y_t,\ S_2 = \sum_{t=m+1}^{2m} y_t,\ S_3 = \sum_{t=2m+1}^{3m} y_t, \quad (14)$$

And there is formula(15):

$$\begin{cases} S_1 = \sum_{t=1}^{m} \hat{y}_t = \sum_{t=1}^{m} (K + ab^t) = mK + ab(1 + b + b^2 + \cdots + b^{m-1}) \\ S_2 = \sum_{t=m+1}^{2m} \hat{y}_t = \sum_{t=m+1}^{2m} (K + ab^t) = mK + ab^{m+1}(1 + b + b^2 + \cdots + b^{m-1}) \\ S_3 = \sum_{t=2m+1}^{3m} \hat{y}_t = \sum_{t=2m+1}^{3m} (K + ab^t) = mK + ab^{2m+1}(1 + b + b^2 + \cdots + b^{m-1}) \end{cases} \quad (15)$$

Where $(1 + b + b^2 + \cdots + b^{m-1})(b-1) = b^m - 1$

The formula(16) can be obtained:

$$\begin{cases} S_1 = mK + ab\dfrac{b^{m-1}}{b-1} \\ S_2 = mK + ab^{m+1}\dfrac{b^{m-1}}{b-1} \\ S_3 = mK + ab^{2m+1}\dfrac{b^{m-1}}{b-1} \end{cases} \quad (16)$$

Thus the formula(17) can be obtained:

$$\begin{cases} b = \left(\dfrac{S_3 - S_2}{S_2 - S_1}\right)^{\frac{1}{m}} \\ a = (S_2 - S_1)\dfrac{b-1}{b(b^m-1)^2} \\ K = \dfrac{1}{m}\left[S_1 - \dfrac{ab(b^m-1)}{(b-1)}\right] \end{cases} \quad (17)$$

In addition, when the predict response data need to be test the method was expressed by formula(18):

$$\frac{y_{t+1} - y_t}{y_t - y_{t-1}} \approx b \quad (18)$$

It followed an exponential curve correction mathematical model about each index on Table 1, and finally obtained the following prediction on Table 4 and Table 5 .

Through the data changes could be found that a sharp increase in the number of sites and pages,the rate of increase was also on the rise.This indirectly led to the occurrence of cyber attacks.With the dramatic increase in the number of sites and pages,attack tools would be more complex,attack speed gradually increased.Individual pages and the website would become source place to network attacks.

In addition,popularity of the Internet, increasing number of Internet users,Internet international outlet bandwidth,Internet broadband access ports and Internet broadband access users were in skyrocketed.

Table 4. Internet-related predicting data

Project	Forecast data	
	2015	2016
The number of sites (ten thousand)	358.69	394.73
Number of pages (ten thousand)	17924521.9	18849281.7
Internet penetration (%)	52.4	59.8
Number of Internet users (million) Internet access	66921	69248
Internet dial-up users (million)	553.29	601.54
Internet international outlet bandwidth (Mbps)	3956248.66	4219578.23
Internet broadband access ports (ten thousand)	45369.13	49216.32
Internet broadband subscribers (million)	25957.61	29352.73

Table 5. The data of increasing rate

Project	The data of increasing rate		
	2013-2014	2014-2015	2015-2016
The number of sites (ten thousand)	0.048	0.069	0.100
Number of pages (ten thousand)	0.106	0.080	0.052
Internet penetration (%)	0.079	0.061	0.141
Number of Internet users (million) Internet access	0.050	0.032	0.035
Internet dial-up users (million)	0.035	0.102	0.087
Internet international outlet bandwidth (Mbps)	0.065	0.090	0.067
Internet broadband access ports (ten thousand)	0.116	0.131	0.085
Internet broadband subscribers (million)	0.115	0.233	0.131

This also led to the Internet faster and faster. Thereby it provided a convenient for the automation of network attacks.

5. The block growth model

The malthusian model introduced an item that anti-virus software is increasingly mature,

$$r(x) = r - sx(r, s > 0) \tag{19}$$

when x is very small r is the inherent growth rate, x_m is the inherent growth rate and then differential equation can be get :

$$\frac{dx}{dt} = r(1 - \frac{x}{x_m})x \tag{20}$$

$$x = \frac{x_m}{1 + Ce^{-rt}} \tag{21}$$

$$C = \frac{x_m}{x_0} - 1 \quad (x(0) = x_0) \tag{22}$$

$$\lim_{t \to +\infty} x_t = x_m \tag{23}$$

$$y = \frac{dx / dt}{x} \approx \frac{\Delta x}{x \Delta t} \tag{24}$$

$$s = \frac{r}{x_m} \tag{25}$$

$$y = r - sx \tag{26}$$

Because people's response to cyber attacks and people's security consciousness was improving, growth rate would eventually become flat.

6. Model Test and simulation

The least square method was used to estimate the parameters of the statistical data for calculating the block growth model. the results of the data were get by this method as shown in Table 6.

Table 6. The contrast of predicting results

time \ times	actual value	A prediction of block	forecast
2008	0.41	0.41	0.50
2009	0.87	0.83	0.85
2010	1.34	1.26	1.08
2011	1.62	1.67	1.54
2012	1.83	1.92	1.89
2013	2.46	2.52	2.52
2014	3.60	3.04	3.68
2015		4.02	6.32

The three sets of values by curve fitting was shown in the graph, without any interference, the number of network attacks would increase rapidly, like an exponential growth, and if we continue to update anti-virus software, improve security of Internet users actively guide awareness, the network can not be an infinite number of attacks increase, which can get another prediction curve.

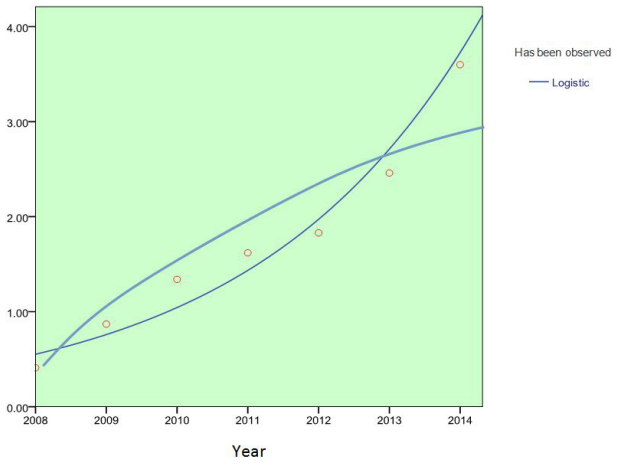

Figure 3. The tendency of forecast

It can be found from Figure 3 that the growth tended to slow, which would not grow indefinitely, so as to get more accurate and reasonable prediction results. On this basis, this statistical data found in a variety of attacks proportion of cyber attacks. In response to network attacks, we should be able to design the main browser configuration How to prevent tampering, network security and software facilities

and the direction of data file corruption. Improve security efficiency. The proportion of attack in the network was found on this basis. In response to network attacks, the main design was made how to prevent and control the browser configuration tampered, damage of data-file and other direction of network security software facilities, which improved the safety and prevention efficiency.The following figure shows the serious attacks in several ways, such as:

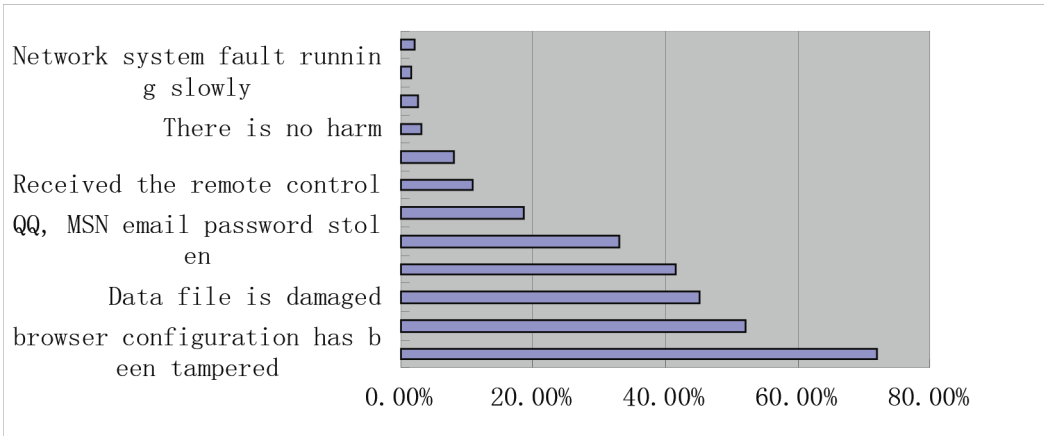

Figure 4. Several ways of network attacks

The development trend of network attacks could be predicted in future.The tools of cyber attacks would be more sophisticated and the speed of cyber attacks would become faster and faster.Meanwhile the automation of cyber attacks would be increasing.

6. Conclusion

This article predicted the development trend of network attacks through the mechanism of analysis. Firstly,the principle of analysis was made and the concept of network attacks was briefly introduced. Secondly,the relevant data of the internet through national database was collected in the part of experimental simulation.And the simulation was made by the modified exponential curve so that the trends and prediction in data could be found eventually.The current forecast was the risk management of network attacks.It is an important method that could be sustained on the network and dynamic network attacks prediction might reflect the network security incidents. Meanwhile it was the way to analyze network attacks seized the main direction of network security software development and guide the direction of cyber attacks which would be controlled within a reasonable number. Thereby the development trend of network attacks was more complicated and the speed of attack was faster and faster.

References

1. Qiaoyun Gu,Yulong Sun(2013) The Model and Application of Network Attack and Defense based on Game Theory. *Technology Research*, 22(1), p.p.52-54.
2. Zichun Wang,Guangqiu Huang(2011)Network Attack and Defense Strategy based on Rough Bias Game.*Computer Application*, 31(3), p.p.784-789.
3. Xiaoxue Yang(2015) Discussion of Network Attack and Defense Experiment Platform based on Cloud Computing Technology. *Wireless Internet Technology*, 3(5), p.p.51-52.
4. Chunliang Li,Yanzheng Wang(2013) Review of Computer Network Attack and Defense Modeling and Simulation. *Computer Simulation*, 30(11), p.p.1-5.
5. Cong Wang,Anqi Zhang(2014) Research on Key Technologies of Network Attack and Defense. *Silicon Valley*, 24(11), p.p.54-55.
6. Yanguang Li(2014) Design and Implementation of Terminal Subsystem of Network Attack Defense Simulation System. *Computer and Modernization*, 27(3), p.p.169-185.
7. Zhongxun Yin,Junhu Zhu(2011)The Design and Implementation of Network Attack and Defense Drilling Platform.*Computer Education*, 36(2), p.p.108-112.
8. Yiyan Kong(2012) Design and Implementation of Network Attack and Defense Simulation Experiment Platform. *Communications Technology*, 45(11), p.p.37-40.
9. Yuan Wang(2010) Design and Implementation of Network Attack and Defense Training Simulation System. *Computer Technology and Development*, 20(7), p.p.172-174.
10. Hongshan Kong(2011)Design and Implementation of Network Attack and Defense Simulation Platform based on SITL.*Computer Application Research* , 28(7), p.p.2715-2718.
11. Wang min, Tang Jun(2010) Network Attack and Prevention Research.*Journal of Network Security Technology and Applications*, 18(11), p.p.17-19.