International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.347-358
http://dx.doi.org/10.14257/ijsia.2016.10.12.28

Network Security Prediction Method Based on Kalman Filtering Fusion Decision Entropy Theory

Liang Huang, Xinhao Chen and Xinsheng Lai

School of Mathematics & Computer Science, Shangrao Normal University, Shangrao, 334001Jiangxi, China
{Liang. Huang} light_h@163.com

Abstract

Network security situation prediction is of great significance for the use of the Internet, and it is the focus of production and life issues. Under the guidance of the model combination forecasting method, In this paper, based on the Kalman filtering model a new method of network security prediction is presented, which is based on the theory of decision entropy. In this method, the Kalman state equation and measurement equation are constructed according to the key attributes of the network security state, and then combined with the decision entropy theory to predict the future state of network security. The experimental results show that the proposed method has high prediction accuracy and is suitable for the state prediction of network security.

Keywords*: network security, decision entropy, Kalman filtering, attack strength*

1. Introduction

With the rapid development of the computer, people's daily life has been inseparable with the network. The computer network has penetrated into all areas of people's lives, including scientific research, education, government, national defense and other fields [1]. In today's society is about to enter the era of cloud computing, the influence of computer network on society will be more and more big. With extensive distribution network system, network system structure is becoming more and more complex, the network is facing more and more attacks and threats faced by the network is becoming more and more serious, various network security incidents and vulnerabilities becomes more and more frequent, including hacker attacks, virus [2-3]. This not only damages the interests of individuals and enterprises, resulting in the loss of people's property, but also reduces the people's trust in the network. Ensuring network information security has become one of the important content of national information strategy [4].

For all kinds of network security issues, the traditional network security technology mainly has Vulnerability Detection Technology, Firewall Technology, Intrusion Detection Technology [5]. Vulnerability Detection Technology has improved the level of network security in a certain extent, but can only detect a certain network vulnerability, the limitation is great, unable to detect the whole network, so the vulnerability detection technology plays a limited role in improving network security [6]. Firewall between the internal and external network built a high wall, increases the degree of security of Intranet Network. However, the role of firewall in network security is limited. First of all, there is no wall can block bypass attacks, there are many intrusion techniques to bypass the firewall; Secondly, the firewall is a defense technology built between the internal and external network, can effectively detect the transmission of data packets between the internal and external networks, but the network attacks are helpless [8]. Therefore, the role of firewall to network security is limited. The development of Intrusion Detection Technology is although relatively mature, due to the intrusion detection equipment of

ISSN: 1738-9976 IJSIA

alarm information is massive, and the presence of false negatives, false positives and so, it could not reflect the true state of the network [9].

Network security situational awareness is a technology that can not only reflect the current network status, but also can predict the future development trend of the network security status. Therefore, the network security situation awareness has gradually become one of the hot spots in the field of network security.

Nguyen developed a Security Situation Assessment and Response Evaluation (SSARE system), the situation assessment software system organically combines the attack detection, situation assessment and response evaluation in a wide area network [10]. By combining the security status of each host, using the hidden Markov model Nisbet described the possibility of security state transitions to determine the risk level of the network [11]. Singh proposed a network security situation assessment method based on asynchronous data stream, the multi-agent structure is adopted to analyze the asynchronous data streams from multiple data sources to obtain the network situation, so as to make the decision [12]. Boubiche proposed a network security risk detection model based on artificial immune system. According to the similarity of the network security situation and the human security, modeled on the human immune system to establish the clonal selection of network system, the use of antibody concentration to calculate the network security situation [13]. Sicari proposed a hierarchical network security situational awareness method based on IDS alarm log, from the service, host, system and other levels to assess the threat situation, and draw a picture of the security situation [14].

On the network security situation assessment and network security situation prediction and other aspects of the study, Cao carried out a comprehensive [15]. In the aspect of information fusion, Chin combines the simple weighted and gray theory, and proposes a new network security situational awareness framework [16]. Scott proposed a data fusion method based on multi level support vector machine, which can be used to solve the data fusion of multi-source heterogeneous sensor [17]. By using the method of model combination or combination of results, we can make full use of the information of time series to achieve the goal of improving the accuracy of prediction. Model combination method is to combine two or more models to form a new model. Fragouli combines grey system theory and Markov prediction theory, puts forward a new kind of Grey Markov model. The model uses grey theory to predict the trend of the future change tendency, using Markov prediction of random factors [18]. Lee combines the grey theory with the artificial immune theory, and puts forward a new gray artificial immune model. Result combination method refers to the combination of two or more prediction results in a loose coupling way, and the appropriate weight should be selected in the combination process [19]. Fernandez combined with the results predicted by Markov and ARMA, and achieved the desired effect [20].

Under the guidance of the model combination forecasting method, this paper combines the Kalman Filtering Method and the Gray Decision Entropy Theory, and presents a new method for the prediction of network security situation. In this method, the Kalman state equation and measurement equation are constructed according to the key attributes of the network security state, and then combined with the decision entropy theory to predict the future state of network security.

2. The Network Security Prediction Model

Classic prediction algorithm based on artificial immune network security situation assessment algorithm to get the value of network security situation to provide the basis for prediction. Because prediction algorithms are generally combined with the influence factors of network security situation, it is the key to find and collect more factors that affect the security situation of network. Therefore the lowest level module in the prediction framework is a data collection module, this module is responsible for collected

by pheromone. Because there are many factors that affect the network security situation, in order to weigh the prediction accuracy and efficiency, this paper uses the gray correlation analysis method to select the key factors which are related to the security situation.

The framework of network security situation prediction model proposed in this paper is shown in Figure 1.

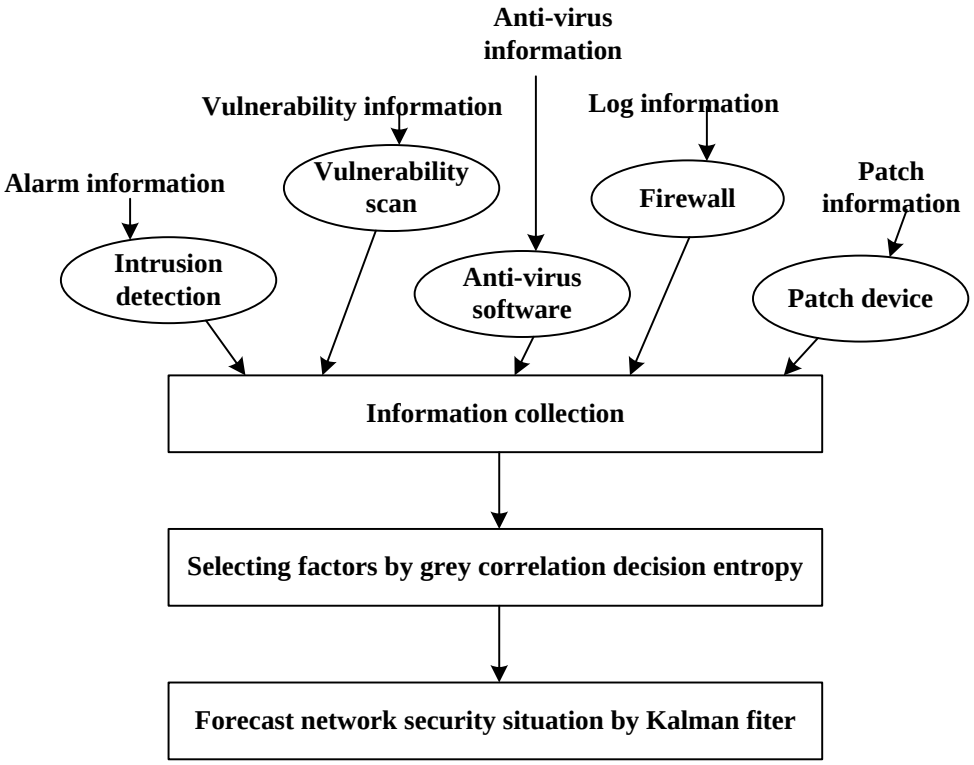


Figure 1. The Structure of Network Security Prediction Model

3. Proposed Network Security Prediction Algorithm

3.1 Kalman Filtering Algorithm for Network Security Situation

Kalman filter can be used to deal with the discrete control process of system. The prediction of network security situation is in line with the characteristics of discrete control switching system, so it can be expressed by the state equation of state and the observation equation of describing the observation.

The equation of state:

$$Y(k+1) = G(k+1,k) \cdot Y(k) + U_1(k) \quad (1)$$

$Y(k)$ represents a state vector of dynamic system at time k; $F(k+1,k)$ represents the transfer of system from the state at time k to the state at time $k+1$, is the state transition matrix; $U_1(k)$ is the process noise vector, represents noise or error generated in the process of transfer.

The observation equation:

$$z(k+1) = B(k) \cdot Y(k+1) + U_2(k) \quad (2)$$

$z(k+1)$ represents the observation vector in the system at time $k+1$; $B(k)$ is the observation vector, the state vector $Y(k+1)$ is changed to be observable after the observation vector description; $U_2(k)$ represents the observation noise at time k.

Therefore ,the principle of network security situation prediction based on Kalman algorithm is: according to the key influencing factor value and network security situation value seeking the state vector $Y(i)$ for $k \geq 1$,when $i > n$ the state vector of the next time period of time n is obtained, and according to the current state vector by observation vector description obtaining the network security situation value in the next time period at the time of n.

3.2The New Information Estimation for Network Security Situation

According to the definition of new information theory, the new information process of a process is not related to the original process, but it is a new information process with Hilbert space. $M(k)$ represents the new information at time k, the new information process of network security situation $z(k)$ is defined as follows:

$$M(k) = z(k) - z_1(k), k = 1,2,\cdots \tag{3}$$

$z_1(k)$ is estimated by the least square method, that is, the estimated value of network security situation $z(k)$.

The new information method has the following properties:

First, new information of time k and all the observed data $z(1)$, $z(2)$, $z(3)$, $\cdots$, before time k respectively orthogonal.

Second, new information process vector $M(1), M(2), M(3), \cdots, M(k)$ orthogonal to each other.

Third, observation data $z(1)$, $z(2)$, $z(3)$, $\cdots$, $z(k)$ and the new information process vector $M(1), M(2), M(3), \cdots, M(k)$ are corresponding one by one.

From the nature of the new information, it is concluded that the physical meaning is the information $M(k)$ of the time k is independent of all the observed data $z(1)$, $z(2)$, $z(3)$, $\cdots$, $z(k)$ before time k that is, the new information process is a stochastic process which is not related to the original process and has the characteristics of white noise. But it can provide the new information about $z(k)$, which can correct the least squares estimator.

3.3 Decision Entropy Fusion Kalman Filtering Network Security Situation Prediction Algorithm

As mentioned above, the network security situation prediction algorithm based on Kalman filter has the advantages of less model parameters, simple calculation and high real-time performance. In this paper, firstly, the key factors affecting the security situation of network are selected by using the method of decision entropy analysis, and then combining the key factors to establish the multi relationship model of network security situation. The following is Kalman prediction algorithm based on decision entropy combined with m factors modeling , the specific steps are as follows:

Step one, let $z(k)$ is the network security situation value of time k, $z(k+1)$ is the network security situation value of the next time period after time k, $y_i(i=1,\cdots,m)$ are the m selected key factors according to the grey entropy correlation degree, $y_i(k)$ is the value of factor i at time k, $y_i(k+1)$ is the value of factor i for a period of time after time k. The regression equation between the key factors and the situation is as follows:

$$\begin{cases} z(k+1) = b_{00}z(k) + b_{01}y_1(k) + \cdots + b_{0m}y_m(k) + \delta_0 \\ y_1(k+1) = b_{10}z(k) + b_{11}y_1(k) + \cdots + b_{1m}y_m(k) + \delta_1 \\ \cdots \\ y_m(k+1) = b_{m0}z(k) + b_{m1}y_1(k) + \cdots + b_{mm}y_m(k) + \delta_m \end{cases} \tag{4}$$

Here, parameter b_{00}, b_{01}, $\cdots$, b_{mm} and δ_0, δ_1, $\cdots$, δ_m are all the regression coefficients ,and can be obtained by the least square method.

$$\begin{bmatrix} \delta_0 & \delta_1 & \cdots & \delta_m \\ b_{00} & b_{10} & \cdots & b_{m0} \\ \vdots & \vdots & & \vdots \\ b_{0m} & b_{1m} & \cdots & b_{mm} \end{bmatrix} = \left[T' \cdot T\right]^{-1} T' \begin{bmatrix} z(2) & y_1(2) & \cdots & y_m(2) \\ z(3) & y_1(3) & \cdots & y_m(3) \\ \vdots & \vdots & & \vdots \\ z(n) & y_1(n) & \cdots & y_m(n) \end{bmatrix} \tag{5}$$

Here, $T = \begin{bmatrix} 1 & z(1) & y_1(1) & \cdots \\ 1 & z(2) & y_1(2) & \cdots \\ \vdots & \vdots & \vdots & \\ 1 & z(n-1) & y_1(n-1) & \cdots \end{bmatrix}$

Step two, according to the formula (4) to establish the Kalman filtering process equation and the observation equation, as follows:

$$\begin{cases} Y(k+1) = G(k) \cdot Y(k) + U_1(k) \\ z(k+1) = B(k) \cdot Y(k+1) + U_2(k) \end{cases} \tag{6}$$

Among them, $Y(k) = \begin{bmatrix} z(k) \\ y_1(k) \\ \vdots \\ y_m(k) \end{bmatrix}$ and $G(k)$ is the state transition matrix, $G(k) = \begin{bmatrix} b_{00} & b_{01} & \cdots & b_{0m} \\ b_{10} & b_{11} & \cdots & b_{1m} \\ \vdots & \vdots & & \vdots \\ b_{m0} & b_{m1} & \cdots & b_{mm} \end{bmatrix}$; $B(k)$ is the observation matrix, $B(k) = [1 \quad 0 \quad \cdots \quad 0]$; $U_1(k)$ is the model noise, $U_1(k) = \begin{bmatrix} \delta_0 \\ \delta_1 \\ \vdots \\ \delta_m \end{bmatrix}$, its covariance matrix is $R(k)$; $U_2(k)$ is the

measurement noise at time k, assuming zero mean white noise, the covariance matrix is $S(k)$

Among them, $B(k)G(k)Y_i(k-1)$ represents the least squares estimate of $z(k)$. The new information can be used to correct the measured value of the state. Recursive calculation is as follows:

$$\begin{aligned} &q(k \mid k-1) = G(k)q(k-1)G'(k) + R(k-1) \\ &kh(k) = \frac{q(k \mid k-1)B'(k)}{B(k)q(k \mid k-1)B'(k) + S(k)} \\ &M(k) = z(k) - B(k)G(k)Y_1(k-1) \\ &Y_1(k) = G(k)Y_1(k-1) + kh(k)M(k) \\ &q(k) = [I - kh(k)B(k)]q(k \mid k-1) \end{aligned} \tag{8}$$

Here, kh represents the Kalman gain coefficient, q is the corresponding covariance of Y. After the end of the cycle, the value of the network security situation is calculated by the formula $z(k) = B(k-1)Y(k)$.

4. Experimental Results and Analysis

4.1. Experimental Scene Configuration

In order to verify the effectiveness of the decision entropy fusion Kalman filtering network security situation prediction method in this paper, the following simulation experiments are carried out. Computer hardware configuration used for simulation experiments are: Core Duo CPU, single core clocked at 2.8GHz, 4G memory; The computer software configuration used in the simulation experiment are: Windows 8 operating system, Matlab programming language, omnet++ software.

Analog configure the same 3 hosts in omnet++ to detect it. Partial data of KDDcup99 is selected as the experimental data source, the use of denial of service attacks land, Smurf, a variety of ports and vulnerabilities scanning attacks nmap and other attacks guess_passwd, Perl, etc, to attack all kinds of virtual servers in the network. The risk parameter of Perl and other risk parameters are set to be 0.4, 0.6, etc., the weight of the three hosts are set to be 0.2, 0.5, 0.3.

4.2 Network Security Situation Calculation

According to the computer artificial immune method to calculate the network security situation. According to the relationship between the changes of antibody concentration in the human immune system and the pathogen invasion intensity, the network security situation is calculated by the antibody concentration. The method can obtain accurate network security situation value. When some attacks continued to attack the network, the corresponding antibody concentration will increase continuously; when the attack strength decreased, then the concentration of antibody decreased, but the rate of decline is less than the rate of the attack strength; when some kind of attack occurs again in a certain period of time, the corresponding antibody concentration is still higher, it shows that the network security situation is higher, the network management should prepare for the defense. According to the concentration of antibody, we can calculate the value of network security situation.

Set m_i is the number of antibodies detected on the host i, m_{ij} is the number of antibodies that can be detected in class j attacks on the host i, θ_j is the risk of class j

attacks, ϑ_i indicates the importance of the host i, y_i is the number of antibodies detected by host i under normal network conditions. Calculated risk values in the following three cases:

Calculation of the risk value for the host:

$$S_h = 1 - \frac{1}{1 + \ln(\vartheta_i |m_i - y_i| + 1)} \tag{9}$$

When subjected to class F attacks, calculation of system risk value:

$$S_j^{sys} = 1 - \frac{1}{1 + \ln(\theta_j \sum \vartheta_i |m_{ij} - y_i| + 1)} \tag{10}$$

The calculation of risk value for the whole system

$$S_{sys} = 1 - \frac{1}{1 + \ln(\sqrt{\sum_i (\vartheta_i |m_i - y_i|)^2 + 1})} \tag{11}$$

Network security situation value can be obtained from the host and the antibody concentration in the system according to the formula (9-11), the higher the value of the network security situation is, the more dangerous the system is. The network security situation value is normalized, and the network security situation value is normalized to 0~1, and the normalized formula is as follows:

$$y_1 = \frac{y - y_{\min}}{y_{\max} - y_{\min}} \tag{12}$$

In the formula, $y_{\max}$ is the maximum value of the situation, $y_{\min}$ is the minimum value of the situation, y is the current situation. After normalization, the situation value is controlled between 0 and 1. In order to reduce the "large number" to eat "fractional" phenomenon, do the same treatment for the network security factors.

After processing, the network security situation, the influencing factors of attack strength, network flow and variable rate of network flux are as shown in table 1.

Table 1. Calculation of network security situation

	Aituation value	Attack strength	Network flow	Variable rate of network flux
Group 1	0.19	0.10228	0.14393	0.1693
Group 2	0.20	0.10459	0.69257	0.0388
Group 3	0.22	0.11546	0.21284	0.6217
Group 4	0.24	0.12371	0.81769	0.0547
Group 5	0.25	0.13244	0.60245	0.2372
Group 6	0.24	0.13469	0.16575	0.6781
Group 7	0.24	0.14689	0.64291	0.0492
……	……	……	……	……
Group 21	0.36	0.14127	0.18433	0.9908

Group 22	0.37	0.14381	0.16214	0.2042
Group 23	0.38	0.15273	0.33091	0.1002
Group 24	0.42	0.16585	0.42384	0.1435
Group 25	0.44	0.17192	0.15299	0.5229
Group 26	0.41	0.14833	0.17750	0.1683
Group 27	0.42	0.14271	0.15653	0.2263
……	……	……	……	……

Part of experimental data of the network security situation, the influence factors of attack strength, network traffic and flow rate are listed in Table 1. The first 10 groups of data, the first 20 groups and 30 groups are respectively carried out grey correlation entropy analysis.

(1) The results of the entropy analysis of the first 10 groups of data

With the network security situation value as the reference sequence, the analysis results are shown in table 2:

Table 2. Decision Entropy Analysis of the First 10 Groups of Data

	Attack strength	Network flow	Variable rate of network flux
Decision entropy	2.3014	2.2851	2.2927
Maximum entropy of information difference		2.4233	
Decision entropy correlation degree	0.8925	0.7536	0.7688

According to the decision entropy judgment criterion, the relationship between the intensity of attack and the situation is the biggest.

(2) The results of grey relational entropy analysis of the first 20 groups of data

With the network security situation value as the reference sequence, the analysis results are shown in table 3:

Table 3. Decision Entropy Analysis of the First 20 Sets of Data

	Attack strength	Network flow	Variable rate of network flux
Decision entropy	2.3358	2.2911	2.3024
Maximum entropy of information difference		2.9157	
Decision entropy correlation degree	0.8887	0.7431	0.7762

According to the decision entropy judgment criterion, the relationship between the intensity of attack and the situation is the biggest.

(3) The results of grey relational entropy analysis of the first 30 groups of data

With the network security situation value as the reference sequence, the analysis results are shown in table 4:

Table 4. Decision Entropy Analysis of the First 30 Sets of Data

	Attack strength	Network flow	Variable rate of network flux
Decision entropy	3.3369	3.2853	3.3106
Maximum entropy of information difference		3.3928	
Decision entropy correlation degree	0.8351	0.7526	0.7498

According to the decision entropy judgment criterion, the relationship between the intensity of attack and the situation is the biggest.

As shown in Table 2, Table 3 and Table 4, the decision entropy of attack strength and situation are all the biggest. In order to reduce the amount of computation, only the key factor which is the most important factor in the experiment is used as a parameter, and based on the key factors, the prediction model of the similar formula (4) is established.

4.3 Network Security Situation Prediction

Take the 30 groups of attack strength data in table 1 as the network security situation of the data, with the help of the decision entropy fusion Kalman filtering network security prediction algorithm for data fitting, the fitting results shown in Figure 2.

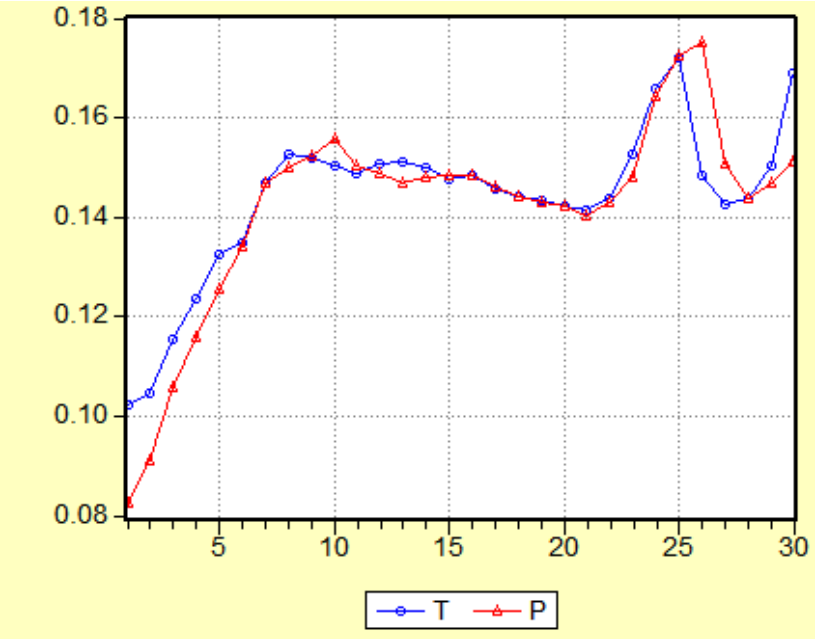


Figure 2. Fitting Curves of the First 30 Groups of Data

Figure 2, T represents the true value of the network security situation, P represents the predictive value of the decision entropy fusion Kalman filtering prediction method. From the curve in Figure 1 can be seen that the two curves achieved a better fit after the 6th values, this state has been sustained to the 25th values. After that, because of the sharp change of the T curve, the P curve and the T curve has a certain deviation, but the trend has been fitted well.

On the basis of the fitting process, further to predict the follow up 20 groups data , and the results are shown in Figure 3.

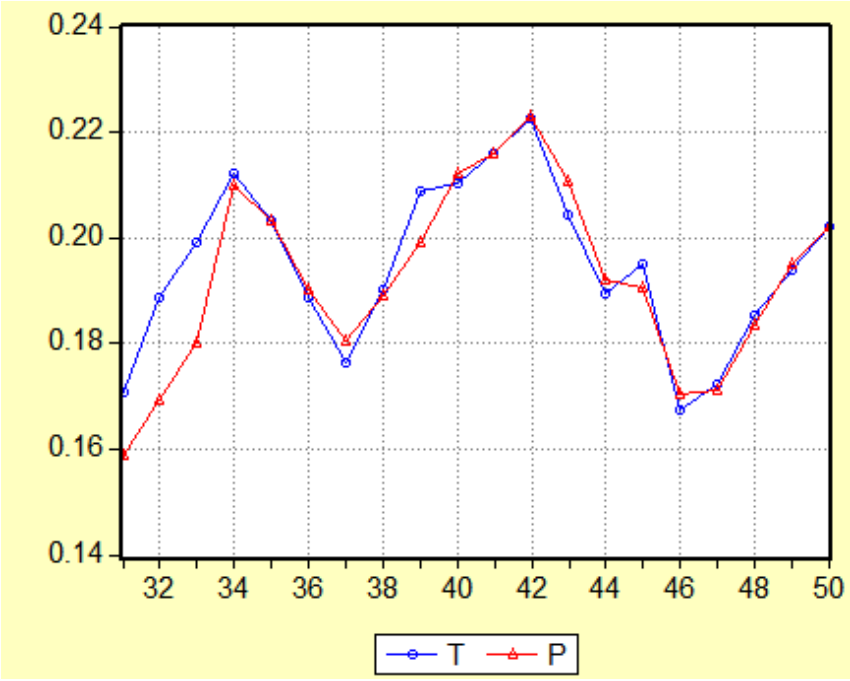


Figure 3. Prediction Curve of the Later 20 Groups of Data

As can be seen from Figure 3, the decision entropy fusion Kalman filtering method accurately predicts the network security situation in the next 20 times, the true value of the network security situation is in agreement with the true value of the network security situation The result shows that: first, after 30 data training, the decision entropy fusion Kalman filtering model has been suitable for the prediction of the experimental conditions; second, prediction method of decision entropy Kalman filter fusion has the best prediction performance and prediction accuracy.

5. Conclusion

A Kalman filtering prediction algorithm based on decision entropy theory is proposed for the prediction of network security situation. In this method, based on the computer artificial immune algorithm, the key characteristics of network security are calculated; secondly, the Kalman state equation and the measurement equation of the network security state are constructed; thirdly, with the help of the new information theory, predict the new state of network security; lastly, the Kalman prediction of network security situation is realized by using the theory of decision entropy. In the experiments, monitoring the three attributes including the attack strength, network flow and variable rate of network flux at the same time, finally selects the attack strength as the features of network security situation, using 30 groups of data to complete the training of prediction model. From the prediction curve of 20 groups data can be seen that, the decision entropy fusion Kalman filtering method has achieved the accurate prediction of network security situation. The work of this paper lays a foundation for the better control of the network security.

Appendix

This paper is a revised and expanded version of a paper entitled [Research on Network Security Prediction Method Based on Kalman Filtering Fusion Decision Entropy Theory] presented at The 9th International Conference on Security Technology (SecTech 2016), 24-26 November 2016，Jeju Island, Korea.

Acknowledgments

This paper is supported by the National Natural Science Foundation of China (No. 61562071) and the Natural Science Foundation of Jiangxi Province (No. 20151BAB207020).

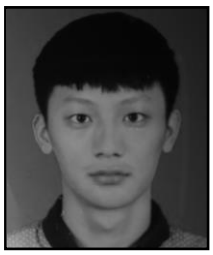
Reference

[1] Ghadi Musab, Laouamer Lamri, Moulahi Tarek. Securing data exchange in wireless multimedia sensor networks: perspectives and challenges[J]. Multimedia Tools and Applications, 75(6): 3425-3451. **(2016)**
[2] Ge Lin, Ji Xinsheng, Jiang Tao. Hierarchical situation evaluation model for network information content security incidents[J]. Journal of Jilin University, 46(2): 556-567. **(2016)**
[3] Kim Daehee, Kang Sangwook, An Sunshin. Secure and efficient time synchronization for border surveillance wireless sensor networks[J]. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 1: 385-401. **(2016)**
[4] Smith Bailey, Caruthers Whitney, Stewart Dalton. Network modeling for security analytics[C]. Proceedings of the 11th Annual Cyber and Information Security Research Conference, **(2016)**
[5] Massonet Philippe, Levin Anna, Celesti Antonio. Security requirements in a federated cloud networking architecture[J]. Communications in Computer and Information Science, 567: 79-88. **(2016)**
[6] Dang Pham Duy, Pittayachawan Siddhi, Bruno Vince. Exploring behavioral information security networks in an organizational context: an empirical case study[J]. Journal of Information Security and Applications, **(2016)**.
[7] Vien Quoc Tuan, Le Tuan Ahh, Nguyen Huan X. A secure network coding based modify-and-forward scheme for cooperative wireless relay networks[C]. IEEE Vehicular Technology Conference, **(2016)**.

[8] Tellez Mauricio, EI Tawab Samy, Heydari Hossain M. Improving the security of wireless sensor networks in an loT environmental monitoring system[C]. IEEE Systems and Information Engineering Design Symposium, 72-77. **(2016)**
[9] Liu Cricket. Actively boosting network security with passive DNS[J]. Network Security, 5: 18-20. **(2016)**
[10] Nguyen Nam Phong, Thanh Tu Lam, Duong Trung Q. Secure communications in cognitive underlay networks over Nakagami-m channel[J]. Physical Communication, **(2015)**
[11] Nisbet Alastair, Woodward Andrew. A comparison study of wireless network security in several Australasian cities and suburbs[J]. Lecture Notes in Computer Science, 9722: 115-127. **(2016)**
[12] Singh Ninni, Saini Hemraj. Formal verification of secure authentication in wireless mesh network[J]. Advances in Intelligent Systems and Computing, 381: 375-388. **(2016)**
[13] Boubiche Sabrina, Boubiche Djallel Eddine, Bilami Azzedine. An outline of data aggregation security in heterogeneous wireless sensor networks[J]. Sensors, 16(4): 111-116. **(2016)**
[14] Sicari Sabrina, Rizzardi Alessandra, Miorandi Daniele. Security policy enforcement for networked smart objects[J]. Computer Networks, 108: 133-147. **(2016)**
[15] Cao Yulin, Wang Xiaoming, He Zaobo. Optimal security strategy for malware propagation in mobile wireless sensor networks[J]. Acta Electronica Sinica, 44(8): 1851-1857. **(2016)**
[16] Chin Tommy, Xiong Kaiqi. MPBSD: A moving target defense approach for base station security in wireless sensor networks[J]. Lecture Notes in Computer Science, 487-498. **(2016)**
[17] Scott Hayward Sandra, Natarajan Sriram, Sezer Sakir. A survey of security in software defined networks [J]. IEEE Communications Surveys and Tutorials, 8(1): 623-654. **(2016)**
[18] Fragouli Christina, Soljanih Emina. Linear network coding multicast: a theoretical minimum and some open problems [J]. Designs Codes and Cryptography, 78(1): 269-310. **(2016)**
[19] Lee Jong Ho. Optimal power allocation for physical layer security in multi-hop DF relay networks [J]. IEEE Transactions on Wireless Communications, 15(1): 28-38. **(2016)**
[20] Fernandez Ruiz Pedro. Mobility and security in a real VANET developed in a heterogeneous networks [J]. Security and Communication Networks, 9(3): 208-219. **(2016)**

Authors

Liang. Huang (1981-), Associate Professor, Master, mainly engaged in Network Safety and Cloud Computing.



Xinhao.Chen (1995-), Student, major in Computer Science and Technology.

XinSheng.Lai (1972-), Professor,Doctor degree, mainly study intelligent Computing.

