Network Security Situation Prediction: A Review and Discussion

Yu-Beng Leau* and Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
11800, Bayan Lepas, Penang, Malaysia
{beng,selva}@nav6.usm.my
http://www.springer.com/lncs

Abstract. The rapid development of information technology exposes peoples life and work to the network. While people are enjoying in sharing their resources in the convenient condition, network security issues have emerged. Instead of considering security of single device in the network, researchers have shown an increased interest to grasp the overall network situation as a big picture in order to create situation awareness which consists of event detection, situation assessment and situation prediction. As the highest level in situation awareness, Network Security Situation Prediction makes quantitative prediction of incoming network security posture based on historical and present security situation information. The purpose is to provide an informational reference to network managers for helping them in formulating and implementing timely preventive measures before the network is under attack. In this paper, the authors group the existing network security situation prediction mechanisms into three major categories and review each model in the aspect of its strengths and limitations. The authors conclude that adaptive Grey Verhulst is more suitable to be used in predicting incoming network security situation.

Keywords: Network Security Situation Prediction, Machine Learning, Markov Model, Grey Theory.

1 Background

Recent years, network penetrates into our life and work with providing convenience services such as information sharing, resource accessing and etc. However, new security challenges are emerging while people are sharing their resources in this convenient condition. An investigation report stated that there have 63,437 security incidents recorded by 50 organizations from various industries around the world in 2013 [1] and it has reached an alarming level and begins to threaten the internet users in their daily activities. In fact, literatures showed that Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have

* National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, 11800, Bayan Lepas, Penang, Malaysia.

R. Intan et al. (Eds.): ICSIIT 2015, CCIS 516, pp. 424–435, 2015.
DOI: 10.1007/978-3-662-46742-8_39

become preferred security defence mechanisms in many companies. They use IDS to analyze the audit log and suspicious packets and IPS to take the appropriate response against the attacks. Unfortunately, in a study done by University of South Wales in 2013 on nine big-brand IPS systems, they found that seven out of them were failed to detect and block 34%-49% of attacks that target vulnerabilities in web-based application [2]. All the remedies only can be taken after the suspicious attempts being detected. It directs the company network to a risky state where they are unable to predict the future security situation of the network.

2 Situation Prediction in Network Security Situation Awareness

Network Security Situation Awareness (NSSA) is first introduced by Tim Bass which adapted from the concept of Situation Awareness introduced by Endsley in 1988 [3]. He claimed that the next generation cyberspace IDS should fuse the network data from multiple or heterogeneous distributed sensors which located at network border and interpret them by decision maker in order to frame NSSA [4]. Basically, NSSA can be divided into three stages which are event detection, current situation assessment and future situation prediction. Event Detection identifies the abnormal and malicious activity in the network and translates them into logical format. Current Situation Assessment is a process to evaluate the security situation of the entire network by using the information obtained from previous stage. Last stage is Future Situation Prediction is aimed to forecast the future network security tendency according to the current and historical network security situation status. It purposes to provide an informational reference to network managers which able to help them in formulating and implementing timely preventive measures before the network is under attack. This changing of network security management from passive to active is tends to reduce the potential harm caused by attacks by improving the emergency response capacity. At present, the existing network security prediction techniques can be grouped into three main categories which are Machine Learning, Markov Model and Grey Theory. In this paper, the authors review each of them in terms of their strengths and limitations.

2.1 Based on Machine Learning

Machine learning is a scientific discipline that applies a computer-based resource to implement learning algorithms which enable computer to recognize pattern automatically and making decision intelligently based on training sample data without explicitly programmed. It detects the patterns in data and adjusts algorithm actions accordingly. The self-learning and adjusting features in its application has been extended to predict network security situation recent years. Researchers begin to apply the concept of Machine Learning such as Neural Network and Support Vector Machine to design their security situation prediction models.

Neural Network. Neural networks represent a kind of computing that simulates the way that the brain performs computations. It is a computer program that attempt to recognize underlying relationship in a set of data by using a process that mimics the way the human brain operates and learn from these identified relationships to predict the future patterns. The field of neural networks was pioneered by McCulloch and Pitts when they introduced the first neural network computing model in 1943 [5]. Basically, a Neural Network consists of four main parts which are processing units, weighted interconnection among processing units, an activation function in input signals to produce or activate the output signal and a learning function that makes the weights for a given input/output pair adjustable. There are three layers in a Neural Network which are input layer, hidden layer and output layer. There are built up of a number of interconnected nodes which contain an activation function. Various patterns from heterogeneous observation are presented to the network through the input layer which communicates to one or more nodes in hidden layer. The actual processing is done in hidden layer with its learning function on weighted connections. This layer links to an output layer where the evaluation of values of output variables allows user to be aware of a situation. The advantages of Neural Network is its high degree of fault tolerance with its variable connection weights matrix between the neurons, ability in self-learning and self-organizing and strong nonlinear mapping and generalization in complex system [6,7]. With these significant features in Neural Network, it has become an ideal tool used to predict the network security situation recently [8].

In 2008, Zongming et. al. proposed a network security situation model by using Back Propagation (BP) Neural Network [9]. This variant of neural network is a feed-forward network with multi-layers and spreading error from back to front while adjusting the parameters [10]. The network requires iterated modification of weight value and threshold value until the convergence error met. To optimize the BP Neural Network, the proposed model applies Particle Swarm Optimization (PSO) to reach global optimization of its weight value and threshold value. The flexibility in modifying these parameters is able to enhance the precision rate but the training to the sample is required. Consequently, over adaptation may occur where the network remembers the trained sample but lacks generalization ability of new sample.

Few years later, a network security situation prediction method based on dynamic BP Neural Network with covariance in 2011 [11] and 2012 [12,13]. In their model, the impact of sample covariance and noise on the network training is considered and the traditional function of error is replaced by the maximum likelihood error function. Through the error analysis, the predicted error value will be obtained and feedback to the prediction model as the training signal for the situation index weights adjustment. The improvement of precision could be achieved by taking previous prediction error into account for next prediction process. Unfortunately, training is required and the success of application is highly depends on the quality of training sample. Furthermore, it is not suitable for small scaled data because less input information will slower the convergence.

Aside from BP Neural Network, there is a kind of neural network called Wavelet Neural Network also had been applied to predict the network security situation [14]. Wavelet Neural Network was firstly introduced by Zhang Qinghua in 1992 [15]. The network uses wavelet analysis as the front-end processor to process the data and supplies the input vector to the neural network in loose combination mode and then replaces this function with activation function of hidden nodes directly in compact combination. With optimizing the model by improved genetic algorithm to encode, compute the fitness and operate the genetic before forecasting the non-linear time series of network security situation, this proposed model has high convergence rate, strong fault tolerance capacity and excellent in self-learning and adaption. But the model limited to certain application which the function to be chosen due to its suitability of the architecture. Moreover, the training is needed to gain the architecture parameters, weight value, dilation coefficient and translation coefficient.

Due to the uncertainly changing security environment in a complex system, a set of more flexible adaptive learning neurons has been introduced into the neural network concept for security situation prediction [6]. The neurons are able to work well in three basic functions in the model. There are positive dissemination of information, inverse dissemination of error and adjusting their parameters by themselves. The model has good performance where the functions can be done in parallel with these independent neurons and only the parameters of attacked neuron need to be revised instead of all neurons in the network. Nevertheless, to establish self-learning neuron is a difficult task and adjusting the steepness of activation function of situation prediction neuron is also challenging.

Notably, all the neural network prediction models are require training algorithm to generate the trained sample for prediction the incoming security situation. In order to simplify the training process, a network security situation prediction method based on small-world Echo State Networks has been suggested in 2013 [16]. Generally, Echo State Networks was initiated by H. Jaeger of Germany Jacobs University in 2001 [17]. A dynamic reservoir which is constructed by numerous neurons was allocated in the hidden layer of the network. The training algorithm in the model is simple and it is suitable to be used in approximating nonlinear dynamic system. However, adequate training data as input is needed and the output weight in the model is difficult to be prepared.

Support Vector Machine. Support Vector Machine (SVM) was proposed by Vapnik et al. in 1992 [18] and widely used in classification and regression. It maps the input space vector to a high-dimensional feature space. In other words, the nonlinear regression problem in low dimensional feature space has been converted to linear regression in high-dimensional feature space.

Compared with Neural Network, SVM has quick convergence rate and strong ability to resists a fitting [7]. The concept has been adopted by Xiaorong Cheng and the team to design their network security situation prediction model in 2012 [19]. In order to avoid the transformation of high-dimensional hyperplane in SVM, the kernel functions were introduced. With given training set, the model chooses the appropriate precision parameter and kernel function. Then

using these parameters, the model tries to solve the optimization problem. The strength of this SVM prediction model is relatively easy to train and seek the overall optimally. Furthermore, the model is also able to control the complexity and error of the classification. Unfortunately, adequate training sets are needed to gain the optimized parameters. In addition, the parameters of punishment factor and kernel functions are hardly to be determined in this proposed model. Blindness of parameters selection of SVM training process is also a main consideration when using it in prediction [7].

2.2 Based on Markov Model

Markov Model is a stochastic approach to describe the transitions from one state to another with its probabilities associated with various state-changes [20]. In a Markov Model, it consists of a list of the possible states of that system, the possible transition paths between those states and the probabilities of those transitions. The applications for machine learning is broad which cover from speech and handwriting recognition, medical diagnosis, credit card fraud detection as well as stock market and currency rate prediction.

In 2010, Dapeng Man et. al. has proposed a combination model for security situation prediction which combined with Autoregressive-Moving-Average (ARMA) model and Markov model [21]. They claimed that precision can be improved with fully utilizing each prediction method. In their model, the previous data will be used as input for both models separately to obtain its prediction value. The previous error of each model will be relatively calculated in order to obtain the weight for prediction model. Then the prediction value from combined model is expressed as

$$\sum_{n=1}^{N} w_n f_{nt} = w_1 f_{1t} + w_2 f_{2t} + ... + w_n f_{nt} \tag{1}$$

where f_{nt} represents the combined predicted value of the n kind of prediction models at time t and w_n represents the weight of the n^{th} prediction model. Compared with single prediction model, the proposed model has achieved higher precision rate. But the difficulties in selecting appropriate parameters in each model will affect the model performance. Moreover, their claim is arguable while high precision rate is not guaranteed if the combination is more than two prediction methods or from other different methods. In addition, although taking previous error into next prediction process is encouraged, but it is unable to improve significantly the precision in the next prediction.

Instead of designing combination model, GuangCai Kuang et. al. has presented a fuzzy prediction method of network security situation based on Markov [20]. In the proposed model, the correlation of network security is represented as Markov state transition matrix. With the current status of security situation, the improved linear weighted Zadeh formula is applied and membership effect matrix is used to calculate security situation values of predicted network. This

model has high precision rate with taking into account the impacts and influences of vulnerability but the training dataset is needed in constructing reference Markov matrix. Besides this, the assessment and prediction value in this model are keep increasing and they will reach the maximum point if the total length of time is big. Furthermore, determining the probability of all possible states and transitions subjectively especially in a complex network is a challenge.

A similar prediction model as previous work which based on fuzzy Markov Chain also been presented in 2014 [22]. The model utilizes historical data of safe behavior with the level of threat to forecast the network situation. After calculating threat value of particular period by using text categorization and threat level division technique, a set of fuzzy states with its membership degree has been built. Then the fuzzy state transition frequency has been calculated. Although the researcher claimed there is a good predictive performance for this proposed method, but assigning threat values according to five levels of attack without considering the various t level of the attack towards different devices is inappropriate. Additionally, the training is needed to derive the most suitable membership degree equation in different system. Another limitation of the model is it unable to handle unknown threat since it is based on the classification of known threats.

2.3 Based on Grey Theory

Grey Theory was initiated by Deng Ju-Long in 1982 in China [23]. It is used to predict from the grey system which lack of information. In this context, grey means poor, small-scaled, incomplete, uncertain data [24], which means the system information is partly know and partly unknown. With this noticeable feature, grey theory is widely used in various system to provide better prediction in short-term forecasting by capturing dominance at small sample. Basically, grey theory is applied to build a dynamic model with a group of differential equations [25,26], which is called Grey Model (GM) by using the least 4 data to replace difference modeling in vast quantities of data [24]. It does not need many data on the particular probability distribution. As superiority to statistical models, the model is able to prevail over the weakness of probability [27] and discovered the relationship among the limited and confused data [28]. It utilizes the sequence generated by Accumulated Generating Operation (AGO) to weaken the randomness of the original sequence [28]. This makes the process to find out the variation regularity in the sequence easier and use this regularity to forecast [29]

Grey Model (1,1). In grey theory, a First-order One-variable grey model (GM(1,1)) is the most widely used grey model. The modeling algorithm is described below:

Step I: Assume that the original raw data series $x^{(0)}$ with n samples is expressed as:

$$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), ..., x^{(0)}(n)\}, n \geqslant 4 \tag{2}$$

where $X^{(0)}$ is a non-negative sequence and n is the sample size of the data.

Step II: A new series $X^{(1)}$ is generated by applying Accumulating Generation Operation (AGO)

$$X^{(1)} = \{x^{(1)}(1), x^{(1)}(2), ..., x^{(1)}(n)\}, n \geqslant 4 \tag{3}$$

where

$$x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i), k = 1, 2, 3, ..., n \tag{4}$$

Step III: A series $Z^{(1)}$ is generated by applying the MEAN operation to $X^{(1)}$

$$Z^{(1)} = \{z^{(1)}(1), z^{(1)}(2), ..., z^{(1)}(n)\}, \tag{5}$$

where $z^{(1)(k)}$ is the mean value of adjacent data such as

$$z^{(1)}(k) = 0.5x^{(1)}(k) + 0.5x^{(1)}(k-1), k = 2, 3, ..., n \tag{6}$$

The least square estimate sequence of the grey difference equation of GM(1,1) is defined as follows [24]:

$$x^{(0)}(k) + az^{(1)}(k) = b \tag{7}$$

and its whitening equation is

$$\frac{\partial x^{(1)}(k)}{\partial t} + ax^{(1)}(k) = b \tag{8}$$

in which a and b are the interim parameters. The parameter matrixes are

$$\hat{a} = \begin{bmatrix} a \\ b \end{bmatrix} = (B^T B)^{-1} B^T Y \tag{9}$$

where $$B = \begin{bmatrix} -z^{(1)}(2) & 1 \\ -z^{(1)}(3) & 1 \\ \vdots & \vdots \\ -z^{(1)}(n) & 1 \end{bmatrix} \tag{10}$$ $$Y = \begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix} \tag{11}$$

According to equation (7), the solution of $x^{(1)}(t)$ at time k is

$$x_p{}^{(0)}(k+1) = \left[x^{(0)}(1) - \frac{b}{a}\right] e^{-ak} + \frac{b}{a} \tag{12}$$

Step IV: To obtained the predicted value of the primitive data at time *(k+1)*, the Inverse Accumulating Generation Operation (IAGO) is used to establish the following grey model.

$$x_p{}^{(0)}(k+1) = \left[x^{(0)}(1) - \frac{b}{a}\right] e^{-ak}(1 - e^{a}) \tag{13}$$

In 2006, Lai Jibao claimed that the grey theory is suitable for building the prediction model and able to ensure its prediction. Hence, he first applied grey

theory in constructing the network security situation prediction model based on grey theory which is built by past and current network security situation [30]. After three years, a dynamic prediction model has been presented by Fengli Zhang. He proposed to estimate the overall network security situation by applying grey forecast model. By using classical GM(1,1), the models calculates the future value of situation and computes the absolute difference and relative difference between the forecast and real values. If the square sum of remnant difference is very large which represent less precision in forecast value, the model will modify the value by referring to the remnant difference [31]. Without any training on the input data, both of the proposed GM(1,1) models are working well with linear situation but not suitable for non-stationary random sequence.

To overcome the limitation of GM(1,1) model, Li Juan has proposed a hybrid prediction model which can be used in high fluctuation system in 2009. They combined unbiased Grey Theory and Markov forecasting theory to predict network security dynamic situation. Firstly, unbiased GM(1,1) model is used to obtain the forecasting value. Then by adjusting the result of unbiased GM(1,1), Markov model is used to determine the state, calculate the evaluation value and construct the transition probability matrix. The median of gray interval is used as forewarning value after the tendency of the system condition developing has been decided [32]. Unfortunately, there is a challenge to determine subjectively the probability of state. On the other side, Liu Nian also suggested another hybrid model to forecast the network security situation in the same year. He applied the combination of Grey Theory and Markov Theory to predict the incoming network security situation which is high randomness, uncertainty and fluctuation. During the process, classical GM(1,1) model is used to predict the situation data and find out its changing trend. Then, Markov Theory is employed to modify the error in the model in order to improve the prediction accuracy of network security situation changing trend [33]. Both of these hybrid models require training value to divide the original data into different states and modify the error in the model respectively. In order to improve the precision rate of GM(1,1) model, Rongzhen Fan has included a three-phase grey residual error correction model in GM(1,1) model. The proposed correction model used concept of GM(1,1) to calculate difference of the predict value and original accumulate value in particular time-frame [34]. The good thing of his work is taking into consideration the residual error for predicted value. But in the same time, high processing power is needed for recurrent residual error correction process.

In fact, the conventional GM(1,1) model is only suitable for the prediction with strong exponential law and it only able to depict the monotone variation [35]. The model is imperfect when the series increases in the curve with S type or the increment of series is in the saturation stage [36]. These limitations have sparked the argument on suitability of classical GM(1,1) to be used to predict accurately the future status of network security situation which has variation characteristics [16]. Instead of depending on linear differential equation in GM(1,1), a variant of grey model called Grey Verhulst model has been used in predicting the non-linear series.

Grey Verhulst. The Verhulst model was first introduced by a German biologist, Pierre Franois Verhulst in 1837 to describe the increasing process like S-curve which has a saturation region, namely the process is increasing slowly at initial stage, then speed-up and finally grow slowly or stop growing [37]. Same as GM(1,1), Grey Verhulst model has superiority in small sample. The Grey Verhulst model can be defined as follows [38]):

The equations (1) to (5) in GM(1,1) are same in Grey Verhulst Model. To predict the S type curve, the model is applying a non-linear difference equation as below

$$x^{(0)}(k) + az^{(1)}(k) = b(z^{(1)}(k))^2 \tag{14}$$

and its whitening equation is

$$\frac{\partial x^{(1)}(k)}{\partial t} + ax^{(1)}(k) = b(x^{(1)}(k))^2 \tag{15}$$

in which a is defined as the development coefficient and b is grey input. As equation (9), the parameter matrixes B and Y are

$$B = \begin{bmatrix} -z^{(1)}(2) & (z^1(2))^2 \\ -z^{(1)}(3) & (z^1(3))^2 \\ \vdots & \vdots \\ -z^{(1)}(n) & (z^1(n))^2 \end{bmatrix} \tag{16}$$

$$Y = \begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix} \tag{17}$$

By calculating equation (15), the solution of $x^{(1)}(t)$ at time k is

$$x_p{}^{(1)}(k+1) = \frac{ax^{(0)}(1)}{bx^0(1) + (a - bx^{(0)}(1))e^{ak}} \tag{18}$$

In the equation (19), $x^{(0)}(1) = x^{(1)}(1)$. It is assumed that the n-dimension data sequence is selected to fit the model. The fitted model can be used to predict the future value as

$$x_p{}^{(0)}(k+1) = x_p{}^{(1)}(k+1) - x_p{}^{(1)}(k), k \geq n \tag{19}$$

where

$$x_p{}^{(0)}(1), x_p{}^{(0)}(2), x_p{}^{(0)}(3), ..., x_p{}^{(0)}(n) \tag{20}$$

are called Grey Verhulst fitted sequence, while

$$x_p{}^{(0)}(n+1), x_p{}^{(0)}(n+2), x_p{}^{(0)}(n+3), ..., x_p{}^{(0)}(n+t) \tag{21}$$

are called Grey Verhulst predicted values.

In Grey Verhulst model, a and b are the key parameters to guarantee the precision of the model. The values of them can be obtained by applying least square method into the generation sequences $Z^{(1)}$ as equation (5). This feature is only allow the Grey Verhulst model to generate appropriate parameters in the small time interval and the AGO curve varies smoothly.

In 2010, Hu Wei found out that the generated sequence will make the prediction generate the advance or delay error which will depress the model precision. Thus, he first adopts the adaptive determination of the grey parameters to Grey Verhulst model to guarantee the precision. He made the assumption of the function of AGO curve as

$$X^{(1)}(t) = \frac{1}{\alpha e^{\beta t}} \tag{22}$$

and calculating the area below the curve by integration method [29]. His model is only applicable to estimate the curve trend accurately if the S-type risk growing situation is matches to the AGO curve function. Furthermore, the model is also limited to a single-peak situation variation instead of multiple-peaks.

3 Conclusion

In this study, the authors conclude that each group of prediction mechanism has its strengths and limitations. Machine Learning is excellent in self-learning and self-adaption and able to provide high convergence rate as well as strong fault tolerance capacity. But the adequate training data is required to gain the parameters and it is difficult to establish the neurons with self-learning and adaption capabilities. For Markov Model, although it is able to perform in various time series prediction, a set of training data is still needed. Moreover, all possible states and its transitions especially in a complex network are hardly to identify. Meanwhile, Grey Theory can provide better prediction in short-term forecasting with small sample data without any training required. Even though GM(1,1) is only limited to linear time series prediction and the generation sequence with mean is only suitable for small time interval, but adaptive Grey Verhulst is surpassing with its adjustable generation sequence and non-linear S-curve time series prediction. Considering the chronology of intrusion attack, Grey Verhulst is more suitable to predict the incoming network security situation with its remarkable features.

Acknowledgement. The authors would like to thank the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia for supporting this research project.

References

1. 2014 Data Breach Investigations Report. pp. 1-60. United States: Verizon Enterprise (2014)
2. Xynos, K., Sutherland, L., Blyth, A.: Effectiveness of Blocking Evasions in Intrusion Prevention System. University of South Wales, pp. 1–6 (2013)
3. Endsley, M.R.: Situation Awareness Global Assessment Technique (SAGAT). In: 1988 National Aerospace and Electronics Conference, pp. 789–795. IEEE Press (1998)
4. Bass, T.: Intrusion Detection Systems and Multisensor Data Fusion. Communications of the ACM 43(4), 99–105 (2000)

5. McCulloch, W.S., Pitts, W.: A Logical Calculus of the Ideas Immanent in Nervous Activity. The Bulletin of Mathematical Biophysics 5(4), 115–133 (1943)
6. Li, J., Dong, C.: Research on Network Security Situation Prediction-Oriented Adaptive Learning Neuron. In: Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), pp. 483–485. IEEE Press (2010)
7. Wei, X., Jiang, X.: Comprehensive Analysis of Network Security Situational Awareness Methods and Models. In: 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), pp. 176–179. IEEE Press (2013)
8. Xi, R., Jin, S., Yun, X., Zhang, Y.: CNSSA: A Comprehensive Network Security Situation Awareness System. In: IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 482–487. IEEE Press (2011)
9. Lin, Z., Chen, G., Guo, W., Liu, Y.H.: PSO-BPNN-based Prediction of Network Security Situation. In: 3rd International Conference on Innovative Computing Information and Control, pp. 37–41. IEEE Press (2008)
10. Zhang, Y., Jin, S., Cui, X., Yin, X., Pang, Y.: Network Security Situation Prediction Based on BP and RBF Neural Network. In: Yuan, Y., Wu, X., Lu, Y. (eds.) ISCTCS 2012. CCIS, vol. 320, pp. 659–665. Springer, Heidelberg (2013)
11. Tang, C., Xie, Y., Qiang, B., Wang, X., Zhang, R.: Security Situation Prediction Based on Dynamic BP Neural with Covariance. Procedia Engineering 15, 3313–3317 (2011)
12. Tang, C., Wang, X., Zhang, R., Xie, Y.: Modeling and Analysis of Network Security Situation Prediction Based on Covariance Likelihood Neural. In: Huang, D.-S., Gan, Y., Premaratne, P., Han, K. (eds.) ICIC 2011. LNCS, vol. 6840, pp. 71–78. Springer, Heidelberg (2012)
13. Zheng, R., Zhang, D., Wu, Q., Zhang, M., Yang, C.: A Strategy of Network Security Situation Autonomic Awareness. In: Lei, J., Wang, F.L., Li, M., Luo, Y. (eds.) NCIS 2012. CCIS, vol. 345, pp. 632–639. Springer, Heidelberg (2012)
14. Lai, J.B., Wang, H.Q., Liu, X.W., Liang, Y., Zheng, R.J., Zhao, G.S.: WNN-based Network Security Situation Quantitative Prediction Method and Its Optimization. Journal of Computer Science and Technology 23(2), 222–230 (2008)
15. Zhang, Q., Benveniste, A.: Wavelet Networks. IEEE Transactions on Neural Networks 3(6), 889–898 (1992)
16. Chen, F., Shen, Y., Zhang, G., Liu, X.: The Network Security Situation Predicting Technology Based on the Small-world Echo State Network. In: 4th IEEE International Conference on Software Engineering and Service Science, pp. 377–380. IEEE Press (2013)
17. Jaeger, H.: Tutorial on Training Recurrent Neural Networks, Covering BPPT, RTRL, EKF and the" Echo State Network" Approach. GMD-Forschungszentrum Informationstechnik (2002)
18. Cortes, C., Vapnik, V.: Support-vector Networks. Machine Learning 20(3), 273–297 (1995)
19. Cheng, X., Lang, S.: Research on Network Security Situation Assessment and Prediction. In: Fourth International Conference on Computational and Information Sciences, pp. 864–867. IEEE Press (2012)
20. GuangCai, K., XiaoFeng, W., LiRu, Y.: A Fuzzy Forecast Method for Network Security Situation Based on Markov. In: International Conference on Computer Science and Information Processing, pp. 785–789 (2012)

21. Man, D., Wang, Y., Wu, Y., Wang, W.: A Combined Prediction Method for Network Security Situation. In: International Conference on Computational Intelligence and Software Engineering, pp. 1–4. IEEE Press (2010)
22. Wang, Y., Li, W., Liu, Y.: A Forecast Method for Network Security Situation Based on Fuzzy Markov Chain. In: Huang, Y.-M., Chao, H.-C., Deng, D.-J. (eds.) Advanced Technologies, Embedded and Multimedia for Human-centric Computing. LNEE, vol. 260, pp. 953–962. Springer, Heidelberg (2014)
23. Ju Long, D.: Control Problems of Grey Systems. Systems & Control Letters 1(5), 288–294 (1982)
24. Deng, J.-L.: Introduction to Grey System Theory. The Journal of Grey System 1(1), 1–24 (1989)
25. Deng, J.-L.: Modelling of the GM model of Grey Systems, pp. 40–53 (1988)
26. Deng, J.-L.: Properties of the Grey Forecasting Model of GM(1,1). Grey System, pp. 79–90 (1988)
27. Liu, S., Forrest, J., Yang, Y.: A Brief Introduction to Grey Systems Theory. Grey Systems: Theory and Application 2(2), 89–104 (2012)
28. Kordnoori, S., Mostafaei, H., Kordnoori, S.: The Application of Fourier Residual Grey Verhulst and Grey Markov Model in Analyzing the Global ICT Development. Hyperion Economic Journal 2(1), 50–60 (2014)
29. Hu, W., Li, J.-H., Chen, X.-Z., Jiang, X.-H.: Network Security Situation Prediction Based on Improved Adaptive Grey Verhulst Model. Journal of Shanghai Jiaotong University (Science) 15, 408–413 (2010)
30. Jibao, L., Huiqiang, W., Liang, Z.: Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory. In: International Conference on Computational Intelligence and Security, pp. 1545–1548. IEEE Press (2006)
31. Zhang, F., Wang, J., Qin, Z.: Using Gray Model for the Evaluation Index and Forecast of Network Security Situation. In: International Conference on Communications, Circuits and Systems, pp. 309–313. IEEE Press (2009)
32. Juan, L., Tao, L., Gang, L.: A Network Security Dynamic Situation Forecasting Method. In: International Forum on Information Technology and Applications, pp. 115–118. IEEE Press (2009)
33. Diangang, W., Xuemei, H., Sunjun, L., Kui, Z.: Research on Network Security Situation Awareness Technology Based on Artificial Immunity System. In: International Forum on Information Technology and Applications, pp. 472–475. IEEE Press (2009)
34. Rongzhen, F., Mingkuai, Z.: Network Security Awareness and Tracking Method by GT. Journal of Computational Information Systems 9(3), 1043–1050 (2013)
35. Liu, S.F., Lin, Y.: An Introduction to Grey Systems Theory. IIGSS Academic Publisher, Grove City (1998)
36. Guo, Z., Song, X., Ye, J.: A Verhulst Model on Time Series Error Corrected for Port Throughput Forecasting. Journal of the Eastern Asia society for Transportation studies 6, 881–891 (2005)
37. Wang, Z., Dang, Y., Wang, Y.: A New Grey Verhulst Model and Its Application. In: International Conference on Grey Systems and Intelligent Services, pp. 571–574. IEEE Press (2007)
38. Wen, K.-L., Huang, Y.-F.: The Development of Grey Verhulst Toolbox and the Analysis of Population Saturation State in Taiwan-Fukien. In: International Conference on Systems, Man and Cybernetics, pp. 5007–5012. IEEE Press (2004)