Send Orders for Reprints to reprints@benthamscience.ae

Research on the Evaluation and Prediction Model of Network Security Situation Based on Multi Sensor Data Fusion

Zheng Yiping* and Liu Fang

Xidian University, Shanxi, Xi'an 710126, China

Abstract: Along with the unceasing expansion of computer network scale, sharp growth of network user quantity, and various kinds of network security incidents also emerged in an endless stream, so computer networking faces severe challenges. At present, the research on network security is mainly concentrated on the research on intrusion detection method, but with the network's complexity and uncertainty increases, the research on network security situation is bound to become a trend. Research on network security situation warrants that the security state should be integrated into various safety factors for the whole dynamic response of the whole network, and to make timely and accurate prediction of the state of safety. This paper establishes the evaluation and prediction model of computer network security situation. After analyzing and summarizing the existing methods of some network security situation evaluation and prediction algorithm, this paper proposes a model for network security situation assessment and prediction of the trend of multi sensor data fusion.

Keywords: Information system, Security situation, Situation assessment, Situation prediction.

1. INTRODUCTION

In the traditional network management mechanism in the network, each sensor of the work is independent of each other. Since there is no effective information extraction and fusion, so the overall state of the network is not reflected, not only they failed to achieve the effect of strengthening management, but also increased the administrator's burden, and need analysis results in the detection of multiple sensors [1-5]. In the complex network environment network management must be able to collect the data of multiple sensors, collect the uncertain information standardization processing, integrate, evaluate, make the evaluation results in visual manner, and for auxiliary network managers to quickly make a decision; the problem of network security thus appears to be repaired [6]. Therefore, the concept of network security situation emerged as the time's requirement, and it can effectively integrate information of multiple sensors, the macro reaction of the current operation state of the whole network [7, 8].

Research on network security situation is mainly divided into two stages: prediction of network security situation assessment and security situation. Network security situation assessment refers to a certain scale under the network environment, collected from multiple sensors which can affect various data and the current state of the network, obtain, and understand certain mathematical operation, so as to get the current network operation state; the results are displayed [9]. Network security situation prediction, is mainly the use of past and present network security situation prediction of future value [10, 11]. The two stages are not studied in isolation, since every stage of the results plays a crucial role in the final decision.

At present, due to the rapid expansion of the scale of the Internet, network applications are vulnerable to the network attack behavior. As the impact of the harm will expand, so the importance of the study of network security continues to be apparent. Previous research focused on network security situation awareness and sketched the basic research framework: prediction of four modules of data acquisition, situational understanding, situation assessment, and trends. But those studies mostly lack overall consideration on the network security elements, used single data source; the results of the assessment is not comprehensive enough; and mostly using hierarchical weighted analysis method, with a certain degree of subjectivity; and also need practical experience. Keeping in view the above problems, this paper puts forward a set of network security situations assessment based on the analysis, considering the network traffic information, IDS alarm information, host log information, using the theory of set pair analysis of multisensor information fusion safety situation of each node, security situation combined with the weight of a plurality of nodes to get the whole network, finally draw the situational network security graph.

2. RELATED THEORY

2.1. The Research Status of Network Security

The concept of network security situation awareness (Cyberspace Situation Awareness) was first introduced in 1999 by Tim Bass [11, 12]. The so-called network security situational awareness refers to large-scale network environment, the use of multiple sensors to collect various data

*Address correspondence to this author at the Xidian University, Shanxi, Xi'an710126, China; Tel: +8618289856582;
E-mail: zhengyiping65@126.com

1874-4443/15

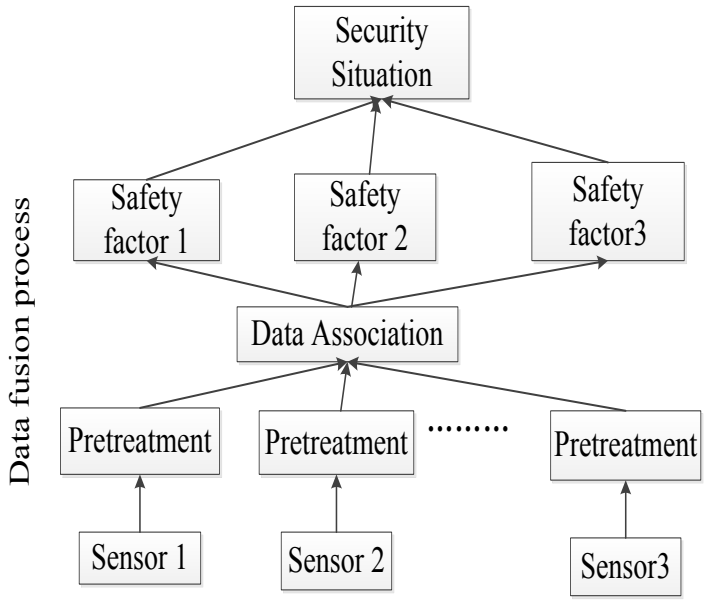

Fig. (1). Network security situation based on multi sensor data fusion model.

whose security state can affect the network, then the original data analysis, understanding, fusion, get the current situation of network security at the same time, and the safety state of the future network prediction. The ultimate goal of network security situation awareness is the results of NSSA that are applied to the network management [13], in the complicated network environment, for collecting multiple sensor data, and the uncertainty evaluation of information fusion and local characteristics. Therefore, a comprehensive network security is required to reflect the overall state of the network, for network administrators to provide quick support to make a decision. Bass did not implement the prototype system of concrete.

At present, research on network security situation is mainly concentrated in the aspects of situation assessment and situation visualization of [14]. Domestic and foreign experts and scholars according to different evaluation algorithms, and model predictive algorithms, designed and implemented a variety of network security situation awareness models [15, 16].

2.2. The Key Technology of Network Security Situation Awareness

At present, there are various network applications, which make the network structure complicated, and the network traffic is also very big, with complexity and a certain amount of redundant network, largely exist due to original data collection. So, our research should consider the network security situation involving many key technologies. We mainly introduced three technologies of network security situation awareness to apply to the data mining technology: technology forecast, situation evaluation and situation of technology.

Network security situation based on multi sensor data fusion model is shown in Fig. (**1**).

Parameter generation Opg: The algorithm first choose groups G and GT of prime order p such that an admissible pairing e:

$$G \times G \rightarrow G_T \tag{1}$$

can be constructed and choose a random generator

$$g \in G, k+1 \tag{2}$$

additional random generators

$$u', u_1, u_2, \ldots, u_k \in G. \tag{3}$$

Key genetation Okg: Pick random

$$\alpha \leftarrow {}_R Z_p \tag{4}$$

and set

$$A \leftarrow e(g,g)^{\alpha} \tag{5}$$

The public key pk is

$$A \in G_T \tag{6}$$

The private key s_k is θ. Signing OSign: On inputs ski,

$$n=(n_1, n_2, \ldots, n_k) \in \{0,1\}^k \tag{7}$$

$$L = (p k_1, \ldots, p k_{i-1}) \tag{8}$$

and an OMS-so-far θ' ,the algorithm first verifies that OVf

$$(L, m, \theta') = \text{valid} \tag{9}$$

as defined below and if not, outputs $\perp$ and halt. For a first signer, θ' is defined as (I_G , I_G , I_G). Then parse θ' as

$$(S', R', T') \in G3 \tag{10}$$

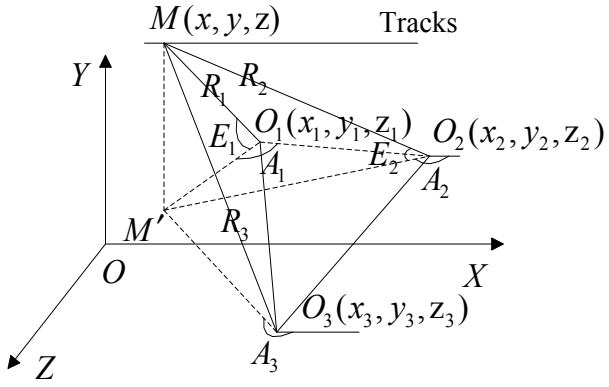

Fig. (2). The coordinate O-XYZ cartesian coordinate system.

Choose random

$$r_i, t_i \in Z_p \tag{11}$$

3. NETWORK SECURITY SITUATION ASSESSMENT MODEL

3.1. Positioning Netting Optimization Mathematical Model

The number of track measuring instrument in the test set is 3, coordinate O- XYZ Cartesian coordinate system is shown in Fig. (**2**).

Position three coordinates measuring instrument; the measured dynamic target coordinates location for M (x, y, Z) for plane shadow M formed in three stations (1,2,3); three measurement target measuring instrument M, the azimuth angle (pitch for the goal of measuring the obtained angle E(1,2,3) for measuring instrument to the distance measured target M. Track measuring slant range, azimuth and elevation data of Ei that can use the position parameter X, Y, Z in rectangular coordinates are expressed as:

$$R_i = [(X - X_i)^2 + (Y - Y_i)^2 + (Z - Z_i)^2]^{1/2} \tag{12}$$

$$A_i = \begin{cases} 0^\circ + \arcsin[(Z - Z_i)/L_i] & X - X_i \geq 0 \\ 180^\circ - \arcsin[(Z - Z_i)/L_i] & X - X_i \geq 0 \end{cases}$$

$$E_i = \arctan[(Y - Y_i)/L_i] \tag{13}$$

In the formula, Xi, Yi and Zi represent the i track of the Cartesian coordinate measuring instrument. The nonlinear equations are converted into linear equations after Taylor launched position parameters that are calculated using the least squares estimation of target trajectory.

$$\Delta L = A\Delta X + \xi \tag{14}$$

A measurement data track measuring instrument based on the target trajectory parameters X, Y, Z of the partial derivative matrix Jacobi is:

That is:

$$A^T = \begin{bmatrix} \frac{\partial R_1}{\partial X} & \frac{\partial A_1}{\partial X} & \frac{\partial E_1}{\partial X} & \frac{\partial R_2}{\partial X} & \frac{\partial A_2}{\partial X} & \frac{\partial E_2}{\partial X} & \frac{\partial R_3}{\partial X} & \frac{\partial A_3}{\partial X} & \frac{\partial E_3}{\partial X} \\ \frac{\partial R_1}{\partial Y} & \frac{\partial A_1}{\partial Y} & \frac{\partial E_1}{\partial Y} & \frac{\partial R_2}{\partial Y} & \frac{\partial A_2}{\partial Y} & \frac{\partial E_2}{\partial Y} & \frac{\partial R_3}{\partial Y} & \frac{\partial A_3}{\partial Y} & \frac{\partial E_3}{\partial Y} \\ \frac{\partial R_1}{\partial Z} & \frac{\partial A_1}{\partial Z} & \frac{\partial E_1}{\partial Z} & \frac{\partial R_2}{\partial Z} & \frac{\partial A_2}{\partial Z} & \frac{\partial E_2}{\partial Z} & \frac{\partial R_3}{\partial Z} & \frac{\partial A_3}{\partial Z} & \frac{\partial E_3}{\partial Z} \end{bmatrix} \tag{15}$$

3.2. Method Based on Pattern Recognition

Pattern recognition theory developed in the 60's, which has attracted wide attention in many academic fields, promoting the development of artificial intelligence theory. Usually, using time and space information observation specific things called patterns are formed, and then the pattern recognition will map the information as an abstract concept.

Using K-NN to calculate an integer K needs experiment based on an already sorted training set, *i.e.* a calculation method of shortest distance. As shown in Fig. (**3**) There are three sorting classifications, when a new target enters it needs to find a suitable classification to sort itself into it.

3.3. Intrusion Detection System

The system is divided into three layers: system layer, platform layer, application layer. Fig. (**4**) shows the system model in cloud environment, where the system layer includes a virtual host and a network service, such as the Amazon EC2 service. The platform layer is the second layer of cloud system, including the operating system virtualization and running environment, and APIs, such as Windows Azure. It provides some APIs, and used to store and manage independent of some common language runtime environments (CLR). The application layer as the top of the cloud system is responsible for providing virtual applications, such as Google App Engine. The customer can write and upload some Web applications, which can be executed on the GAE and can be accessed *via* Web.

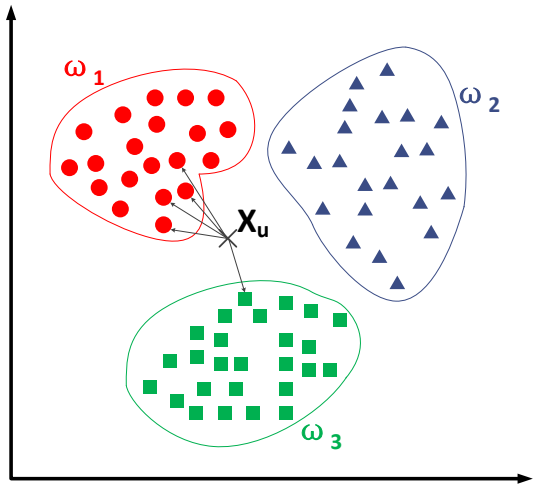

Fig. (3). The three classification example.

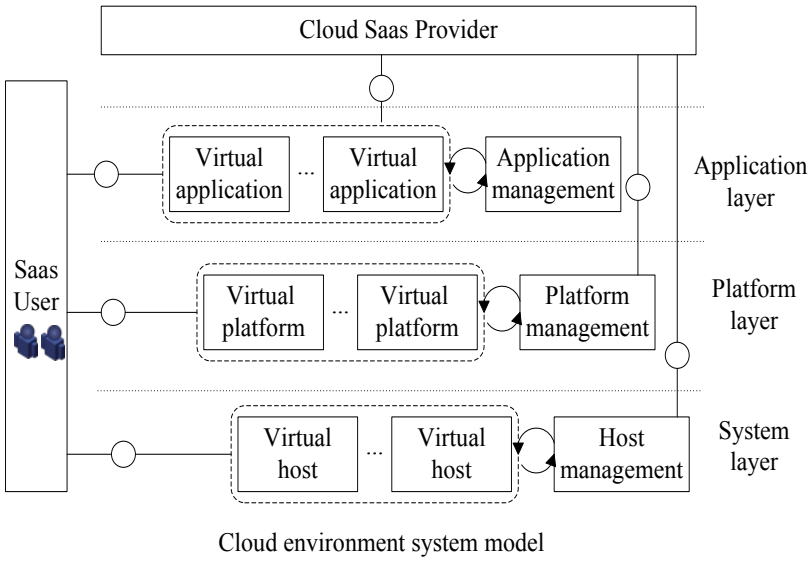

Fig. (4). The system model in cloud environment.

Host intrusion detection system for the host monitoring and analysis of the collected information, such as file systems, networking events, and system call, to detect intrusion information. Through the observation of the host kernel modifications to the host file system and the behavior of the program, when detected with unexpected behavior, it reports of the possible attacks. The efficiency of HIDS depends on the characteristics of the monitoring system as shown in Fig. (**5**).

Network security situation analysis based on connection degree is unique. The security situation on the network level has made a clear division. And through this value position at 12 levels, we are aware of the degree of danger to current network security situation. Unlike the traditional model NSSA obtained a network security situation value but can't find the value of the degree of risk on behalf of the network administrator in order to understand the situation, to facilitate rapid decisions.

4. EXPERIMENTAL RESULTS

4.1. Data Standardization Processing

Now suppose that there are n assessing network servers, denoted $M=\{M_1, M_2,..., M_n\}$, for each server with m index, denoted by $I=\{I_1, I_2,..., I_m\}$,the first measure i server M_j first kind j index value is $i \in (1,2,...,n), j \in (1,2,...,m)$, then each index value of n servers constitute the matrix F .

The data set does not provide the topological structure of network, host service information and vulnerability information; analysis of DARPA2000 about network topology is shown in Fig. (**6**). This paper collected information from snort (Table **1**).

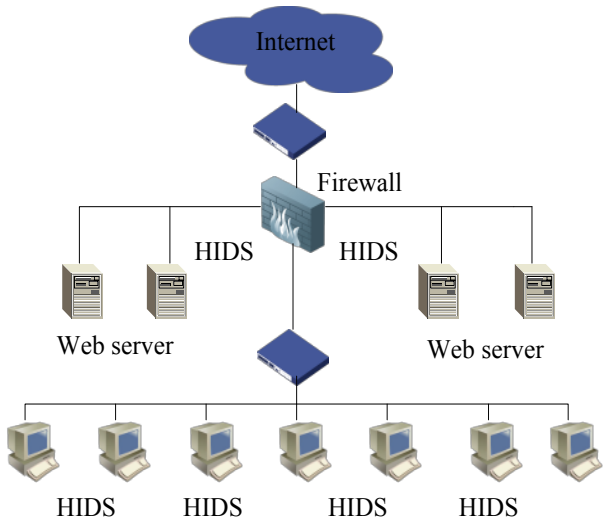

Fig. (5). The efficiency of HIDS depends on the characteristics of the monitoring system.

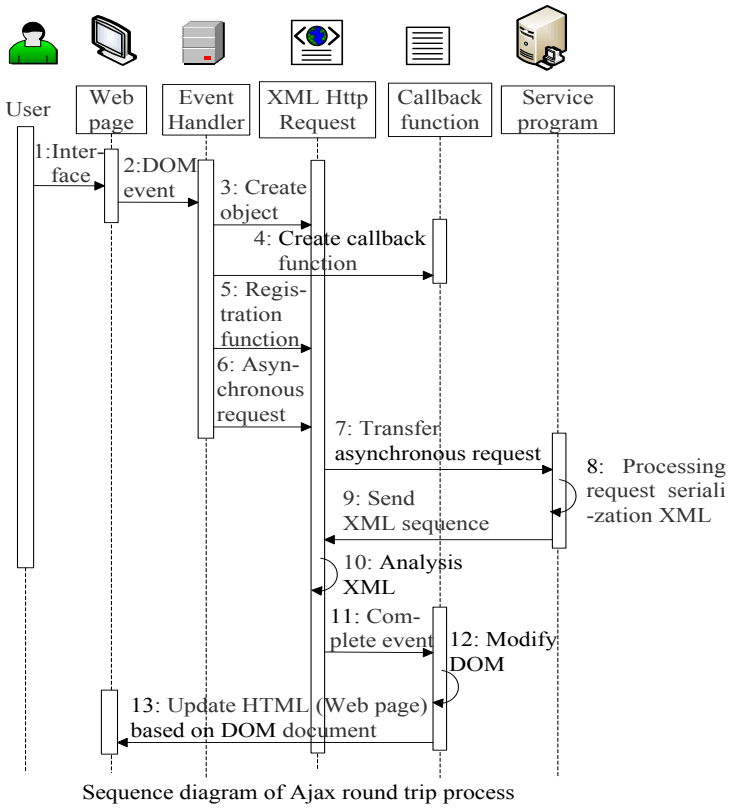

Fig. (6). The analysis of DARPA2000 about network topology.

4.2. Classification of Multi Sensor

According to the technical approach to classification, sensors can be classified as radar, signals intelligence sensors, radiometer, photoelectric sensors, remote sensors, ground battlefield sensor and acoustic detection sensor [9]. These sensors can be deployed on the ground, coastal, surface and underwater or mounted on a single soldier, ships, submarines, balloons, aircraft, and satellite motion platform, as shown in Fig. (**7**).

Optimization of technology directly originated from the military practice of sensor stations cloth branching linear programming, search theory, network and data processing statistics. It directly originated from the two tactical warfare i.e. evaluation and improvement of military application.

Echo state network model is a new neural network model. It is unique in that it invented the concept of the reserve pool, *i.e.* sparsely connected neurons consist of reserve pool instead of hidden layer neural network; a nonlinear descrip-

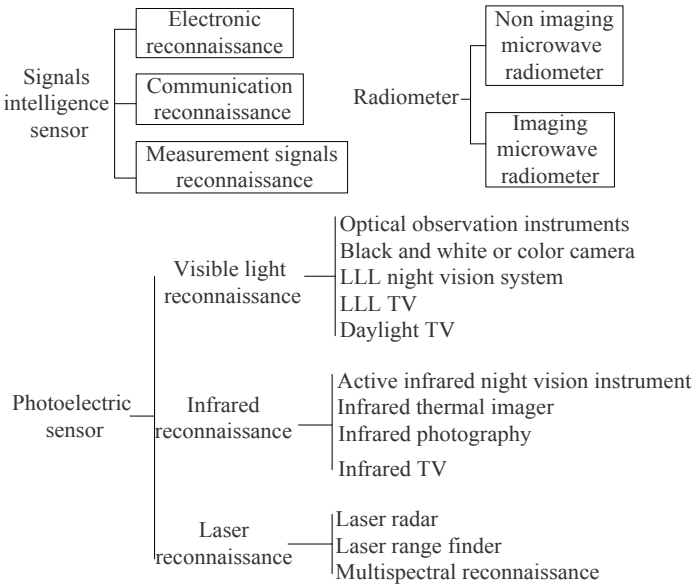

Fig. (7). Sensors deployed in the ground, coastal, surface and underwater.

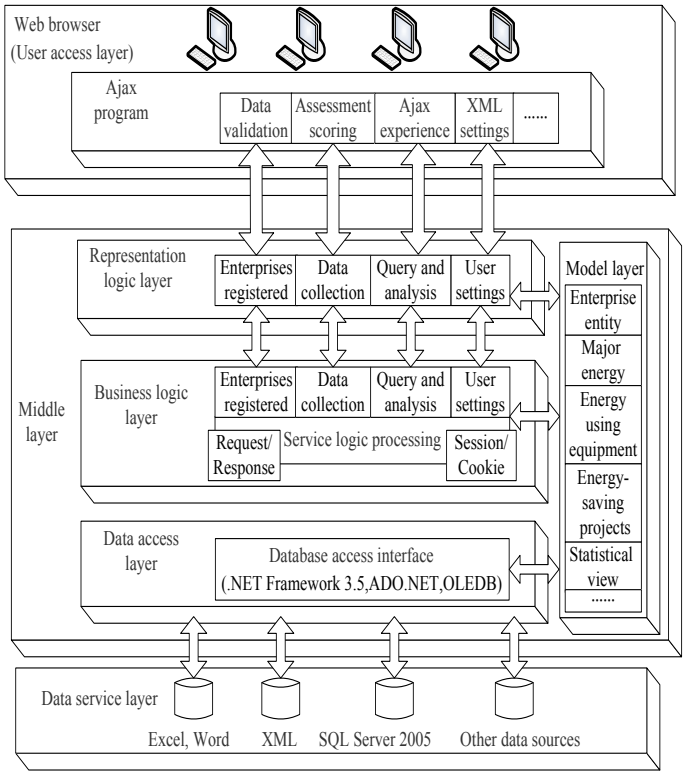

Fig. (8). Basic structure echo state network.

tion can describe it as high dimension input data. The training process generates a reserve pool process but the echo state network is independent of each other, so it only needs to use the linear method that can provide output layer weights during training reserve pool, which makes the training process simplified and ensures that the weights have the global optimality and good generalization ability. Basic structure of echo state network is shown in Fig. (**8**).

The Radial Basis Function (RBF) neural network model is a very effective three-layer feedforward, its continuous function can approximate any arbitrary accuracy of the performance, gives the best approximation, can be handled within the system to parse law, and also has good generalization ability. In RBF as a network of local approximation, each input needs to adjust only a few weights, so relative to the BP network, RBF network has a faster convergence speed.

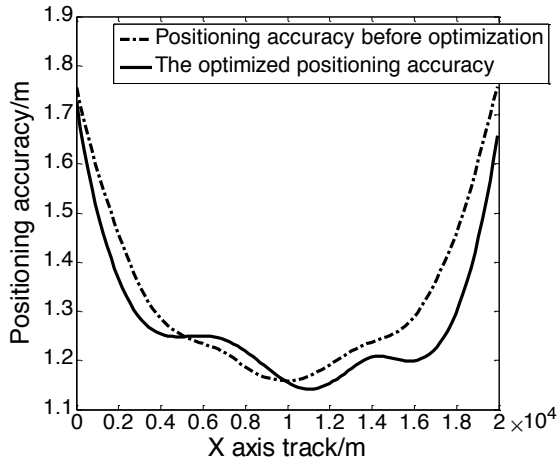

Fig. (9). The hidden node width.

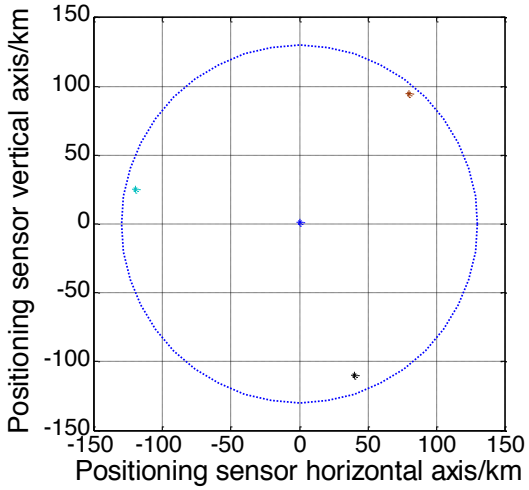

Fig. (10). The trained network and the actual value comparison.

Table 1. Index value of n servers constituting the matrix *F*.

	I_1	I_2	…	I_m
M_1	t_{11}	t_{12}	…	t_{1m}
M_2	t_{21}	t_{22}	…	t_{2m}
…	…	…	…	…
M_n	t_{n1}	t_{n2}	…	t_{nm}
M^+	h_1	h_2	…	h_m
M^*	I_1	I_2	…	I_m

K is the number of hidden nodes of RBF neural network, obtained through training; hidden node width, is shown in Fig. (**9**).

The prediction results obtained from the trained network and the actual value comparison are shown in Fig. (**10**).

CONCLUSION

This paper first introduces the research background, summarizes the status of domestic and international network security situational awareness, provides detailed introduction of the concept of network security situation awareness and multi sensor data fusion technology, analyses, contrasts and

sums up several main methods of current network security situation assessment and network security situation prediction. The current research aiming at multi-source data in the network characteristics and network security situation having some shortcomings, puts forward the assessment and prediction of the trend of network security situation based on multi sensor data fusion model, which makes up for the traditional use of single sensor data sources led to the network security situation whose value is not comprehensive and have integrated disadvantages. To overcome the problems in traditional sources of network security situational awareness single data, we derived a network security situation model from the original data with more comprehensive characters, such as host vulnerability and network attack sensing, ensuring the safety status of the whole network.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] T. Dutkevych, A. Piskozub, and N. Tymoshyk, "Real-time intrusion prevention and anomaly analyze system for corporate networks biteliigent data acquisition and advanced computing systems," In: *Technology and Applications*, IDAACS 2013. 4th *IEEE Workshop on IEEE*, 2013, pp. 599-602.

[2] M. C. Kim, J. Park, W. Jung, H. Kim, and Y. J. Kim, "Development of a standard communication protocol for an emergency situation management in nuclear power plants," *Annals of Nuclear Energy*, vol. 37, no. 6, pp. 888-893, 2010.

[3] C. H. Lien, H. C. Chen, Y. W. Bai, and M.B. Lin, "Power monitoring and control for electric home appliances based on power line communication," In: *Instrumentation and Measurement Technology Conference Proceedings*, 2008, pp. 2-79.

[4] L. Xu, T. Chen, Z. Ren, and D. Wu, "Resource management for uplink OFDM wireless communication system," In: *Global Mobile Congress*, 2007, pp. 284-288.

[5] K. Majid, and G. Saleh, "Beamforming and Power control for interference reduction in wireless communications using particle swarm optimization," *International Journal of Electronics and Communications*, vol. 64, no. 6, pp. 489-502, 2010.

[6] A. Radonjie, and V. Vujicie, "Integer SEC-DED codes for low power communications," *Information Processing Letters*, vol. 110, no. 12-13, pp. 518-520, 2010.

[7] S. W. Kim, J. Park, S. Han, and H. Kim, "Development of extended speech act coding scheme to observe communication characteristics of human operators of nuclear Power Plants under abnormal conditions," *Journal of Loss Prevention in the Process Industries*, vol. 23, no. 4, pp. 539-548, 2010.

[8] A. Vacearo, and D. Villacei, "Performance analysis of low earth orbit satellites for Power system communication," *Electric Power Systems Research*, vol. 73, no. 3, pp. 287-294, 2005.

[9] Y. Chung, C. Paik, and H. Kim, "Sub gradient approach for resource management in multi-user OFDM systems," In: *1st International Conference on Communications and Elcetronies*, vol. 5, pp. 203-207, 2007.

[10] I. Gutierrez, F. Bader, S. B. Slimane, J. Pijoan. "Adaptive resource management for a MC-CDMA system with mixed QOS classes using a cross layer strategy", In: *IEEE 65th Vehicular Technology Conference, VTC2007*, Spring, April 22-25, 2007, pp. 3036-3040.

[11] C.R. Dongarsane, and A.N. Jadhav, "Simulation study on DOA estimation using MUSIC algorithm", *International Journal of Technology and Engineering System*, vol. 2, no. 1, pp. 54-57, 2011.

[12] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt. "Zero-forcing methods for downlink spatial multiplexing in multiuser mimo channel", *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 461-471, 2004.

[13] M. Sadek, A. Tarighat, and A. H. Sayed, "A leakage-based precoding scheme for downlink multi-user MIMO channels", *IEEE Transactions on Wireless Communications*, vol. 26, no. 8, pp. 1505-1515, 2008.

[14] A. Tarighat, M. Sadek, and A. H. Sayed, "A multi user beamforming scheme for downlink MIMO channels based on maximizing signal-to-leakage ratios", In: *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005, pp. 1129-1132.

[15] J.van de Beek, O. Edfors, M. Sandell, S. Wilson, and P. Borjesson, "On channel estimation in OFDM system", In: *Proceedings of the IEEE Vehicular Technology Conference*, 1995, pp. 815-819.

[16] K. Wong, R. Cheng, K. B. Letaeif, and R. D. Murch, "Adaptive antennas at the mobile and base stations in an OFDM/TDMA system", *IEEE Transactions on Communications*, vol. 49, no. 1, pp. 195-206, 2001.

Received: May 26, 2015 Revised: July 14, 2015 Accepted: August 10, 2015