International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.129-138
http://dx.doi.org/10.14257/ijsia.2016.10.5.12

Network Information Security Situation Assessment Based on Bayesian Network

Wang Xing-zhu[1]

1. Furong College Hunan University of Arts and Science Hunan Changde 415000, China
wangxzhu@sina.com

Abstract

The situation of information security is difficult to be precise, autonomous and controllable. In this situation, the situation of the system is based on Fuzzy Dynamic Bayesian network. The model of situation awareness and situation estimation is constructed. The simulation results are compared with that of static Bayesian network model. The experimental results show that this method can better reflect the dynamic changes of network space operations.

Keywords*: Bayesian network; Network space operation; Information security; Situation assessment*

1. Introduction

The concept of information security defense (IA), mainly refers to the sensor, command and decision maker and combat unit into a whole, the information fusion technology, command decision support technology and GIG as the basis, to understand and grasp the battlefield information security situation and grasp the information security situation and the important degree of real-time as well as interactive operation. The purpose is to generate combat power. Foreign research in this field has developed rapidly, the research and development of the theory and the system has achieved great results. The research is still in its initial stage, the research method is not very specific, mainly for the information security defense system of Battlefield Network to carry out static assessment. The analysis is not complete, so that the situation cannot be effectively controlled and it cannot effectively deal with the information security situation caused by unknown and uncertain information. Fuzzy dynamic Bayesian network (fuzzy dynamic Bayesian network) is in recent years space situation assessment using the method of field of a development direction, when the trend of sensor information is in fuzzy state and the timing is uncertain and dynamic. Through the establishment of FDBN assessment model can make it be of the entire battlefield network system of information changes in the effects of continuous perception and evaluation. Providing the space information network security defense with grasp of the situation judgments and a more active and accurate quantitative analysis. Meanwhile, it offers problem solving method and an assistant decision-making means.

2. Dynamic Bayesian Network Inference and Fuzzy Comprehensive Evaluation

2.1. Selection of Dynamic Bayesian Networks

Dynamic Bayesian network (DBN) is a Bayesian network (BN). It has the function of static Bayesian network, and it is more accurate in time domain. It is

ISSN: 1738-9976 IJSIA

also more accurate in time domain. It is suitable for the estimation of the threat of the whole system. The temporal causal relationship is between adjacent time slices and the causal relationship in the same time, and the dynamic Bayesian network can be simply defined as BN (T0), which can be obtained from the BN structure of P (X0).

DBN has the fusion of new knowledge, the full expression of things, derivation and learning function, the problem of modeling and analysis of the uncertainty problem with random process has good effect, DBN network structure is shown in Figure 1:

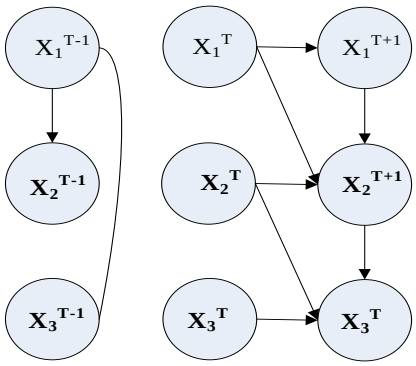

Figure 1. Dynamic Bayesian Network Structure

2.2. Dynamic Bayesian Network Inference Algorithm

The dynamic Bias network inference algorithm is derived from the formula (1) Bias formula:

$$p(x|y)=\frac{p(yx)}{p(y)}=\frac{p(yx)}{\sum_{x}p(yx)} \tag{1}$$

The reasoning process is the same as the static Bayesian network. Discrete static Bayesian networks with n hidden nodes and M observation nodes can be used to reflect the mathematical process of the type (2) according to their conditional independence:

$$p(x_1,x_2,...,x_n|y1,y2,...,y_m)=\frac{\prod_j p(y_j|p_a(Y_j))\prod_i p(x_i|p_a(X_i))}{\sum_{x_1,x_2,...,x_n}\prod_j p\left(yj|p_a(Yj)\right)\prod_i p\left(x_i|p_a(X_i)\right)} \quad i\in[1,n],\ j\in[1,m] \tag{2}$$

The value of a x_i state X_i in which the Y_j parent node is set $p_a(Y_j)$.

Network hidden nodes, observed fewer nodes or node coupling strong, less network hierarchical structure, considering the time slice is less, the DBN each time slice can be as a static Bayesian networks, nodes gradually increased or the node coupling enhancement, in the field can get a T time slice of DBN and its reasoning process can be reflected type (3):

$$p(x_{11},...,x_{1n},...,x_{T1},...,x_{Tn}|Y_{11o},Y_{12o},...,Y_{1mo},...,Y_{T1o},Y_{T2o},Y_{Tmo})=$$

$$\sum_{y_{11}y_{12}...y_{Tm}}\frac{\prod_{i,j}p(y_{ij}|p_a(Y_{ij}))\prod_{i,k}p(x_{ik}|p_a(X_{ik}))\prod_{i,j}p(Y_{ijo}=y_{ijo})}{\sum_{x_{11},x_{21},...,x_{T1}...x_{Tn}}\prod_{i,j}p\left(y_{ij}|p_a(Y_{ij})\right)\prod_{i,k}p\left(x_{ik}|p_a(X_{ik})\right)} \quad i\in[1,T],\ j\in[1,m],K\in[1,n] \tag{3}$$

The value of x_{ij} a state X_{ij}, i for the time slice, j is the representative of the hidden nodes, y_{ij} is the value of the observation variables Y_{ij}, $p_a(Y_{ij})$ is the collection of two parent nodes, the observation state Y_{ijo} of the observation node in the i time, $p(Y_{ijo} = y_{ijo})$ is the continuous observation value belongs to the state of the membership degree y_{ij}.

2.3. Dynamic Bayesian Network Model for 2.3 Situation Assessment

In situation assessment, two types of nodes are used in the model, such as -situation and -event, which are shown in Figure 2. In the dynamic Bayesian network model, the circular nodes represent the single element state node. Each node represents a specific situation.

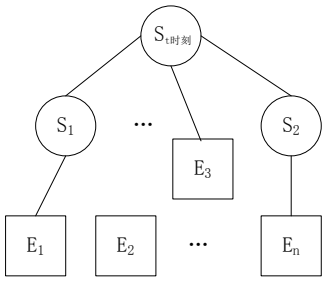

Figure 2. Dynamic Bayesian Network Situation Assessment Model

2.3.1. Situation –Situation Connection: If a situation node S is formed by the mutual independence of the situation $s_1, s_2, s_3 ... s_n$, the mutual relationship between them can be expressed as follows:

$$Bel(S) = \sum_{i=1}^{n} Bel(s_i) \tag{4}$$

Bel is a trust function, which indicates that the confidence level of a state node is independent of the situation of each sub node and the confidence level of the sub state node is not greater than that of the parent state. If the confidence level of the occurrence of a situation is very small, they can not take into account the sub trend. This can reduce the number of nodes in the process of situation assessment.

2.3.2. Situation – Event Connection: This connection represents a causal relationship between the situation and the related event, if an event E_i has n state, the probability matrix can be expressed as follows:

$$P(E_i | S) = (P_{11,} ... P_{n1})^T \tag{5}$$

2.3.3. Event-event Connection

The connection represents the logical reasoning relationship between different event E_w nodes, if there is a conditional probabi b lity matrix expressed as the conditional probability matrix of the $a \times b$ event node of BN and the event of a state: P_{ab}

$$P_{ab} = \begin{vmatrix} p_{11} & p_{12} & \cdots & p_{1b} \\ p_{21} & p_{22} & \cdots & p_{2b} \\ \cdots & \cdots & \cdots & \cdots \\ p_{b1} & p_{b2} & \cdots & p_{ab} \end{vmatrix} \quad (6)$$

On the formula $p_{ij} = p(E_{kj} \mid p_{wi})$, the probability E_w of occurrence of the event's E_{wi} state is represented by a node E_k state.

3. Building Evaluation Model

3.1. Network Space Operational Information Security Defense Situation Awareness Model

The main task of the situation assessment is to realize the situation awareness of the assessment object and to establish the model of situation awareness, it is necessary to form a comprehensive understanding of the important situation factors, otherwise it will increase the probability of the formation of the error situation.

From data acquisition, perception, forecast and in-depth data mining to the whole process of [4], and ultimately form a reasonable defense program, so the network space information security defense situation awareness includes not only from the recognition of information, but also includes information fusion through the object and the important degree of the event , forming a structure planning trend image. Including information security environment, such as target status, attributes, dynamic and other elements of the extraction, the current situation assessment and future trend prediction, the process is mainly covered the following aspects: first, to determine the depth of the event and to determine the occurrence of the event. Situation elements are mainly involved in the information assets, the threat of the enemy, the fight according to the perception of the defensive situation in the model, the current battlefield network space security, risk assessment [5]. Network space defense situation awareness model is shown in figure 2.

3.2. Analysis on the Security of Information Security in Network Space Operations

Situation factors including information security measures, security and defense force support capabilities, information environment factor and so on, usually by observing the situation, against the trend, defensive posture, emergency situation four trend categories and each category by different foundation parameters, see Table 1 through to one's own network by threat level assessment makes on defense so as to adjust focus on defense, clearly it should be improved and perfected. The interaction of these factors, which determines the threat of cyberspace operations that is the data acquired in the assessment of [6]

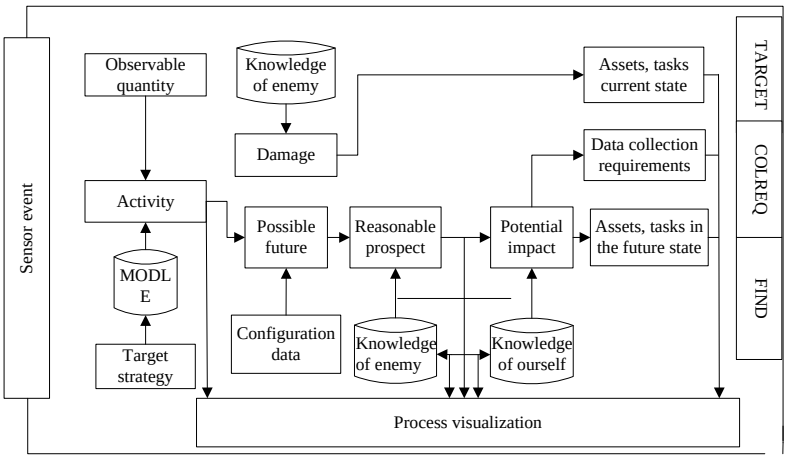

Figure 3. Cyberspace Situation Awareness Information Security Defense Model

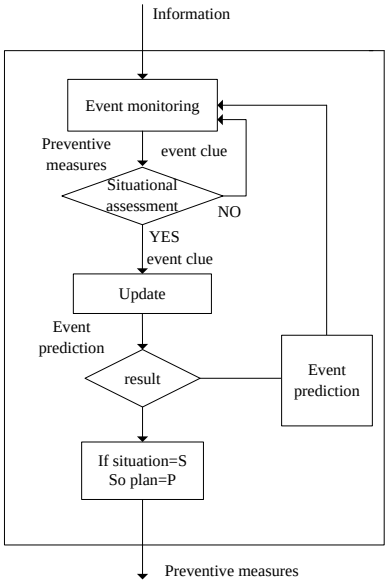

Figure 4. Situation Assessment Decision-Making Process

The decision-making process of situation assessment is shown in Figure 4, mainly including the following steps:

1) surveillance event. Gather information on the current assessment of the situation related to the event information.
2) to evaluate whether the information is based on the information. If the event information is in line with the situation that has been obtained, then continue to monitor; if the result is different, there is a new event, then the next step is to continue.
3) the distribution of the reliability of the update situation. In accordance with the updated event situation set the reliability of the distribution, reevaluation.
4) assess the new trend. Judging whether the distribution of the status of the update is consistent with the current defense scheme. If there is conflict, the next step; otherwise, continue to monitor new events.
5) programmed formulation. In accordance with the new situation assessment results, to trigger the corresponding defense program.

3.3. Establish a dynamic bayesian evaluation network

Threat assessment of one's own network is mainly obtained through situation awareness system information to complete the protective network threat level evaluation, the main principle is in compared on the basis of situation factors related to state change of the characteristic, further quantitative characteristic parameters of the comparison results. Finally, it is synthetically considering various parameters of evaluation results and determining the trend level. According to the expert knowledge of the related fields, the AHP fuzzy comprehensive evaluation method is used to establish the fuzzy sets of the state of the situation and the dynamic Bayesian network model of the threat estimation is shown in Figure 3.

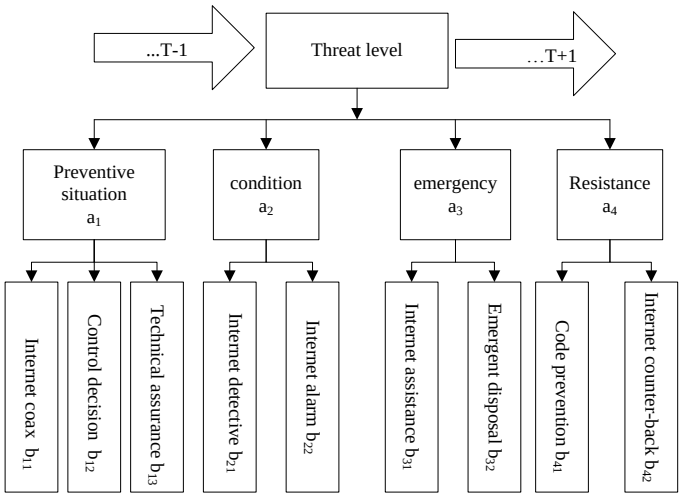

Figure 5. Cyberspace Defense Posture Dynamic Bayesian Network Structure

According to the operational experience, expert system and the key parameters of different situation factors, the status of the state of the situation is classified, and the numerical value is obtained by [8] (network detection test), which is based on the B21 (network detection test):

$$f(x_i) = \frac{x_i}{x_0} = y_i \tag{7}$$

Type x_i in the B21 of the parameters of the parameters in a time slice of the observation value is greater than 0 of a numerical value which is normalized post-processing data.

The weight sum of the normalized data in the fuzzy comprehensive evaluation is determined by

AHP (6): $$\sum_{i=1}^{n} y_i \cdot w(x_i) = z \tag{8}$$

The $w(x_i)$ weight value of each factor is the value of B21, and the value range of the process can be obtained, which can be divided into different thresholds $[z_1, z_2], [z_2, z_3], [z_1, z_4]$.

Thus on the situation factors of state description to construct a fuzzy set, and $S_{b_{22}}$ S_A = (high threat, threat and low threat); and,, S_{a_1} S_{a_2} $S_{b_{12}}$ $S_{b_{32}}$ = (high stability, stability, low stability); S_{a_4} = (disaster recovery capability is strong, disaster

recovery capability of the general and disaster recovery capability of the weak),,, $S_{b_{41}}$ $S_{b_{42}}$ $S_{b_{13}}$ = (strong, weak); S_{a_3} = (high robustness, robustness medium, robustness low).

4. Experiments and Analysis

Based on the evaluation model, the BNT MATLAB toolbox is used to carry out the inference engine. Network space defense forces have very limited information before the attack and the initial state of the threat level is high, medium and low probability distribution (0.4,0.3,0.4), which is consistent with the actual conditions, reflecting the uncertainty of the decision maker. After the model is initialized to wait state, once the update of the situation information input network nodes, the network inference algorithm to update the status of each network node [11], and finally get the probability distribution of node state.

We find the other side to attack our network system, assuming that the attack time is continuous, sensor network system to monitor the situation of real-time monitoring, continuous observation of 9 moments, according to the different time to set the data set.

1) situation assessment based on Dynamic Bayesian network. In the dynamic Bayesian network evaluation model, the conditional probability distribution of initial network nodes, network state transfer probability distribution, and the observation data of 9 time are analyzed. The results of the comprehensive defense situation assessment are shown in Figure 4.

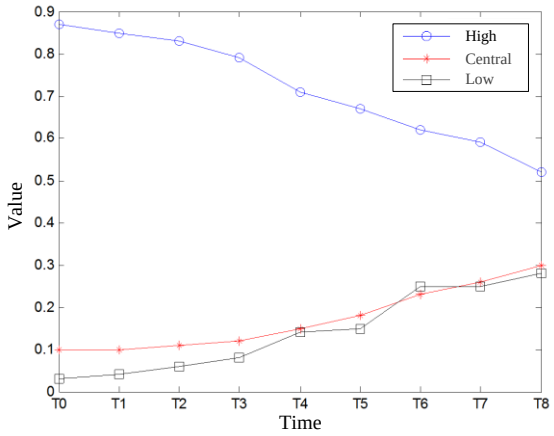

Figure 6. Fuzzy Dynamic Bayesian Network Threat Level Simulation Results

2) a static Bayesian network model is established and the input table 2- table 6 of the data is obtained by the evaluation values shown in Figure 5.

Probability from the point of view of the experimental results: with increasing activity against frequency, one's own protection network by threat level "high" state probability decreased gradually, and "in" or "low" state in increased gradually and tends to be stable, indicating that in the confrontation to confrontation, strength, defense information system security protection gradually improve.

From Figure 4 and figure 5 contrast, it can be seen with the use of a static Bayesian network compared, dynamic Bayesian network model of assessment results combined with posture more elements of the feedback relationship and observation information, which can be more accurate and continuously reflecting the network operational information security defense posture with the objective law of the time change, so decision makers can better grasp the direction of defense and

key, the situation factors with increased frequency of confrontation, the probability distribution changed gradually and tends to be stable, defense posture toward have been conducive to the development of the Allied trend.

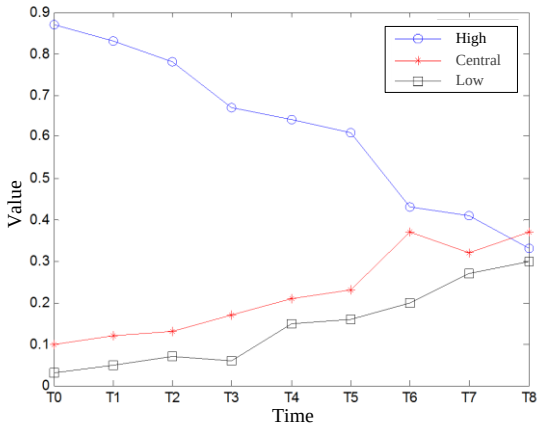

Figure 7. Threat Level Static Bayesian Network Simulation Results

5. Conclusion

Information security defense in network space is a trend assessment concept, which is proposed by the network eccentric warfare and constructs the dynamic Bias network to evaluate the network space defense operations. It can be quickly and effectively, providing a kind of high efficiency information assistant decision support.

Acknowledgements

This work was supported by .Hunan Province Natural Science Foundation Project No. 14JJ2124.

Reference

[1] Y. Lin, J. Yang J and Z. Lv, "A Self-Assessment Stereo Capture Model Applicable to the Internet of Things", Sensors, vol. 15, no. 8, **(2015)**, pp. 20925-20944.
[2] J. Yang, B. Chen and J. Zhou, "A Low-Power and Portable Biomedical Device for Respiratory Monitoring with a Stable Power Source", Sensors, vol. 15, no. 8, **(2015)**, pp. 19618-19632.
[3] Z. Lv, A. Halawani and S.Fen, "Touch-less Interactive Augmented Reality Game on Vision Based Wearable Device", Personal and Ubiquitous Computing, **(2015)**.
[4] W. Gu, Z. Lv and M. Hao, "Change detection method for remote sensing images based on an improved Markov random field", Multimedia Tools and Applications, **(2015)**, pp. 1-16.
[5] Z. Chen, W. Huang and Z. Lv, "Towards a face recognition method based on uncorrelated discriminant sparse preserving projection", Multimedia Tools and Applications, **(2015)**, pp. 1-15.
[6] D. Jiang, X. Ying and Y. Han, "Collaborative multi-hop routing in cognitive wireless networks", Wireless Personal Communications, **(2015)**, pp. 1-23.
[7] Z. Lv, A. Halawani and S. Feng, "Multimodal hand and foot gesture interaction for handheld devices", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 11(1s), **(2014)**, pp. 10.
[8] X. Li, Z. Lv and J. Hu, "XEarth: A 3D GIS Platform for managing massive city information", Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015 IEEE International Conference on. IEEE, **(2015)**, pp. 1-6.
[9] X. Li, Z. Lv and J. Hu, "Traffic management and forecasting system based on 3d gis", IEEE International Symposium on Cluster, Cloud and Grid Computing (CCGrid), **(2015)**.
[10] S. Zhang and H. Jing, "Fast log-Gabor-based nonlocal means image denoising methods", Image Processing (ICIP), 2014 IEEE International Conference on. IEEE, **(2014)**, pp. 2724-2728.

[11] D. Jiang, Z. Xu and Z. Chen, "Joint time-frequency sparse estimation of large-scale network traffic", Computer Networks, vol. 55, no. 15, **(2011)**, pp. 3533-3547.
[12] D. Jiang, Z. Xu and W. Li, "An Energy-Ecient Multicast Algorithm with Maximum Network Throughput in Multi-hop Wireless Networks", Journal of Communications and Networks, **(2015)**.
[13] Y. Liu, J. Yang and Q. Meng, "Stereoscopic Image Quality Assessment Method based on Binocular Combination Saliency Model", Signal Processing, **(2015)**.
[14] J. Yang, S. He and Y. Lin, "Multimedia cloud transmission and storage system based on internet of things. Multimedia Tools and Applications, **(2016)**.
[15] T. Li, X. Zhou and K. Wang, "A convergence of key-value storage systems from clouds to supercomputers", Concurrency and Computation: Practice and Experience, **(2015)**.

Author

WANG Xingzhu. WANG Xingzhu, male, was born in 1974, in Hunan province. Now, he is an associate professor in Furong College Hunan, University of Arts and Science. His Main research area is network security.